The review of the adequacy and effectiveness of the enterprise risk management processes
August 2017

INTERNAL AUDIT REPORT ON THE REVIEW OF THE ENTERPRISE RISK MANAGEMENT PROCESSES

REPORT NUMBER: REG-ODG ERM1 2016/17

August 2017
The review of the adequacy and effectiveness of the enterprise risk management processes
August 2017

DISTRIBUTION LIST:

This report is distributed to the following members of management:

<table>
<thead>
<tr>
<th>MANAGEMENT</th>
<th>DESIGNATION</th>
<th>REQUIREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mr D Mogajane</td>
<td>Director General</td>
<td>For Information</td>
</tr>
<tr>
<td>Ms O Matloa</td>
<td>Audit Committee Chairperson</td>
<td>For Information</td>
</tr>
<tr>
<td>Mr S Mngomezulu</td>
<td>Deputy Director General - Corporate Services</td>
<td>For Information</td>
</tr>
<tr>
<td>Ms S Kubheka</td>
<td>Chief Financial officer</td>
<td>For Information</td>
</tr>
<tr>
<td>Mr L Mangquku</td>
<td>Risk Committee Chairperson</td>
<td>To secure action</td>
</tr>
<tr>
<td>Mr L Giba</td>
<td>Chief Risk Officer</td>
<td>To action</td>
</tr>
</tbody>
</table>
The review of the adequacy and effectiveness of the enterprise risk management processes
August 2017

REPORT AND EXECUTIVE SUMMARY

SECTION A...........................................................................................................................................2

INTRODUCTION AND BACKGROUND ..............................................................................................2
TERMS OF ENGAGEMENT ..................................................................................................................2
OBJECTIVES AND SCOPE ...................................................................................................................4
AUDIT APPROACH ............................................................................................................................7
SCOPE EXCLUSION ............................................................................................................................5
KEY TO AUDIT OPINION ON CONTROL ENVIRONMENT ...............................................................8
AUDIT OPINION ON CONTROL ENVIRONMENT ...............................................................................9
OVERAL AUDIT OPINION ..................................................................................................................7
FRAUD AND INTERNAL CONTROL .................................................................................................9
LIMITATION OF USE ..........................................................................................................................9

SECTION B ..........................................................................................................................................10

KEY TO RISK RATING .......................................................................................................................10
SUMMARY OF POSITIVE AUDIT FINDINGS ..................................................................................12
SUMMARY OF DETAILED AUDIT FINDINGS ....................................................................................14

Internal Audit Report No: REG- ODG ERM1 2016/17
Section A
Executive Summary
SECTION A

INTRODUCTION AND BACKGROUND

In terms of the 2016/17 Internal Audit annual plan, approved by the National Treasury's Audit Committee, an audit on the review of the adequacy and effectiveness of the Enterprise Risk Management (ERM) processes was scheduled for the fourth quarter (January 2017 to March 2017) of the 2016/17 financial year.

Section 38(a) of the PFMA states that the accounting officer has a duty to ensure that the department has and maintains effective, efficient and transparent systems of financial and risk management and internal control.

The role of internal auditing in ERM

According to International Standards for the Professional Practice of Internal Auditing, 1220.A1 internal auditors must exercise due professional care by considering the:

- Extent of work needed to achieve the engagement's objectives.
- Relative complexity, materiality, or significance of matters to which assurance procedures are applied.
- Adequacy and effectiveness of governance, risk management, and control processes.
- Probability of significant errors, fraud, or noncompliance.
- Cost of assurance in relation to potential benefits.

According to International Standards for the Professional Practice of Internal Auditing 2120 internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

Internal auditing is an independent, objective assurance and consulting activity. Its core role with regard to ERM is to provide objective assurance to the board (EXCO) on the effectiveness of risk management.

Internal auditors will normally provide assurances on three areas:

- Risk management processes, both their design and how well they are working;
- Management of those risks classified as 'key', including the effectiveness of the controls and other responses to them; and
- Reliable and appropriate assessment of risks and reporting of risk and control status.

Figure 1 (below) presents a range of ERM activities and indicates which roles an effective professional internal audit activity should and, equally importantly, should not undertake. The key factors to take into account when determining internal auditing's role are whether the activity raises any threats to the internal audit activity's independence and objectivity and whether it is likely to improve the organization's risk management, control and governance processes.
The review of the adequacy and effectiveness of the enterprise risk management processes August 2017

Figure 1 – Internal auditing’s role in ERM

Core internal audit roles in regard to ERM
Legitimate internal audit roles with safeguards
Roles internal audit should not undertake
Enterprise-wide risk management (ERM) is a structured, consistent and continuous process across the whole department for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives. The National Treasury (NT) recognizes that effective risk management is imperative for the NT to fulfill its mandate and that it is an integral part of responsible and accountable management. It further acknowledges that although management is responsible for risk management, formal processes and support are required to ensure that risk management is integrated into the NT operations and that a healthy risk culture is created throughout the institution. The Accounting Officer is ultimately responsible to ensure that there is a system of effective and efficient risk management in the institution. This function has been delegated to the Risk Committee (RC) of the NT that is accountable to the Accounting Officer.

The NT subscribes to the fundamental principles that all resources are applied economically to ensure:

- The highest standards of service delivery;
- A management approach containing appropriate tools aimed at minimising risks and costs in the interest of all stakeholders;
- Education and training of all staff to allow for continuous improvement of knowledge, skills and capabilities in order to keep abreast with latest trends in their respective environments; and
- An environment which promotes the right attitude and sensitivity towards internal and external stakeholder satisfaction.

TERMS OF ENGAGEMENT

Internal Audit operates in accordance with the Public Finance Management Act (PFMA), Treasury Regulations and the Internal Audit Charter (mandate). The Audit Charter sets out the nature, role, responsibility, status and authority of internal audit. Copies of the Audit Charter can be made available to you on request.

Internal audit work (planning, execution and reporting) was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing.

OBJECTIVES AND SCOPE

The objective of this audit is to assess the adequacy and effectiveness of the Enterprise Risk Management processes.

Taking cognisance of the objective of this audit, the scope and information gathering approach to be utilised during this review is outlined in the table below:

<table>
<thead>
<tr>
<th>Scope Definition</th>
<th>Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role of EXCO regarding ERM</td>
<td>Reviewed the strategic direction of EXCO in terms of their roles and responsibilities regarding ERM:</td>
</tr>
<tr>
<td></td>
<td>- Determining and approving of the risk appetite, risk tolerances and risk profile;</td>
</tr>
<tr>
<td></td>
<td>- Understanding the priority risks;</td>
</tr>
<tr>
<td></td>
<td>- Ensuring that risk responses for the priority risks are effective;</td>
</tr>
<tr>
<td></td>
<td>- Ensuring that the risk management framework is efficiently implemented and maintained; and</td>
</tr>
<tr>
<td></td>
<td>- Structure of ERM and their reporting lines.</td>
</tr>
</tbody>
</table>
The review of the adequacy and effectiveness of the enterprise risk management processes
August 2017

- Assessed whether EXCO Support and drive the vision and mission of ERM through monitoring the achievement of the strategic, operational and tactical objectives.

