national film and video foundation
SOUTH AFRICA
an agency of the Department of Sport, Arts and Culture

ENTERPRISE RISK MANAGEMENT MANUAL

MARCH 2022

Issue date: March 2022	Version: 1.0	**Signatures**
Approval date (Council):	24 March 2022	
Chief Financial Officer **Mr. Peter Makaneta**	Process Owner	
Chief Executive Officer **Ms. Makhosazana Khanyile**	Doc Reviewer	
Audit and Risk Committee Chairperson **Ms. Zanele Nkosi**	Doc Reviewer	

APPROVAL

The signatories hereof, confirm their acceptance of the content and authorise the adoption thereof.

Ms. Tholoana Ncheke Date: April 2022

Chairperson of Council

NFVF RISK
MANAGEMENT POLICY

MARCH 2022

Table Of Contents

MARCH 2022

1. DOCUMENT CHANGE HISTORY

2. DEFINITIONS

3. LIST OF ABBREVIATIONS

4. PURPOSE

5. SCOPE

6. OBJECTIVES

7. KEY PRINCIPLES

8. EFFECTIVE DATE

9. REFERENCE DOCUMENTATION

10. COMPLIANCE WITH POLICY

11. EXEMPTIONS

12. ROLES AND RESPONSIBILITIES

13. POLICY STATEMENTS

14. REPORTING AND MONITORING

15. CONCLUSION

1. DOCUMENT CHANGE HISTORY

PUBLICATION DATE	AUTHOR	REVISION NO	CHANGE DESCRIPTION

2. DEFINITIONS

Term	Definition (in the context of this policy)
Accounting Authority	The Council of the National Film and Video Foundation.
Corporate Governance	The system of rules, practices and processes by which an organisation is directed and controlled.
Employees	All individuals employed by the organisation, on a permanent, temporary and/or contractual basis, incurring costs in the name of the organisation.
Management Committee (MANCO)	The Committee made up of the Heads of Department and the leadership team and chaired by the Chief Executive Officer.
Emerging Risk	A risk that is perceived to be potentially significant, but which may not yet be fully understood and difficult to quantify due to lack of data and/or volatility and may be beyond one's direct capacity to control. Such risk's consequences, implications and interconnectedness with other risks may be ambiguous and difficult to assess in the present day until more data becomes available.
Inherent Risk	The exposure arising from risk factors in the absence of deliberate management intervention(s) to exercise control over such factors – *as per National Treasury Public Sector Risk Management Framework.*
Residual Risk	The remaining exposure after the mitigating effects of deliberate management intervention(s) to control such exposure (the remaining risk after Management has put in place measures to control the inherent risk) – *as per National Treasury Public Sector Risk Management Framework.*

Management	Senior, middle and lower-level management, responsible for identifying and managing risk(s) within areas under their control.
Risk	An unwanted outcome, actual or potential, to the Institution' s service delivery and other performance objectives, caused by the presence of risk factor(s). Some risk factor(s) also present upside potential, which Management must be aware of and be prepared to exploit. This definition of "risk" also encompasses such opportunities – *as per National Treasury Public Sector Risk Management Framework.*
Risk Appetite	The aggregate quantifiable value and type of risk that an organisation is willing to tolerate in order to achieve its strategic objectives <u>or</u> The amount of residual risk that the Institution is willing to accept - *as per National Treasury Public Sector Risk Management Framework.*
Risk Assessment	The overall process or method of: • identifying risk factors; • risk analysis: • risk evaluation; and • determination of appropriate ways/steps to eliminate the risk, or to control the risk if it cannot be eliminated.
Risk Culture	The beliefs, attitudes and behaviors related to risk awareness, risk taking and risk management.
Risk Management	A systematic and formalised process to identify, assess, manage and monitor risks - *as per National Treasury Public Sector Risk Management Framework.*
Risk Matrix	A tool used to complete a quantitative assessment of the probability/likelihood and the impact of a specific risk materialising. The matrix uses a point scale (zero, low, medium, high) to determine the residual risk rating for the specific risks identified during a risk assessment process.

Risk Owner	An employee who is ultimately accountable for ensuring that risk is managed appropriately. There may be multiple personnel who have direct responsibility for, or oversight of activities to manage each identified risk, and who collaborate with the accountable risk owner in his/her risk management efforts.
Risk Champion	A person who by virtue of his/her expertise or authority champions a particular aspect of the risk management process, but who is not the risk owner - *as per National Treasury Public Sector Risk Management Framework.*
Risk Register	A standard risk management tool used as a repository for identified risks, characteristics and mitigation strategies.
Risk Tolerance	The amount of risk the Institution is capable of bearing (as opposed to the amount of risk it is willing to bear) - *as per National Treasury Public Sector Risk Management Framework.*

3. LIST OF ABBREVIATIONS

Abbreviation	Full term
NFVF	National Film and Video Foundation
ARC	Audit and Risk Committee
CEO	Chief Executive Officer
ERM	Enterprise Risk Management
MANCO	Management Committee
RMC	Risk Management Committee
IA	Internal Audit
ICT	Information and Communication Technology
IP	Intellectual Property
PFMA	Public Finance Management Act
POPIA	Protection of Personal Information Act

4. PURPOSE

The purpose of this policy is to provide direction and guiding principles regarding risk management within the National Film and Video Foundation (NFVF) in order to enable the achievement of the strategic goals and objectives of the organisation.

This policy further seeks to ensure that there is general certainty, formality and consistency in the application of the risk management processes and procedures in the organisation.

5. SCOPE

This policy applies to all NFVF governance structures, employees (permanent, contract and temporary, inclusive of studentships and interns) and any third parties that are legally and/or contractually obligated to conform thereto.

This policy is supported by and must be read in conjunction with all other policies, frameworks and standards used in the organisation as internal risk management control mechanisms, the same being too comprehensive to be explicitly included herein.

6. OBJECTIVES

The objectives of this policy are to ensure that ERM supports the organisation through the implementation of effective and efficient risk management practices through:

6.1. A consistent and effective approach to risk management that is guided by the organisation's mission and vision;

6.2. Fostering and encouraging a risk culture, where risk management is part of the organisation's operational activities and an integral part of decision-making processes;

6.3. Ensuring effective risk management that is aligned to the organisation's tolerance and risk appetite levels;

6.4. Enabling the implementation of a sound and effective fraud prevention plan that aims to eradicate fraudulent behavior at all levels within the organisation; and

6.5. Enabling the implementation of a sound and effective compliance management framework that would ensure compliance to statutory and regulatory requirements.

7. KEY PRINCIPLES

7.1. In principle, risk management enables the NFVF to achieve its goals and objectives and to improve the outcomes of its core business activities in all key performance areas including financial management, project management, corporate governance, information management and health and safety, amongst others.

7.2. Fundamentally, for the risk management process to be effective, it is essential that the NFVF consciously and systematically ensures that there is alignment between its core business strategy, organisational culture and organisational resources. The principles of the Policy are to:

7.2.1. Address enterprise-wide risks as outlined in the NFVF’s Risk Management Framework;

7.2.2. Establish and maintain an integral part of all organisational processes in a systematic, structured and timely manner based on the best available information;

7.2.3. Respond promptly to both internal and external events, changes in the environment, new knowledge and opportunities, the results of the monitoring and reviewing of activities, new risks that emerge, and existing risks that changes or disappear;

7.2.4. Ensure the NFVF constantly improves its operations by developing and implementing strategies to improve its risk management maturity;

7.2.5. Remain in compliance with regulatory requirements and leading risk-management practices;

7.2.6. Align to good corporate governance and acceptable standards; and

7.2.7. Encourage the accountability, ownership, responsibilities, expectations, as well as the required conduct and mindset regarding the risk-management responsibilities of Council and its committees, management at all levels, staff members and interns/students; and third parties undertaking work for and on behalf of the NFVF.

8. EFFECTIVE DATE

This policy is valid from the “Effective Date” of 1 April 2022.

9. REFERENCE DOCUMENTATION

As noted in clause 5 of this document, this policy is supported by and must be read in conjunction with all other regulations, policies, frameworks, charters and standards used in the organisation as internal risk management control mechanisms.

Table 1 below makes reference to the key applicable best practice, standards, regulatory requirements, internal policies etc., that are applicable to the NFVF business environment and compliance therewith being essential to ensure effective risk management in the organisation.

Table 1: Key applicable reference documentation

Number	Reference	Name of the Regulation /Document
1	Regulatory Framework	Public Finance Management Act, No. 1 of 1999

Number	Reference	Name of the Regulation /Document
2	Regulatory Framework	National Treasury Regulations and Guidelines
3	Regulatory Framework	National Film and Video Foundation Act, No. 73 of 1997 (as amended)
4	Regulatory Framework	Protection of Personal Information Act, No. 4 of 2013 (POPIA)
5	Best Practice	King IV Code of Corporate Governance (King IV)
6	Best Practice	ISO 31000 - Risk Management
7	Other NFVF Internal Policies/Documents	• Risk Management Framework; • Risk Appetite and Tolerance Framework; • Finance Policies and Procedures Manual; • NFVF Council Charter; • NFVF Audit and Risk Committee Charter; • Delegation of Authority Framework; • Materiality and Significance Framework; • Conditions of service; • Code of ethics; and • All other policies, guidelines, frameworks and standards designed to manage risks in the organisation e.g., NFVF Funding Policy, etc.

10. COMPLIANCE WITH POLICY

All governance structures, employees and any other third parties contractually or otherwise legally obligated must comply with this risk management policy and supporting standards, processes and procedures. Failure and/or refusal to abide by this policy shall be deemed as misconduct which may result in a disciplinary action being instituted against an offending individual. A claim of ignorance as to the existence and/or application of this policy shall not be grounds for justification of non- compliance.

Non-adherence to this policy must be promptly reported to the CEO, or the delegated authority, who would initiate an investigation (of any form) into any potential contravention. Any employee or third party legally obligated to comply with this policy but fails to do so, shall be subjected to the appropriate disciplinary and/or legal action.

11. EXEMPTIONS

Exemptions, exceptions or deviations from this policy may only be considered if they are warranted and lawful and in the best interest of the organisation. Only the Management Committee and/or a properly delegated authority can approve exemptions, exceptions or deviations from this policy. Approval requests must be submitted in writing for authorisation to the Management Committee or properly delegated authority. Each exemption, exception or deviation from this policy shall be considered on a case-by-case basis, and approval of an exemption, exception or deviation does not constitute precedent to maintain or an amendment of this policy.

12. ROLES AND RESPONSIBILITIES

The roles and responsibilities associated with this policy are outlined below. More details on the specific roles, functions, responsibilities, activities and tasks related to risk management are defined and documented in supporting frameworks, standards, guidelines, processes and procedures governing and informing ERM.

12.1. The Council

As the Accounting Authority, which would be the equivalent of a Board as defined in King IV, the NFVF Council remains ultimately accountable for the appropriateness of the risk management system and would:

12.1.1. Be accountable for risk governance in the organisation;

12.1.2. Be accountable to the shareholder, to oversee/govern the implementation of an effective system of risk management in the organisation;

12.1.3. Approve the Risk Management Policy and any amendments thereto;

12.1.4. Provide oversight of the organisation’s risk universe;

12.1.5. Be responsible for the establishment of a sub-committee of the Council that is responsible for Audit and Risk Management in the organisation (ARC);

12.1.6. Oversee the effectiveness of the ARC;

12.1.7. Set and approve the terms of reference of the ARC;

12.1.8. Appoint the members of the ARC;

12.1.9. Assess whether an independent external opinion is necessary to assess the effectiveness of regulatory risk management; and

12.1.10. Review and ratify the risk appetite and tolerance that articulates the nature, types and levels of risk that the organisation is willing to pursue through the ARC as articulated in the Risk Appetite and Tolerance Framework of the NFVF.

