

**Loreburn Group**

**Risk Management Policy**



**Creating Great Places to Live**

<b>Policy</b>	Risk Management							
<b>Version Reference</b>	3							
<b>Approved by</b>	Management Committee							
<b>Date of Approval</b>	November 2021							
<b>Review Period</b>	2 Yearly <b>or</b> as substantive changes occur							
<b>Review Due</b>	November 2023							
<b>Policy Champion</b>	Director of Finance & Corporate Services							
<b>Who this policy affects</b>	Staff	<input checked="" type="checkbox"/>	Customers	<input checked="" type="checkbox"/>	Contractors	<input checked="" type="checkbox"/>	Members of the Public	<input checked="" type="checkbox"/>
<b>Where this policy affects</b>	General needs	<input checked="" type="checkbox"/>	Sheltered	<input checked="" type="checkbox"/>	Supported	<input checked="" type="checkbox"/>	Offices/staff base	<input checked="" type="checkbox"/>

## 1. Purpose of the Policy

- 1.1. This policy sits under the Risk Management Strategy which defines the Management Committee's appetite for risk as:
  - Zero tolerance for activity which could result in failure to comply with relevant law and regulatory standards
  - Very low risk appetite for activities which could threaten the solvency, liquidity, reputation or long-term viability of the organisation
  - Medium risk appetite for activities which are expected to deliver reduced operating costs
  - A mixed approach to development risk depending type of project being undertaken
- 1.2. This Policy, and supporting procedure document, defines the organisational requirements for managing risk. It seeks to promote a positive culture where risk management is lived and understood at all levels of the business to ensure our corporate ambitions are achieved in a creative and innovative way.
- 1.3. To achieve our corporate ambitions this will involve a degree of risk and it is essential that these risks are identified, recorded, and actively managed.

## 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.
  - Set out clear roles and responsibilities in relation to risk management.
  - Set out how to identify, record and score risk and what actions need to be taken.
- 2.2. This policy, and the management of risk, is to be considered in all aspects of the business, alongside all existing strategies and policies. As such, all policies contain a section on Risk Management, which refers them to this policy.

## 3. Risk Management Framework

- 3.1. 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.
- 3.2. Loreburn's risk management framework is set out in its Risk Management Strategy. The framework is a tool to ensure managing risk is a continuous process and it becomes embedded within our systems to support decision making, create accountability and allows the business to evolve. The risk management framework is noted below.



3.3. We follow the framework so that we;

1. **Clarify Outcomes Required** – We are clear at the outset what it is we are trying to achieve. Our Corporate Plan provides this direction for corporate objectives.
2. **Identify and Record Risks** – Once we are clear on what we want to achieve will look at all the factors that can impact on success and recorded these as risks. We will use a variety of tools when assessing risk but would expect as a minimum that a SWOT and PEST analysis be completed.
3. **Manage Risk Controls and Actions Put in Place** – Once the barriers to success are identified we will seek to put controls and actions in place to minimise risk.  
The controls will seek to ensure the risk is mitigated to an acceptable residual level. Controls will be tested to ensure they work and operative as required.  
All controls will be clearly documented within our suite of policies and procedures and the review period of these documents forms part of control testing.  
Actions are put in place to either create additional controls, strengthen existing controls or to mitigate any inherent risk.
4. **Monitor Risk Management Actions** – The organisation adopts a culture of Monitor, Evaluate and Learn. Controls and actions need to be constantly monitored and evaluated for effectiveness. We should take any learning from this and make necessary changes.
5. **Adjust Risk Management if Required** – This forms the leaning part from point 4. Having monitored and evaluated the controls and actions we should take the learning from this and adjust our risk management process if required.

## 4. Responsibilities

- 4.1. To ensure the culture of risk management is achieved there are key sets of responsibilities within the organisation as follows;

### Management Committee

- 4.2. The Management Committee are responsible for setting the Risk Management Strategy and defining our 'risk appetite'.
- 4.3. 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 the organisation.
  - Ensuring that 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 high level risks at Management Committee Meetings.
  - Complete SWOT analysis at each strategic away day and discuss these.
- 4.4. Only risks with a certain residual level on the register are highlighted to the Management Committee in line with the process detailed at 4.10 of this policy.
- 4.5. Management Committee (and all sub-committee) will end each Board meeting by asking whether any of the discussions or decisions has had an impact on the risk profile and if so, the Risk Register will be amended.

