National Consumer Commission

Risk Management Strategy

Annex B

NATIONAL CONSUMER COMMISSION

RISK MANAGEMENT STRATEGY AND METHODOLOGY

Contents

1. Purpose of the Risk Management Strategy 4
2. Risk Management Overview 4
3. Risk Management Implementation Plan 5
4. Roles and Responsibilities 8
4.1 Risk Management Focus Areas 8
5. Risk Management responsibilities and roles 11
5.1 Senior Managers/Managers/Deputy Managers 12
5.2 Divisions and business units Management 13
6. Risk Model 14
6.1 Risk Assessments 14
6.2 Definition of risk categories 14
6.3 Impact Definitions 17
6.4 Likelihood Definitions 18
6.5 The Risk Register Template (Excel document) 19
7. Risk Management Process 20
7.1 Identify and understand objectives 20
7.2 Identify and understand activities 20
7.3 Identify and understand risks 20
7.4 Identify current controls 21
7.5 Assess the existing controls 21
7.6 Assess the impact and the likelihood of the risk 22
7.7 Rate the risk based on the existing controls 22
7.8 Determine risk response strategy 22
7.9 Determine action plan, responsible person and the target date 22
7.10 Monitoring 23
8. Monitoring is critical to the entire process. 24
8.1 Reporting 24
8.2 Reporting Frequency 24
8.3 Reporting Levels 24
9. Reporting format and content 26
10. Risk Appetite and Evaluation Criteria 27

10.1 Risk Rating (Risk Matrix) 27

1. Purpose of the Risk Management Strategy

The purpose of the Risk Management Strategy is to outline the minimum requirements and approach for risk management in the NCC, in order to address the requirements of the NCC Risk Policy.

The Risk Management Strategy and Methodology is recommended by EXCO to the Accounting Officer for approval.

2. Risk Management Overview

Good risk management is fundamental to effective corporate governance and has recently become a focus area in all corporate governance frameworks.

Enterprise is the undertaking of risk for reward. A thorough understanding of the risks accepted by the NCC in the pursuance of its objectives, together with those strategies employed to mitigate those risks, is thus essential for a proper appreciation of the NCC's affairs by the Accounting Officer and Senior Management.

Risk management is ultimately about proactively **identifying** and understanding the factors and events that may impact the achievement of strategic and operational objectives, then **managing, monitoring** and **reporting** these risks. Good risk management is not about eliminating or avoiding risks, but rather taking acceptable risks and managing them well.

3. Risk Management Implementation Plan

This is a well sequenced plan of date linked steps towards implementing the risk management framework

3.1 Risk Management Policy

The main aim of risk management policy is to achieve the following:

- To communicate the NCC's risk management philosophy
- To commit the NCC to implementing and maintaining an effective, efficient and transparent system of risk management
- To define risk in the context of the NCC and its operations
- To outline the objectives of risk management function
- To identify key role players and their responsibilities
- To monitor implementation of risk management processes

3.2 Establishment of Executive Committee (ECXO)

The core functions of EXCO regarding risk management include, amongst others:

- To assist the accounting officer in discharging his responsibilities of risk management
- To have members with the ability to act independently and objectively in the interest of the NCC
- To assess the implementation of risk management policy, strategy and plan
- To evaluate the effectiveness of mitigating strategies implemented to address material risks identified
- To interact with Audit and Risk Committee to share information relating to material risks of the NCC
- To provide timely and useful reports to the Accounting Officer on the state of risk management

3.3 Risk Management Strategy/Methodology

The main aim of implementing the risk management strategy/methodology is to achieve the following:

- To outline the risk management approach
- To describe the NCC's risk management modality
- To outline the NCC's plan of action in improving the risk maturity of the organization
- To provide a user guideline and details for review and risk management processes

3.4 Fraud Prevention Policy

The main aim of establishing the fraud prevention policy is to achieve the following:

- To provide a focus point on the prevention of fraud and corruption
- To express the NCC's commitment in managing fraud and corruption
- To make fraud reduction a priority in all independent structures of the NCC (e.g. Internal Audit and Audit and Risk Committee)
- To review and understand our fraud risks on a regular basis
- To monitor direct and indirect losses incurred via fraud, through effective information and communication.
- To form strategic alliances in combating fraud and corruption

3.5 Risk Management Plan

The main aim of implementing the risk management plan is to achieve the following:

- To maximize the possibility of achieving project objectives by managing risks.
- To manage risks such that an acceptable risk profile is established for the NCC
- To create a robust risk management framework for the NCC.
- To set achievable objectives for risk management function

3.6 Fraud Prevention Plan

The main aim of implementing the fraud prevention plan is to achieve the following:

- To develop a fraud prevention strategy and plan
- To guide in the implementation of the fraud prevention policy
- To implement the prevention plan in all structures of the NCC
- To embrace and acknowledge the contribution of all employees and members of the community who assist in the combatting and prosecution of fraudsters.
- To give cognizance to fraud risk in all procedure changes
- To form strategic alliances in combatting fraud

3.7 Risk Management Yearly Calendar for EXCO

The main aim of formulating the Audit and Risk Committee yearly calendar is to achieve the following:

- To provide information on the date, time and venues for EXCO on risk management meetings
- To book and commit EXCO members well in advance for risk management meetings

4. Roles and Responsibilities

4.1 Risk Management Focus Areas

The purpose of this diagram is to document the responsibility structure for risk management in the NCC.

4.1.1 Financial risk

There are three main sources of financial risk:

Financial risks arising from NCC's exposure to changes in market prices and economic conditions, such as interest rates, exchange rates, and commodity prices which might result in non availability of funds from the National Treasury to fund all the operations of the NCC

Financial risks arising from the actions of, and transactions with, other organizations such as vendors, customers, and counterparts in derivatives transactions

Financial risks resulting from internal actions or failures of the organization, particularly people, processes, and systems

Non compliance with the PFMA, National Treasury Regulations, Division of Revenue Act and other relevant prescripts and legislation

4.1.2 Fraud & Corruption Prevention and Awareness

The programme is intended to set down the attitude and stance of the NCC to fraud and corruption.

It also sets down the NCC's attitude towards reinforcing existing systems, policies, procedures, as well as the rules and regulations of the NCC aimed at deterring, preventing, detecting, reacting to and reducing the impact of fraud and corruption.

In addition, the purpose of this document is to confirm that the NCC supports a culture of zero tolerance towards fraud and corruption.

4.1.3 Functional Risks

Understanding the objectives is first step in the risk management process. Without this understanding, risks that could prevent the achievement of objectives cannot be identified completely.

These objectives should be aligned throughout the NCC to ensure that direction and focus of the different levels of management are fully integrated.
These objectives need to flow from a strategic level, to a business and ultimately a process level to ensure this alignment as set out below.

Strategic: The NCC's objectives that are informed by NCC's Annul Performance Plan;

Operational: Objectives that are set by the Divisional Head and Business Unit Managers to support the achievement of the strategic objectives

Process: Objectives that are set by the Senior Managers at process level to support the operational / business objectives

Understanding of objectives should take place as part of the existing strategic and operational planning processes.
This should further be supported by the budgeting and forecasting and performance management processes (i.e. KPA's and KPI's).

5. Risk Management responsibilities and roles

The Risk Manager reports directly to the Commissioner on functionality and governance issues.

The Risk Manager performs the following roles:

- A facilitating, supporting and enabling role to EXCO and the NCC in its performance of risk management processes;
- Providing a central source of information and guidance on risk management;
- Encouraging and creating awareness of risk management throughout the NCC;
- Ensuring consistency in evaluation and reporting of risks throughout the NCC;
- The person in this role will perform a risk report co-ordination and collating role on behalf of both EXCO and the Commissioner.