12.2. The Audit and Risk Committee

12.2.1. Provides advice to the Council on audit and risk management;

12.2.2. Oversees the organisation’s system of risk management and internal control;

12.2.3. Reviews the operational effectiveness of this policy and related risk management frameworks, standards, guidelines, processes and procedures;

12.2.4. Reviews reports from management to ensure that material business risks are being managed effectively;

12.2.5. Reviews and makes recommendations to the Council in relation to the management of incidents that pose a risk to the organisation; and

12.2.6. Reviews updates and/or changes in the Strategic Risk Register, Risk Management Policies and Risk appetite and Tolerance for recommendation to Council for their approval on a quarterly basis.

12.3. Chief Executive Officer

The CEO as the Accounting Officer has the responsibility of ensuring that the organisation has and maintains an effective, efficient and transparent system of financial, risk management and internal control as mandated by section 38(1)(a)(i) of the PFMA, No. 1 of 1999, as amended.

12.4. MANCO and RMC

Although the CFO and/or the Risk Management Officer is tasked with the responsibility of facilitating risk management in the NFVF, MANCO members who for the purposes of ERM would fulfil the role of a Risk Management Committee (RMC), shall collectively be responsible for:

12.4.1. Ensuring that risk assessments are conducted on a regular basis in accordance with this Policy and related risk management frameworks, standards, guidelines, processes and procedures;

12.4.2. Reviewing reports of significant incidents, including the evaluation of the effectiveness of the response plans to prevent re-occurrence;

12.4.3. Ensuring adequate risk informed short term insurance cover and manage the organisation’s claims process;

12.4.4. Driving the embedment of a positive risk culture;

12.4.5. Providing risk reporting support to the line management, MANCO, Executive Management, ARC and the Board/Council;

12.4.6. Maintaining an acceptable risk profile for the organisation.

12.4.7. Managing risks that could impact negatively on the realization of the strategic objectives;

12.4.8. Analysing, assessment and prioritization of risks identified;

12.4.9. Implementation of risk mitigation strategies that would help manage business risks to acceptable levels;

12.4.10. Reporting to the Council, ARC and Manco on a quarterly basis on the state of risks in the organisation;

12.4.11. Developing operational risk registers for their different departments and report to Manco on a monthly basis, the implementation of risk treatment plans;

12.4.12. Entrenching a culture of risk management in the organisation as a whole but also at a departmental level; and

12.4.13. Assess, source and petition ad-hoc and independent external assurance services to audit the effectiveness of the system of risk management in the organisation.

12.5. Employees

12.5.1. Employees are responsible for managing risk(s) within their departments and in their areas of responsibility; and

12.5.2. Monitoring and reporting of risks to Head of Departments and respective risk owners.

12.6. Internal Audit (IA)

The role of IA is to provide an independent and objective assurance on the adequacy and effectiveness of risk management and the internal control environment, as well as provide recommendations for improvement in areas of weakness.

The IA would collaborate with the Risk Management Committee and/or the Risk Management Officer to develop a combined assurance model that incorporates and optimises all assurance services and functions, to enable an effective control environment and support the integrity of information used for internal decision-making by management. This would also ensure a risk-based audit plan to ensure that adequate attention is provided in relation to significant risks.

13. POLICY STATEMENTS

13.1. General

This policy would be reviewed every three years from the Effective Date, or when the need arises. This policy would be operationalised through the implementation of the ERM Framework which provides structural processes, standards and procedures of risk management in the organisation.

The NFVF regards the risk management as an integral part of the NFVF's governance and accountability arrangements, performance management, planning and processes of reporting.

Effective risk management must:

- Feature in day-to-day decision-making at operational, management, strategic planning and execution levels;
- Ensure commitment by all in identifying, analysing, evaluating and mitigating exposures that may impact on the NFVF achieving its objectives;
- Provide a commitment to training and knowledge development in the area of risk management, ensuring that all staff particularly those with management and decision-making responsibilities obtain sound understanding of the principles of risk management; and
- Provide a sound commitment to monitor performance whilst improving the risk culture and maturity of the NFVF.

13.2. Risk Owners and Risk Champions

Risk Owners are responsible for the management and control of all aspects of the risks assigned to them, including implementation of risk response actions to address threats and maximise opportunities.

The responsibility for implementation of risk response actions may be delegated to a named individual, the Risk Champion, who support and take direction from the Risk Owner.

13.3. Approach to Integrated Risk Management

The integration of risk management into business process shall be supported by the NFVF philosophy and culture that encourages everyone to manage risks and be risk cognisant in the performance of day-to-day activities. Effective risk management cannot be practiced in isolation but needs to be built into existing decision-making structures and processes. As risk management is an essential component of good governance, integrating the risk management function into existing strategic management and operational processes would ensure that it is an integral part of day-to-day activities.

In addition, risk management and internal controls would be incorporated in the performance management system of the NFVF to ensure that all employees take accountability and are measured accordingly as part of inculcating ERM as part of the organisational culture.

Risk is inherent in all the NFVF's activities. The NFVF's approach to risk management must include the following essential characteristics:

- Conducted in an integrated and structured manner;
- Forms an integral part of the NFVF's strategic management process and planning and budget cycle;
- Always supports the NFVF's vision, mission, strategies, goals and objectives;
- Embedded in all business processes, including project and contract management;
- Forms part of every Line manager's (risk owner) area of responsibility and is included in their job description and is part of their KPI's and performance management; and
- Risk treatment strategies would always be implemented on a cost-benefit approach.

13.4. Risk Philosophy

The philosophy of the NFVF is to recognise that risk management is an essential component of good corporate governance and as such integral to sound business principles and practices. The NFVF embraces risk management for the contribution it makes to achieving the NFVF's strategies and its mandate. The Key Risk Indicators (KRI's) and KPI's management (strategic and operational) are developed, maintained, monitored and updated regularly and submitted to the Management Committee, Audit and Risk Committee and the Council in the form of Risk Registers and reports.

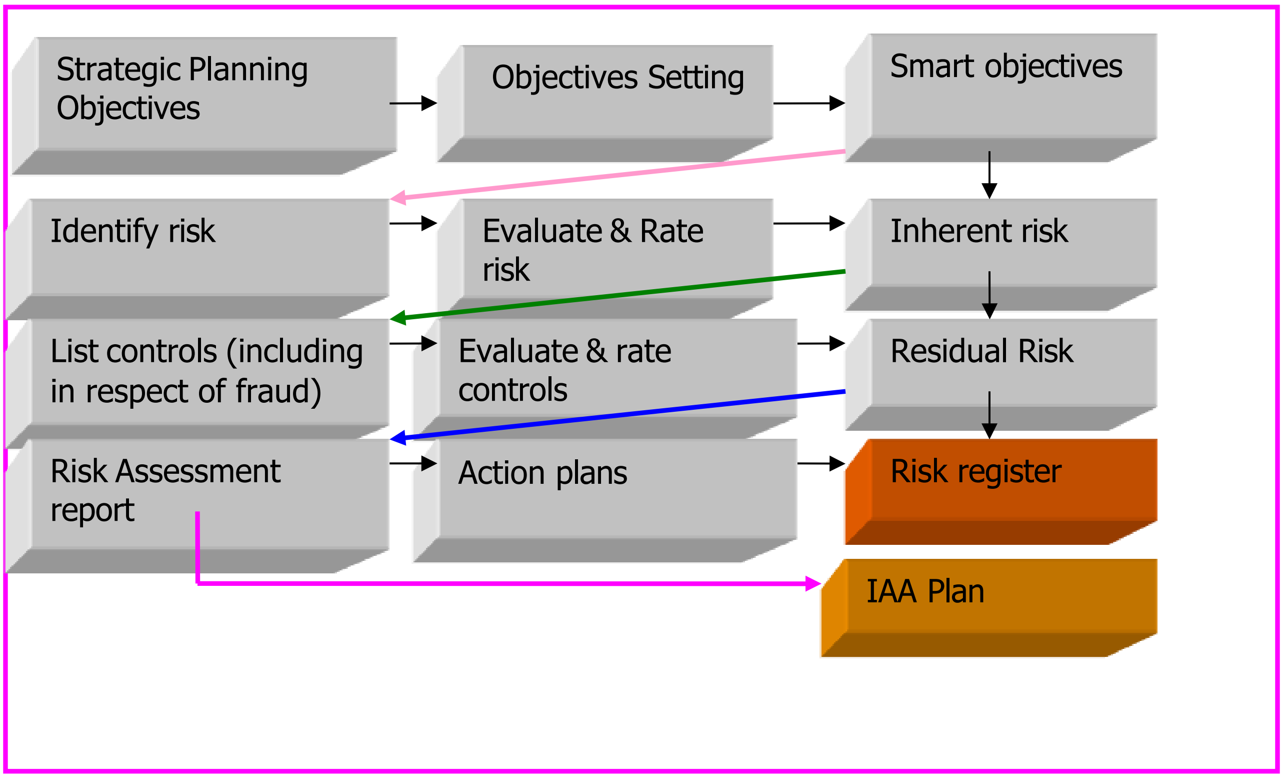
13.5. Risk Management Framework

An important element of risk management is the framework within which it operates as it provides the foundations and organisational arrangements within which risk management operates. This framework assists the NFVF community to manage risks in an efficient and effective manner through the application of a structured risk management approach and process. The risk management framework is guided by the NFVF's risk management philosophy and operates within the specific NFVF's organisational culture and integrated into the strategic planning process and business processes of the NFVF. Regular communication of the Risk Management Policy, processes and guidelines is essential. Risk management requires a planned and systematic approach to the identification, assessment and mitigation of the risks that could hinder the achievement of the NFVF's strategic objectives.

The NFVF's approach allocates responsibility for risk management and establishes a framework within which risks are identified and evaluated so that an appropriate response can be determined and effected. Risk management is undertaken as an integral part of strategic and operational management. Strategic and operational plans would include an assessment of the risks and mitigating actions associated with each objective, which are reviewed regularly. Risks must be identified and assessed as part of the business case for all new schemes, investments and projects. Risk Registers form the basis for action plans designed to address weaknesses in controls identified and mitigate risks where this is considered to be necessary.

13.6. The Risk Management Process

The risk management process describes the process that should be followed. It requires that a context be established, risks to be identified, analysed, assessed and risk treatment strategies designed. Enterprise Risk Management should be performed at the NFVF strategic and operational level. The diagram below depicts how ERM would be rolled-out in the NFVF (high-level):



The overall flow of the Enterprise Risk Management process would determine:

- A clear and unambiguous understanding of the NFVF's strategies, goals and objectives;
- Environmental scans that keeps the institution updated on its operating environment;
- A risk identification exercise for the year ahead;
- Evaluation of identified risks using risk assessments (matrix);

- Manage risks through application of risk management techniques;
- Record and monitor risks using Risk Registers and applicable governance tools;
- Assigning responsibility for risks to appropriate individuals in line with their roles; and
- Ongoing reporting of the risk profile of the NFVF.

13.7. Strategic Planning

This forms the basis of the risk management process. The risk management process shall commence in the strategic planning activities at the outset of each year led by the NFVF Council. Such strategic planning in respect of risk would give direction and set smart objectives from which risks are identified and mitigated by Senior Management led by CEO to ensure the achievement of the set objectives.

13.8. Risk Identification

The NFVF is operating within a dynamic and political environment which is constantly changing. It is, therefore, prudent for management to consider risk identification as ongoing and continuous.