<table>
<thead>
<tr>
<th>Scope Definition</th>
<th>Approach</th>
</tr>
</thead>
</table>
| **Role of Risk Committee** | - Assessed whether committee members were appointed formally by the DG and whether appointed members were consistent in attending RC meetings.  
- Assessed whether Risk Committee members have sufficient risk experience and expertise:  
  ▪ Reviewed whether there was a criterion in place when selecting the risk committee members; and  
  ▪ Reviewed whether risk committee members were trained on Risk (terms used).  
- Reviewed the RC's terms of reference to determine whether they were approved and reviewed on an annual basis; and also determined whether the under mentioned roles and responsibilities were performed as per their terms of reference and best practise:  
  ▪ Assessed whether the committee reviewed institution’s risk identification and assessment processes in obtaining reasonable assurance of the completeness and accuracy of the risk register;  
  ▪ Assessed whether the committee evaluated the effectiveness of mitigating strategies to address the material key risks of National Treasury;  
  ▪ Assessed whether the committee reviewed material findings and recommendations by assurance providers on the system of risk management and monitored that appropriate action was instituted to address the identified weaknesses;  
  ▪ Assessed whether the committee provided proper and timely reports to the Accounting Officer on the state of risk management, together with aspects requiring improvement accompanied by the Committee’s recommendations to address such issues; and  
  ▪ Assessed whether the committee monitored compliance with the organisation policies and investigating allegations of breaches of those policies.  
- Assessed whether the chairperson of the Audit Committee seated in the RC meeting as an invitee. |
| **Role of Audit Committee** | - Assessed the roles and responsibilities of Audit Committee in terms of the following component:  
  ▪ Financial reporting and risks;  
  ▪ Reviewing of internal financial controls;  
  ▪ Fraud risks; and  
  ▪ Information technology (IT) risks.  
- Assessed whether the Audit Committee provided input and/or report back regarding the issues raised by CRO.  
  ▪ Reviewed the minutes of AC meetings to determine whether ERM issues were discussed; and |
The review of the adequacy and effectiveness of the enterprise risk management processes
August 2017

<table>
<thead>
<tr>
<th>Scope Definition</th>
<th>Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Review the reports to determine whether AC has provided their inputs to issues raised by CRO.</td>
</tr>
</tbody>
</table>

### Role of Chief Risk Officer (CRO)

- Assessed whether the CRO engaged EXCO, AC and RC on issues relating to Risk Management;
- Assessed whether the CRO has established and communicates the Risk Management vision and mission;
- Assessed whether the CRO ensures that the Risk Committee and Management were adequately trained on Risk Management;
- Assessed whether key performance indicators were set for the CRO in respect of risk management. To determine whether risk management was operating effectively in leading the Institution’s in achieving its strategic objectives and goals; and
- Reviewed whether the risk management strategic, operational and tactical objectives were set and aligned with overall objectives of National Treasury.

### Risk Management Process

<table>
<thead>
<tr>
<th>Scope Definition</th>
<th>Approach</th>
</tr>
</thead>
</table>
|                                  | Reviewed the Risk Management Policy/ Strategy to determine the organisation’s business strategies, risk management philosophy and methodology; and
| Framework/ Strategy              | Determined whether the ERM framework/ strategy has been approved and reviewed on an annual basis.                                         |
| Maturity level                   | Assessed whether the maturity level of the organisation meet its level requirements.                                                      |

### Formal processes (identification, assessment, response and mitigation)

- Risk Identification process:
  - Reviewed whether key risks were identified, including strategic, project and operational risks have been identified; and
  - Reviewed whether risk identification process was robust, and structured.
- Risk Assessment:
  - Reviewed whether risks were rated and prioritised according to guidelines provided;
  - Inherent and Residual risk were assessed; and
  - Financial and non-financial factors were taken into account when rating risks.
- Risk Management Response strategy:
  - Risk responses have been identified for each risk; and
  - Risk owners were assigned for each risk.
- Control Activities:
  - Reviewed whether policies and procedures were established and implemented.
- Information and Communication:
  - Reviewed whether ERM took a root commitment through: raising awareness by conducting workshops, training on a regular basis.
- Monitoring and review:
The review of the adequacy and effectiveness of the enterprise risk management processes
August 2017

<table>
<thead>
<tr>
<th>Scope Definition</th>
<th>Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- All significant risks were reported to the board/EXCO and/or relevant management at regular intervals;</td>
</tr>
<tr>
<td></td>
<td>- Risk registers were updated quarterly and reported to the Manager: Enterprise Risk Management/CRO;</td>
</tr>
<tr>
<td></td>
<td>- New/emerging risks were considered and included in the risk register as relevant; and</td>
</tr>
<tr>
<td></td>
<td>- Verified existence of projects risk register.</td>
</tr>
<tr>
<td></td>
<td>- Assessed whether the Barnowl system was utilised and operating effectively.</td>
</tr>
</tbody>
</table>

- Benchmarking

<table>
<thead>
<tr>
<th>Scope Definition</th>
<th>Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Benchmarking</td>
<td>- Benchmark with other Departments that have a functioning Enterprise Risk Management process:</td>
</tr>
<tr>
<td></td>
<td>- Review their Organisational structure, Strategy Direction, Risk Management processes, the functions of Risk Committee, Risk Committee composition and determination of Risk Appetite and Risk Tolerance.</td>
</tr>
</tbody>
</table>

AUDIT APPROACH

- Documented the process to be audited;
- Audit execution, including the compilation of audit programs and testing;
- Prepared a schedule of findings and discussing these with the responsible managers prior to finalisation, with the objective of sourcing the root cause in order to recommend corrective measures to be implemented by management; and
- Prepared an audit report summarising our findings.

SCOPE EXCLUSION

Benchmarking with other Departments that have a functioning Enterprise Risk Management process: Reviewing their Organisational structure, Strategy Direction, Risk Management processes, the functions of Risk Committee, Risk Committee composition and determination of Risk Appetite and Risk Tolerance was not performed.
### KEY TO AUDIT OPINION ON CONTROL ENVIRONMENT

<table>
<thead>
<tr>
<th>CONTROL ENVIRONMENT</th>
<th>DEFINITION</th>
<th>INDICATOR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Adequate</strong></td>
<td>Audit results indicate that sufficient reliance can be placed on the design and operation of internal controls to mitigate the risks to which the activity under review is exposed.</td>
<td>• Primarily “Low” risk findings. • Overall control environment for the audited process / focus area is of the required standard.</td>
</tr>
<tr>
<td><strong>Satisfactory</strong></td>
<td>Despite the fact that some control weaknesses were identified, the existing key controls are considered to be generally adequate and effective to ensure the audited business process/ focus area will achieve its objectives.</td>
<td>• Primarily “Low and a few Medium” risk findings. • Adequate compensating controls in place. • Overall control environment for the audited process / focus area is of an adequate standard.</td>
</tr>
<tr>
<td><strong>Requires Improvement</strong></td>
<td>Audit results indicate that limited reliance can be placed on the design and operation of internal controls to mitigate the risks to which the activity under review is exposed.</td>
<td>• Primarily “Medium” risk findings. • Inadequate compensating controls. • Overall control environment of the audited process / focus area is of a vulnerable standard.</td>
</tr>
<tr>
<td><strong>Unsatisfactory</strong></td>
<td>Audit results indicate that insufficient reliance can be placed on the design and operation of internal controls to mitigate the risks to which the activity under review is exposed.</td>
<td>• A breakdown in the overall management of a part of the business or the process being reviewed. • Primarily “High” risk findings. • Actions likely to bring the National Treasury brand and reputation into disrepute. • A breakdown in accounting, reporting and other key financial and operating controls.</td>
</tr>
<tr>
<td><strong>Inadequate</strong></td>
<td>Audit results indicate that no reliance can be placed on the design and operation of internal controls to mitigate the risks to which the activity under review is exposed.</td>
<td>• Inadequate management of the business or process being reviewed. • Primarily “Catastrophic” risk findings. • Actions likely to bring the National Treasury brand and reputation into disrepute. • Non-existent financial and operating controls. • Non-compliance to laws and regulations.</td>
</tr>
</tbody>
</table>
AUDIT OPINION ON CONTROL ENVIRONMENT

The table below provides the audit opinion for each focus area of the review after careful consideration, understanding and testing of the control environment:

<table>
<thead>
<tr>
<th>Process</th>
<th>Number of controls tested</th>
<th>Overall control rating</th>
<th>Overall control rating</th>
<th>Findings rating</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organisational Governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The role of EXCO regarding ERM</td>
<td>7</td>
<td>Unsatisfactory</td>
<td></td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Role of Risk Committee</td>
<td>9</td>
<td>Unsatisfactory</td>
<td></td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Role of Audit Committee</td>
<td>6</td>
<td>Adequate</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Role of the Chief Risk Officer</td>
<td>5</td>
<td>Unsatisfactory</td>
<td></td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Role of Management</td>
<td>2</td>
<td>Unsatisfactory</td>
<td></td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Risk Management Process</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Framework Strategy</td>
<td>3</td>
<td>Medium</td>
<td></td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Formal processes</td>
<td>15</td>
<td>Unsatisfactory</td>
<td></td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>TOTAL</td>
<td>47</td>
<td></td>
<td></td>
<td>0</td>
<td>7</td>
</tr>
</tbody>
</table>

OVERALL AUDIT OPINION

Based on the results of the assessment of the Enterprise Risk Management, including the design, implementation adequacy and effectiveness thereof, we are of the opinion that limited reliance can be placed on the design and operation of internal controls to mitigate the risks to which the activity under review is exposed. The control environment is Unsatisfactory.

