Risk Management Policy

Effective: 27 January 2021
Owner: Company Secretary
Approval: Board
Reviewed: Annually

POLICY	Effective risk management and stress testing enables the Company to protect and add value for investors while practicing good corporate governance.
PURPOSE	This policy outlines RFM's objectives and commitments in achieving these goals and the risk assessment process which will enable consistent and reproducible risk assessments to be conducted on RFM activities.
SCOPE	This policy applies to RFM and all entities which are owned and/or managed by RFM. All employees and contractors are expected to incorporate RFM's risk management practices into decision-making processes as part of normal business practice. RFM's approach to Risk Management is consistent with the International Standard ISO 31000:2018.
NEED HELP?	Any queries regarding this Policy should be directed to the Compliance Department.

Risk Management Framework

Principles

1. In order to design an effective risk management system and create a risk management culture, RFM has incorporated the following principles into its risk management framework. Risk management:
    a. creates and protects value;
    b. is an integral part of all organisational processes;
    c. is part of decision making;
    d. explicitly addresses uncertainty;
    e. is systematic, structured and timely;
    f. is based on the best available information;
    g. is tailored to RFM's external and internal context and risk profile;
    h. takes human and cultural factors into account;
    i. is transparent and inclusive;
    j. is dynamic, iterative and responsive to change; and
    k. facilitates continual improvement of the Company.

Objectives

2. The objectives of the framework are to:
    a. provide the foundations for RFM's risk management process;
    b. assist in the implementation of effective risk management policies;
    c. ensure adequate reporting is undertaken; and
    d. provide a basis for decision making and accountability at all levels.

Components

3. RFM acknowledges that the success of risk management depends on the effectiveness of the management framework and, in designing its risk management practices and processes, it has adopted the following components:

4. **Leadership and commitment**: the Company's management is responsible for:

   a. defining and endorsing RFM's risk management policy;

   b. ensuring that the Company's culture and risk management policy are aligned;

   c. aligning risk management objectives with the Company's objectives and strategies;

   d. ensuring legal and regulatory compliance;

   e. ensuring that the necessary resources are allocated to risk management;

   f. assigning accountabilities and responsibilities at appropriate levels within the Company and communicate the benefits of risk management to all stakeholders; and

   g. ensuring that the framework for managing risk continues to remain appropriate.

5. **Design of framework for managing risk**

   it is important to evaluate and understand both the external and internal context of the organisation, namely:

External drivers	- the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment (international, national, regional, local); - key drivers and trends having impact on the objectives of the organisation; and - relationships with, and perceptions and values of, external stakeholders; - contractual relationships and commitments; - the complexity of networks and dependencies
Internal drivers	- vision, mission and values; - governance, organisational structure, roles and accountabilities; - policies, objectives and the strategies that are in place to achieve them and standards, guidelines and models adopted by the organisation; - organisational resources (capital, time, human, technology etc.) and the organisational culture; - information systems, information flow and decision making processes (both formal and informal); - relationships with, and perceptions and values of, internal stakeholders; - the form and extent of contractual relationships

   a. The Company has established a Risk Management Policy and maintains a Consolidated Risk Register, Business Continuity and Disaster Recovery Plan, HSE Management System and AML/CTF Program. The risk policy forms an integral part of the Company's internal processes. Risk management has been integrated into RFM's policies and procedures, guidelines and models, business and strategic planning and management processes.

   b. RFM will ensure the identified risk owners have the accountability, competence and authority to manage those risks and that there is a clear understanding of the roles and responsibilities and reporting requirements in relation to managing risks and the risk management process.

c. Management will be responsible for allocating appropriate resources (people, skills, experience and competency) to risk management and ensuring well documented processes and procedures, appropriate training programs and methods and tools for managing risk are in place.

d. RFM will maintain continual communications, including regular comprehensive and frequent reporting of risk, providing feedback and communicating any modifications to the risk management framework, as part of good governance.

e. Where a staff member is eligible to receive a bonus, the award of such bonus will be partly dependent on compliance with RFM's risk management policy.

6. **Implementation:** the Company's management is responsible for implementing the framework for managing risk, developing the Company's policy and risk management processes, communicating with all stakeholders and providing ongoing training in relation to risk management.

7. **Evaluation:** the Company is committed to ensuring RFM's risk management processes, the risk management framework and the Company's policy are regularly reviewed to assess the appropriateness and effectiveness of these measures and the Company's risk policy.

8. **Improvement:** based on results of monitoring and reviews, changes to the risk management framework may be made to continually improve the Company's risk management and its risk management culture.

Risk Management Process

Objectives

9. The objectives of this Risk Management Policy are:

   a. to determine to what extent risks may affect the business;

   b. to use a structured approach to enable a valid assessment of risk which will ultimately lead to effective management of specific risks; and

   c. to manage, or control, risk by implementing strategies to either:

      i. avoid the risk;

      ii. transfer the risk to another party;

      iii. mitigate the probability of the risk arising; or

      iv. accept that the risk may occur and implement procedures to mitigate the consequences associated with the risk.

Steps

10. RFM will maintain procedures (refer to Schedule 2) to provide the Company with an up to date assessment of the risks faced in the course of farming, funds management and general business activities.

11. In developing, implanting and reviewing its risk management system, RFM will consider the industry standards and requirements applicable to the nature of its business, including the International Standard ISO 31000:2018 and ASIC Regulatory Guide 259 Risk management systems of responsible entities.

12. This requires RFM to:

    a. **Establish the scope, context and criteria**: This is the strategic, organisational and risk management context (both external and internal) against which the rest of the risk management process in the Company will take place.

    b. **Identify Hazards/Risks**: This is the identification of where, when, why and how events arise as the basis for further analysis.