13.9. Risk Rating and Classification

Risk would be rated in terms of the Likelihood of occurrence and the Impact/Consequence should it happen. The following table of Absolute risk ranking i.e., Risk Impact and Consequences for programmes is relied on for rating risk:

Impact	**Rating**
Catastrophic	5
Major	4
Medium	3
Low	2
Insignificant	1

Likelihood	**Rating**
Certain	5
Almost certain	4
Likely	3
Rare	2
Unlikely	1

Severity	**Threshold**
High	17-25
Medium	9-16
Low	1-8

Definitions of Impact (consequence) & Likelihood (Frequency, Probability)

Score	**Rating**	**Description**	**Rating**	**Description**
5	Catastrophic	Loss of ability to sustain ongoing operations. A situation that would cause a stand-alone business to cease operation	5	The risk is almost certain to occur more than once within the next 12 months. (Probability = 100% p.a.)
4	Major	Significant impact on achievement of strategic objectives and targets relating to organisational plan.	4	The risk is almost certain to occur once within the next 12 months. (Probability = 50 – 100% p.a.)
3	Moderate	Disruption of normal operations with a limited effect on achievement of strategic objectives or targets relating to Organisational plan.	3	The risk could occur at least once in the next 2 – 10 years. (Probability = 10 – 50% p.a.)
2	Minor	No material impact on achievement of the organisation's strategy or objectives.	2	The risk could occur at least once in the next 10 - 100 years. Probability of
1	insignificant	Negligible impact.	1	The risk would probably not occur, i.e., less than once in 100 years. (Probability = 0 – 1% p.a.)

From 13 to 25	High
From 8 to 12	Medium
From 1 to 7	Low

13.10. Managing Risk

Management, assisted by Risk management Committee and/or or the Risk Management Officer, would analyse major inherent risks and implement effective mitigating strategies to reduce these to acceptable levels. These could include, but are not limited to:

- Internal controls and procedures and the implementation of relevant policies;
- Outsourcing of key processes and systems;
- Insurance and other forms of risk transfer;
- Monitoring of risk, and
- Setting strategy.

13.10.1. **Listing of Controls**

Where there are already controls in existence, such controls would be listed and rated using the same criteria as applicable to risk rating (estimates). Management would use their professional judgment

(assessment) to rate the controls between 1 and 25. When the control rating is subtracted from the risk rating, the remaining value constitutes the residual risk. This exercise is called the control assessment process.

The output of both risk assessment and the control assessment forms the Risk Assessment Report. The RMC working with the Risk Management Officer establishes the Risk Registers, and the Internal Audit would use these registers in developing the three-year internal audit rolling plan and an annual audit plan.

The Risk Registers should, at minimum, include:

a) The risks identified;

b) The risks root-causes;

c) The risks likelihood and impact;

d) The risks current controls;

e) The risks rating for inherent and residual;

f) The appropriate official and sub-group responsible for the monitoring of the risk;

g) The action plan to address the risks; and

h) The expected implementation dates.

When identified risks have been addressed and mitigated, they should be escalated to the low residual risk level to be prioritised by the IA for assurance as agreed with management.

Risk registers would be monitored by the RMC and/or the Risk Management Officer on a monthly or quarterly basis as agreed with Heads of Departments/ risk owners, who would compile reports from their registers to form part of the RMC, audit committee and plenary reports.

13.10.2. Risk Management Strategies

Risk Exposure falls into two types, risk control and risk financing. Risk control techniques prevent or reduce the frequency or severity of losses. Risk financing techniques, e.g., retention, insurance, and non-insurance transfers of financial obligations, pay for losses that occur despite the best risk control efforts. Risk control strategies may be categorised as follows:

13.10.2.1. **Risk Avoidance** – this approach simply means that the NFVF identifies a risk and does not undertake an activity, action or programme that would produce an undesirable loss exposure.

13.10.2.2. **Risk Prevention** – this technique focuses on reducing the frequency of losses e.g., frequent inspections of an office for overload electrical outlets are a fire prevention technique.

13.10.2.3. **Risk Reduction** – based on the assumption that “it is not feasible” or “it is impossible” to eliminate or prevent an exposure, this method serves to minimise occurrence, e.g., the use of a sprinkler system would reduce the amount of damage from the fire.

13.10.2.4. **Segregation of Exposures** – with this approach, the NFVF’s activities and programmes may be either separated, diversified, or duplicated so a single risk would not cause a catastrophic loss to all, e.g., storing supplies in several different locations instead of one large warehouse, diversifying cash assets, and backing up all computer data and storing off-site.

13.10.2.5. **Risk Transfer** – transferring, normally through a contract, the financial and or legal liabilities associated with an identified risk to an outside organisation e.g., a building lease, as opposed to ownership of a building, transfers certain risk exposures from the lessee to the lessor, or the owner

13.10.2.6. **Risk Tolerance** – these are risk levels the NFVF is willing to live with/ accept. This relates to the set risk appetite. Resources would be used to address risks for which the ratings are higher than 10 using any of the above highlighted strategies. When all risks identified are reduced to the acceptable level, the NFVF may reset the risk appetitive until the tolerance is zero, and this means that it would treat every risk identified. Refer to the risk appetite and tolerance framework for more details on this aspect.

14. REPORTING AND MONITORING

14.1.1. Significant NFVF risks are recorded in the strategic risk register, along with their potential impact and likelihood on the business and management’s mitigating actions/treatment plans are documented. Flowing from the strategic risk register, departments are required to develop operational risk registers to identify risks that they may be subject to at a department level, evaluate their impact on the business and document the risk management procedures and treatment plans in place. This risk information is reported at an organisational level where the risks are evaluated and the NFVF strategic risk register updated as required.

14.1.2. Reporting and monitoring internally would be bottom-up: management will periodically report its agreed risk registers with the required information to MANCO. The NFVF consolidated Strategic Risk Register including summary update on Operational Risks progress would form the basis of reporting to ARC on a quarterly basis. After ARC review, the NFVF consolidated Strategic Risk Register would be a standing agenda item at Council on a quarterly basis. Changes to risk information, including tolerance levels, would be made to the NFVF strategic risk register and communicated to the departments for updating of their registers.

15. CONCLUSION

We accept that risk management, including risk reporting, is a continuous process and would be improved as opportunities arise; however, risk assessments should be re-performed for the key risks in response to significant environmental and/or organisational changes (risk factors), at least once a year, to ascertain the shift in the magnitude of risk and the need for further management action as a result thereof – *as per National Treasury Public Sector Risk Management Framework.*

NFVF RISK APPETITE AND TOLERANCE FRAMEWORK

MARCH 2022

Table Of Contents

MARCH 2022

1. PURPOSE

2. BACKGROUND

3. OBJECTIVE

4. APPLICATION OF THE RISK APPETITE

5. DETERMINING THE RISK APPETITE

6. NFVF'S RISK APPETITE

7. ROLES AND RESPONSIBILITIES

1. PURPOSE

The purpose of this document is to communicate the Risk Appetite and Tolerance Framework of the National Film and Video Foundation (NFVF) as revised periodically and the process and procedures that shall be pursued to implement the framework.

2. BACKGROUND

The King Code on Corporate Governance prescribes that the board of an organisation shall determine the levels of risk appetite and risk tolerance applicable to such an organisation.

The Council remains ultimately accountable for appropriateness of the risk management system, including:

- Accountability for formulating clear overall risk appetite statement which is aligned with NFVF's strategy;
- Ensuring suitability and effectiveness and proportionality of the risk management system; and
- Approving the Risk Management Framework.

The Risk Appetite Framework facilitates the determination, review and oversight of risk appetite. It acts as a bridge between the organisation's strategy and its Risk Management Framework.

The risk appetite should be updated periodically in line with the changes to the organisational strategy, *(and vice versa, as neither the strategy not the appetite should be developed in isolation from the other but rather as part of a unified process)* and should also evolve in line with the development of its risk management framework.

3. OBJECTIVE

NFVF's risk management systems and procedures are reviewed and refined on an ongoing basis in order to comply, in substance, with what the organisation identifies as the relevant market standards, recommendations and best practices.

The principle also applies to NFVF's risk appetite framework, which seeks to achieve the following:

- To provide the basis for more responsive strategic decision making;
- To increase understanding of NFVF's material risk exposures and raise awareness across the organisation;
- To positively impact the defined risk maturity;
- To support the Council and Executive Management in planning, formulating and executing

strategic business decisions to achieve the set strategic objectives;

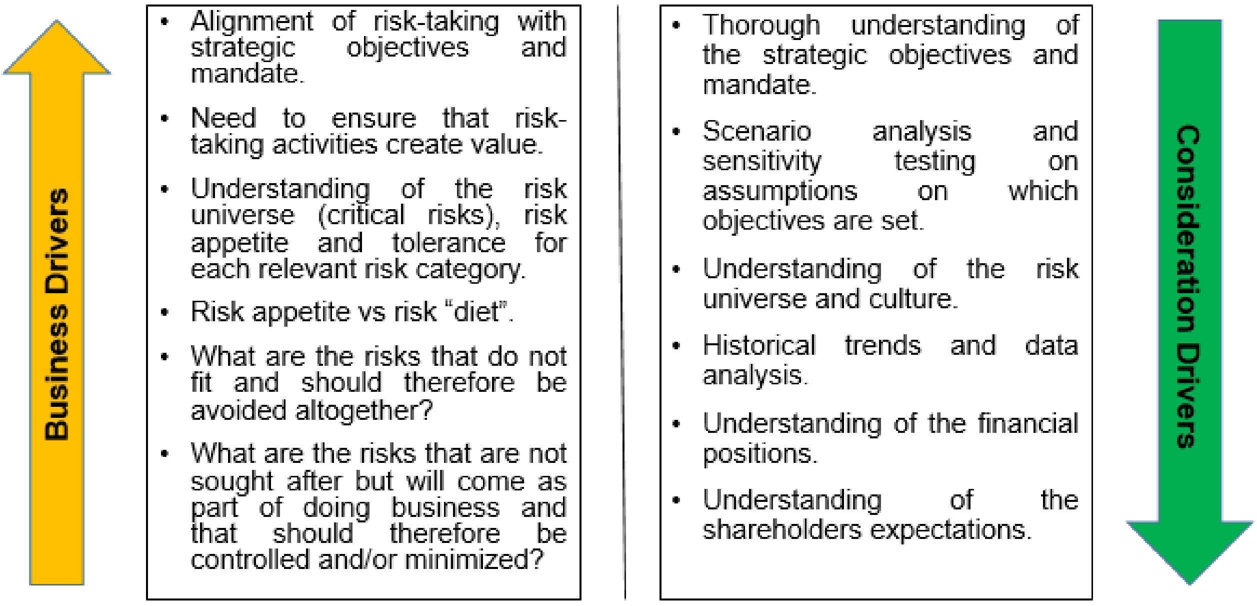
- To provide means for the Council and Executive Management to engage in discussions on risk-taking, risk management and business strategy and their interlinkages; and
- To provide tools for the Council and Executive Management to continuously monitor and align the NFVF's actual risk profile with the risk appetite.

4. APPLICATION OF THE RISK APPETITE

In line with the King Code principles, NFVF has adopted an approach of becoming a "Risk Intelligent Organisation". This approach entails viewing risk management as an opportunity that enables NFVF to see what is coming next, accurately predict and take advantage of future trends.

As such, the NFVF is committed to taking calculated and reasonable risks to generate the reward or return envisaged by its strategy. The measures intended by this Framework should be an input to the strategic and operational decisions taken and link risk-taking (based on comprehensive and forward-looking risk-based information) to the support and evaluation of sustainable strategic outcomes.

4.1 Drivers of Risk Appetite



- Alignment of risk-taking with strategic objectives and mandate.
- Need to ensure that risk-taking activities create value.
- Understanding of the risk universe (critical risks), risk appetite and tolerance for each relevant risk category.
- Risk appetite vs risk "diet".
- What are the risks that do not fit and should therefore be avoided altogether?
- What are the risks that are not sought after but will come as part of doing business and that should therefore be controlled and/or minimized?

- Thorough understanding of the strategic objectives and mandate.
- Scenario analysis and sensitivity testing on assumptions on which objectives are set.
- Understanding of the risk universe and culture.
- Historical trends and data analysis.
- Understanding of the financial positions.
- Understanding of the shareholders expectations.

4.2 Definitions

The ISO 31000:2018 standard for risk management includes a set of definitions extracted from a guide for risk management terminology, the ISO Guide 73.

Both these documents define risk appetite as *the amount and type of risk that an organisation is prepared to pursue, retain or take.* The objective of risk appetite is to indicate the point at which a risk becomes serious enough to the organisation to start committing time and effort into the management of the risk.