For details, please refer to detailed findings under Section B.

FRAUD AND INTERNAL CONTROL

While we have identified certain areas of departure from the key controls, internal audit procedures alone, even when carried out with due professional care, do not guarantee that all fraud and errors will be detected. We have ensured that all internal audit work conducted is planned with a reasonable expectation of detecting significant control weaknesses in the specific areas reviewed. However, our reviews and investigations as internal auditors should not be solely relied upon to disclose all matters of fraud or other irregularities, which may exist. Management’s attention is drawn to the inherent limitations in the reliance on internal controls and procedures mentioned above.

LIMITATION OF USE

Any documentation or information brought to our attention subsequent to the date of this final report which would affect the findings detailed below, will require our findings to be adjusted and qualified accordingly. This report is strictly private and confidential, and is intended solely for the reporting on our findings to the audit committee and the relevant management of DG’s office and should therefore
The review of the adequacy and effectiveness of the enterprise risk management processes
August 2017

not be utilised for any other purposes. No part may be quoted, referred to or disclosed in whole or in part, by any other party, without our prior consent.
Section B
Detailed Findings
SECTION B

SUMMARY OF POSITIVE AUDIT FINDINGS

Based on the results of our review, we have identified that the following key controls were adequately implemented and operating effectively:

Role of Risk Committee

With the appointment of an acting RC chairperson, the following is under development and/or progress:

- The RC’s terms of reference are in the process of being reviewed and approved;
- The RC is in the process of reviewing the institution’s risk identification and assessment processes or ensure that reasonable assurance of the completeness and accuracy of the risk register;
- The RC is in the process of reviewing the effectiveness of mitigating strategies to address the material key risks of National Treasury; and
- On a quarterly basis, the acting chairperson of RC prepares a report to the Accounting Officer on the state of risk management, together with aspects requiring improvement accompanied by the Committee’s recommendations to address such issues.

Role of Audit Committee

- Financial reporting and risks

Audit committee assessed and reviewed the annual financial statements of National Treasury, Accounting Standard Board, Cooperative Banks Development Agency as well as Government Technical Advisory Centre on an annual basis; inputs are provided to relevant officials for the amendments of the financials before submission to Auditor-General for review. Internal Audit also assist audit committee by conducting annual financial statements reviews, issues identified are also submitted to relevant officials for amendments of the financials.

- Reviewing of internal financial controls

On an annual basis, Internal Audit conducts Critical Financial Reporting Controls reviews on behalf of the Audit Committee. Such reviews helps the audit committee to formulate their opinion on the overall control environment of National Treasury, Accounting Standard Board, Cooperative Banks Development Agency as well as Government Technical Advisory Centre. The overall control environment opinion were disclosed on the annual report of both institutions.

- On a quarterly basis Audit Committee receive a quarterly report from the CRO, analysed it and provided input and/or report back regarding the issues raised by CRO.

Role of the Chief Risk Officer

The CRO has ensured that the risk management strategic, operational and tactical objectives were set and aligned with overall objectives of National Treasury.
The review of the adequacy and effectiveness of the enterprise risk management processes
August 2017

Framework Strategy
The Risk Management Policy/ Strategy to determine the organisation’s business strategies, risk
management philosophy and methodology are in place, and the new RC is in the process of reviewing
them.

Formal processes
Risk Identification process
- Key risks are identified, including strategic and operational risks.

Risk Assessment
- Risks are rated and prioritised according to guidelines provided;
- Inherent and Residual risk are assessed; and
- Financial and non-financial factors are taken into account when rating risks.

Risk Management Response strategy
- Risk responses have been identified for each risk; and
- Risk owners are assigned for each risk.

Monitoring and review
- Risk registers are updated quarterly and reported to the Manager: Enterprise Risk
  Management/CRO;
The review of the adequacy and effectiveness of the enterprise risk management processes
August 2017

KEY TO RISK RATING

<table>
<thead>
<tr>
<th>Risk Rating</th>
<th>Risk rating description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Catastrophic</td>
</tr>
<tr>
<td></td>
<td>A catastrophic level of residual risk exposure due to extreme inefficient and ineffective operation of controls which needs excessive effort and urgent attention for improvement.</td>
</tr>
<tr>
<td>4</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>A high level of residual risk exposure due to inefficient and ineffective operation of controls which needs major effort and urgent attention for improvement.</td>
</tr>
<tr>
<td>3</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>A medium level of residual risk exposure due to satisfactory controls to provide management with reasonable assurance those risks will not materialise but there is room for improvement.</td>
</tr>
<tr>
<td>2</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>A low level of residual risk exposure due to effective and efficient operation of controls which provides management with reasonable assurance those risks will not materialise and that the process objectives will be achieved.</td>
</tr>
<tr>
<td>1</td>
<td>Insignificant</td>
</tr>
<tr>
<td></td>
<td>An insignificant level of risk exposure due to extremely effective and efficient controls which provide management with reasonable assurance those risks will not materialise and that the process objectives will be achieved.</td>
</tr>
</tbody>
</table>

SUMMARY OF DETAILED AUDIT FINDINGS

The following weakness has been identified during our review and our recommendations are submitted with a view to enhance the operational internal control function of the process reviewed.

<table>
<thead>
<tr>
<th>No.</th>
<th>Detailed Audit Findings</th>
<th>Risk Rating</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>INADEQUATE SUPPORT BY EXCO IN FULLFILING THEIR ROLES AND RESPONSIBILITY WITH REGARD TO ERM</td>
<td>High</td>
<td>15-18</td>
</tr>
<tr>
<td>2</td>
<td>INEFFECTIVE FUNCTIONING OF THE RISK MANAGEMENT COMMITTEE</td>
<td>High</td>
<td>19-21</td>
</tr>
<tr>
<td>3</td>
<td>INADEQUATE EXECUTION OF THE ROLES AND RESPONSIBILITY BY THE CHIEF RISK OFFICER</td>
<td>High</td>
<td>22-24</td>
</tr>
<tr>
<td>4</td>
<td>INADEQUATE EXECUTION OF THE ROLES AND RESPONSIBILITIES BY MANAGEMENT</td>
<td>High</td>
<td>25-26</td>
</tr>
<tr>
<td>5</td>
<td>INADEQUATE RISK IDENTIFICATION PROCESS</td>
<td>Medium</td>
<td>27-29</td>
</tr>
<tr>
<td>6</td>
<td>RISK ASSESSMENT AND RISK REVIEWS ARE NOT PERFORMED CONSISTENLY ACCROSS ALL DIVISIONS.</td>
<td>High</td>
<td>30-31</td>
</tr>
<tr>
<td>7</td>
<td>INADEQUATE EVIDENCE FOR DOCUMENTATION OF EMERGING RISK FOR DAY-TO-DAY OPERATIONS</td>
<td>High</td>
<td>32-33</td>
</tr>
<tr>
<td>8</td>
<td>ADEQUATE EVIDENCE COULD NOT BE OBTAINED FOR THE ANNUAL PERFORMANCE PLAN</td>
<td>High</td>
<td>34-35</td>
</tr>
</tbody>
</table>
1. INADEQUATE SUPPORT BY EXCO IN FULLFILING THEIR ROLES AND RESPONSIBILITY WITH REGARD TO ERM

Standard

Section 38(a) i of the PFMA states that the accounting officer is responsible for the risk management, while section 76 empowers the National Treasury (NT) to issue instructions that will assist in the application of the Act. The Risk Management Framework as established by NT is applicable to all public sector institutions.

