Loreburn Group

Risk Management Policy

Creating Great Places to Live

Policy	Risk Management Policy														
Version Reference	2														
Approved by	MC X EMT ☐ MT☐														
Date of Approval	October 2018														
Review Period	Annual **or** as legislation or substantive changes occur														
Review Due	October 2019														
Policy Champion	Director of Finance and Corporate Services														
Who this policy affects	Staff	X	Customers	X	Contractors	X	Members of the Public	X							
Where this policy affects	General needs	X	Sheltered	X	Supported	X	Offices/staff base	X							

1. Purpose of Policy

1.1 This policy sits under the Risk Management Strategy which defines the Management Committee's appetite for risk as 'optimistic and risk aware'. This Policy provides a framework for the management of risk as a continuous process central to the achievement of our key objectives and the continuing success of the organisation.

1.2 This Policy defines processes for managing risk and promotes a positive culture where risk management is lived and understood at all levels of the business and embedded into everyday working practices.

2. Aims of this Policy

2.1 This policy aims to:

- Empower staff to identify and assess risks to make informed decisions
- Detail a clear process and framework for identifying, assessing, recording and monitoring risks
- Establish communication and escalation of risk information from staff to EMT and EMT to Management Committee
- Provide a framework for staff to enable Loreburn Group to embrace opportunities and become one of the best housing associations in Scotland.

2.2 This Policy and the management of risk is to be considered in all aspects of the business and alongside all existing strategies and policies.

3. What is Risk and how can it be addressed?

3.1 Risk is defined as an event that can have a negative impact. Conversely an event that can have a positive impact is an opportunity. Risks and opportunities are inevitably intertwined. In general, risks involving people and organisations occur because an opportunity is being sought. There are risks and opportunities associated with current activities together with anything new and untried. We are committed to embracing new opportunities and recognise that it will rarely be possible to remove all risk associated with new opportunities completely.

3.2 Taking risks in a controlled manner is essential to innovation and the building of the entrepreneurial culture we strive to achieve. Our aim is to identify, manage and minimise, rather than eliminate risks, which may prevent the organisation achieving its objectives.

3.3 There are four options to addressing risk:

- **Acceptance** - Risk acceptance does not reduce any effects however it is still considered a strategy. This strategy is a common option when the cost of other risk management options such as avoidance or limitation may outweigh the cost of the risk itself.

- **Avoidance** – Risk avoidance is the opposite of risk acceptance. It is the action that avoids any exposure to the risk whatsoever. Risk avoidance is usually the most expensive of all risk mitigation options.

- **Mitigation** - Risk mitigation is the most common risk management strategy. This strategy limits a company's exposure by taking some action. It is a strategy employing a bit of risk acceptance along with a bit of risk avoidance or an average of both. An example of risk limitation would be a company accepting that a disk drive may fail and avoiding a long period of failure by having backups.

- **Assignment** - Risk assignment is the involvement of handing risk off to a willing third party. For example, numerous companies outsource certain operations. This can be beneficial for a company if a transferred risk is not a core competency of that company. It can also be used so a company can focus more on their core competencies.

3.4 It is impossible to make an informed decision between these four options unless we fully understand the underlying risk, the probability that we will suffer harm and the potential loss that would result. Once we know the level the level of risk we can then perform a cost/benefit analysis to determine which of the four options above is the most practical.

4. Responsibilities

4.1 Responsibility for risk management is embedded across the organisation.

4.2 This culture is set through the Strategy and achieved through core briefings, team meetings and one to one sessions etc.

Management Committee

4.3 The Management Committee are responsible for setting the Risk Management Strategy and defining our 'risk appetite'.

4.4 The Management Committee will:

- Demonstrate high standards of corporate governance at all times, including using the Audit and Compliance Committee to help them address the key risks facing Loreburn Group.
- Ensuring that Loreburn Group's plans and finances are sufficiently robust to manage potential scenarios that would increase cumulative risk to the business.
- Manage financial risk through scenario planning and stress testing of annual 30 year financial plan.
- Review corporate risk at Management Committee Meetings.

4.5 Only risks with a certain inherent level on the register are highlighted to the Management Committee in line with the process detailed at 7.8 of this policy.

Audit and Compliance Committee

4.6 The Audit and Compliance Committee is responsible for ensuring proper arrangements exist for risk management and internal control.

4.7 It considers and advises the Management Committee on:

- The strategic processes and policies for risk, control and governance and compliance, prior to endorsement by the Management Committee.