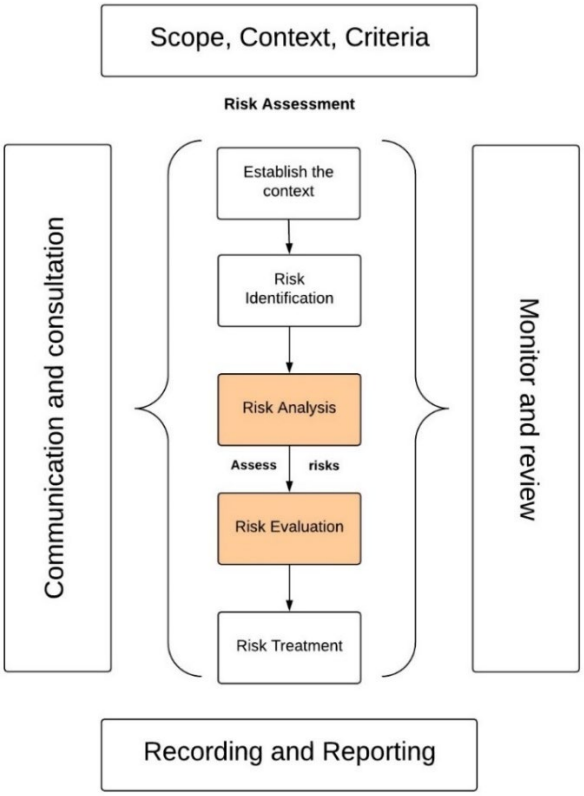
    c. **Analyse Risks**: This is the determination of existing controls and the analysis of risks in terms of the consequence and likelihood in the context of those controls.

    The analysis should consider the range of potential consequences and how likely those consequences are to occur. Consequence and likelihood are combined to produce an estimated risk rating (i.e. level of risk).

    d. **Evaluate Risks**: This is a comparison of estimated risk levels against pre-established criteria, i.e. the company's risk appetite. This enables risks to be ranked and prioritised.

    e. **Risk Treatment**: For higher priority risks, the Company is required to develop and implement specific risk management plans. Lower priority risks may be accepted and monitored.
    Monitor and Review: This is the oversight and review of the risk management system and any changes that might affect it. Monitoring and reviewing occurs on an ongoing basis throughout the risk management process.
    Communication and Consultation: Appropriate communication and consultation with internal and external stakeholders should occur at relevant stages of the risk management process.

13. Schematically, the risk management process is depicted in the following diagram:



High level risk assessment process

14. This is a broad review of the business risks to determine whether the risks associated with the business warrant a detailed risk assessment. This type of assessment is likely to be required where:

    a. Corporate Governance policies are impacted - eg. Australian Financial Services licence authorisations or conditions are varied, regulatory changes to the Corporations Act or ASX listing rules, Privacy Act, etc.;

    b. Business acquisitions are substantially different to those already under management; and

    c. Changes in the external operating environment occur – e.g. regulatory or political changes.

Detailed risk assessment process

15. The formal process used to identify specific business risks is to evaluate the likelihood of the risks being realised and determine the business' vulnerability to the risks. These guidelines will assist managers to identify risks as required by this policy.

RFM consolidated Risk Register

16. A consolidated Risk Register will be maintained in the Tickit compliance system (Tickit) and can be accessed by all registered Tickit users via the link on the RFM Intranet.

17. This register provides the basis for monitoring and reviewing ongoing business risks.

18. Risks are characterised and defined by the following categories in Tickit:

Risk name	The name of the risk. The name should be broad to capture the risk for the organisation as a whole. The name should be logical and easy to understand
Risk category	A risk category is used to group information together for management and reporting purposes. It is a way of categorising the risks into meaningful groups of data. The risk categories in Tickit are defined at Table 1 of the Risk Appetite Statement
Risk sub-category	Sub-categories within the main risk categories, for example Environmental and Workplace health and safety within the HSE category (refer to Table 1 – Risk Appetite Statement)
Risk type	Further risk description to group information, for management reporting, i.e. Board and the Internal Compliance Committee. The risk types in Tickit are Strategic, Operational, Project, Governance, Market & Investment Risk and Liquidity Risk (refer to Table 2 – Risk Appetite Statement)
Risk definition	A definition (description) of the risk. The initial risk definition is broad as it captures the definition for the whole organisation
Potential impact	An impact of the risk if the risk is not controlled effectively. Examples of potential impact may include financial loss, reputational damage, injury to personnel, increased workers' compensation insurance costs, loss of licence etc

Risk assessment

19. A risk assessment is completed for each main risk or sub-risks, as applicable. Each business unit can have multiple risk assessments (for assessing multiple risks or sub-risks). Not all main risks will have sub-risks.