The principle of Batho Pele require prudent risk management to form the basis for government’s services delivery programmes. The Risk Management Framework establishes the need to set objectives that are aligned to the institution mission, and is the reference point for compliance with this principle.

EXCO should take an 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 Institution against significant risks.

Management is responsible and accountable to the accounting officer for managing and owning the risks facing the institution.

Policies, frameworks, strategies, plans and codes that facilitate the management of risk within the National Treasury are regarded as enablers. These governance documents should be reviewed on an annual basis to keep the department abreast with global risk management best practice.

Risk management enablers include the following governance documents:

- Risk Management Framework- A document which incorporates processes that guide Risk Management through the adoption of key policy principles and structures; and
- Risk Management Strategy- The Risk Management Strategy is a plan that describes the manner in which risk management is rolled out in NT.

Finding

During our audit review of the NT ERM we could not satisfy ourselves that EXCO is providing strategic direction in terms of their roles and responsibility, the following was noted;

- We could not verify whether EXCO has formally determined and approved
  - the risk appetite, risk tolerance and risk profile for NT;
  - the understanding of the priority risks;
  - that the risk responses for the priority risk are effective;
  - that the risk management framework is efficiently implemented and maintained; and
  - the appropriateness of the structure of ERM and their reporting lines.

- We couldn’t verify whether EXCO support and drives the vision and mission of NT ERM through monitoring the achievement of the strategic, operational and tactical objectives. Minutes of the Exco meeting held on the following dates make no mention of ERM related matters:

<table>
<thead>
<tr>
<th>No. of minutes reviewed</th>
<th>Meeting date</th>
<th>Agenda item of ERM</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>13 April 2016</td>
<td>No discussions</td>
</tr>
<tr>
<td>2</td>
<td>16 May 2016</td>
<td>No discussions</td>
</tr>
<tr>
<td>3</td>
<td>11 July 2016</td>
<td>No discussions</td>
</tr>
<tr>
<td>4</td>
<td>21 September 2016</td>
<td>No discussions</td>
</tr>
</tbody>
</table>
Furthermore, we noted that the following key governance documents that are regarded as risk management enablers were last updated on April 2013. The documents are listed below:

- Risk Management Framework- A document which incorporates processes that guide Risk Management through the adoption of key policy principles and structures; and
- Risk Management Strategy- The Risk Management Strategy is a plan that describes the manner in which risk management is rolled out in NT.

**Cause**

Inadequate review of governance documents; and Non-existence of risk tolerance and appetite framework for NT.

**Risk/Impact**

- Failer to update governance documents for risk management within NT may result in the ERM unit processes being outdated and not keeping abreast with global risk management best practice; and
- Failer to develop risk tolerance and appetite framework within NT may result in the organization not knowing the amount and type of risk that an organisation is willing to take in order to meet their strategic objectives and what an organisation can actually cope with.

**Recommendation**

- The development of the processes of risk management and monitoring should be the responsibility of the EXCO. EXCO should decide the department appetite for risk – those risks it will take and those it will not take in the pursuit of its goals and objectives. EXCO should calculate the department risk-bearing capacity and the tolerance limits for key risks, to ensure that these two metrics do not exceed the organization risk appetite;
- An organisation’s risk appetite should be communicated via a risk appetite statement, which has no fixed / defined format. The statement should include a range of quantifiable values defining the acceptable levels of risk that the board is willing to accept in pursuing the risks required to take in order to meet its objectives.
- Risk Tolerance can be expressed at a more granular / absolute level, for example “we will not expose more than x% of our capital to losses in a certain line of business” or “we will not deal with certain types of customer”. Tolerance levels can also be graphically represented alongside the appetite levels on what is referred to as a risk matrix or heat map;
- The role of the CRO should be to facilitate and coordinate the development and implementation of risk management in the organisation. Because of the strategic and multi-faceted nature of risk management, the function should be positioned at an executive level within the organization;
- The CRO should have ready and regular access to the Accounting Officer and the chairperson of the risk committee. EXCO and the management should establish an appropriate level of support for and commitment to risk management;
- EXCO should not rely solely on the embedded monitoring processes within the organization to discharge its responsibilities. It should, at appropriately considered intervals, receive and review risk management reports. In this regard, EXCO should ensure that a comprehensive risk assessment, as well as a systematic, documented review of the processes and outcomes surrounding key risks, is undertaken: on a regular basis; and following significant changes to, or shocks within, the organization operating environment;
- EXCO ultimate responsibility for the process of risk management should be expressed in its charter and supported by training and induction processes;
EXCO has an obligation to demonstrate that it has dealt comprehensively with the issues of risk management. This requires appropriate disclosure on matters such as risk tolerance and the risk management process in the integrated report; and

ERM unit should ensure that their governance documents are up to date and in line with best practice as well as latest development. The relevant authority should approve the updated documents.

Management Comments

In general, whilst we agree that certain aspects of EXCO engagement in the risk process could be improved, it is not necessarily agreed that discussions of risks at EXCO is the only avenue to demonstrate support by EXCO in fulfilling its role and responsibilities. Currently, process that shows that exco does infect fulfil its roles and responsibilities about risk management include:

- The DG has appointed and independent RC chairperson to fulfil his roles and responsibilities in terms of the PFMA with regards to risk management.
- The DG and DDG’s for each division have delegated representatives to the risk committee to represent those divisions in fulfilling their roles and responsibilities.
- Divisional Risk Registers are signed off by the divisional head, which are in turn presented at the risk committee.
- Key aspects of the risk committee proceedings are formally reported to the Audit Committee in which the DG and DDG’s are represented.
- Key aspects of the risk committee proceedings are formally reported to the DG.
- Similarly, to IA, it cannot be said that because internal audit reports and internal audit aspects are not reported at EXCO therefore EXCO does not fulfil its roles and responsibilities.

In addition, the CRO office and the risk committee had identified areas of improvement that could ensure an entrance role of EXCO in risk management being:

- Aligning risk management process with the strategy planning process, and in this regard a partnership with CD: Strategy Planning and Monitoring was formed wherein risks are identified at strategy setting and identified by the divisional head and senior management.

We agree that the outstanding item concerning this finding is the finalisation of the risk tolerance and appetite framework which has already been tabled at the risk committee for approval by the DG.

Agreed Action Plan

Approval of the risk tolerance and appetite framework.

<table>
<thead>
<tr>
<th>RESPONSIBLE PERSON</th>
<th>IMPLEMENTATION DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lwazi Giba – Chief Risk Officer</td>
<td>31 July 2017</td>
</tr>
</tbody>
</table>

Auditors Comments

It is important for the CRO and EXCO to note that:

- EXCO and NT management cannot be expected to deal with unexpected events or opportunities in a structured, planned, and confident manner if such events are not anticipated and planned for. Risk management is the process of planning, organising, directing, and controlling resources and operations (by EXCO) to achieve given objectives, despite the uncertainty of events.
Risk management should form an integral part of NT’s processes and, if fully integrated, it will enhance the strategic management process of the department. It is not a stand-alone activity (as suggested by the CRO in his management comment above) that can be separated from the main activities and processes of the department, and should not be managed within functional silos. Risk management is a management responsibility (EXCO), and forms an integral part of all NT’s processes, including strategic planning, project- and change management processes.

As a result, EXCO should specify responsibilities across multiple ‘lines of defence’ as appropriate to NT. These would generally include the executive leadership team, risk practitioners (such as a chief risk officer), management, and the overall workforce.