The Risk Manager supports EXCO and report to the Audit and Risk Committee, at least initially, in the following roles:

- A monitoring and operational role for EXCO regarding the status of risk and risk management processes in the NCC in general; and
- A monitoring and operational role on behalf of the Accounting Officer and / or Audit and Risk Committee regarding the status of risk management throughout the NCC.

The detailed tasks role includes:

- Reviewing / establishing the appropriate risk management policy and strategy for the NCC;
- Assisting the Accounting Officer and EXCO with setting their risk tolerance / appetite and establishment of related risk strategies and processes;
- Assisting with the communication of the risk management policy, strategy and methodology to the NCC;
- Risk management reporting from all Divisions and business units will be reported through risk management so that they obtain overview and report on a high level to the Accounting Officer, EXCO and the Audit and Risk Committee;
- Ensuring consistency of risk management practices and reporting throughout the NCC to enable consolidation of results;
- Where gaps in the risk management process are observed, risk management should facilitate the process to ensure that management action plans are sufficient and adequate to close the gaps, thereby ensuring the effectiveness of risk management processes;

- Provide the NCC Audit and Risk Committee with assurance that business throughout the organization have appropriate risk management processes in place to enable management to discharge their accountability for risk management and make their disclosures;
- Assisting the Accounting Officer with a continuous monitoring process that ensures that the Accounting Officer is able to perform his/ her annual review of risk management effectiveness and make any disclosure. EXCO cannot rely solely on the fact that risk management is embedded;
- Assisting Management to discharge its responsibility and comply with any statutory or regulatory requirements by facilitating the development, establishment and maintenance of an efficient and effective risk management process;
- Ensuring that risk management is aligned throughout the NCC to ensure that no duplication occurs and all risk management silos are integrated;
- Undertake training within the NCC regarding risk management, as and when required;
- Liaise with Internal Audit to facilitate the generation of a risk based internal audit plan;
- To provide input, where necessary, for insurance and compliance budgets; and
- Financial quantification of losses or potential losses as a result of risk events. This information must be provided to the Audit and Risk Committee.

5.1 Senior Managers/Managers/Deputy Managers

Program Managers are responsible for ensuring the effective performance of risk management throughout the NCC (i.e. executing the risk management policy).

This will entail:

- Identifying strategic risks at a the NCC level;
- Evaluating the impact of these risks on the achievement of strategic objectives and the likelihood of these risks occurring;
- Deciding on the best management and control strategies to manage these risks to an acceptable level,
- Ensuring that management processes (controls) are adequate and effective to manage risks;
- Monitoring the status of risks and business environment factors affecting risks;
- Reviewing the risk reports filtered from strategic level to ensure that risk management is effective at operational levels and that significant risks are included in the NCC's risk profile; and
- Reporting on the above processes to the Accounting Officer and Audit and Risk Committee.

5.2 Divisions and Senior Management

Senior Managers and Managers within Divisions are accountable for the management of risk, achieving business objectives at Divisional and business unit level. Divisions and business units need to set appropriate goals, objectives, targets and performance indicators for all their functions. This includes the responsibility for designing, implementing and monitoring the process of risk management and integrating it within the operational management processes of their respective Divisions and business units.

They need to meet all applicable laws and regulations as a minimum, as well as where appropriate, apply international best practice. Management should build on and use existing operational management structures and processes to embed risk management in their Divisions/Business units.

Responsibilities in terms of risk management entail the following:

- Ensuring that at all levels employees collectively have the competence and responsibility through selection, retention, education, training and awareness to implement these guidelines;
- Identifying significant risks at a Divisional/Business unit level, whichever is applicable;
- Evaluating the impact of these risks on the achievement of operational and process objectives and the likelihood of these risks occurring;
- Deciding on the best management strategy to manage these risks to an acceptable level;
- Ensuring that the management processes (controls) which are put in place to manage risks, are adequate and effective;
- Monitoring the risks and the business environment factors that affect the risk;
- Reviewing the risk reports filtered from the units within the Divisions/Business units and ensuring that all significant risks are effectively managed, and summarized to reflect an overall Divisional/Business unit risk profile; and
- Reporting on the above processes both at an EXCO Level and Audit and Risk Committee level.