Risk tolerance, on the other hand, although sometimes incorrectly used interchangeably with risk appetite, is defined in ISO 31000 as *an organisation's or stakeholders readiness to bear the risk after risk treatment in order to achieve its objectives.*

Risk Bearing Capacity (RBC) *is the maximum amount of risk that an organisation is able to accept in line with its mission/values/strategic goals, without exposing it to the point where its survival is under threat and faces financial constraints.* The RBC for NFVF may be characterised by the following financial constraints being encountered:

- Inability to fill critical and key vacant posts;
- Inability to pay suppliers on time;
- Requesting additional funding "bail out" from the shareholder and/or National Treasury;
- A continuous reduction in Other Income, i.e., inability to perform additional activities and related services that generates Other Income; and
- Inability to undertake critical maintenance.

4.3 Where Is Risk Appetite Applied?

The risk appetite if applied on the following:

- Annual Performance Plan target – to ensure that the targets are with risk appetite;
- Changes in the risk profile to check if they are not outside / above the risk appetite;
- Risk mitigation plans – to ensure that mitigations that are put in place to manage the risks are within the risk appetite;
- Tracking and monitoring of Key Risk Indicators (KRIs) – to indicate when risks are outside the risk appetite;
- Emerging risks – to highlight those emerging risks which should they occur will be above the risk appetite;
- Risk events / near misses / materialised risks – to highlight those risks which have materialised and whose impact is above the risk appetite; and
- Accepted risks – to ensure that the risks that are accepted are within the risk appetite.

5. DETERMINING THE RISK APPETITE

Risk appetite represents willingness to undertake risk in order to gain reward and has a direct link to strategy and growth ambitions. The true test of a successful risk appetite approach is to ensure that risk appetite and strategy are aligned and making sure that the organisation is not operating beyond its capacity to bear risks.

Setting the risk appetite and tolerance will assist in improving the Council’s risk oversight and communicates the Council’s risk-taking expectations to management with regards to business and strategic decisions.

This should encourage conscious and effective risk-taking by management and improve the allocation of resources realising the best possible rewards commensurate with risk. Risk appetite is used to set up boundaries for risk taking and plays a crucial role in corporate governance and should ensure that management:

- Does not make decisions that expose the NFVF to an excessive amount of risk by investing in risky activities or reducing expenditure on risk control; and
- Does not male conservative decisions that expose the NFVF to too little risk (opportunity) and hence generating an insufficient return on its activities and effort.

The NFVF’s risk appetite and tolerance levels have been linked to and derived from the organisation’s strategic thrusts, long-term and short-term objectives.

5.1 Considerations

5.1.1 Strategic Objectives

In determining risk appetite and tolerance for any specific issue, the evaluation of such issue must consider the potential influence thereof on the strategic objectives, in other words, will it have a positive, negative or no influence at all.

5.1.2 Stakeholder Expectations

In determining the risk appetite and tolerance for a specific issue, the expectations of all key stakeholders in relation to such issues must be considered and evaluated. Stakeholders should be determined at the time of reaching agreement on the risk appetite and tolerance levels including for example:

- Department of Arts, Sports and Culture (DSAC);
- Council;

- Management and employees;
- Regulatory or statutory bodies;
- General public / communities; and
- Service providers.

5.1.3 Financial Position

- NFVF's financial / balance sheet position, together with the risk transfer mechanisms in place, must be taken into account to determine financial levels of risk appetite and tolerance.
- The values at which certain events and specifically losses can be accommodated within the stated financial budgets and financial performance parameters are valuable in determining the suggested risk appetite position.
- The financial values at risk, where serious and material compromise of the NFVF's going concern would be experienced, are used to assist in defining the risk tolerance of specific risks, events or loss scenarios.

5.1.4 NFVF's Delegation of Authority

The Delegation of Authority, together with the financial information and insurance/risk transfer information are also important considerations when determining risk appetite and tolerance positions of certain risks.

5.1.5 Risk Impacts

- The impacts / consequences of all key risks associated with the issue in questions should be evaluated according to the NFVF's Impact Rating Scale.
- The risk appetite debate should take place with the Delegation of Authority, and the answer to the question *"Does this fit within our risk appetite or not?"* will take place at a level commensurate with the risk implied in the issue under debate.
- The values at which certain events and specifically losses can be accommodated within the stated financial budgets and financial performance parameters are valuable in determining the suggested risk appetite position.
- The financial values at risk, where serious and material compromise of the NFVF's going concern would be experienced, are used to assist in defining the risk tolerance of specific risks, events or loss scenarios.

6. NFVF’S RISK APPETITE

The below appetite statements are not an exhaustive list of all material aspects of risk management in the organisation. A Risk Matrix alongside other crucial information are used as a baseline to determine the risk appetite level for each category. The risk appetite levels will be reviewed on an ongoing basis to align to the organisation’s mandate and compliance to the relevant regulatory and legislative requirements.

6.1 Overall Strategy

The organisation has a **moderate to high-risk** appetite in pursuit of its strategic objectives.

The organisation has a **low-risk** appetite for activities that are not aligned with its strategic direction.

6.2 Research, Development and Innovation

The organisation has a **high-risk** appetite for investment to grow its RD&I strengths through research partnerships and industry collaboration.

The organisation has a **zero-risk** appetite for research conduct that is unethical or non-compliant with legislation or that compromises quality.

6.3 Intellectual Property (IP)

The organisation has a **low-risk** appetite for any activity or event that threaten the security of the organisation's proprietary information and intellectual property rights.

6.4 Reputation and Brand

The organisation has a **zero-risk** appetite for activities that have the potential to tarnish its brand reputation and core values.

6.5 Fraud, Theft and Corruption

The organisation has a **zero-risk** appetite for corrupt and fraudulent activities, including theft.

6.6 Prejudice and Associated Compromising Behavior

The organisation has a **zero-risk** appetite for prejudice including but not limited to prejudice based on race, gender, religion and any associated or personal life choices and belief and associated harassment or exclusionary behavior.

6.7 Health, Safety and Environment

The organisation has a **zero-risk** appetite for activities that have an adverse impact to the health, safety and wellbeing of employees and visitors.

The organisation has a strong interest in protecting and preserving the environment, hence, accepts a **low-risk** appetite for activities that will significantly degrade the environment.

6.8 Regulatory and Statutory Compliance

The organisation has a **zero-risk** appetite for non-compliance to regulatory and statutory requirements.

6.9 Financial Sustainability

The organisation has a **zero-risk** appetite for irresponsible use of its resources and unnecessary liabilities.

The organisation has a **moderate to high-risk** appetite for being more commercially adept and explore avenues to diversify revenue streams through commercially viable arrangements and partnerships.

6.10 Information and Communication Technology (ICT)

The organisation has a **moderate to high-risk** appetite to invest in ICT infrastructure and systems that are in line with the strategic direction and enables the delivery of sustainable services to the organisation and key stakeholders.

The organisation has a **low-risk** appetite for ICT infrastructure and systems downtime/failures that compromise the sustainability and quality of services.

The organisation has a **zero-risk** appetite for information security breaches and incidents that will expose the organisation to unauthorised access to sensitive and confidential data/information, including exposure of private and personal information (POPIA).

6.11 Service Delivery

The organisation has a **low-risk** appetite for business interruptions on the operations that in turn impact negatively on service delivery to all its stakeholders.

7. ROLES AND RESPONSIBILITIES

7.1 Oversight

7.1.1 The NFVF Council

The Council is responsible for overseeing the complete spectrum of governance within NFVF. This responsibility includes:

- Approving NFVF’s Risk Appetite and Tolerance Framework and ensure it remains consistent with NFVF's strategy; and

- Hold the Chief Executive Officer (CEO) accountable for the integrity of the framework, including the timely identification, management and escalation of breaches in risk limits and of material exposures.

7.1.2 The Audit and Risk Committee (ARC)

In discharging its oversight responsibilities relating to the Risk Appetite and Tolerance Framework, ARC should:

- Ensure the Risk Appetite and Tolerance Framework is approved by the Council;
- Evaluate the effectiveness of the mitigating strategies implemented to address the material risks of NFVF (treatment action plans);
- Ensure ARC is informed of all changes to the risk management strategy, implementation plan, policy and framework;
- Review and monitor the effectiveness of risk control systems, the reliability and accuracy of risk management reporting and fraud prevention plan;
- Review any material findings and recommendations by assurance providers on the risk management system and monitor that appropriate action is instituted to address the identified weaknesses; and
- Provide guidance to the Head of Risk Management / to the person responsible for Risk Management and other relevant risk management stakeholders on how to manage risks within the risk appetite level.

7.2 Implementers

7.2.1 The CEO

- The CEO is ultimately responsible for risk management with the NFVF. The CEO is accountable to the Council regarding the effectiveness of the risk management process. By setting the tone at the top, the CEO promotes accountability, integrity and other factors that create a positive environment.
- The roles of the CEO relating to the risk appetite and tolerance include the following:
  - Establish am appropriate risk appetite and tolerance for the NFVF (in collaboration with the Risk Management function) which is consistent with the NFVF's strategy;
  - Be accountable, together with the Risk Management function for the integrity of risk management; and
  - Ensure that the risk appetite is appropriately translated into risk limits for strategic planning.

7.2.2 Management

- Management at all levels within NFVF owns the risks, thus in taking that ownership they are also accountable to the CEO for integrating the principles of risk management into their daily routines to enhance the achievement of their objectives;

- In discharging their high-level responsibilities relating to risk appetite, management:

  - Ensure alignment between the approved risk appetite and business planning;

  - Embed the risk appetite statement and risk limits into management's activities so as to embed prudent risk taking into NFVF's risk culture and day-to-day management of risk;

  - Establish and actively monitor adherence to approved risk limits;

  - Act in a timely manner to ensure effective management, and where necessary, mitigation of material risk exposures, in particular those that exceed or have the potential to exceed the approved risk appetite and/or risk limits; and

  - Escalate promptly breaches in risk limits and material risk exposures to the Risk Management function and senior management in a timely manner.

7.3 Support

7.3.1 Risk Management function / Person responsible for Risk Management

- Provides specialist expertise in providing a comprehensive support service to ensure systematic, uniform and effective enterprise risk management;

- Develop am appropriate risk appetite for NFVF;

- Obtain ARC and Council approval of the developed risk appetite;

- Actively monitor NFVF's risk profile relative to its risk appetite, strategy and risk capacity;

- Establish a process for reporting on risk and on alignment (or otherwise) of risk appetite and risk profile with the NFVF's risk culture;

- Ensure the integrity of risk management techniques and information systems that are sued to monitor NFVF's risk profile relative to its risk exposure;

- Independently monitor NFVF's risk limits aggregate risk profile to ensure they remain consistent with NFVF's risk appetite; and

- Escalate promptly to the CEO, ARC and Council any material risk limit breach that places NFVF at risk of exceeding its risk appetite, and in particular, of putting in danger its financial sustainability.

NFVF ENTERPRISE RISK MANAGEMENT FRAMEWORK

NOVEMBER 2020

Table of Contents

1. INTRODUCTION

2. DEFINITIONS

3. LEGAL MANDATE FOR ERM

4. CORPORATE GOVERNANCE PRINCIPLES

5. ENTERPRISE RISK MANAGEMENT STANDARDS

6. ERM ROLES AND RESPONSIBILITIES

7. COMPONENTS OF THE ENTERPRISE RISK MANAGEMENT PROCESS

8. PROJECT RISK MANAGEMENT

9. ERM ENHANCEMENT AND ENTRENCHMENT PLAN

10. COMBINED ASSURANCE PLAN

Annexure A: Impact Parameter

Annexure B: Likelihood Parameter

Annexure C: Control Effectiveness Rating

Annexure D: Risk Rating

Annexure E: Risk Escalation Matrix

1. INTRODUCTION

The National Film and Video Foundation (NFVF) is a Schedule 3A Public Entity in terms of the PFMA. The NFVF is governed by the National Film and Video Foundation Act 73 of 1997 as amended by the Cultural Laws Amendment Act 36 of 2001.