It is of paramount importance that Enterprise-wide risk management forms part of Exco Main Stream discussions.

Management comments and agreed action plan (commitment) regarding the approval of NT’s risk appetite and risk tolerance, and aligning risk management process with the strategy planning process, and in this regard a partnership with CD: Strategy Planning and Monitoring is noted.
2. INEFFECTIVE FUNCTIONING OF THE RISK COMMITTEE

Standard

The Risk Committee is appointed by the Accounting Officer / Authority to assist them to discharge their responsibilities for risk management. The chairperson of the Risk Committee should be an independent external person, appointed by the Accounting Officer / Authority.

The membership of the Risk Committee should comprise both management and external members with the necessary blend of skills, competencies and attributes. The responsibilities of the Risk Committee should be formally defined in a charter approved by the Accounting Officer / Authority.

In discharging its governance responsibilities relating to risk management, the Risk Committee should: (a) review and recommend for the Approval of the Accounting Officer / Authority, the: (i) risk management policy; (ii) risk management strategy; (iii) risk management implementation plan; (iv) Institution’s risk appetite, ensuring that limits are:

- supported by a rigorous analysis and expert judgment;
- expressed in the same values as the key performance indicators to which they apply;
- set for all material risks individually, as well as in aggregate for particular categorizations of risk; and
- Consistent with the materiality and significance framework.

Finding

During the review of the effective functioning of the RC, the following weaknesses were identified:

- The following roles and responsibilities of the RC could not be verified:
  i. The Accounting Officer has not appointed the chairperson of the Risk Committee, as the letter of appointment was not made available to us for confirmation.
  ii. The risk committee members have not being inducted and trained on risk management matters.

- Our review of the RC charter/terms of references established that they were last updated/revised in 2013; it is only now that management are in the processes of updating the TOR.

- Contrary to King code of governance principles, the following roles and responsibilities of RC couldn’t be verified:
  i. That the committee reviewed the NT’s risk identification and assessment processes for obtaining reasonable assurance of the completeness and accuracy of the risk register;
  ii. That the committee evaluated the effectiveness of mitigating strategies to address the material key risks of NT;
  iii. That the committee monitors compliance with the organization policies and investigation allegation of breaches of policies; and
  iv. Proof could not be obtained to enable internal audit to confirm that the committee reviews material findings and recommendations by assurance providers on the system of risk management and monitor that appropriate action was instituted to address the identified weakness.

Cause

- Inadequate review of governance documents; and
- Inadequate configuration of the risk committee.
The review of the adequacy and effectiveness of the enterprise risk management processes
August 2017

Risk/Impact

The organisation might not be able to implement the appropriate governance of risk resulting in management being reactive to risk rather than being proactive; and

Failer to update governance documents for risk management within NT may result in the ERM unit processes outdated and not keeping abreast with global risk management best practice.

Recommendation

- The Accounting Officer may appoint a dedicated risk committee to assist him/her in carrying out responsibilities in relation to risk management, where a risk committee is established, membership of the committee should include executive and non-executive directors, members of senior management and independent risk management experts, if necessary. The relationship of these experts should be defined contractually and, in order to avoid them being deemed to be directors, they should not have a vote;
- The risk committee should have a minimum of three members but with no limit to the total number of members. The risk committee should convene at least twice a year. Reports to the committee should provide the members with sufficient information to effectively discharge their responsibility;
- The committee should review the risk management maturity of the organization, the status of risk management activities and the significant risks facing the organization. The organization risk management arrangements should incorporate risk reporting processes, including risk trends, risk materialization, forecasting and emerging risks;
- The risk committee should consider the risk management strategy and policy and should monitor the risk management process. Effective and continuous monitoring is an essential part of the risk management process;
- The risk committee should consider and evaluate, among others, the following:
  - A register of key risks;
  - Estimated costs of significant losses; whether risk management costs are consistent with the risk profile of the business;
  - Material losses;
  - Reduction in earnings or cash flows caused by unforeseen incidents;
  - Material changes to the risk profile;
  - Details of risk finance arrangements that could expose the organization;
  - The risk bearing capacity of the business; and
  - Due diligence activities; and information technology risks.

Management Comments

- The Risk Committee chairperson was appointed effect from 1st August 2016 but his letter of appointment was signed June 2017 by the DG. The delays to his appointment were due to the reconfiguration of the risk management governance structure, the splitting of the entities from the audit and risk committee and therefore additional risk committees that had to be formed of which the RC chair was also to be appointed to, the number of additional independent members to serve in those committees which were not known at the time.
- With regards to induction and training of members, the CRO tabled a report at the risk committee of the 17 March 2017, specifically geared at ensuring that members are inducted on the revised risk management processes. In addition, the CRO has started a process of workshopping divisions and the entities with the first workshop done for GTAC June 2017.
- Governance documents were presented and approved at the risk committee in each of the years 2014/15/16 and it is only in 2016 that governance documents had to undergo a major revision. It is therefore not true that governance documents were not revised.
With regards to RC reviewing risk identification and assessment process, a number of RC minutes can be provided to indicate that such a review was constantly reviewed.

Risk Management Dashboards were developed for each division highlighting key risks of that division and mitigating strategies. These dashboards were tabled at the risk committee since 2014 and were presented to the risk committee by the divisions concerned. The committee members would then query such presentations and mitigations strategies and changes effected where necessary.

Both the CFO and the anticorruption unit were always presented at the RC and submitted reports, among others, on compliance breaches with policy and investigations into allegations of breaches.

As indicated above a report was tabled at the RC on the 17 March 2017 that highlighted to the RC findings of risk management assurance providers with regards to risk. It must be noted that the auditor general for the past 3 years had never raised any adverse findings with regards to risk management. IA had been conducting this audit so that both the CRO and RC can be appressed of gaps identified.

The key outstanding item with regards to this finding is the finalisation of the risk tolerance and appetite framework which has already been tabled at the risk committee for approval by the DG. It should be noted that there currently is no guideline for developing such a framework and at the time of writing this response the OAG was still in the process of developing such a guideline.

**Agreed Action Plan**

Finalise the risk tolerance and appetite framework and get approval from the DG for risk management framework

<table>
<thead>
<tr>
<th>RESPONSIBLE PERSON</th>
<th>IMPLEMENTATION DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lwazi Giba – Chief Risk Officer</td>
<td>31 July 2017</td>
</tr>
</tbody>
</table>

**Auditors Comments**

- The appointment letter of the Risk Committee chairperson was not made available to IA during the audit, as a result no evidence has been provided to provide this fact otherwise;
- The induction and training of members has not taken place, the tabling of a report by the CRO at the risk committee of the 17 March 2017 doesn’t resolve the fact that new RC members have not yet being trained/and or inducted;
- Contrary to management comments above, no minutes of the RC for the 2016/17 financial year could be provided to IA for audit purposes. As a result the following could not be verified by IA:
  i. Governance documents were presented and approved at the risk committee for the 2016/17 financial year;
  ii. RC reviewed risk identification and assessment process during the 2016/17 financial year; and
  iii. Risk Management Dashboards were developed for each division highlighting key risks of that division and mitigating strategies.
- For both RC meetings (01 August 2016 and 07 December 2016), there was no report tabled and discussed in both meetings, as a result the CRO’s management comment that “With regards to financial analyses - the CFO was always required to present on the state of finances” doesn’t hold.
Achieved and agreed action plans mentioned above by management will be followed up on a quarterly basis through the findings register process.
3. INADEQUATE EXECUTION OF THE ROLES AND RESPONSIBILITY BY THE CHIEF RISK OFFICER

Standard

The ERM unit mandate is to ensure that the responsibility of risk management is communicated and discharged across the department and the necessary capacity, structure and risk reporting lines to support ERM are established and maintained.