Business Unit	Part of business to which the risk is relevant, i.e. RFM Corporate (funds management), Horticulture, Viticulture, Cropping, Cattle etc
Description	A customised risk, or a sub-risk, that can be added depending on each individual business requirements, e.g. Risk Name: Operation of plant and equipment, Sub-risk 1: Fans, Sub-risk 2: Generators, etc. (see figure 4 below)
Inherent risk (pre-control)	The likelihood of an event happening is mapped against the consequence of that event happening
Control measures/risk treatments	Various measures to mitigate the risk. These can include RFM policies, procedures and other processes, engineering controls, isolation or substitution of the risk, staff education, insurance and other commercial arrangements. It can also include risk acceptance however "Extreme" risks should never be accepted and appropriate control measures should be identified and implemented
Residual risk (post-control)	The residual risk is calculated by mapping the Control Effectiveness (i.e. a measure of how effective our existing controls are in managing risk – non-existent, poor, fair, good, very good) against the Inherent Risk rating
Risk Owner	The risk owner is the Tickit user who is responsible for the ongoing review of the Risk Assessment of the business unit and the general management of that particular risk
Timing/Frequency	This determines the timing and frequency, i.e. monthly, quarterly, annually etc., of the risk assessment and should be scheduled at least annually
Notes	Notes for further actions and improvement plans, other notes e.g. for the Board's attention or additional detail relating to the risk
Risk appetite	Risks can be evaluated against the company's risk appetite as the company may have a higher risk tolerance in some areas compared to others. This feature allows a comparison between the Residual Risk and the risk appetite in reporting. However, please note this feature is not currently used

Maintenance of the consolidated Risk Register

20. The Risk Officer will maintain the Risk Register. The Risk Officer is responsible for recording any new risk names or changes to existing risk in the register and general maintenance of the register. New risks and changes to existing risks are reported to the Risk Officer via the Risk Report Form available through **Tickit Web Kiosk** (all staff) or by submitting the form through Tickit, **Events** Tab (registered Tickit users).

21. The nominated Risk Owners are responsible for reviewing and updating Risk Assessments for risks relevant to their business unit. Risk owners are also able to add new sub-risks.

Risk Appetite Statement

General statement of appetite

22. RFM is responsible for the strategic direction and day to day management of each of the Funds, including the timing of asset acquisitions and sales, investment structure and portfolio composition.

23. This statement emphasises RFM's commitment to risk management and establishes the Board's expectation with respect to how strategic, financial and operational decisions throughout the business are undertaken.

24. RFM has a varying risk appetite depending on the entity. RFM makes resources available to control risks to acceptable levels, whilst realising it is not possible, nor sometimes desirable, to entirely eliminate risk. Below is a breakdown of the risk appetite accepted by the Board for the different entities with their exposure to the operations of RFM.

Fund	**Categories**	**Risk Appetite**
RFM*	Responsible Entity	Medium
RFF/RFA	Listed Entity – ASX	Low
Schemes (RAF, MP07)	Operations	Medium

**** RFM has subsidiaries that undertake operations which are included as part of the RFM risk appetite.***

Table 1: Risk categories - definitions

Categories	Subcategories	Definition
AML and CTF		Risks that RFM may unwittingly facilitate money laundering or financing of terrorism by providing Designated Services to its Customers
Assets and Property		Risks that have the potential to impact on RFM's real and intellectual assets and property. Risks include those related to interest rate fluctuations, economic downturn, property market & environmental impacts
Commercial	Contract Management	Risks that have the potential to put RFM in breach of key commercial contract obligations
	Market Risk	External factors adversely affecting investment management and recommendations by external financial planners
	Financial	Risks associated with financing including funding, transactions, fraud and liquidity
Farm Management		Risks with the potential to adversely affect farm management including produce, disease and pests, productivity, regulatory changes
Governance and Compliance		Risk of non-compliance with stated requirements, internal policies and procedures, governance programs, legislation and other regulations
HSE	Environmental	Elements of workplace environment/condition/design that adversely affects the health and safety of the environment

Categories	Subcategories	Definition
	Workplace Health and Safety (WHS)	Elements of workplace environment/condition/design that adversely affect the health and safety of employees, contractors and visitors
Human Resources		Risks related to the management of people and related programs and processes within the organisation
Information Technology		Risks related to the operation, management and adoption of information technology in the organisation, including security and data reliability
Media and Communications		Adverse event derived from internal and/or external communications. This includes risks relating to social media

Table 2: Risk types: definitions

Risk type	Definition
Strategic	A risk arising from business decisions, implementation of decisions, or responsiveness to industry changes
Operational	A risk arising from the execution of business functions focusing on risks that arise from people, systems and processes
Project	A risk arising from a specific project
Governance	A risk that threatens the ability of the RE to make reasonable and impartial business decisions in the best interest of members
Market and investment risk	A risk that a scheme operated by the RE will not meet its objectives
Liquidity risk	A risk that the responsible entity will not have adequate financial resources to meet its financial obligations or needs, either at RE level or scheme level

Strategic goals and objectives

25. RFM acknowledges that the success of risk management depends on the effectiveness of the management framework and risk management practices and processes. The objectives of RFM's risk management framework are shown in paragraph 9.

Risk management capabilities

26. RFM recognises that effective risk management and stress testing where appropriate enables the Company to protect and add value for investors while practicing good corporate governance. RFM's capabilities extend to:

    a. RFM's approach to risk management aligns with the Guidelines to ISO 31000:2018 – Risk management principles and guidelines;

    b. a Risk Manager who is responsible for overseeing the risk management function;

c. a risk framework/process has been developed which allows RFM to effectively identify and assess risk;

d. a risk profiling system has been adopted which analyses the likelihood of a particular risk event occurring, and the potential consequences if the event was to occur and having regard to the overall control effectiveness of existing mitigation strategies;

e. a Compliance program has been implemented in accordance with the International Compliance Standards ISO 19600, through which key risk controls are monitored;

f. a Complaints Handling Policy has been implemented which captures critical key risk indicators;

g. an on-line policy management system, staff induction and training programs have been implemented; and

h. a web based risk management software that is ISO 27001:2013 certified and aligned with ISO 31000:2018 is used for the risk management process.