The National Film and Video Foundation (NFVF) is committed to a process of enterprise risk management that is aligned to the Public-Sector Risk Management Framework as well as best practices.

The Enterprise Risk Management Framework specifically addresses the structures, processes and standards implemented to manage risks on an enterprise-wide basis in a consistent manner. The standards further address the specific responsibilities and accountabilities for the Enterprise Risk Management process and the reporting of risks and incidences at various levels within the NFVF. As the field of Enterprise Risk Management is dynamic, this policy and framework document is expected to change from time to time.

Current trends in good corporate governance have given special prominence to the process of Enterprise Risk Management and reputable businesses are required to demonstrate that they comply with expected Enterprise Risk Management standards. This means that NFVF must ensure that the process of Enterprise Risk Management receives special attention throughout the organisation and that all levels of management know, understand and comply with the framework document.

The purpose of the Enterprise Risk Management Framework is to:

- Advance the development and implementation of modern management practices and to support innovation throughout NFVF;
- Contribute to building a risk-smart workforce and environment that allows for innovation and responsible risk-taking while ensuring legitimate precautions are taken to protect stakeholders, the public interest, maintain public trust, and ensure due diligence;
- Provide a comprehensive approach to better integrated Enterprise Risk Management into strategic decision-making; and
- Provide guidance for the Council, management and staff when overseeing or implementing the development of processes, systems and techniques for managing risk, which are appropriate to the context of the organisation.

2. DEFINITIONS

Risk

The Institute of Internal Auditors defines risk as "…*the uncertainty of an event occurring that could have an impact on the achievement of objectives. Risk is measured in terms of consequences and likelihood."*

Enterprise Risk Management

In reference to the COSO framework (The Committee of Sponsoring Organisations of the Tredway Commission), "*Enterprise Risk Management is a continuous, proactive and systematic process, effected by the Council of Directors, Executive Management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and* manage *risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity's objectives."*

Other definitions

TERM	DESCRIPTION
Audit and Risk Committee	An independent committee constituted to review the control, governance and Enterprise Risk Management within the organisation.
Consequence	An outcome of an event/ risk, whether positive or negative.
Contributory (risk) factor	Any threat or event which contributes to the risk materialising or has the potential to contribute to the risk materialising.
Control effectiveness	A measure of how well management perceives the design and functionality of controls for managing risk.
Employee/s	Permanent employees of the NFVF, contract employees of the NFVF, and/or programme employees of the NFVF.
Enterprise Risk Management	Integrated process of Enterprise Risk Management that allows the organisation to identify, prioritise, and effectively manage its material risks.
Inherent risk	The combined level of risk likelihood and risk impact before the consideration of any effect of controls. *Alternatively,* the exposure

TERM	DESCRIPTION
	arising from risk factors in the absence of deliberate management intervention(s) to exercise control over such risk factors.
Internal Audit	An independent, objective assurance and consulting activity designed to add value and improve NFVF's operations. It helps NFVF to accomplish its objectives by bringing a systematic, disciplined approach to evaluating and improving the effectiveness of Enterprise Risk Management, control, and governance processes.
Key risk indicators	Metrics used by management to provide an early signal of increasing risk exposure or emerging risk.
Residual risk	The level of risk that remains after risk mitigation measures have been implemented.
Risk acceptance	An informed decision by management to accept the likelihood and impact of a particular risk thus not implementing any further risk mitigation measures.
Risk analysis	Systematic use of information to identify sources of risk and to estimate the level of risk.
Risk appetite	The level of risk that the organisation is prepared to accept in pursuit of value.
Risk exposure	Extent to which the organisation is subject to a risk event.
Risk assessment	Overall process of risk identification, risk quantification and risk evaluation in order to identify potential opportunities or minimise loss.
Risk avoidance	Decision not to become involved in, or action to withdraw from a risk situation.
Risk Champion	A person who by virtue of his/her expertise or authority champions a particular aspect of the Enterprise Risk Management process, but who is not necessarily the risk owner.

TERM	DESCRIPTION
Risk identification	Process of recognising and describing the risks.
Risk owner	The person with the accountability and authority to manage a particular risk.
Enterprise Risk Management	Enterprise Risk Management is the identification and evaluation of actual and potential risk areas as they pertain to the organisation, followed by a process of, avoiding, sharing/ transferring, accepting and mitigating of each risk, or a response that is a combination.
Enterprise Risk Management policy	Statement of overall intentions and direction of the organisation related to Enterprise Risk Management.
Enterprise Risk Management strategy and plan	A document setting out the planned Enterprise Risk Management activities to be conducted during the year as well as the initiatives aimed at improving the maturity of the Enterprise Risk Management process.
Risk maturity assessment	An assessment of the level of sophistication of the organisation's Enterprise Risk Management process and structures.
Risk mitigation	Management action to reduce the likelihood of a particular risk from materialising, and/or the limitation of the negative consequences of any risk event.
Risk profile	The relevant risks and the applicable priority thereto. This will normally be presented as a listing of risks with relevant prioritisation/ rating.
Risk register	A formal listing of risks identified, together with the results of the risk analysis and evaluation together with details of risk treatment strategies, risk controls in place and risk action plans.
Risk response/ treatment	Process of selection and implementation of measures to manage risk.

TERM	DESCRIPTION
	Risk response measures can include avoidance, sharing/transfer, acceptance and mitigation.
Risk tolerance	The acceptable level of variances arising out of risk relative to the achievement of objectives.
Risk transfer	Sharing with another party the burden of loss or benefit of gain, for a risk. Risk transfer can be carried out through insurance or other agreements.

3. LEGAL MANDATE FOR ERM

3.1. Section 51(a) (i) of PFMA

Section 51(a) (i) states that “The accounting authority must ensure that the public entity has and maintains effective, efficient and transparent systems of financial, Enterprise Risk Management and internal control...”

3.2. Treasury Regulations

Section 27.2.1 of the Treasury regulations states the following:

“The accounting authority must facilitate a risk assessment to determine material risks to which the entity may be exposed and to evaluate the strategy to manage these risks. The strategy must be used to direct the internal audit effort and priority.”

4. CORPORATE GOVERNANCE PRINCIPLES

The following recommendations are made in Section 3 of the King IV Report on Governance Principles for South Africa and are adjusted for NFVF as follows:

a. The Board is responsible for the total process of Enterprise Risk Management, as well as forming its own opinion on the effectiveness of the process.

b. The Audit and Risk Committee should consider the risk strategy and policy and should monitor the process at operational level and the reporting thereon.

c. Management is accountable to the Board for designing, implementing and monitoring the process of Enterprise Risk Management and integrating it into the day-to-day activities of the department.

d. Enterprise Risk Management constitutes an inherent operational function and responsibility.

e. Risks should be assessed on an on-going basis and control activities should be designed to respond to risks throughout the company. Pertinent information arising from the risk assessment, and relating to control activities should be identified, captured and communicated in a form and timeframe that enables employees to carry out their responsibilities properly. These controls should be monitored by both line management and assurance providers.

f. A systematic, documented assessment of the processes and outcomes surrounding key risks should be undertaken at least annually.

g. The institution should develop a system of Enterprise Risk Management and internal control that builds robust business operations. The systems should demonstrate that the key risks are being managed in a way that enhances shareowners' and relevant stakeholders' interests.

5. ENTERPRISE RISK MANAGEMENT STANDARDS

The standards constitute the main tasks of the ERM process. These standards are non-negotiable. The Enterprise Risk Management Standards should be read in conjunction with section 3 - ERM roles and responsibilities.

Ref.	Standard	Responsibility	Frequency
Oversight Responsibilities:			
01	The Council will review Enterprise Risk Management progress at least quarterly.	Chairperson: Council	Quarterly
02	The Audit and Risk Committee will review Enterprise Risk Management progress at least quarterly.	Chairperson: ARC	Quarterly
Reporting Responsibilities:			
03	The Audit and Risk Committee will submit high-level Enterprise Risk Management reports to the Council on a quarterly basis.	Chairperson: ARC	Quarterly

04	Exco will submit Enterprise Risk Management reports to the Audit and Risk Committee on a quarterly basis. These reports will focus on the following: • The strategic risks; • Progress with implementing corrective actions per risk; • Any new and emerging risks, risk developments, including incidents.	ERM Manager / Coordinator	Quarterly
05	The ARC will submit its independent assessment on the management of risks and the Enterprise Risk Management process to the Council on a quarterly basis.	Chairperson: ARC	Quarterly
Risk Assessment Responsibilities:			
06	The Council will ensure that a complete review of the risks of the NFVF is done at least once a year.	Chairperson: Council	Annually
07	All projects shall have a formal Enterprise Risk Management plan which should be informed by a project risk assessment.	Heads of Departments	On-going
08	Operational risk assessments will be conducted at business unit level (operational) at least annually.	Heads of Departments	Annually
09	Fraud risk assessments will be conducted at least annually.	ERM Manager /Coordinator	Annually
10	Detailed technology risk assessments will be conducted at least annually.	Chief Financial Officer	Annually
11	Business unit heads will review the operational risk registers and update the registers' contents to reflect any changes without the need for formal reassessment of the risks.	Heads of Departments	Quarterly
Risk Mitigation Responsibilities:			
12	The Audit and Risk Committee will receive and consider management's report concerning the effectiveness of internal controls on a quarterly basis.	Chairperson: ARC	Quarterly
13	The Audit and Risk Committee will consider management reports regarding the performance of internal controls for those risks in the risk register which they are responsible for.	Chairperson: ARC	Quarterly

14	The risk register will contain action plans for improving risk controls and risk interventions. Progress in implementing these actions should be monitored.	ERM Manager / Coordinator	Monthly
Governance Responsibilities:			
15	Each risk will have a nominated owner, who will be responsible for the following: • Updating the risk information; • Providing assurance regarding the risk controls; • Coordinate the implementation of action plans for managing the risk; and • Reporting on any developments regarding the risk.	ERM Manager / Coordinator	Monthly
16	Internal Audit will use the outputs of risk assessments to compile the internal audit plan and will investigate the effectiveness of risk mitigating controls.	Internal Audit	Annually
17	The Audit and Risk Committee will facilitate a review of the effectiveness of the entity's Enterprise Risk Management processes.	Chairperson: ARC	Annually
18	A Business Continuity Plan will be developed, implemented and tested annually.	Chief Financial Officer	Annually
19	A fraud policy and prevention plan should be implemented and monitored.	ERM Manager / Coordinator	Quarterly

6. ERM ROLES AND RESPONSIBILITIES

6.1. Roles, responsibilities and governance

- All employees have some level of responsibility for ERM;
- The Council is ultimately responsible for ERM and should assume overall ownership;
- Exco is responsible for ensuring that ERM is effectively implemented and practiced;
- The Audit and Risk Committee provides important ERM oversight; and
- A number of external stakeholders often provide information useful in effecting ERM, but they are not responsible for the effectiveness of the ERM process.

6.2. Council

The Council is ultimately accountable for the total process and success of Enterprise Risk Management. It may elect to fulfil some of its functions through delegation to committees including the Chief Executive Officer and Management. Responsibilities for Enterprise Risk Management:

6.2.1 The Council is responsible for:

- the total process of Enterprise Risk Management, which includes a related system of internal control;
- for forming its own opinion on the effectiveness of the process;
- providing monitoring, guidance and direction in respect of Enterprise Risk Management;
- ascertaining the status of Enterprise Risk Management within the organisation by discussion with senior management and providing oversight with regard to Enterprise Risk Management;
- identifying and fully appreciating the risk issues affecting the ability of the organisation to achieve its strategic purpose and objectives;
- ensuring that appropriate systems are implemented to manage the identified risks, by measuring the risks in terms of impact and probability, together with proactively managing the mitigating actions to ensure that the organisation's assets and reputation are suitably protected;
- ensuring that the organisation's Enterprise Risk Management mechanisms provide it with an assessment of the most significant risks relative to strategy and objectives;
- considering input from, the Audit and Risk Committee , Exco, Internal Auditors, External Auditors and subject matter advisors regarding Enterprise Risk Management;

- utilising resources as needed to conduct special investigations and having open and unrestricted communications with internal auditors, external auditors and legal counsel; and
- for disclosures in the annual report regarding Enterprise Risk Management (ERM).