- The promotion, co-ordination and monitoring of risk management activities, including regular review and input to the corporate risk map; and
- Assurances relating to the adequacy and governance processes for the organisation, with particular reference to the management of key risks to the achievement of objectives and targets.

4.8 The Audit and Compliance Committee will be provided with:

- A live review of the Corporate Risk Map that will be undertaken at each meeting; and
- Opportunities to review Loreburn Group's Risk Management Strategy and risk map and proposals for continuous improvement of the risk management process and culture as appropriate.

Executive Management Team

4.9 In managing risk the Executive Management Team are responsible for ensuring that:

- A system of risk management is maintained to inform decisions on financial and operational planning and to assist in achieving objectives and targets;
- The Management Committee are involved in the risk management system and the risk map.

4.10 This includes:

- Communicating the Risk Management Strategy and promoting the risk culture;
- Providing leadership and direction over the risk map; and
- Conducting an annual review of the effectiveness of the system of internal control
- Developing and implementing the process for risk management
- Maintaining the corporate risk map (via Risk Manager) which will be reviewed at EMT meetings through review of operational risk maps.
- Informing Management Committee of risks with an inherent score of 16 or greater at Management Committee Meetings.
- Informing Management Committee of the steps being taken to mitigate inherent risks with a score of 16 or higher.
- Informing Management Committee of any new severe risks (20 or higher) as soon as practicable.
- Facilitating discussions of risk with the management team as an integral part of the business plan process to establish residual and target risk scores where relevant.

Management Team

4.11 In Managing Risk all Managers are responsible for:

- Identifying and monitoring risks and maintaining operational risks maps (via Risk Manager). This is a live process however a review of the operational risk map is required to be completed **once a month as a minimum**.
- Highlighting any new or increased risk to their Director as soon as practicable after they are identified.
- Ensuring risks identified by any team members or customers are appropriately considered and added to the risk map as required.
- Embedding and inspiring a culture of risk management across their teams and ensure risk is discussed at team meetings and 1-2-1s.

- Considering whether risks identified at team level have the potential to impact other departments and raise with relevant managers and directors as soon as practicable.

All staff

4.12 The Strategy sets a risks management culture across the organisation and all staff have a responsibility to understand:

- The risks that relate to their roles and their activities
- How the management of risk relates to the success of the organisation
- How the management of risk helps them to achieve their own goals and objectives
- Their accountability for particular risks and how they can manage them
- How they can contribute to continuous improvement of risk management
- That risk management is a key part of the organisation's culture
- The need to report in a systematic and timely way to senior management any perceived new or emerging risks, near misses or failures of existing control measures within the parameters agreed.

Internal Audit

4.13 Internal Audit plays a key role in evaluation the effectiveness of, and recommending improvements to, the risk management process. This is based on the systematic review and evaluation of the policies, procedures and operations in place to:

- establish and monitor the achievement of the organisation's objectives;
- identify, assess and manage the risks to achieving the organisation's objectives;
- advise on, formulate, and evaluate policy;
- ensure the economical, effective and efficient use of resources;
- ensure compliance with established policies (including behavioural and ethical expectations), procedures, laws and regulations;
- safeguard the organisation's assets and interests from losses, including fraud, irregularity or corruption; and
- ensure the integrity and reliability of information, accounts and data, including internal and external reporting and accountability processes.

4.14 In addition, Internal Audit aims to add value through:

- supporting and facilitating the identification of risks and the development of processes and procedures to assess and effectively respond to risks;
- the identification and recommendation of potential process improvements;
- the provision of advice to manage risks in developing systems, processes, projects and procedures and
- the provision of best practice advice to all sections of the organisation; and encouraging best practice and embedding continuous improvement.

5. Risk Maps

5.1 Risk Manager software is used to produce risk maps which capture, monitor and assess risks throughout the organisation.

5.2 The Corporate Risk Map documents the risk assessment in order to:

- facilitate the identification of risk priorities;

- capture the reasons for decision made about what is and is not tolerable exposure;
- record the way in which it is decided to address risk;
- allow all those concerned with risk management to see the overall risk profile and how their areas of particular responsibility fit into it; and
- facilitate the review and monitoring of risks.