Our appetite for risk

27. RFM's appetite for risk is influenced by a range of factors including strategic goals and objectives, the amount of risk RFM will accept given the organisational constraints, RFM's system of ethics, values and risk-based behaviours as well as the level of maturity of RFM's internal risk and internal control programs.

28. For this reason, it is not possible to precisely measure RFM's risk appetite. The approach is rather to set the tone from Board level and ensure that the organisational infrastructure will identify and manage key risks as they arise.

29. The key risk areas that are relevant to RFM and the entities it manages or owns are listed in Schedule 1.

30. The risk management system will assess each of the key risk areas by evaluating risks against the risk matrix identified under risk categories. The Board **will not** tolerate a residual risk rating of ***Extreme*** whilst a risk rated as ***High*** must be assessed regularly as part of the risk assessment process.

Risk reporting

31. RFM risk assessment, including the Risk Appetite Statement, is reviewed annually in accordance with the Risk Management Policy and the HSE Management System. Risks which have a residual risk rating of ***Extreme*** or ***High*** are subject to ongoing monitoring. Projected risks for various projects are identified and managed during the life of the project.

32. Significant risk and material business issues are reported to the Board monthly as part of standard board reporting. An annual risk review and HSE audit is reported to the Board each year. The Internal Compliance Committee reviews risk reports at its quarterly committee meeting.

Ongoing Risk Management Review And Monitoring

Risk Register – review and audit

Annual review

33. Risk Assessments will be subject to an annual review in accordance with this policy and the HSE Management System Policy.

34. Auditing of HSE risks will be conducted in accordance with the HSE Management System.

35. It is recommended that specific business units conduct an annual risk identification and review meeting with key members of their team and can be assisted by the Risk Officer, if required. The purpose of this review is to:

    a. Review and re-assess, if necessary, the identified (current) risks to ensure their risk rating has not changed, control actions are still appropriate and whether further controls are required;

    b. Use Risk Identification and Assessment Guidelines to identify and analyse other/additional risks that might have arisen in specific parts of the business and how these can be managed including putting effective controls in place to eliminate or minimise these risks;

    c. Report new risks to the Risk Officer for inclusion in the Consolidated Risk Register; and

    d. Retire risks that no longer present a threat.

Ongoing monitoring

36. Risks which have a high residual risk rating (Extreme, High), or represent an increased risk that RFM may be unable to perform its duties as responsible entity, or breach any of its AFS licensing conditions, are subject to ongoing monitoring and reporting to the Board on an ongoing basis, or until the risk has been satisfactorily mitigated.

Project risks

37. Specific risks associated with various projects will be managed by the relevant Project Manager during the life of the project.

Risk reporting to Board and Internal Compliance Committee

38. Monthly reporting: Risk Owners report to the Board on significant risks and material business issues as part of their monthly operations board report.

39. Annual review and audit: the outcome of the annual risk review and the HSE audit will be reported to the Board together with any recommendations to effectively manage the risks.

40. Internal Compliance Committee (ICC): the ICC is provided with quarterly risk reports (consisting of the consolidated risk register) and any associated reporting. The ICC review and advises the Board of any issues.

Risk management meetings

41. The Risk Manager, Risk Officer or National Managers can arrange and convene a meeting of all, or team-based, Risk Owners if circumstances warrant this course of action be taken.

Risk assessment process

42. The main objective of a risk assessment is to proactively identify and manage events that could harm people, property or the environment. RFM has adopted a risk assessment process which involves the following steps:

    a. Establish the context and understand the work process/es that may present risks;

    b. Identify hazards/risks and associated impacts;

    c. Assess the inherent likelihood and consequence of each impact occurring during the process/es;

    d. Consider, document and implement control measures to mitigate the likelihood or consequence of the impact;

    e. Assess the effectiveness of the control measures to determine the residual risk; and

    f. Document any significant conclusions, actions or comments from the risk assessment.

Individual or team-based risk assessments

43. Risk assessments can be undertaken either by an individual or team, depending on the purpose and nature of the risk assessment. Team based risk assessments involve the assembly of a group of multidisciplinary individuals to undertake the risk assessment.

44. It is recommended that team-based risk assessment workshops be utilised for the following risk assessments:

    a. General corporate, i.e. funds and marketing, finance etc. that may require an input from a number of team members, and HSE risk assessments;

    b. Job Safety & Environmental Analysis & Work Permit (JSEA's); and

    c. Operational HSE Risk Register reviews.

45. Risk assessments may be undertaken by an individual (i.e. outside of a team environment) in the following instance:

    a. JSEAs for a task being undertaken by a single individual.

Table 3: RFM risk assessment tools, application and sign-off

Risk Assessment Tool	Individual or team-based risk assessment	Application
Corporate / Operational / HSE Risk Review	Team-based	• Required annually • Reviews all corporate, HSE operational / regional risks across the business • Used as the foundation of corporate management plans and HSE improvement plans • Sign-off by Business Manager or National Manager
Project Risk Assessment	Team-based	• To occur for discrete projects managed independently of the overall operations

		• Reviews all risks including HSE risks applicable to the project • Sign-off by Business Manager or National Manager
Job Safety and Environmental Analysis (JSEA)	Team-based or individual	• To occur for tasks associated with an operation or regional activity that does not have an existing procedure or a Work Permit (see JSEA Procedure undertaken by a single individual • Sign-off occurs from Business Manager or National Manager

Team-based risk assessment

46. Planning the Team based Risk Assessment Review: the completed risk register and assessments should be circulated by the Risk Officer to provide context to risk assessment participants.