Each member of the Council must understand his/her accountability for Enterprise Risk Management within the NFVF. Although the Council may choose to delegate or nominate one member of the Council as the coordinator of Enterprise Risk Management reporting requirements, it must be clear that all members have accountability for Enterprise Risk Management.

6.2.2. Providing stakeholder assurance

In providing stakeholders with assurance that key risks are properly identified, assessed, mitigated and monitored the Council must:

- receive credible and accurate information regarding the Enterprise Risk Management processes of NFVF in order to give the necessary assurance to stakeholders. The reports must provide an evaluation of the performance of Enterprise Risk Management and internal control;
- ensure that the various processes of Enterprise Risk Management cover the entire spectrum of risks faced by NFVF; and
- provide stakeholders with the assurance that management has formal, effective and pro- active Enterprise Risk Management processes.

6.2.3. Maintenance of the ERM policy

It is appreciated that stakeholders need to understand the Council' standpoint on risk. The Council will therefore maintain the formal Enterprise Risk Management policy, which decrees NFVF's approach to risk. The policy can be used as a reference point in matters of dispute and uncertainty.

6.2.4. Defining risk appetite and tolerance levels

The Council will define the formal risk appetite and risk tolerance levels. Risk appetite and tolerance limits are vital because they determine and influence the decision-making processes. Risk appetite and tolerance levels are defined by the Council and are set in relation to stakeholder expectations. Limits may be expressed in a number of ways according to category of risk concerned. The establishment of risk appetite and tolerance limits shapes the exception reporting processes. Risk tolerance limits will be determined in accordance with the risk-taking propensity of the organisation and the organisational culture of risk acceptability. The outcomes of risk assessment processes often assist the Council in determining the risk appetite and tolerance limits.

6.2.5. Evaluation of the effectiveness of the Enterprise Risk Management process

The Council will assess the effectiveness of the NFVF's Enterprise Risk Management processes on an annual basis. The Council' evaluations will be ***formally recorded in the minutes of meetings***. The Council' evaluation of Enterprise Risk Management can be supplemented by an ***independent review*** to be performed by the Internal Auditors or other such nominated assurance provider.

Management must ensure that sufficient independence is maintained in conducting the annual review and that clear criteria for the evaluation have been established. Assurance of the processes surrounding key risks must be given.

6.2.6. Confirmation that the Enterprise Risk Management process is accurately aligned to the strategy and performance objectives

The Council will ensure that the Enterprise Risk Management processes address risk in a balanced way, giving due attention to all types of risk. The Council will evaluate whether appropriate resources are being applied to the management of the various categories of risk. The Council will evaluate whether Enterprise Risk Management processes are aligned to the strategic and performance objectives of NFVF. A balanced perspective of risk and Enterprise Risk Management is required in proportion to the weighting of potential risk impact across NFVF. The Council must ensure that a future-looking orientation is included in the consideration of risk.

6.3. Audit and Risk Committee

The Committee is an integral component of the Enterprise Risk Management process and specifically the Committee must **review**:

- the nature, role, responsibility and authority of the Enterprise Risk Management function within the organisation and outline the scope of Enterprise Risk Management work;
- the development and annual review of a policy and plan for Enterprise Risk Management;
- the implementation of the policy and framework for Enterprise Risk Management;
- recommendations to the Council concerning the levels of tolerance and appetite and monitor that risks are managed within the levels of tolerance and appetite as approved by the Council;

- that the Enterprise Risk Management framework is widely disseminated throughout the organisation and integrated in the day-to-day activities of the organisation;
- that risk assessments are performed on a continuous basis;
- that frameworks and methodologies are implemented to increase the possibility of anticipating unpredictable risks;
- that management considers and implements appropriate risk responses;
- that continuous risk monitoring by management takes place;
- the monitoring of external developments relating to the practice of corporate accountability and the reporting of specifically associated risk, including emerging risks and prospective impacts thereof;
- that the Exco together with the organisation's Legal Advisor review any legal matters that could have a significant risk and impact on the organisation's business; and
- the insurance coverage arrangements to ensure these are adequate.

Each member of the Audit and Risk Committee must understand his/her accountability for Enterprise Risk Management within the organisation. Although the Audit and Risk Committee may choose to nominate one member of the committee as the coordinator of Enterprise Risk Management reporting requirements, it is clear that all members have accountability for Enterprise Risk Management in the organisation.

6.4. The Chief Executive Officer

The Chief Executive Officer's responsibilities include ensuring that all components of Enterprise Risk Management are in place. The Chief Executive Officer fulfils this duty by:

- Providing leadership and direction to management and staff. The Chief Executive Officer shapes the values, principles and major operating policies that form the foundation of NFVF's Enterprise Risk Management processes; and
- Meeting periodically with HODs and Managers responsible for major business units and functional areas to review their responsibilities, including how they manage risk. The Chief Executive Officer must gain knowledge of risks inherent to the operations, risk responses and control improvements required and the status of efforts underway. To discharge this responsibility, the Chief Executive Officer must clearly define the information he/she needs.

The Chief Executive Officer is required to assess the organisation's Enterprise Risk Management capabilities and practices. One of the most important aspects of this responsibility is ensuring the presence of a positive internal environment for Enterprise Risk Management. The Chief Executive Officer sets the tone at the top that influences internal environmental factors of ERM.

6.5. Heads of Departments (HODs)

Business unit heads are accountable to Exco through the Chief Executive Officer for designing, implementing and monitoring the process of Enterprise Risk Management and integrating it into the day-to-day activities of NFVF.

More specifically HODs are responsible for:

- Deciding on the manner in which risk mitigation will be embedded into management processes;
- Creating a culture of Enterprise Risk Management within NFVF;
- Updating risk registers and providing Enterprise Risk Management reports to the Chief Audit Executive pertaining to risk and control;
- Identifying positive aspects of risk that could evolve into potential opportunities for NFVF by viewing risk as an opportunity, by applying the risk/ reward principle in all decisions impacting on NFVF;
- Taking responsibility for appropriate mitigation action and determining action dates;
- Utilising available resources to compile, develop and implement plans, procedures and controls within the framework of the Risk Policy of NFVF to effectively manage the risks within the organisation;
- Ensuring that adequate and cost-effective Enterprise Risk Management structures are in place;
- Identifying, evaluating and measuring risks and where possible quantifying and linking each identified risk to key risk indicators;
- Developing and implementing Enterprise Risk Management plans including:
    - actions to optimise risk/ reward profile, maximise reward with risk contained within the approved risk appetite and tolerance limits;
    - implementation of cost-effective preventative and contingent control measures; and
    - implementation of procedures to ensure adherence to legal and regulatory requirements.
- Monitoring of the Enterprise Risk Management processes on both a detailed and macro basis by evaluating changes, or potential changes to risk profiles;
- Implementing and maintaining adequate internal controls and monitoring the continued effectiveness thereof;
- Implementing those measures as recommended by the internal and external auditors, which, in their opinion, will enhance control at a reasonable cost; and
- Providing policies, frameworks, methodologies and tools to the business units and key functional areas for identification, assessment and management of risks.

6.6. Risk Champions

The Risk Champions are responsible for:

- Updating risk registers on behalf of the risk owner and liaising with Enterprise Risk Management Unit on risk related matters;
- Escalating instances where the Enterprise Risk Management efforts are stifled, such as when individuals try to block ERM initiatives;
- Providing guidance and support to manage “problematic” risks and risks of a transversal nature;
- Acts as a change agent in the ERM process by acting as trouble shooters that facilitate resolution of risk related problems; and
- In order to be an effective and efficient risk champion, should:

- Have a good understanding of risk concepts, principles and processes;
- Have good analytical skills to assist with the analysis of root causes to risk problems;
- Have leadership and motivational qualities; and
- Have good communication skills.

6.7. ERM Manager / Coordinator

The ERM Manager / Coordinator is responsible for:

- Deciding on a methodology and framework for Enterprise Risk Management;
- Performing reviews of the Enterprise Risk Management process to improve the existing process;
- Facilitating risk assessments;
- Developing systems to facilitate risk monitoring and risk improvement;
- Aligning the risk identification process with NFVF’s business objectives;
- Identifying relevant legal and regulatory compliance requirements;
- Compiling a consolidated risk register on an annual basis;
- Costing and quantifying actual non-compliance incidences and losses incurred and formally reporting thereon;
- Formally reviewing the occupational health, safety and environmental policies and practices;
- Consolidating all information pertaining to all risk related functions, processes and activities;
- Transferring the knowledge in respect of an effective and sustainable process of risk identification, quantification and monitoring to management;
- Recording the decisions regarding mitigation for every key risk facing NFVF in the risk register;
- Deciding upon central solutions for common risks and for risks where central facilities

are available;

- Implementing a formalised risk information system (as applicable);
- Ensuring that Enterprise Risk Management training is conducted at appropriate levels within the entity to inculcate an Enterprise Risk Management culture;
- Communicating the risk framework and methodology to all management levels and to employees;
- Ensuring that the necessary Enterprise Risk Management documentation is developed in respect of the Enterprise Risk Management process;
- Enabling Exco and the Audit and Risk Committee to fulfil their responsibilities with regards to Enterprise Risk Management; and
- Working with management to ensure business plans and budgets include risk identification and management.

6.8. Internal Audit

The role of Internal Audit in corporate governance is defined by the South African Institute of Chartered Accountants as follows: “To support the Council and Management in identifying and managing risks and thereby enabling them to manage the organisation effectively”. This is achieved by:

- Enhancing their understanding of Enterprise Risk Management and the underlying concepts;
- Assisting them to implement an effective Enterprise Risk Management process, and
- Providing objective feedback on the quality of organisational controls and performance.”

Internal Audit is responsible for:

- Providing assurance that management processes are adequate to identify and monitor significant risks;
- Using the outputs of risk assessments to direct internal audit plans;
- Providing on-going evaluation of the Enterprise Risk Management processes;
- Providing objective confirmations that the Council and Committees receive the right quality of assurance and reliable information from management regarding risk;
- Providing assurance regarding ERM processes from both a design and functional perspective;
- providing assurance regarding the effectiveness and efficiency of risk responses and related control activities; and
- Further providing assurance as to the completeness and accuracy of ERM reporting.

7. COMPONENTS OF THE ENTERPRISE RISK MANAGEMENT PROCESS

A holistic approach to Enterprise Risk Management is required. This entails a coordinated enterprise-wide approach in which all risks are considered for the entire organisation and its departments. This approach includes all role players, policies, protocols, methodologies, reporting requirements and deliverables interacting within the Enterprise Risk Management processes.

The implementation of Enterprise Risk Management is guided by the methodology outlined in this document. The methodology is aligned to the ERM ***COSO*** best practice as well as the King IV report on corporate governance. The methodology allows for a consistent approach to be applied throughout NFVF and facilitates the interaction, on Enterprise Risk Management matters.

Control Environment: Values, ethics, integrity and culture. (These are normally captured and re-affirmed in the Enterprise Risk Management policy).	
Objective Setting	Specific, Measurable, Attainable, Relevant and Time-bound.
Risk Identification	Identification of events that could affect achievement of objectives.
Risk Assessment	Rating identified risks to determine order of significance on likelihood and impact.
Control Strategy	Manage or avoid? How will risks be managed? By whom? What structures?
Risk Reporting	Build awareness and regular risk reporting upwards and downwards.
Control Activities	Assurance on risks to be given by management and the Council. Consider combined assurance.
Monitoring	Set and monitor key risk indicators to embed proactive risk response.
Enterprise Risk Management Strategy: To drive Enterprise Risk Management, a formal Enterprise Risk Management strategy should be formulated. Set objectives and consider risk improvement strategies.	