5.3 The Corporate Risk Map themes risks by type to enable Management Committee to view the cumulative risk associated with a business activity. Risk types include:

- Financial
- Safety / Compliance
- Service Delivery / Development
- Strategic / Governance
- Reputational

6. Identifying and Addressing Risk

6.1 The purpose of addressing risks is to turn uncertainty to Loreburn Group's benefit by constraining threats and taking advantage of opportunities. The appropriate response to each risk will depend on its nature and the outcome of the risk assessment.

6.2 Risk consists of two components:

- the probability that a negative or harmful event will occur;
- the amount of loss or expense that will result from the event.

6.3 There are also two kinds of risks considered. Inherent Risk and Residual Risk. The Inherent Risk is the risk at the time it is identified in it's raw or untreated form. The residual risk is the level of risk perceived once controls have been considered and put in place.

6.4 The prioritisation of risk is achieved through a series of questions:

- How important is the asset/issue/event?
- How vulnerable is the asset/issue/event to a negative affect?
- How likely it is that someone would try to exploit the vulnerabilities?
- What controls do we have in place to protect the asset/issue/event from these vulnerabilities?
- If the controls do not provide sufficient protection, what additional controls can Loreburn Group employee to reduce the risk to an acceptable level?

6.5 The answers to such questions shape the risk management approach when agree the likelihood and impact on the risk scale.

7. Assessing and Scoring Risk

7.1 As set out in the Risk Management Strategy the aim of the process and associated documents is not to remove all risk but to recognise that some level of risk will always exist. It is recognised that taking risks in a controlled manner is fundamental to innovation and the building of an entrepreneurial culture.

7.2 Risks will be scored by Managers and Executive Management Team using Risk Manager.

7.3 Risk is scored by allocation a score between 1 to 5 against the likelihood and impact of each risk as defined below:

Residual Likelihood	
1	Rare - Highly unlikely, but it may occur in exceptional circumstances. It could happen, but probably never will.
2	Unlikely - Not expected, but there is a slight possibility it may occur at some time.
3	Possible - The event might occur at some time as there is a history of occurrence here or in similar organisations.
4	Likely - There is a strong possibility the event will occur as there is a history of frequent occurrence here or in similar organisations.
5	Almost Certain - The event is expected to occur in most circumstances as there is a history of regular occurrence or it is already occuring.

Residual Impact	
1	Insignificant
2	Minor
3	Moderate
4	Major
5	Catastrophic

7.4 The risk owner is responsible for making this assessment. Risk Manager will calculate the overall inherent and residual risk score however the information is based on the Managers individual assessment of the risk likelihood and impact. Managers should seek advice from their Director as required when assessing and categorising levels of risk.

7.5 Failure to correctly assess risk at operational level may result in risks not being captured in the corporate risk map and may expose the organisation to significant risk.

7.6 Depending on the risk type (as set out at 5.3 of this policy), Risk Manager will provide further guidance on scoring by amending the likelihood and impact tables with expanding wording which will take account of the consequences of the nature of the risk i.e. where reputation is selected Risk Manager will prompt the scorer to consider negative media attention.

Calculating Risk

7.7 To calculate the risk, Risk Manager will first take the likelihood score and multiply this by the impact score. This will be done for both inherent and residual risk. For example:

A likelihood of **4** multiplied by an impact of **3** would give an overall risk of **12**, indicating moderate risk to the Association.

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

7.8 A table summarising the risk assessment totals can be found below. This table explains the further actions required at each level of risk:

Key	Inherent Score	Action	Escalation Procedure
Severe	20-25	Unacceptable level or risk exposure which requires immediate corrective action to be taken.	CEO to be notified immediately. CEO will notify Office Bearers as soon as possible. CEO and Office Bearers will agree if any regulatory notifications are required i.e. SHR, Care Inspectorate, HSE etc.
Major	16-19	Unacceptable level or risk exposure which requires constant active monitoring as well as measures to be put in place to reduce exposure.	EMT to be notified immediately. Relevant Director to advise CEO as soon as possible. EMT will advise Management Committee in line with reporting procedures at next possible Management Committee and Audit and Compliance Sub-Committee Meeting.
Moderate	11-15	Acceptable level or risk exposure subject to regular active monitoring measures.	Managers to add and monitor risks through Operational Risk Maps and advise relevant Director when a new moderate risk is added. EMT advised through Operational Risk Maps and Corporate Risk Map reviews at EMT meetings. Management Committee will not be notified of Moderate risks.
Minor	6-10	Acceptable level of risk subject to regular passive monitoring measures.	Managers to add and monitor risks through Operational Risk Maps. EMT advised through Operational Risk Maps and Corporate Risk Map reviews at EMT meetings
Insignificant	1-5	Acceptable level of risk subject to periodic passive monitoring measures	Managers to add and monitor risks through Operational Risk Maps. EMT advised through Operational Risk Maps and Corporate Risk Map reviews at EMT meetings

7.9 Loreburn will closely manage **all** inherent risks scoring **16+** and may not wish to tolerate risks scoring **20+** however each risk is assessed individually and discussed at Management Committee.