6. Risk Model

6.1 Risk Assessments

All Divisions will be required to compile a risk register at least once a year (i.e. after the approval of strategic plan and annual performance plan) through risk assessment workshops.

Risk registers will be reviewed and updated once every two months through meetings with risk and action plan owners

After any strategic/policy/mandate/structural changes a risk assessment workshop will be conducted to review and update a risk register

Report once a month on the implementation of action plans

6.2 Definition of risk categories

In terms of the NCC's policy, risks in the NCC will be categorized as in the Risk Model.

This Risk Model is consistent with the National Treasury's Risk Model, with the exception of the risk category Operational and sub-category the NCC, which has been added.

A risk framework has been developed which sets out the various risks that need to be considered as part of the risk identification process. The sub categories reflected should not be regarded as comprehensive but merely as a guide to facilitate the risk identification process. The framework assists in the identification of risks, and in reporting risks by category instead of risks being reported individually.

Each risk should be rated and categorized in terms of the impact the risk may have and should it be in line with the guidelines provided below.

The impact ratings to be used as a guideline when rating the risks at Strategic (Programme), Operational (Divisions/Business units) levels are:

Risk Category	Definition
Asset Management	These risks relate to the misuse, damage, theft or underutilization of physical NCC Assets
Compliance/ Regulatory	These risks arise as a result of the failure to comply, monitor or enforce compliance with legislation including the risk of not responding to changes to the regulations/ legislation
Cultural	Failure to create an achievements culture which aligns NCC business objectives with our individual objectives. A poor culture may arise when there is an inadequate corporate structure, a lack of clarity around roles and responsibilities, low ethical standards and values, a lack of cultural integration, inappropriate management style and a lack of communication. It includes failure to manage change and its impact on people.
Disaster Recovery	These risks relate to business interruptions, and the processes and procedures that NCC has in place to manage these interruptions.
Economic	The risk of an economic downturn impacting NCC. Underdevelopment
Environmental (Nature)	Failure to comply with environmental requirements/ responsibilities leading to a depletion of natural resources and environmental degradation.
Financial	These risks relate to: - Cash Flow - Financial Loss - Financial Statement Integrity - Revenue Maximization This collection of risks identifies the financial areas we need to manage.
Fraud and Corruption	Employees/ Non-employees engaging in illegal acts, fraud or corruption. This would include nepotism.
Health and Safety	These risks relate to environmental and health and safety requirements/ regulations which may lead to illness, injury or death to both employees and non-employees.
Human Resources	These risks arise from inadequate human resources both in terms of skill and capacity, a lack of equity in the workplace, lack of motivation and productivity of staff and significant turnover in staff turnover numbers.
Information	These risks relate to the availability, integrity, retention and safeguarding of information.
Information Systems	These risks relate to NCC's dependence on information technology as a

	business, within the areas of: Availability of information systems Integrity of information systems Effectiveness of information systems
Litigation	These risks relate to legal claims from employees and non-employees and NCC's failure to exercise its legal rights.
Material Resources	These risks relate to the availability, cost and quality of material resources as well as the wastage of these resources
Operational	These risks relate to the day to day operational processes that fall outside of any of the other risk categories. Wherever possible this should only be used in the event that no other risk category could be used.
Reputation	These risks relate to action/s or non-action/s that may harm the reputation of NCC. Inappropriate or ineffective communication within NCC (internal and external communication)
Service Delivery	Inadequate service/ project management leading to inappropriate activities, increased costs, inadequate change management and late delivery.
Strategic	The Strategy of NCC determines its direction and sets out how it will achieve the budget/financial returns which are required by the stakeholders. The risks within this category consider factors which can influence the strategic direction or the ability of NCC to execute the plan.
Third Party Performance	Inadequate management of third party performance which leads to increased costs, inadequate change management, late delivery or implementation failure.