7.1. Control Environment

NFVF's control environment is the foundation of Enterprise Risk Management, providing discipline and structure. The control environment influences how strategy and objectives are established, NFVF activities are structured, and risks are identified, assessed and acted upon. It influences the design and functioning of control activities, information and communication systems, and monitoring activities.

The control environment comprises many elements, including NFVF's ethical values, competence and development of personnel, management's operating style and how it assigns authority and responsibility.

The Council is a critical part of the control environment and significantly influences other control environment elements. As part of the control environment, management establishes an Enterprise Risk Management philosophy, establishes NFVF's risk tolerance levels, inculcates a risk culture and integrates Enterprise Risk Management with related initiatives.

The control environment consists of ten different layers that should all be present and functioning. The ten layers are as follows:

- Enterprise Risk Management Philosophy;
- Risk tolerance;
- Risk culture;
- Council oversight;
- Integrity and values;
- Commitment to competence;
- Management's philosophy and operating Style;
- Organisational structure;
- Authority and responsibility; and
- HR policies and procedures.

The existing controls in place for identified risks must be documented. The term "control" should not be construed only as a financial term. It is now the commonly accepted term to describe any mitigating measure for any particular type of risk. Controls may take the form of financial mitigations such as hedges, insurance or securities. They may be managerial in nature such as compliance procedures, policies and levels of authority. Controls may be strategic in nature such as diversification and investment related. Controls may be legal such as contracts and indemnities.

7.2. Objective Setting

Objectives must exist before management can identify events potentially affecting their achievement. Enterprise Risk Management ensures that management has a process in place to both set objectives and align the objectives with NFVF's mission and vision and is consistent with NFVF's risk tolerance. The setting of these objectives is usually completed during the "Strategic planning and Budgetary process."

Having confirmed and clearly documented NFVF objectives, it is necessary to identify all the potential risks and threats relating to processes, assets and strategy. These are the possible problems and situations that may hinder the achievement of the objectives of the operation.

7.3. Risk Identification

During the phase of risk identification, management considers external and internal, as well as financial and non-financial factors that influence the entity's policy and management agenda. Identifying major trends and their variation over time is particularly relevant in providing early warnings.

Some external factors to be considered for potential risks include:

- Political: the influence of international governments and other governing bodies;
- Economic: international, national markets and globalizations;
- Social: major demographic and social trends; and
- Technological.

Events potentially either have a negative impact, a positive impact or both. Events that have a potentially negative impact represent risks, which require management's assessment and response. Accordingly, risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives.

Events with a potentially positive impact represent opportunities or offset the negative impact of risks. Those representing opportunities are channeled back to management's strategy or objective-setting processes, so that actions can be formulated to seize the opportunities, whereas events potentially offsetting the negative impact of risks are considered in management's risk assessment and response.

7.3.1. NFVF's Risk Assessment Methodology

NFVF's simple 5-step methodology for risk assessments is depicted as follows:

Objectives

Step 1:

Identify Objectives / Level of Objective

Risks

Step 2:

- Identify Risks preventing achievement of Objectives; and
- Identifying the potential root causes of risk events

Root causes are components of operational risk. Root causes are factors that contribute or increase the likelihood that risks could occur. In other words, risks are the potential negative consequence of a contributory factor. Root causes can be divided into the following major categories:

- People;
- Internal Environment;
- Processes;
- External Environment; and
- Systems.

Root causes have a many-to-one relationship with risk. Often more than one contributory factor could contribute to the same risk. Root causes also have a one-to-many relationship to risk meaning that one contributory factor could contribute to or increase the likelihood of more than one risk.

Step 3:

Inherent Risk Rating:

- Determine the likelihood and Impact

Controls

Step 4:

- Identify and Capture Controls; and
- Link Control to root

causes; Step 5:

- Determine control adequacy and rate residual risk.

Risk Response

Step 6:

- Capture Action Plans; and
- Assign Owner / Identify Implementation or due date.

7.4. Risk Assessment

Risk assessment allows an entity to consider how potential events might affect the achievement of objectives. Management assesses risk events by analysing their impact and likelihood using the **Impact (Annexure A) and Likelihood (Annexure B) parameters.**

7.4.1. Inherent risk rating

The inherent risk analysis is determined by calculating the **likelihood** (Probability of occurrence - **Annexure B***))* and **impact/consequence (Annexure A)** of a risk before consideration of existing controls. This analysis should consider the worst-case scenario and also consider the business environment in which the organisation operates. ***Inherent risk rating = impact x likelihood***

7.4.2. Residual Risk

Residual risk is determined by calculating the inherent risk rating after taking into account the adequacy and effectiveness of existing controls.

Based on the relative score of the residual risk exposure, **management will need to decide whether or not they are willing to accept the identified level of residual risk exposure.** If the residual risk is considered to be too high, then an action plan will then need to be developed outlining the identified action/s to reduce the risk to a level that is more acceptable to management and other stakeholders.

Management actions may include the re-examination of the control design and / or the business / quality objective identified earlier in the Enterprise Risk Management process. The action plans must clearly identify:

- The required action;
- The person responsible for implementing the action; and
- The expected date of implementation.

7.5. Risk Response Strategy

Management should recognize that some level of residual risk will always exist, not only because resources are limited, but also because of inherent future uncertainty and limitations inherent in all activities. Before making the determination on the basis of the above, risks should be plotted

on a heat-map **(Annexure D)** and risk escalation matrix **(Annexure E)** should be considered to determine the level of risk.

The usage of both the heat map and the risk escalation matrix ensures that the business directs its efforts not only to its highest risk exposures but also at those risks which are highly pervasive, or which have the ability to cripple the organisation, should they occur. Management identifies risk response strategies and consider:

- The effect on event likelihood and impact;
- Costs versus benefits; and
- Thereafter design and implement response options.

The consideration of risk responses is integral to Enterprise Risk Management and requires that management select a response that is expected to bring risk likelihood and impact within NFVF's risk tolerance level. The following risk response strategies should be considered by management:

- **T**ransfer e.g., through insurance cover;
- **T**olerate;
- **T**reat/ mitigate through rigorous management practices; or
- **T**erminate the risk by eliminating a process, a product, or a geographical zone.

After the control strategy decision, the current controls to manage the risk in question are identified. It is necessary to assess the adequacy of these controls. This is a measure of how well management perceives the identified controls to be designed to manage the risks. Management does this by determining the respective impact of the controls on either the inherent impact or likelihood of the specific risk.

7.6. Information and Communication

Pertinent information – both from internal and external sources, financial or non-financial – must be identified, captured and communicated in a form and timeframe that enable personnel to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across and up the organisation, as well as the exchange of relevant information with external parties, such as customers, suppliers, regulators and shareholders.

Information is needed at all levels of an entity to identify, assess and respond to risks, and to otherwise run the entity and achieve its objectives. An array of information is used, relevant to one or more objectives categories. Information comes from many sources – internal and external, and in quantitative and qualitative forms – and allows Enterprise Risk

Management responses to changing conditions in real time.

7.7. Control Activities

Control activities are the policies and procedures that help ensure Enterprise Risk Management strategies are properly executed. They occur throughout the entity, at all levels and in all functions. Internal control is an integral part of Enterprise Risk Management.

Control procedures relate to the actual policies and procedures in addition to the control environment that management has established to achieve NFVF's objectives. Policies and procedures help create boundaries and parameters to authority and responsibility, and also provide some scope of organisational precedent for action.

7.8. Monitoring

Enterprise Risk Management should be regularly monitored – a process that assesses both the presence and functioning of its components and the quality of their performance over time. Monitoring can be done in two ways: through on-going activities or separate evaluations. This will ensure that Enterprise Risk Management continues to be applied at all levels and across the entity.

7.8.1. Key risk indicators

Key risk indicators are intended to assist management to monitor risks. Key risk indicators have two focal points i.e., the inherent risk itself as well as losses, incidents and variances. Each key risk should have a key risk indicator to serve as a risk warning mechanism.

Each business unit is responsible for defining, monitoring and reporting on key risk indicators for all key risks identified.

7.8.2. Risk tolerance limits

Risk tolerances are the acceptable levels of variation relative to the achievement of objectives. Risk tolerances can be measured, and often are best measured in the same units as the related objectives. Performance measures are aligned to help ensure that actual results will be within the acceptable risk tolerances. In setting risk tolerances, management considers the relative importance of the related objectives and aligns risk tolerances with risk appetite. Operating within risk tolerances provides management greater assurance that the entity remains within its risk appetite and, in turn, provides a higher degree of comfort that the entity will achieve its objectives.

The risk appetite and tolerance thresholds are defined in a separate risk appetite statement.

7.8.3. Incident reporting

This is an internal management function and will form part of the Enterprise Risk Management process. Incident reports should incorporate:

- Incidents of non-compliance to approved standards (whether losses were incurred or not); and
- Losses arising from particular incidents.

The destination of incident reports will be determined by the nature of the potential or actual loss. Incidents and losses that originate from risks contained in the key risk registers must always be elevated to higher levels of management with risk-related variance reports being incorporated into routine management reporting processes.

7.8.4. Performance measurement

Management's performance with regards to Enterprise Risk Management will be measured and monitored through the following performance management activities:

- Monitoring of progress made by management with the implementation of the Enterprise Risk Management methodology;
- Monitoring of key risk indicators;
- Monitoring of loss and incident data;
- Management's progress made with risk mitigation action plans; and
- An annual quality assurance review of Enterprise Risk Management performance.

8. PROJECT RISK MANAGEMENT

It must be noted that this ERM framework applies across a broad range of risk categories that would include project risks. However, the purpose of this section is to provide additional guidance on the manner in which the ERM framework is to be applied in project efforts. The absolute requirement is that all project efforts include a formal Enterprise Risk Management plan.

8.1. Introduction

Risk refers to any factor (or threat) that may adversely affect the successful completion of the project in terms of achievement of its outcomes, delivery of its outputs, or adverse effects upon resourcing, time, cost and quality. Successful projects try to resolve risks before they impact the project, and alternatively have sufficient plans to address the impact of risk when it occurs. It should be noted that sometimes risks may also be associated with opportunities, such as the use of a new technology, and acceptance of the risk needs to be based upon the costs of rectifying the potential consequences versus the opportunities afforded by taking the risk.

Project risk management describes the processes concerned with identifying, analysing and responding to project risk. It consists of risk identification, risk analysis, risk evaluation and risk treatment including issues management. The processes are on-going throughout the life of the project and should be built into the project management activities.

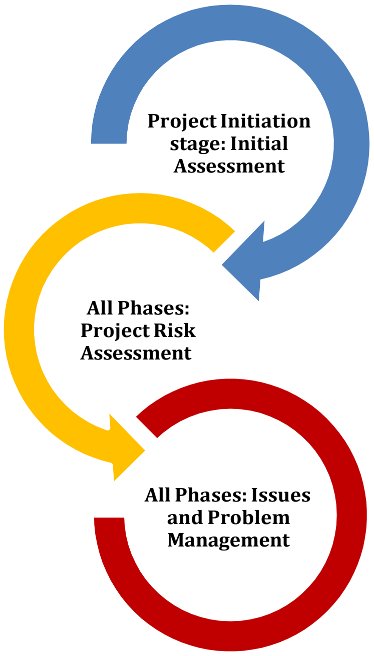
Project risk management is conducted initially as part of the assessment of the project's viability and is conducted throughout the project to ensure that changing circumstances are tracked and managed. All projects require a degree of Risk Management, but the effort expended will depend on the size and scope, including outcomes, customers, outputs, work and resources. Larger projects involving significant investment and/or major outcomes will receive formal and detailed Enterprise Risk Management activities on an on-going basis.

Issues management and project risk management are closely linked, as some issues may become risks. This is why it is recommended that major issues are also identified and managed as part of the same holistic risk framework. A proposed framework for effective Enterprise Risk Management requires that issues management be combined with normal Enterprise Risk Management initiatives.