47. Undertaking the HSE Risk Review: the National Manager will record the outcomes of the review. The National Manager must assess each risk by working through the risk assessment process. Decisions will be made on the inherent probability and consequence, as well as the relevant controls and their effectiveness to assess the residual risk. Where consensus cannot be reached by the group, the National Manager maintains the responsibility to make an overriding decision.

Tolerance levels for certain risks

48. Tasks involving risks with a residual risk rating of ***Extreme*** are not to be completed, unless sign-off is obtained by the National Manager or Chief Operating Officer. Tasks involving residual risk ratings of ***High*** must be revisited as part of the Risk Assessment process, to assess whether the residual risk rating is as low as reasonably practicable. Where this is the case, the task may proceed as planned.

Responsibility and accountability

49. The **RFM Board** has ultimate responsibility for risk management and the implementation of this policy. The Board is responsible for reviewing and approving this policy every two years.

50. All management personnel are expected to coordinate risk management activities within their own business units and/or areas of expertise.

    a. The **Risk Officer** may be the same person as the one that performs the company's compliance functions. The Risk Officer is responsible for:

        i. Ensuring that officers and employees are aware of the Risk Management Policy and Risk Register;

        ii. Maintaining the consolidated risk register;

        iii. Reporting to the Board and Internal Compliance Committee; and

        iv. Convening meetings to review risk requirements and breaches, if required.

51. The **Risk Manager** is responsible for ensuring a risk management culture is promoted within RFM and for ensuring appropriate risk management strategies are implemented.

52. **Business Managers, National Managers** and all other Risk Owners are responsible for managing risks within their area as identified in the Risk Register. They are also responsible for identifying any potential risks and bringing these to the attention of the Risk Officer or the Risk Manager and the Board.

53. **All Staff** have a responsibility to assist in the identification of potential risks and to notify the Risk Officer.

Definitions

Term	Definition
Board	RFM Board of Directors
Company	Rural Funds Management Limited
Consequence	Outcome of an event affecting objectives. An event can lead to a range of consequences and can be certain or uncertain and can have positive or negative effects on objectives. Consequence can be expressed quantitatively, i.e. in financial terms, or qualitatively being a loss, injury, disadvantage or gain
Consolidated Risk Register	RFM Consolidated Risk Register which lists and describes all risks, potential impact, determined severity and management control strategies
Control and/or Risk Treatment	A measure that is modifying risk; controls include any process, policy, device, practice, or other actions which modify risk consequence or likelihood
Control effectiveness	A combination of measures to stop an event occurring, or to minimise the impact of an event that does occur
Impact (effect)	A deviation from the expected and can be positive and/or negative, an impact of the risk if the risk is not controlled effectively
Emergency	Condition that poses a significant threat to health and safety and/or the environment. Typically, such an event is unplanned and requires immediate attention and action
Hazard	Any situation, substance, activity, event or environmental factor that could potentially cause injury, ill health, harm, damage or loss to a person, property or the environment
Inherent risk (pre-control risk)	The true risk of the impact occurring when no controls have been put in place to mitigate the risk
ISO	International Organizations for Standardizations
Likelihood	Likelihood is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as probability or frequency over a given time period.)
Monitoring	Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected
Residual risk	Risk remaining after risk treatment. (i.e. controls have been implemented)

(post-control risk)	
Risk	The likelihood of injury, illness or harm (e.g. damage, loss etc.) resulting from exposure to a hazard
Risk Appetite Statement	The amount of risk that the organisation is willing to accept, or take on in pursuit of vision, strategic goals and objectives
Risk analysis	Process to comprehend the nature of risk and to determine the level of risk. Risk analysis provides the basis for risk evaluation and decisions about risk treatment. Risk analysis also includes risk estimation
Risk assessment	The overall process of risk identification, risk analysis and risk evaluation
Risk criteria	Terms of reference by which the significance of risk is analysed (i.e. consequences, likelihood).
Risk identification	The process of finding, recognising and describing risks
Risk Manager	Company Secretary
Risk management	Coordinated activities (culture, processes and structure) to direct and control an organisation with regard to risk
Risk management framework	Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation
Risk owner	Person/job role with the accountability and authority to manage a risk
Risk Officer	Assistant Manager – Compliance & Risk
Risk rating (level of risk)	Combination of risks, expressed in terms of the combination of consequences and their likelihood, e.g. Low, Moderate, High or Extreme
Risk source (categories)	Environment or a condition which alone or in combination has the intrinsic potential to give rise to risk (can be tangible or intangible)
Risk Treatment and/or Control	A measure that is modifying risk; controls include any process, policy, device, practice, or other actions which modify risk consequence or likelihood
Uncertainty	The state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood

Appendix 1: Sources and types of risks

1. Provided below are a range of risk sources, risk types and treatment of risks to assist in identifying possible risks relevant to RFM and the entities it managers or owns.