The primary responsibility of the Chief Risk Officer is to bring to bear his specialist expertise to assist the Institution to embed risk management and leverage its benefits to enhance performance. The high-level responsibilities of the Chief Risk Officer should include:

(a) Working with senior management to develop the Institution’s vision for risk management;
(b) Developing, in consultation with management, the Institution’s risk management framework incorporating, inter alia, the:
   ▪ Policy, strategy, implementation plan and methodology;
   ▪ Communicating the Institution’s risk management framework to all stakeholders in the institution and monitoring its implementation;
   ▪ Facilitating orientation and training for the Risk Management Committee;
   ▪ Training all stakeholders in their risk management functions;
   ▪ Continuously driving risk management to higher levels of maturity;
   ▪ Assisting Management with risk identification, assessment and development of response strategies;
   ▪ Monitoring the implementation of the response strategies;
   ▪ Collating, aggregating, interpreting and analyzing the results of risk assessments to extract risk intelligence;
   ▪ Reporting risk intelligence to the Accounting Officer / Authority, Management and the Risk Management Committee; and
   ▪ Participating with Internal Audit, Management and Auditor-General in developing the combined assurance plan for the Institution.

Finding

- During our audit review it was establish that the CRO engages EXCO on issues that are not Risk Management related as his roles includes the Facilities and Security Management of NT, which was evidence in the EXCO minutes of the meeting reviewed during the audit;
- Security and facilities matters consume most of the CRO’s time responsibilities and that results in him paying less attention to the core of his function which is enterprise risk management;
- The reporting lines of the CRO is with the DDG CS, all the functions need to be reported via the DDG-CS, which might have an impact on the execution of his role as the CRO;
- The ERM unit services National Treasury, CBDA, ASB and GTAC with only a staff complement of four enterprise risk management analyst, one enterprise risk manager and the CRO, this puts strenuous strain on the already limited resources and
- We could not obtain proof that the CRO executed the following functions:
  ▶ That the CRO has effectively communicated the risk management vision and mission of ERM; and
  ▶ That the Risk Committee and Management are adequately trained on Risk Management.

Cause

Merging of CRO roles and responsibilities with facilities and security.
The review of the adequacy and effectiveness of the enterprise risk management processes
August 2017

Risk/Impact

The CRO may not provide clear guidance and strategy on the core business of ERM unit, which might ultimately lead to risk management processes not adding any value to NT.

Recommendation

ERM unit should conduct a benchmarking exercise with institutions that have similar arrangement whereby CRO office is merge or amalgamated with other unit such as Security management and Facilities. The benchmark exercise should focus mainly on how the unit is structured, what are the reporting lines, how effective is the unit in discharging its responsibilities, what methodologies are in use, etc.

Management Comments

The matters raised in the finding have been discussed a number of times with the DDG: CS, the CAE and recently the chairperson of the risk committee.

 With regards to the inclusion of the facilities and security under the CRO office and through the aforementioned deliberations it was in fact identified that key elements of security and facilities management form fundamental pillars for effective enterprise wide risk management and should not be separated from CRO office. As such, the revised risk management policy and RC terms of reference include these functions for implementation of effective enterprise wide risk management.
 Regarding minutes reflecting facilities and security reporting at exco infect further entrances the view adopted in the paragraph above. What the minutes of EXCO should indicate with reference to issues of facilities and security are actually part key risks that EXCO felt needed to be discussed, and it therefore cannot be said that talking about such issues represent issues that are not risk related.
 With regards to engagement with EXCO – as explained in finding 1 above, it cannot be said that EXCO engagement is the only avenue to engage EXCO on risk matters and therefore if that one such avenue is not utilised there execution of roles and responsibilities is inadequate
 Regarding capacity with reference to GTAC, ASB, and CBDA – It is agreed that the unit could do with additional capacity and this was not unsupported by the the DDG: CS. As of March 2017 the unit has received an additional intern, and discussion have been held with all the entities to discuss interrelated capacity with a view to ensuring that the risk management process runs as efficient and effective as possible

The CRO is still of the view that a consulting engagement to determine the most efficient and effective way to set up oversight structures, deal with shared committee arrangements and the best way to report to senior management should still be engaged on between internal audit and cro office. This will help improve the execution of the role of the CRO in executing his roles and responsibilities.

Agreed Action Plan

Enter into a consulting engagement with IA.

<table>
<thead>
<tr>
<th>RESPONSIBLE PERSON</th>
<th>IMPLEMENTATION DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lwazi Giba – Chief Risk Officer</td>
<td>31 July 2017</td>
</tr>
</tbody>
</table>
Auditors Comments

As mentioned in Finding 1:

- EXCO and NT management cannot be expected to deal with unexpected events or opportunities in a structured, planned, and confident manner if such events are not anticipated and planned for. Risk management is the process of planning, organising, directing, and controlling resources and operations (by EXCO) to achieve given objectives, despite the uncertainty of events.

- Risk management should forms an integral part of NT’s processes and, if fully integrated, it will enhances the strategic management process of the department. It is not a stand-alone activity (as suggested by the CRO in his management comment above) that can be separated from the main activities and processes of the department, and should not be managed within functional silos. Risk management is a management responsibility (EXCO), and forms an integral part of all NT’s processes, including strategic planning, project- and change management processes.

- As a result, EXCO should specify responsibilities across multiple ‘lines of defence’ as appropriate to NT. These would generally include the executive leadership team, risk practitioners (such as a chief risk officer), management, and the overall workforce.

- Internal Audit agrees that the services provided by the Enterprise-Wide Risk Management Unit to ASB, CBDA and GTAC should be properly outlined and formalised. This will include specific details such as:
  i. Is the NT CRO the CRO to ASB, CBDA and GTAC; and/or
  ii. The Enterprise-Wide Risk Management unit of NT provide a full range of services to ASB, CBDA and GTAC as it does to NT or only limited services (risk assessment/identification only).

- IA will wait a formal request from management regarding combining of efforts between IA and ERM.
4. INADEQUATE EXECUTION OF THE ERM ROLES AND RESPONSIBILITIES BY MANAGEMENT

Standard

Management is responsible for executing their responsibilities as outlined in the risk management strategy and for integrating risk management into the operational routines, high level responsibilities of Management should include:

- Executing their responsibilities as set out in the risk management strategy;
- Empowering officials to perform effectively in their risk management responsibilities through proper communication of responsibilities, comprehensive orientation and ongoing opportunities for skills development;
- Aligning the functional risk management methodologies and processes with the Institutional process;
- Devoting personal attention to overseeing the management of key risks within their area of responsibility;
- Maintaining a co-operative relationship with the Risk Management Unit and Risk Champion;
- Providing risk management reports;
- Presenting to the Risk Management and Audit Committees as requested;
- Maintaining the proper functioning of the control environment within their area of responsibility; and
- Holding officials accountable for their specific risk management responsibilities.

Finding

During out audit review it was establish that management relies on Risk Management unit for the management of their risk, with minimum responsibility and accountability for their areas of operations. Through engagement with management of different business units within NT, it was established that their expectation is that the ERM unit is responsible for the identification and management of risk within the organization.

Cause

Lack of understanding the roles and responsibilities of risk management by management

Risk/Impact

National Treasury management is of the view that the management of risk is the role of ERM unit as a result they have minimum role to play on the process which ultimately lead to poor management/inadequate mitigating measures put in place to manage identified risk and failed to identify emerging risk from their day to day operations.

Recommendation

Internal Audit is of the view that ERM unit should have, after the results of the risk management culture survey were presented to the risk committee, developed a proper plan or strategy to address the shortcomings highlighted by the survey. The plan or strategy should include but not limited to:

- Reconfiguration of the risk committee;
- Conducting risk management workshops for all divisions within NT; and
- Forming partnership with CD: Strategy Planning and Monitoring.
Management Comments

The finding is noted and was identified through a risk management culture survey that was presented at the risk committee meeting in August 2016. As such, the risk committee was reconfigured to its current form in order to position it as a proper governance structure with the right level of management, which is representation of divisions at a Chief Director level.

Since this reconfiguration, it was made clear that the representatives should take responsibility of the divisions’ identified risks and as such, the process now followed is that each chief director representing a divisional head must present at the risk committee the division’s current and emerging risks.