7.10 The Management Committee will focus on monitoring those strategic risks with a score of 16 or more on a monthly basis. The Audit and Compliance Committee will review and monitor the whole risk register on a quarterly basis. All Operational risks are reviewed at relevant Management Team and EMT Meetings as well as regular 1-2-1s and team meetings.

7.11 Loreburn Group's risk appetite is not necessarily static. The Management Committee may vary the amount of risk which it is prepared to take depending on the circumstances and the business opportunity.

8. Policy review

8.1 The policy champion is the Director of Finance and Corporate Services.

8.2 This policy will be reviewed by the Policy Champion **annually** or as required due to legislative or regulatory change, or increased risk within the business.

9. Equality and Diversity

9.1 There are many reasons why people may have difficulties accessing our services. These may include dyslexia, illiteracy, language barriers and illness. It is the duty of all staff to ensure these issues are taken into account to ensure that information is appropriately communicated in ways those individuals can understand.

9.2 Loreburn Group is committed to equality of opportunity and will ensure that policy and procedures will not unfairly discriminate against people on grounds of sex or marital status, racial grounds, disability, age sexual orientation, language or social origin, or of other personal attributes, including beliefs or opinions, such as religious beliefs or political opinions.

9.3 Loreburn Group can provide:

- Translation service for those for who English is not their first language.
- Large text or audio tapes for people who are visually impaired.
- Assistance for people who are profoundly deaf.
- Assistance for people who have challenges around literacy and / or numeracy

10. Responsibilities Chart

11.1 The chart below illustrates the responsibilities of all staff in relation to this policy:

Responsibilities	Board/ CEO	Audit & Compliance	EMT	DFCS	MT	All Staff
To set the policy and direction with regards to risk management	✓					
To monitor, manage and mitigate corporate risk	✓	✓	✓			
To support the Management Committee to deal with risk		✓	✓		✓	
Maintain and Monitor live Corporate Risk Map			✓			
Escalate new or increased risks to MC as per escalation procedure			✓			
Maintain live Operational Risk Maps with monthly review as minimum					✓	
Escalate new or increased risks to EMT as per escalation procedure					✓	
Use external auditors / resources to support LHA's risk management strategy		✓				
To monitor, manage and mitigate day to day corporate and operational risk			✓		✓	✓
Day to day operation of the risk management policy and actions					✓	✓
Ensure the approach meets the requirements of the Scottish Housing Regulator	✓	✓				
Policy Champion				✓		
Ensure Loreburn Group has a robust understanding and application of risk management policy		✓	✓		✓	
Ensure effective and clear communication with key stakeholders including customers			✓			
Working with OD/HR arrange appropriate training			✓		✓	
Working collaboratively with BI Team ensure robust risk management processes are applied					✓	
Ensure complaints feedback is used to improve service					✓	
Ensure policy is reviewed annually or as necessary				✓		

Glossary of Key Terms

Assurance	An evaluated opinion, based on evidence gained from review, on the organisation's governance, risk management and internal control framework.
Exposure	The consequences, as a combination of impact and likelihood, which may be experienced by the organisation if a specific risk is realised.
Impact	The probable effect on the organisation if the risk occurs.
Inherent Risk	The exposure arising from a specific risk before any action has been taken to manage it.
Likelihood	The probability or chance of the risk occurring.
Opportunity	An event that can have a positive impact.
Residual Risk	The exposure arising from a specific risk after action has been taken to manage it and making the assumption that the action is effective.
Risk	Risk is defined as an event that can have a negative impact.
Risk Appetite	The amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time.
Risk Assessment	The evaluation of risk with regard to the impact if the risk is realised, and the likelihood of the risk being realised progress.
Risk Management	All the processes involved identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress
Risk Map	The documented and prioritised overall assessment of the range of specific risks faced by Loreburn Group.
Risk Manager	Software used to capture, score and monitor risks. Available within Minute Pad.