Risk Source	Risk Type	Risk Treatment
Commercial and legal relationships	• Related entities • Other organisations / major support network (large shareholders, dealer groups, financial planners) • Suppliers (stationery, printing) • Service providers	• Documenting compliance plans • Implement disaster recovery and business continuity plans
Economic circumstances	• National/international (financial planning, global and national economies and business cycle, global and national markets) • Income fluctuations (assets under management, performance, asset valuations) • Cost increases (rent, infrastructure, human resources) • Finance continuity & interest rates • Share market (business growth, competition)	• Implementing policies and procedures • Continuous monitoring the market of schemes assets
Human resources and human behaviour	• Key persons • Internal (performance) • Sabotage and fraud (internal) • Error (non-deliberate) • Adequacy of human resources • Absence of individual well-being which may arise from a poor working environment e.g. job insecurity, ethnic or religious tensions, harassment, job factors (demanding tasks, ill health)	• Succession planning implemented • Operational procedures documented • Regular training provided for employees • Annual review of policies and procedures
Regulatory and legal relationships	• Regulator investigation (Australian Securities and Investments Commission [ASIC]) • Compliance shortfalls (outsourcing regulated tasks, • verification processes) • Contractual risks (staff, custodian, other third parties)	• Documenting compliance plans for the RE and schemes • Access to legal advice – internal or external • Testing of compliance procedures • Auditing compliance with policies and procedures
Liquidity risk	• Financial resources not adequate to meet financial obligations at a RE level or scheme level	• Documenting compliance plans for the RE and schemes • Implement a liquidity risk management process that includes ongoing assessment at both levels • Internal audit of high-risk areas of the business • Compliance with specific disclosures requirements • Appropriate internal liquidity thresholds

Natural events	• Fire, flood, storm & earthquake, drought, cyclone • Climate change • Pests, diseases	• Regular training for employees • Implement policies and procedures, Safe Operating Procedures (SOP) and Job Safety & Environmental Analysis (JSEA) as guidance for employees
Political circumstances	• Legislative changes (taxation, Corporations Law and other applicable legislation) • Regulatory changes (ASIC) • Trade barriers (import/export) • Terrorism and similar acts	• Documenting compliance plans for the RE and schemes • Access to legal advice – internal or external • Testing of compliance procedures • Auditing compliance with policies and procedures
Technology and technical issues	• Cyber breach of systems • Data storage & retrieval systems • Communications • Dependability • Safety of information	• Regular cyber resilience health checks • Updating policies and procedures • Regular testing of IT systems • Implement disaster recovery and business continuity plans
Management controls	• Change in management • New opportunities / changes in direction • Segregation of duties • Poor planning; lack of management input, control and involvement; infrastructural or resources constraints and limitations	• Succession planning implemented • Operational procedures documented • Effective recruitment policies • Auditing of staff skills
Biological	• Contact with organic materials e.g. fungi, parasites, viruses and bacteria	• Regular training for employees • Training register to be reviewed annually • Implement policies and procedures, Safe Operating Procedures (SOP) and Job Safety & Environmental Analysis (JSEA) as guidance for employees
Chemical	• Chemicals can be hazardous in their 'pure state' or they can become hazardous when their state is altered due to changing conditions or chemical reactions	• Regular training for employees • Training register to be reviewed annually • Implement policies and procedures, Safe Operating Procedures (SOP) and Job Safety & Environmental Analysis (JSEA) as guidance for employees
Environmental	• Air emissions • Discharges to ground and water • Resource use • Waste generation • Changing land use	• Regular training for employees • Training register to be reviewed annually • Implement policies and procedures, Safe Operating Procedures (SOP) and Job Safety & Environmental Analysis

		(JSEA) as guidance for employees
Health and safety	• Inadequate operating procedures • Lack of staff training • Unsafe working conditions or workplace • Lack of workers' compensation insurance • Poor management controls	• Regular training for employees • Training register to be reviewed annually • Implement policies and procedures, Safe Operating Procedures (SOP) and Job Safety & Environmental Analysis (JSEA) as guidance for employees
Physical	• The workplace environment: the design, location (e.g. activities at height or in confined spaces), materials and energy sources used	• Regular training for employees • Training register to be reviewed annually • Implement policies and procedures, Safe Operating Procedures (SOP) and Job Safety & Environmental Analysis (JSEA) as guidance for employees
Ergonomic / Musculoskeletal	• Workplace design • Repetitive motion task demands • Manual materials handling	• Implement policies and procedures, Safe Operating Procedures (SOP) and Job Safety & Environmental Analysis (JSEA) as guidance for employees

2. The types of risks outlined above should not be seen as independent of one another. The sources and classifications are provided as a prompt and not as an all-inclusive list.

3. Examples of risk names and descriptions are provided below.

Regulatory risk	Questions that need to be considered include: • What does the Corporations Act require from the responsible entity and its officers? • Who is responsible for what and to what risks are these people and the scheme exposed? • Almost every product issuer will require a disclosure document. Is due diligence being conducted correctly? • Is the business aware of and meeting industry standards? • Has the responsible entity considered the impact of all relevant legislation? (i.e. taxation, immigration, employment, AUSTRAC) • Does the responsible entity comply with the conditions of its AFS license?
Asset custody	Is the custodian correctly holding scheme assets?
Unit pricing	Are the interests of members being valued regularly depending on the type of scheme asset?
Valuations	Who is conducting the valuations, are they licensed, insured and appropriate?
Cash receipts	What is the process for handling cash, issuing receipts and banking funds? What reconciliations occur and how frequently?