6.3 Impact Definitions

Rating	**Assessment**	Definition
1	Insignificant	The risk will have a negligible impact on the achievement of objectives
2	Minor	The risk will have a very low impact on the achievement of objectives
3	Mild	The risk will have a mild impact on the achievement of objectives
4	Moderate	The risk will have a moderate impact on the achievement of objectives
5	Terrible	The risk will have a terrible impact on the achievement of objectives
6	Tragic	The risk will have a tragic impact on the achievement of objectives
7	Critical	The risk will have a critical impact on the achievement of objectives
8	Disastrous	The risk will have a disastrous impact on the achievement of objectives
9	Catastrophic	The risk will have a catastrophic impact on the achievement of objectives

6.4 Likelihood Definitions

Each risk should be rated in terms of the likelihood of the risk occurring as per the guidelines provided below. The likelihood ratings are consistent for strategic, operational and process risks.

Rating	**Assessment**	Definition
1	Never occurs	The risk is unlikely to occur even in the long term.
2	Very Unlikely	The risk is unlikely to occur in the next 3 years.
3	Seldom	The risk is likely to occur in the next 2-3 years.
4	Sometimes	The risk is likely to occur at least once within the next 12 months.
5	May occur	The risk is already occurring or is likely to occur more than once in the next 12 months.
6	Very likely to occur	The risk might occur in occasional circumstances; or, in the given circumstance, the likelihood is medium.
7	Often occur	The risk might occur in some circumstances; or, in the given circumstance, there is a reasonable chance the risk will occur.
8	Greater chance of occurrence	The risk will probably occur in the majority of circumstances; or, in the given circumstance, the likelihood is high.
9	Will definitely occur	It is expect that the risk will occur in almost all circumstances; or, in the given circumstance, it will almost certainly occur

Likelihood of the risk occurring should be assessed after taking into account current controls and actions to mitigate the risk.

For example, factors related to the accuracy and reliability of information and information systems related to a database of Complaints Handling as well as the processes in place to gather and maintain details and records of complainants should be considered when rating the impact thereof.

6.5 The Risk Register Template (Excel document)

Risk management should be performed at all levels of the NCC i.e. strategic level and operational level.

The overall flow of the Risk Management process will determine:

- A clear and unambiguous understanding of strategic and operational objectives and purpose;
- The obstacles (risks), which can prevent the achievement of these objectives;
- The business environment and contributing factors that can cause the risks to occur;
- An evaluation of the residual impact based on the controls in place to manage the risks if they were to occur;
- A post control evaluation of the risk to determine the likelihood of assurance of the risk and the residual risk exposure;
- The control strategy, which is the response to the risk – This could be to Accept, Insure, Outsource, Avoid and/or to Manage the risk - and the specific risk management processes (controls) to manage the risk;
- Cost benefit considerations will be a factor in deciding on the most suitable response;
- Any enhancements to controls if the residual exposure is still not acceptable to management;
- Ongoing monitoring of the status of risks and business environment factors that may impact the risk; and
- Ongoing reporting on the risk profile of the organization.

7. Risk Management Process

The steps to be followed in a risk management process are listed in the table below:

7.1 Identify and understand objectives

Understanding the objectives of the NCC is the first step in the risk management process. Interrogations and deep analysis of risks that could prevent the NCC from the achievement of its strategic, operational and process objectives cannot be identified completely.

These objectives should be aligned throughout the organization to ensure that direction and focus of the different levels of management are fully integrated. Objectives need to flow from a strategic level, to a business and ultimately a process level to ensure this alignment as set out below.

7.2 Identify and understand activities

The NCC has certain objectives i.e. goals it has set for itself to achieve and after those objectives follows the activities that have to be performed to achieve these objectives. Therefore, having clearly understood the activities at any level of the NCC, it is important to the achievement of strategic and /or business objectives.