8.2. Project Risk Management interventions

In order to simplify the application of the risk framework and to maintain focus on the project risk management and issues management processes through-out the life of the project, the following 3-pillar process to Enterprise Risk Management shows practically how the Enterprise Risk Management process will be executed during the various phases of any project.

8.2.1. Project Risk Governance Process:


Project Initiation stage: Initial Assessment
All Phases: Project Risk Assessment
All Phases: Issues and Problem Management

3-pillar Enterprise Risk Management process in project phases

8.2.1.1. Initial stages (Concept and Initiation) – Risk checklist

At the initial stages of a confirmed (or yet to be confirmed) project and as part of input into the business decision to adopt a project, a high-level risk checklist is completed. This checklist is a list of pre-listed questions, each answered with a simple “yes” or “no” answer. These answers typically then drive a risk rating for the project under specific pre-listed categories.

In the first stage, this checklist will assess relative project risk levels by looking at broad areas that include the following:

- Socio-economic impact/ significance (business case)
- External dependencies
- Organisational alignment
- High-level planning assessment
- Technical considerations

8.2.1.2. Project commencement and implementation stages – Risk assessment and management

Before risks can be managed, they need to be identified. At the onset of a project, a facilitated risk assessment will be conducted. This risk assessment will focus on the specific objectives of the project and the relative risks linked to each of these objectives. Risk identification will involve key project stakeholders. The specific additional requirements with regard to project risk assessments are as follows:

- Project risks must be formally recorded;
- Risk mitigations must be considered and assessed;
- Required risk mitigations and enhancements thereto must be included as milestones in the relevant project plans;
- Responsibilities for risks and mitigation thereof must be formally recorded in the project plan and project risk management plan;
- On-going monitoring and re-assessment of risks on projects is essential and is the responsibility of project implementation managers;
- Project risk assessments and management must be integrated with the process of issues management; and
- Project risk rating criteria are defined in the broad ERM framework of the organisation.

Before conducting the project risk assessment, it is important to have clearly defined the scope of the project so that the identification of risks can remain focused on what potentially threatens the achievement of outcomes, delivery of outputs, level of resourcing, time, cost and quality. Risks can also be categorised, for example in terms of type (i.e., Corporate Risks, Business Risks, Project Risks, and System Risks).

8.2.1.3. Implementation and final stages – Issues management

An issue can be defined as a concern that may impede the progress of the project if not resolved. If issues are not addressed, they may become a risk to the project. Issues must be resolved quickly and effectively.

Issues management involves monitoring, reviewing and addressing issues or concerns as they arise through the life of a project. Issues can be raised by anyone involved with the project including Customers/ Clients, Business Owners, Steering Committee members, Reference or Working Group members, the Project Manager, Project Team members and other key stakeholders.

An Issues Register should be established as part of the on-going project management activities. The Project Manager and team need to have a process for capturing issues as they arise, updating and reviewing them so that they can be managed and resolved as the project moves forward. Once a resolution is agreed on, the appropriate activities are added to the project plan to ensure the issue is resolved and to the project budget, if appropriate.

An Issues Register is basically a systematic record of issues. It will include the following for each issue:

- a unique number;
- a description;
- who raised the issue;
- date reported;
- severity/ priority rating;
- the person or group who is responsible for resolving the issue;
- how resolved;
- adopted status, usually open or closed; and
- date resolved.

Commonly principles in issues management are as follows:

- Solve the root cause of the issue;
- Resolve issues quickly to proceed as quickly as possible;
- It is good practice to encourage people to help identify solutions along with the Issues;
- Engage the Project Sponsor/Steering Committee in the resolution of issues from very early in the project;
- If a large issue looks too difficult to be resolved in a timely manner, break it down into logical sub-issues;
- Inter-related issues should be resolved simultaneously; and
- Resolve major issues before the **point of no return.**

9. ERM ENHANCEMENT AND ENTRANCHMENT PLAN

9.1. Establish an organisational framework of assurance for key risks and control

A framework of assurance must be developed for NFVF’s risks. Key players in the organisation will combine to provide assurance that risks are being appropriately managed. This combined approach to assurance normally involves management, Enterprise Risk Management, compliance and internal and external auditors working together through an integration process coordinated by the Audit and Risk Committee. Other experts must be chosen to provide assurance regarding specialised categories of risk, such as environmental management and capital market risks. The assurance framework must be formalised and must incorporate appropriate reporting processes.

9.2. Internal audit provides assurance on Enterprise Risk Management processes

Internal audit must examine the techniques used to identify risk. The categories and the scope of risk assessments should be considered. The methodologies used to extract risk information must be reviewed. Monitoring processes should be wholly aligned with the results of risk assessments. The internal audit function should particularly seek evidence that the processes of risk identification are dynamic and continuous, rather than attempt to comply with governance expectations. The effectiveness of Enterprise Risk Management processes should be subjected to an audit on an annual basis.

9.3. The outputs of risk assessments are used to direct internal audit plans

Internal audit plans depend greatly on the outputs of risk assessments. Risks identified during risk assessments must be incorporated into internal audit plans, in addition to management and Audit and Risk Committee priorities. The risk assessment process is useful for internal audit staff because it provides the necessary priorities regarding risk as opposed to using standardised audit sheets. The audit activities will focus on adherence to controls for the key risks that have been identified. In addition, internal audit staff may direct management towards the need for better controls around key risks.

9.4. Internal audit provides assurance on quality and reliability of risk information

The internal audit function plays a key role in coordinating the key players in the Enterprise Risk Management process to provide assurance to stakeholders. Internal audit is not normally the only provider of assurance. The function does, however, have an important role in evaluating the effectiveness of control systems. The process of assurance must also involve management, the external auditors, regulators and subject specialists.

9.5. Safety, health and environment

A formal safety management programme is essential for NFVF’s business. The risks will vary according to the entity, but the principles of Enterprise Risk Management will always apply, i.e., risk identification, risk assessment, formal action plans for mitigation, monitoring, reporting and assurance. The scope of NFVF’s safety management programme should include administrative aspects, safety awareness and training, health, hygiene, electrical safety, physical safety, micro- environmental exposures and legislative requirements.

9.6. Business Continuity Management

It is expected that NFVF will have a Business Continuity Management Plan in place, which will be revised and tested annually. The results of such testing and simulations should be reported to the Audit and Risk Committee.

9.7. Fraud Prevention Plan

NFVF is responsible for developing and implementing its own fraud policy and prevention plan.

9.8. Project Risk Management

NFVF will ensure that each project engagement has and maintains a formal Enterprise Risk Management plan, a risk register as well as an incident register which should be reported on in line with project reporting frequencies. The assessment of project risk is performed in line with the same principles of this framework. At a minimum, a quarterly report on project risks and management thereof will be formulated and presented to the Council.

9.9. Governance committees

The terms of reference of the various Committees will be formally reviewed on a regular basis to ensure that they remain relevant and clearly define functions, roles and governance processes for the various committees.

For operational integration, Enterprise Risk Management champions will be nominated to focus on the holistic management of risk and these risk champions will provide support to their business units on a day-to-day basis on risk matters.

9.10. Integration of ERM with Planning Processes

The NFVF will identify, record, evaluate and establish links between objectives and risks and will regularly monitor these.

A periodic risk report will be provided and presented to the Audit and Risk Committee. This report will detail significant risks facing the NFVF, the controls in place to minimise the risks and an assessment of the residual risk. Major changes in risk will be discussed and reported therein also.

10. COMBINED ASSURANCE PLAN

The combined assurance model aims to optimise the assurance coverage obtained from management and internal assurance providers on the risks facing NFVF.

The following table breaks down the combined assurance model:

Line of defense	Assurance Provider	Identification and Management of Risk	Controls	Monitoring and assurance
1st Line	**Management**	Risk identification and management	Control self-assessment	Management assurance
2nd Line	**Risk Management**	Risk Assessment and Support	Control self-assessment review	Risk assurance monitoring
3rd Line	**Internal Audit and External Audit**	Risk assessment	Independent Control assessment and assurance	Control assurance

Annexure A: Impact Parameter.

Score	Impact	Consequence
5	Catastrophic	Loss of ability to sustain on-going operations. A situation that would cause a stand-alone business to cease operations
4	Major	Significant impact on achievement of strategic objectives or targets relating to the organisational plan
3	Moderate	Disruption of normal operations with a limited effect on achievement of strategic objectives or targets relating to the organisational plan
2	Minor	No material impact on achievement of organisational objective or strategy
1	Insignificant	Negligible impact

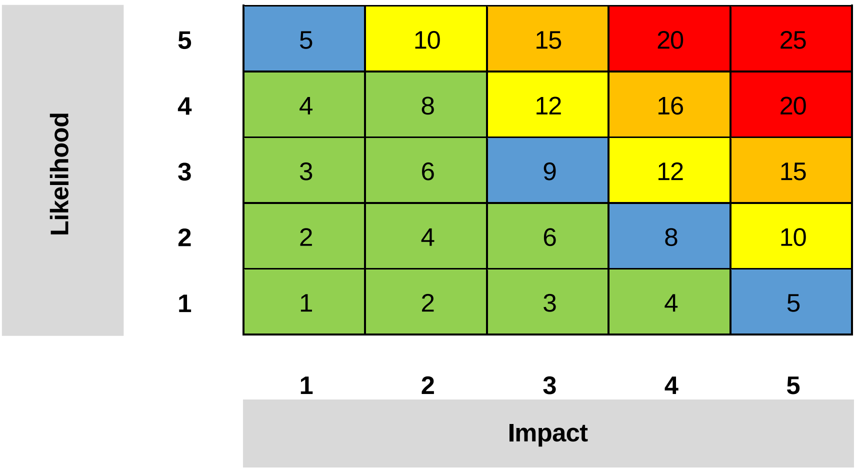
Annexure B: Likelihood Parameter

Likelihood	Occurrence	Description	Score
Almost certain	The risk is already occurring, or has a high likelihood of occurring in the next 12 months	The risk is almost certain to occur in the current circumstances	**5**
Likely	The risk will easily occur and is likely to occur at least once in the next 12 months	More than even chance of occurring	**4**
Moderate	There is an above average chance of the risk occurring more than once in the next 3 years	Could occur often	**3**
Unlikely	The risk has a low likelihood of occurring in the next 3 years	Low likelihood but could happen	**2**
Rare	The risk is unlikely to occur in the next 3 years	Not expected to happen, event would be a surprise	**1**

Annexure C: Control Effectiveness Rating

Effectiveness category	Category definition	Factor
Very good	Risk exposure is effectively controlled and managed	20%
Good	Majority of risk exposure is effectively controlled and managed	40%
Satisfactory	There is room for some improvement	65%
Weak	Some of the risk exposure appears to be controlled, but there are major deficiencies	80%
Unsatisfactory	Control measures are ineffective	90%

Risk exposure = Likelihood x Impact



Likelihood	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Impact				

Annexure E: Risk Escalation Matrix

Thresholds Where the result is:	**Threshold Interpretation**		**Escalation requirements (if any)**	**Action Required**
Between 20 and 25	🟥	**Red – Unacceptable.** ***Very high Risk***	• Council • Audit & Risk Committee • EXCO	Critical risks that requires Council attention. This risk requires intensive management action and constant (Monthly and quarterly) monitoring.
• Between 15 and 195	🟧	**Amber – Cautionary.** ***High Risk***	• Council • Audit & Risk Committee • EXCO	Risks serve as a caution to management and the Council with regards to the level of risk (Monthly and quarterly). These risks require as much attention as the very high risks.
Between 10 and 14	🟨	**Yellow – Tolerable** ***Medium Risk***	• Head of Department • Line manager	Risks are at a tolerable level and requires monitoring at departmental level. May not require intensive control improvements.
Between 5 and 9	🟦	**BLUE – Acceptable** ***Low Risk***	• Line Manager	Risks are at an acceptable level and only requires monitoring by line manager. Control improvements are not required at this level.
Between 1 and 4	🟩	**GREEN – Acceptable** ***Minimum Risk***	• Line Manager	Risks are at an acceptable level and only requires monitoring by line manager. Control improvements are not required at this level.