Cash payments	Who is allowed to issue payments? Are the payments authorised by the constitution?
Distributions	Who performs the calculations? Are they checked? Are they dispatched by direct deposit or by cheque?
Outsourcing	Who is responsible for authorising outsourcing? Is there a list of authorised or approved suppliers? What reviews of their operations have occurred?
Maintenance of adequate and complete records	What records must be kept, and in what format are they maintained? Are back-up and access control systems in place to protect the integrity of their information?
Key individuals	What contingencies have been put in place, and has succession planning been considered?
Investment risks	What are the risks of an incorrect or inappropriate investment being made?
Insurance	The failure to maintain an appropriate level of insurance is a breach of a licence condition
Fraud	Most businesses in some shape or form handle cash and cheques. The misplacement or mishandling of these can expose the business to loss.
Data Breach	An incident wherein information is stolen or taken from a system without the knowledge or authorisation of the system's owner. The data that is stolen or taken may consist of sensitive or confidential information
Inadequate monitoring of the systems	This risk may result in material breaches or errors occurring, which individually result in minimal risk but collectively result in significant risk or loss
Counterpart risk	This is the risk that the other party to the transaction will not complete or only partly complete their obligations
Liquidity risk	If the scheme is liquid, what controls are in place to manage liquidity obligations?
Market risk	If the scheme is subject to market risk, what can be done to minimise and control this?
Constitution contravention	The constitution is the primary contractual document between the responsible entity and the members of the scheme. Is the scheme operated by the responsible entity in accordance with the constitution?
Human resources	Are appropriate due diligence employee checks in place? Does the company have adequate human resources to operate its business efficiently? Does the company comply with the relevant legislation, i.e. employment, taxation laws etc.?
Related party transactions	Are transactions between related parties carried out in accordance with the applicable legislation, are they adequately recorded and notified?
Pests, diseases, fire, water resources, climate	Are there appropriate procedures and management systems in place on the farms to control pests, diseases, fire prevention, management of water resources and adverse weather conditions?

Health, safety and environment	Are adequate operating procedures in place? Are staff and other personnel adequately trained and up to date with safety requirements? Are the working conditions and workplace regularly assessed for safety and employee wellbeing?

Schedule 2: Risk framework/process

1. Risk assessment and categorisation is to be undertaken by the Risk Owner in conjunction with their team or individually. They should follow the process as outlined below.

Step 1. What is the inherent risk?

2. The inherent risk is the true risk of the impact occurring when no controls have been put in place to mitigate the risk.
3. Where a piece of equipment and/or machinery is supplied with some controls already in place (e.g. wheel guards, fan covers etc.) and the manufacturer's warranty covers the equipment with these controls, the inherent risk assessment must be based on the assumption that these controls are effective.
4. If there are controls in place that have been implemented by the Company, or are not covered by the manufacturer's warranty, these should be ignored in the inherent (pre-control) risk assessment, and then taken into consideration in the residual (post-control) assessment.

Step 2. Likelihood parameters

Likelihood	Description
Almost certain	Is expected to occur in most circumstances or expected frequently throughout the year's activities – approximately *multiple times a year*
Likely	Will probably occur in most circumstances or will occur many times during the year's activities – approximately *once per year*, at minimum
Possible	Might occur at some time or will probably occur at some time during the year's activities – approximately *once every 1-3 years*, at minimum
Unlikely	Could occur at some time or is infrequent, may occur at some stage in the year's activities – approximately *once every 4-5 years*
Rare	May occur in exceptional circumstances or is improbable – approximately *once every 6 years or more*

Rural Funds Management

Step 3. Consequence parameters

1. Common sense should be used when assessing the consequences of a risk. The table below provides a guide; it is not an all-inclusive checklist.

Aspect	Insignificant	Minor	Moderate	Major	Catastrophic
Financial impact	Financial loss of <1% FUM*	Financial loss of >1% <3% FUM*	Financial loss of >3% <5% FUM*	Financial loss of >5% <15% FUM*	Financial loss of 15% or more FUM*
Funds under management (FUM): *means total Shareholder and/or Unitholder and/or Grower equity, as per balance sheet, for the relevant entity. This information can be found in the monthly RFM Board Report or shown as total equity in the relevant fund's board report. A summary of the monthly figures can be found as an additional document on the Intranet with this policy.*					
Business Strategy	Negligible impact on objectives	Minor effects present that are easily remedied	Some objectives affected	Some *key* objectives cannot be achieved	Most *key* objectives cannot be achieved
Reputation	No harm to the Company's reputation Complaints resolved by team Manager or member	Local news item, minor adverse publicity in particular locations Minor complaints about products and/or services	Increased attention from media (local level) and/or heightened concern by local community Significant complaints about products and /or services	Significant or consistent adverse national media/public attention (local and state level) Major complaints by stakeholders	Serious adverse public or media publicity (local, state and national level) Loss of confidence by stakeholders and media/public
Intervention by regulators (legal/compliance)	No legal or compliance issues, minor issues not requiring a breach notification	Minor legal or compliance issues - minor breaches (whether reportable to ASIC or not) with no impact on AFSL, the Company, clients or investors	Serious breach of regulation with investigation or report to authority, litigation and/or moderate fines possible, additional regulatory	Major breach of regulation, major litigation, fines, additional regulatory requirements imposed	Significant prosecution and fines. Serious litigation including class actions. Loss of AFSL

Rural Funds Management

Aspect	Insignificant	Minor	Moderate	Major	Catastrophic
			requirements may be imposed		
Business Continuity	Delays to business activities less than 0.5 days	Delays to business activities between 0.5-2 days	Delays to business activities between 2 days to a week	Material disruption to business activities greater than one week but less than one month	Material disruption to business activities greater than one month
WHS Impact (health & safety)	Reversible health effects of low concern (e.g. minor irritation of the eyes, nose, throat or skin, minor muscular or cardiovascular discomfort, headaches, earaches), minor injury requiring first aid treatment, no lost time	Reversible health effects (e.g. sunburn, work-related stress, moderate irritation of the eyes, nose, throat or skin, gastro-intestinal infections), injury requiring medical treatment, up to one day lost time	Severe but reversible health effects of concern (e.g. back/muscle strain, repetitive strain injury, nervous system effects, sunstroke, Hepatitis B & C, acute/short term effects of some chemicals (SO_2, solvents etc.), extensive injuries, hospitalisation, short term health problems to individual from 2 days up to one month	Irreversible health effects or concerns (e.g. noise induced hearing loss, vibration induced degeneration of muscles, bones, joints or peripheral nerves and blood vessels, broncho-pulmonary disease, occupational asthma, allergic skin diseases, cumulative lung damage), serious injuries, long term hospitalisation, long term health problems to individual from 2 months up to 12 months	Life threatening or disabling illness (e.g. respiratory disease, loss of limbs, eyes, paralysis, permanent disability), multiple injuries, extended hospitalisation or fatality, long term health problems to individual greater than 12 months
Damage / Loss (also refer to **Financial impact**	Ability to rectify/fix internally/on-site within 3 days	Ability to rectify/fix internally/on-site	Ability to rectify/fix internally/on-site	External rectification required; rectification	External rectification required; rectification exceeds 1 month