7.3 Identify and understand risks

Risks are the obstacles that can prevent the NCC from achieving its objectives. Therefore, having clearly understood the business objectives at any level of the NCC will make it easier to identify the risks that could prevent the achievement of strategic and /or business objectives.

Risks need to be identified by relevant management and staff. The risk model in the previous section can be used to assist management in the identification of risk.

The following information should be obtained for each risk:

- The business environment and contributing factors that can cause the risks to occur, i.e. the root causes;
- A description of the risk as well as an understanding of which objective it threatens; and

- The allocation of the risk to the relevant risk category and sub category within the risk management framework.

Risk identification is not a once off process but a continuous process.
After completion of the Risk Management process, EXCO in conjunction with the Risk Manager will be responsible for ensuring that they update the risk profile of the NCC by reassessing the status of risks and by identifying new risks arising through change in the business.

New risks would mainly arise through change in the external business environment as well as internal change.

Business environment factors can directly impact the risks that the NCC faces and therefore its objectives. Consideration of the changes in the business environment are also necessary to ensure that management is able to respond to changes in their business environment quickly and to ensure that strategic and operational objectives are realigned. Business environment factors can be both internal e.g. culture or structure; or external to the NCC e.g. competition and legislation.

7.4 Identify current controls

It is important to identify current controls in place that address the risks identified. These should be controls that actually exist and not what should be in place theoretically.
The next step in the process is to determine the control gaps. This can be determined by assessing the change of the impact and likelihood ratings for inherent and residual rating. Refer to the above paragraph.

7.5 Assess the existing controls

The existing controls have to be assessed for adequacy and effectiveness to address the identified risks. The control adequacy should be assessed as adequate, partially adequate or inadequate. Similarly the effectiveness of the controls needs to be assessed as either effective, partially effective or ineffective. It is important to ensure that these assessments match the impact and likelihood ratings. For example a control cannot be regarded as effective if the residual likelihood of the risk occurring is common.

7.6 Assess the impact and the likelihood of the risk

After assessing the existing controls, the impact of the risk has to be assessed. The impact of the risk should be assessed without taking into account the existing control. Once the impact of the risk is scored, based on the impact it will have on the NCC, then the likelihood of occurrence is assessed, taking into account the existing controls.

7.7 Rate the risk based on the existing controls

The risk is rated as a score of risk impact multiplied by the score of the likelihood of the risk to occur. The answer is the risk rating that the NCC should make a decision on whether the risk is within the acceptable or tolerance level or above the tolerance level.

7.8 Determine risk response strategy

Management has to decide whether to **accept** the risk, **manage** the risk, **transfer** (insure or outsource) the risk or **avoid** the risk altogether. The strategies are further explained below:

- Accept risk: simply take the chance that the negative impact will be incurred
- Avoid risk; changing plans in order to prevent the problem from arising
- Manage risk: lessening its impact through intermediate steps
- Transfer risk: outsource risk to a capable third party that can manage the outcome

Depending on the risk response strategy selected management need to consider additional actions/controls to mitigate the risk to an acceptable level.

When identifying possible enhancements, cost benefit considerations need to be taken into account. This step is aimed at optimizing the effectiveness of the NCC's on-going risk management process.

7.9 Determine action plan, responsible person and the target date

Management need to decide whether further action is required to reduce either the impact and/or likelihood of the risk. In many cases the likelihood of risk occurring can be reduced. Consideration should also be taken of the value added by the action. An over controlled environment results in inefficiencies.

It is critical to allocate actions to specific individuals or groups of individuals with clear start and due dates. Where actions are dependent on one another this should also be indicated so that bottlenecks can be avoided.

7.10 Monitoring

Having identified the response strategy, continuous monitoring needs to occur to ensure that the desired response strategy for a risk is implemented successfully. Monitoring is arguably the most important step of the entire risk management process as it provides early warning of where risks may materialise.