Agreed Action Plan

No further action planned

<table>
<thead>
<tr>
<th>RESPONSIBLE PERSON</th>
<th>IMPLEMENTATION DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lwazi Giba – Chief Risk Officer</td>
<td>31 July 2017</td>
</tr>
</tbody>
</table>

Auditors Comments

The configuration of the Risk Committee(s) is not sufficient because it does not deal with the root cause of the finding but rather the symptoms. Internal Audit is of the view that ERM unit should have, after the results of the risk management culture survey were presented to the risk committee, developed a proper plan or strategy to address the shortcomings highlighted by the survey. The plan or strategy should include but not limited to:

- Reconfiguration of the risk committee;
- Conducting risk management workshops for all divisions within NT; and
- Forming partnership with CD: Strategy Planning and Monitoring.
5. INADEQUATE RISK IDENTIFICATION PROCESS

Standard

According to Enterprise Risk Management framework 5.7 and Condensed Public Sector Risk Management Framework, chapter 5, paragraph 14(7) "Risk identification should be strengthened by supplementing Management’s perceptions of risks, inter alia, with: (a) review of external and internal audit reports; (b) review of the reports of the Standing Committee on Public Accounts and the relevant Parliamentary Committee(s); (c) financial analyses; (d) historic data analyses; (e) actual loss data; (f) interrogation of trends in key performance indicators; (g) benchmarking against peer group or quasi peer group; (h) market and sector information; (i) scenario analyses; and (j) forecasting and stress testing."

The objective of risk identification is to understand what is at risk within the context of the Institution’s explicit and implicit objectives and to generate a comprehensive inventory of risks based on the threats and events that might prevent, degrade, delay or enhance the achievement of the objectives. Risk workshops and interviews are useful for identifying, filtering and screening risks but it is important that these judgement-based techniques be supplemented by more robust and sophisticated methods where possible, including quantitative techniques. Risk identification is a deliberate and systematic effort to identify and document the Institution’s key risks.

The ERM Unit should assist management to identify and document internal and external events affecting achievement of the department's objectives, at Strategic, Divisional and Operational levels."

Finding

During our review with ERM management, it was establish that the risk identification process does not consider all of above documents in the risk register. Internal and External audit reports are only considered in the Risk Management Dashboard that was last update in October 2016.

During our review an enquiry with ERM manager concerning attending strategic, divisional or operational meetings, it was mentioned that few of the divisions have been inviting ERM unit for sittings in their meetings, however, no evidence was provided in terms of minutes/documentations to record issues related risk management during such meetings. We were further informed that no minutes of the meeting are being kept by ERM or received from the client.

Cause

Inadequate planning

Risk/Impact

Inadequate preparation before risk assessment workshops with different chief directorates within National Treasury, which may result in other key source of information, not considered during the assessment and ultimately lead to inaccurate outcomes.

Recommendation

ERM unit should ensure that before any risk assessment workshops can be secured with different clients within NT, they should gather enough and relevant information about the area they are going to assess. The information can be gathered through reviewing AG management letter, Internal audit
The review of the adequacy and effectiveness of the enterprise risk management processes
August 2017

Management Comments

- The risk management dashboards incorporate internal audit, auditor general’s findings as part of the risk identification process, and these are revised every quarter and tabled at the risk committee wherein divisions presenting are queried on the findings presented.
- A benchmarking Exercise was done with the South African Reserve Bank in 2015.
- The issue of supplementary information such as market and sector information, scenario analyses, and forecasting and stress testing was discussed at the risk committee, and such the CRO had a number of meetings with one of the members from the CD: Risk Management in the OAG. Through those deliberations, it was agreed that such information should focus on the core business of the NT and through this process the Fiscal Risk Committee was periodical invited to present its report that detail such information.
- With regards to financial analyses - the CFO was always required to present on the state of finances.
- With regards to trends in key performance indicators - in the risk committee of March 2017 a report on trends of performance indicators was tabled and this report has become a standing item for tabling at the risk committee.
- Attendance at divisional meetings was introduced in 2015 as a way of identifying emerging risks and to also provide continuous consciousness of risk. These meetings were meant to supplement the risk management dashboard introduced a year earlier. It had always been understood that it would not be possible to have risk analysts sitting in all 11 divisional meetings, as there are only 4 risk analysts. Divisions do not operate the same in terms of periodical meetings, some prefer to hold informal meetings, some prefer to hold meetings quarterly, monthly etc. Attendance at these divisional meetings was never meant to be fundamental but rather supplementary.
- Attendance at strategic and operational meetings of divisions can be provided as these sessions were attended together with CD: Strategy planning and monitoring.
- Where we further identified existence of other risk committees such as the IFMS risk committee, such committee would be invited to present their register in the NT risk committee.
- We have never considered it important to review SCOPA reports as SCOPA considers the findings of the AG which are already incorporated in the risk management dashboards.
- In addition, reference to risk committee agendas would indicate other reports from internal stakeholders such HR, ICT, Legal that are periodically included in the agenda of the risk committee.

It is therefore our view that we do sufficiently consider internal and external reports to identify risks.

Agreed Action Plan

No further action planned

<table>
<thead>
<tr>
<th>RESPONSIBLE PERSON</th>
<th>IMPLEMENTATION DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lwazi Giba – Chief Risk Officer</td>
<td>31 July 2017</td>
</tr>
</tbody>
</table>

Auditors Comments

For the 2016/17 financial year, the secretariat of the risk committee provided IA with only two sets of minutes, for the meeting held on the 01 August 2016 and 07 December 2016, the following was evident:
For the RC Meeting held on 01 August 2016

i. Fiscal Policy Unit (Fiscal Risk Committee) tabled and presented information (risks) relating to market and sector information, scenario analyses, and forecasting and stress testing.

ii. From the presentation, it is clear that, a separate fiscal risks committee meeting (department wide) was held in May to discuss the risks to the fiscal outlook, issues around economic growth and the financial situation of State-owned companies.

ii. The RC then took the following resolutions, which they have not yet be implemented and or resolved:
   a) All risks highlighted in the Risk Committee should be both the external and internal ones.
   b) Chairperson and CRO to consolidate the input of all the committees that sit and discuss different risks of the National Treasury.

National Treasury having separate risk committee and fiscal risk committee, clearly shows that enterprise risk management is conducted in silos and until the CRO implements resolution taken in the the finding regarding inadequate risk identification process still remains.

For both RC meetings (01 August 2016 and 07 December 2016)

- There was no report tabled and discussed in both meetings, as a result the CRO’s management comment that “With regards to financial analyses - the CFO was always required to present on the state of finances” does not hold. This means the findings regarding inadequate risk identification process still remains.

The partnership between CRO and CD: Planning and Monitoring is newly established and great initiative but its consistent application and benefits going forward will be monitored.
6. RISK ASSESSMENT AND RISK REVIEWS ARE NOT PERFORMED CONSISTENTLY ACROSS ALL DIVISIONS.

Standard

Risk assessment shall be conducted on a regular and on-going basis per division and/or activity within a division, in the manner set up in this strategy (Annexure1). The ERM unit shall prepare an annual risk assessment programme in consultation with the relevant heads of divisions." Further to that, the Condensed Public Sector Risk Management Framework, chapter 6, paragraph 16(7), states that "Risk assessments should be re-performed for the key risks in response to significant environmental and/or organisational changes, but at least once a year, to ascertain the shift in the magnitude of risk and the need for further management action as per result thereof."