Aspect	Insignificant	Minor	Moderate	Major	Catastrophic
to assess any financial loss)		within 4 days up to 2 weeks	from 3 weeks up to 1 month	expected within 1 month	
Human resources	No change to expected staff turnover or key management positions	Minor impact to expected staff turnover or key management positions	Unexpected loss of a key senior manager, or significant staff turnover in key areas, inability to fill vacancies	Unexpected loss of up to two key senior or executive managers, or significant staff turnover in multiple areas, inability to fill vacancies	Unexpected loss of several key personnel/extensive staff turnover in excess of 50%
Natural Environment	Single on-site environmental incident, near-source confined and promptly reversible impact	Single or multiple on-site environmental incident(s) causing minor damage that is easily repairable	On-site environmental damage causing long term damage that is recoverable	Off-site impact with localised harm that can be recovered, e.g. contamination, spill, non-compliance. On-site event causing environmental harm that cannot be immediately recovered, e.g. groundwater contamination	Off-site impact with severe localised or chronic widespread harm, e.g. off-site soil and groundwater contamination. On-site impact with the potential to result in long term off-site harm, e.g. large oil spill, chemical contamination

Step 4. Risk matrix: inherent risks (pre-control risk rating)

	Consequence				
Likelihood	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Almost certain	M	M	H	E	E
Likely	M	M	H	E	E
Possible	L	M	M	H	E
Unlikely	L	L	M	H	H
Rare	L	L	L	M	H

Risk categories (risk rating)

Category	Description	Management actions
Extreme (E)	This is an unacceptable level of risk.	Strong control measures should be developed and implemented immediately, if not already in place. Ongoing monitoring is required at a senior management level. Regular reporting to RFM Board
High (H)	This is a high level of risk and, if not controlled adequately, has the potential to become extreme.	Regular review is required at a senior management level. Adequate controls should be in place and should be reinforced through training and supervision. Regular reporting to RFM Board
Moderate (M)	It is considered unlikely, though still possible, that a consequence may flow from an unattended risk.	Adequate controls should be in place, and management responsibility should be specified
Low (L)	The risk is considered minimal or insignificant.	Risks should be managed by routine procedures (RFM policies, procedures and other processes) and responsibilities should be clearly defined

Step 5. Risk treatment and control effectiveness

5. Risk treatment involves developing a range of options for mitigating the risk, assessing those options, and then preparing and implementing action plans. The highest rated risks should be addressed first. Selecting the most appropriate risk treatment means balancing the costs of implementing each activity against the benefits derived. Generally, the cost of managing the risks needs to be commensurate with the benefits obtained. When making cost versus benefit judgements the wider context should be taken into account. Depending on the type and nature of the risk, the following options are available:

Avoid	deciding not to proceed with the activity that introduced the unacceptable risk, choosing an alternative more acceptable activity that meets business objectives, or choosing an alternative less risk approach or process
Reduce	implementing a strategy that is designed to reduce the likelihood or consequence of the risk to an acceptable level, where elimination is considered to be excessive in terms of time or expense

Accept	making an informed decision that the risk rating is at an acceptable level or that the cost of the treatment outweighs the benefit. This option may also be relevant in situations where a residual risk remains after the other treatment options have been put in place. No further action is taken to treat the risk; however, ongoing monitoring is recommended

6. A range of treatments may be available for each risk and these options are not necessarily mutually exclusive or appropriate in all circumstances. Selection of the most appropriate risk treatment approach should be developed in consultation with relevant stakeholders and process owners.

7. The control effectiveness is a combination of all risk treatments to stop an event occurring, or to minimise the impact of an event that does occur. The control effectiveness should be rated in accordance with the table shown in this Step 5, and then the risk reassessed against the residual risk matrix in Step 6 to determine the residual risk rating.

Control effectiveness	Description
Non-existent	Controls do not exist or else are not operating effectively. Risk will not be controlled, or the Company has accepted the risk
Limited	Basic risk management systems, process controls and procedures are in place. There is no guarantee that risk will be controlled, or the Company has accepted the risk
Fair	Majority of risk management systems, process controls and procedures are in place. Risks will be controlled most of the time
Good	Risk management systems, process controls and procedures are in place and can be relied upon to prevent the risk materialising and/or mitigate the impact of the risk in most circumstances
Very good	Risk management systems, process controls and procedures are in place and can be relied upon to prevent the risk materialising and/or completely mitigate the impact of the risk

Step 6. Residual risk matrix (post control risk rating)

Control effectiveness	Risk Rating (Category)			
	Low	**Moderate**	**High**	**Extreme**
Non-existent	L	M	H	E
Limited	L	M	H	E
Fair	L	M	H	H
Good	L	L	M	H
Very good	L	L	L	L