8. Monitoring is critical to the entire process.

The following techniques should be used to assist with monitoring:

- Identification and tracking of risk indicators that can act as an early warning system. For example, if poor client service is identified as a risk and certain controls have been identified to mitigate the risk, a risk indicator could be the number of client complaints reported. If this is above the acceptable norm it is an indication that the mitigating controls are not working well;
- Internal Audit can be used to provide assurance regarding the adequacy and effectiveness of mitigating controls;
- Progress on risk mitigation should be discussed on regular management meetings.
- Regular risk reporting to EXCO and the Audit and Risk Committee.

8.1 Reporting

Reporting of the results of the risk management process is critical, as this will ensure that the risk management process is ongoing and embedded.

8.2 Reporting Frequency

Reporting frequency will be quarterly for strategic risks and bi-monthly for operational risks and process risks.
Depending on the changes in the operational environment, the reporting can happen any time and will either be reported on the Strategic and Operational risk profile.

8.3 Reporting Levels

The level of management that risks have to be reported to will depend on the nature of the objective, and the related impact and likelihood of the risk.

Strategic (business) risks

- All strategic (business) risks with a risk rating between 61 and 81 (i.e. high risk area) should be reported to the Audit and Risk Committee, as well as the responsible Divisional Head and confirmation is required that controls are in place and are adequate and effective.

- Once reviewed by the Audit and Risk Committee a consolidated report should be forwarded to the Commissioner, and all Divisional heads.

Operational (Divisions and business units level) risks

- All operational risks with a risk rating between 61 and 81 (i.e. high risk area) should be reported to the Audit and Risk Committee, as well as the responsible Divisional Head and confirmation is required that controls are in place and are adequate and effective.
- Once reviewed by the Risk Manager, a consolidated report should be forwarded to the Audit and Risk Committee, the Commissioner, and all Divisional heads and senior managers.

9. Reporting format and content

The purpose of this strategy document is not to prescribe in detail the reporting formats but to specify the minimum requirements in terms of what has to be reported for each risk.

These are:

- A clear description of the risk including context;
- The impact, likelihood and residual risk rating for the risk. Colour codes in terms of the Evaluation Criteria in the next section;
- Current response strategy for the risk including current actions or controls to mitigate the risk;
- Proposed response strategy with additional actions/controls to be implemented;
- Owner of the risk;
- Deadline date for implementation of response strategy; and
- Key risk Indicators to track the status of the risk.

10. Risk Appetite and Evaluation Criteria

The Commissioner, through the Audit and Risk Committee sets the risk appetite for the NCC. Risk appetite is the level of tolerance for risk in the NCC; in other words, at what point does a risk become serious enough for the NCC to start committing resources into the management of the risk.

For example:

- A risk with a very high impact and high likelihood of occurrence. This risk might be totally unacceptable in terms of the risk appetite of the NCC. The management strategy therefore is to implement action plans to reduce the impact or likelihood of occurrence of the risk;
- A risk with a very high impact but low likelihood of occurrence (e.g. fire, flood, earthquake). The management strategy is to manage such a risk and develop appropriate recovery strategies.
- A risk with a low impact and low likelihood of occurrence. Such a risk might be acceptable to the NCC depending on the risk appetite. The management strategy might be to keep the risk on the radar but not commit any resources into the management of the risk. In other words, to live with it.

10.1 Risk Rating (Risk Matrix)

Residual risk is the product of Impact and Likelihood. The risk appetite for company level residual risk is as follows:

Colour	Mitigation strategy	Ratings	Number Range	
Green	Accept	Low Risk Area	**0**	**20**
Blue	Accept	Medium Risk Area	**21**	**40**
Yellow	Manage	Medium-High Risk Area	**41**	**60**
RED	Manage	High Risk Area	**61**	**81**

APPROVAL OF THE RISK MANAGEMENT STRATEGIC DOCUMENT:

EFFECTIVE FROM :Reviewed on the 18 August 2014

APPROVED BY :_____

SIGNATURE :_____

DATE :_____