Finding

During our review, we requested the consolidated risk register from ERM for the financial year 2016/17. The consolidated risk register comprises of 10 Divisions with 64 chief directorates within National Treasury, from the consolidated risk register provided we noted that 17 chief directorates were either not assessed or their registers were still outstanding as at 17 March 2017. On further inspections of the consolidated risk register we also noted that Tax & Financial Sector Policy division risk assessment was last conducted in 2010/2011 financial year, meaning throughout these financial years no risk identification process took place within that particular division. The list below is for divisions without recent risk register:

<table>
<thead>
<tr>
<th>CORPORATE SERVICES</th>
<th>Strategic Projects &amp; Support</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Human Resources Management</td>
</tr>
<tr>
<td></td>
<td>Chief Financial Officer</td>
</tr>
<tr>
<td>ACCOUNTANT-GENERAL</td>
<td>Capacity Building</td>
</tr>
<tr>
<td></td>
<td>MFMA Implementation</td>
</tr>
<tr>
<td></td>
<td>Accounting Support &amp; Integration</td>
</tr>
<tr>
<td></td>
<td>Risk Management</td>
</tr>
<tr>
<td></td>
<td>Financial Systems</td>
</tr>
<tr>
<td></td>
<td>Integrated Financial Management Systems (IFMS)</td>
</tr>
<tr>
<td>TAX &amp; FINANCIAL SECTOR POLICY</td>
<td>Financial Sector Development</td>
</tr>
<tr>
<td></td>
<td>Financial Services</td>
</tr>
<tr>
<td></td>
<td>Financial Stability</td>
</tr>
<tr>
<td></td>
<td>Economic Tax Analysis</td>
</tr>
<tr>
<td></td>
<td>Legal Tax Design</td>
</tr>
<tr>
<td>INTERNATIONAL &amp; REGIONAL ECONOMIC POLICY</td>
<td>African Economic Integration</td>
</tr>
<tr>
<td>CHIEF PROCUREMENT OFFICE</td>
<td>SCM Client Support and Stakeholders</td>
</tr>
</tbody>
</table>

Cause

ERM unit experienced challenges with either initiating or finalizing the risk assessment with the clients

Risk/Impact
The review of the adequacy and effectiveness of the enterprise risk management processes
August 2017

The consolidated risk assessment for the organizations is incomplete which may result in NT not having a holistic view of its risk universe leading to identification of other key risk and implementing adequate corrective measures to mitigate the identified key risk.

Recommendation

Internal audit is of the view that ERM unit should ensure that risk assessment are conducted on time and readily available for consolidation. The assessment should include both strategic and operational risk. Where management encounter challenges, such matters should be escalated to the relevant authorities for resolution.

Management Comments

Whilst we agree that not all risk registers at CD could not be finalised the status above does not reflect the status for the entire 2016/17 financial period as presented to the risk committee on the 17 March 2017.

Please refer to the updated report presented to the risk committee on the 17 March.

We agree that the tax and financial sector division has presented challenges with regards to completing the risk assessment, but already engagements have been held with the divisional head with a view to complete the risk assessment.

Agreed Action Plan

<table>
<thead>
<tr>
<th>RESPONSIBLE PERSON</th>
<th>IMPLEMENTATION DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lwazi Giba – Chief Risk Officer</td>
<td>31 July 2017</td>
</tr>
</tbody>
</table>

Auditors Comments

As at 17 March 2017 and based on the risk management report tabled during the RC, the above mention status is correct.

The issue with tax and financial sector division has been outstanding since 2010/11 financial year; the CRO has continuously made the same commitment mentioned above without any changes or results.
7. **INADEQUATE EVIDENCE FOR DOCUMENTATION OF EMERGING RISK FOR DAY-TO-DAY OPERATIONS**

**Standard**

"Risk management should be practised by all staff in their day to day activities. A culture of risk management should be inculcated in the organization. Risk management should be as simple as possible, in order to involve all employees of the organisation."

**Finding**

After an inquiry for emerging risk document to be sent, the ERM manager mentioned that all evidence is in the risk register and emerging issues will be recorded during a formal sitting with divisions, however on further assessment we could not find any document that shows that emerging risk or day-to-day risk were properly documented and used to update the overall organization risk register/dashboard.

**Cause**

National Treasury consolidated risk register does not incorporate emerging risks

**Risk/Impact**

Inadequate process to identify emerging risk within National Treasury will result in complete organization risk register and ultimately lack of proper correcting measures put in place to mitigate emerging risk.

**Recommendation**

The CRO together with his team should ensure that the consolidated risk register for NT is inclusive of emerging risk that if the materialized can prevent the organization from achieving its sets goals and objectives. ERM should assess emerging risk through different forms and the results thereof should be included in the register and the dashboard in order to track progress.

**Management Comments**

Reference should be made to the risk management dashboard that identifies the emerging risks.

In addition as at the 17 March 17, the CRO tables the CRO report at the risk committee, specifically identifying key emerging risks for consideration by the RC and DG.

We are of the view that sufficient information concerning this will be submitted to the satisfaction of IA.

**Agreed Action Plan**

No further action planned

<table>
<thead>
<tr>
<th>RESPONSIBLE PERSON</th>
<th>IMPLEMENTATION DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lwazi Giba – Chief Risk Officer</td>
<td>31 July 2017</td>
</tr>
</tbody>
</table>
Auditors Comments

Risk management dashboard/ CRO report make no mention of the emerging risk, the top 13 risk profile mentioned in the report doesn’t make mention of any emerging risk

Risk management dashboard / CRO report tabled at the risk committee does not constitute risk registers of individual divisions.

The CRO must consider constituting proper action to ensure that emerging risks identified in the risk management dashboard/ CRO report are also included in the risk registers.
8. ADEQUATE EVIDENCE COULD NOT BE OBTAINED FOR THE ANNUAL PERFORMANCE PLAN

Standard

"EXCO should adopt a Risk Management Plan, (requires annual review; should not be designed by management; should not be isolated from the organization’s strategic plan; should be approved by the relevant authority). In the course of designing the process of risk management, account should be taken of risk appetite, risk philosophy, short and long term philosophies. The priorities and target dates for implementation of the Risk Management Plan should be specified. Risk management processes should be taken into account of when budgeting and preparing the business plan.

Finding

During our audit review, verification of documents presented by ERM unit, it was established that the Enterprise Risk Management Plan, referred as Annual Performance Plan (APP) was not in existence for current financial year of review. The strategic document inclusive of the APP was dated April 2013. The information for the current finalise year or previous year were not presented to us as proof that they were developed or implemented.

Cause

None existence of the risk committee for some parts of the 2015/15 and 2016/17 financial year.

Risk/Impact

Without an approved Enterprise Risk Management Plan, referred as Annual Performance Plan (APP) by the Risk Committee and/or Audit Committee, it shows that the department did not consider risk management processes during its strategic planning processes.

Recommendation

The CRO must ensure that NT has an approved risk management plan that will assist the department with:

- Benefits of risk identification: Risk identification will help NT in fostering the vigilance in times of discipline and calm at the times of crisis;
- Benefits of risk assessment: It has greatest advantage to NT of dealing with the points that are finalized with more solutions. NT will have a sense of all views that turns into accountability of each and every existing, inherent and emerging risks;
- Treatment of risks: This will help NT in treating its own risks that are the subsets of implementing a plan;
- Minimization of risks: The risks that are handled within the given assessments plans are foreseen within the business functions;
- Awareness about the risks: The plan will enable the department to concentrate on the risk treatments within the lessons learnt; and
- Successful business strategies: Risk management strategy is not one-time activity and the graded points are finalized within the recent status.
Management Comments

These plans were submitted to the audit committee for approval in each of the years 2014/15/16. Proof will be provided to IA that shows the plans approved at the risk committee.

Agreed Action Plan

No further action planned

<table>
<thead>
<tr>
<th>RESPONSIBLE PERSON</th>
<th>IMPLEMENTATION DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lwazi Giba – Chief Risk Officer</td>
<td>31 July 2017</td>
</tr>
</tbody>
</table>

Auditors Comments

After further verification by Internal Audit of the 2016/17 RC and AC meetings, it was noted that contrary to the management comments no proof could be found that either RC and/ or AC approved the Enterprise Risk Management Plan, referred as Annual Performance Plan (APP). This finding is still valid and management need to action corrective measures.