#### Audit and Compliance Committee

- 4.6. The Audit and Compliance Committee is responsible for ensuring proper arrangements exist for risk management and internal control testing and review. They are responsible for noting and reviewing the Corporate Risk plan at each quarterly meeting. To do so the agenda for each meeting will be shaped around the corporate risk register.
- 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 the quarterly 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 report summarising any significant changes to the organisations Corporate Risks for each meeting; and
  - Opportunities to review the organisations Risk Management Strategy and risk map and proposals for continuous improvement of the risk management process and culture as appropriate.

#### Loreburn Executive Team (LET)

- 4.9. In managing risk the LET 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;

4.10. This includes:

- Communicating the Risk Management Strategy and promoting the risk culture;
- Providing leadership and direction; 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 LET meetings and taken to quarterly Audit and Compliance meetings for approval.
- Informing Management Committee of risks with a residual score of 16 or greater at Management Committee Meetings.
- 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.
- Descaling risks back down from the Corporate Risk register to the operational risk register after appropriate controls have been put in place.
- Holding quarterly review meetings with Risk Managers to review their risks.
- All papers prepared for board meetings outline the risks associated with the subject that is being presented, where applicable.

Heads of Service

4.11. In Managing Risk all Heads of Service are responsible for:

- Identifying and monitoring risks and maintaining operational risks maps (via Risk Manager). These are living documents which required to be update as required and at a minimum monthly.
- Highlighting any new or increased risk to their Director as soon as practicable after they are identified.
- Where major risk and above are identified these should be notified to the Director immediate for escalation onto the Corporate Risk Register.
- 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.
- 4.13. In line with the Risk Management Strategy and organisational values the organisation accepts that risks will have to be taken to achieve these objectives. So long as everyone follows this policy and procedure the risks can be mitigated to a manageable and acceptable level.
- 4.14. The organisation accepts failure may occur as we strive to achieve our ambitious objectives by seeking new innovative methods. The key is that we take the lessons from and failure and use this to grow the business going forward.

#### Internal Audit

- 4.15. 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.
- 4.16. 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.
- 4.17. The Audit and Compliance Committee are responsible for the Internal Audit. The Standing Orders set their responsibilities in relation to this.
- 4.18. The annual Internal Audit Plan will be shaped around the outcomes from implementing this policy as it will focus on the areas of high corporate risk.

## 5. Risk Maps

- 5.1. Loreburn will use Risk Management software to produce risk maps which capture, monitor, and assess risks throughout the organisation.
- 5.2. The champion for the risk map software is the Head of Finance & Procurement.
- 5.3. The Risk Map documents the risk assessment in order to:
  - establish what risks are corporate risks and what are operational risks;
  - 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.
- 5.4. The 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 Recording Risk

- 6.1. Identifying risk comes in many forms. Risks will be identified from:
  - Management Committee meetings
  - Sub-committee meetings
  - LET meetings
  - Management Team meetings
  - Team Meetings
  - Formal/Informal reviews
  - Ad Hoc meetings
  - Staff going about day-to-day activities
  - Trend analysis from parts of the business, ie Health and Safety/Finance etc
  - Changes in the external environment
  - Sector press
- 6.2. What is key is that staff understand a risk has arisen. A risk will have arisen if it has potential to impact on our ambitions within our strategic plan. 4.12 sets out all staff expectations around risk identification. Section 7.4 ensures risk is continually kept at the forefront off all of staff's minds.
- 6.3. When recording risk Loreburn considers three types of risk - Inherent Risk, Residual Risk and Target Risk.



- 6.4. Loreburn defines Inherent Risk as the current risk level given the existing set of controls rather than the hypothetical notion of an absence of any controls.
- 6.5. Residual risk is then whatever risk level remains after additional controls are applied.
- 6.6. Target risk is the target risk level we are aiming to achieve following completion of any actions.
- 6.7. The procedure document will provide guidance on this in practice.
- 6.8. When we identify and record the risk, we require the risk to be scored. This will be scored on a 1-5 scale on the likelihood and impact of each risk to give an overall rating. The scoring of the risk allows us to assess its impact on the organisation.
- 6.9. The risk owner is responsible for making this assessment. The Risk Manager software will calculate the overall inherent and residual risk score however the information is based on the risk owner's individual assessment of the risk likelihood and impact. Heads of Service should seek advice from their Director as required when assessing and categorising levels of risk. The procedure document provides further guidance on selecting the correct level of risk.
- 6.10. To calculate the risk, Risk Manager will first take the likelihood score and multiply this by the impact score. This will be done for inherent, residual and target 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

- 6.11. A table summarising the risk assessment totals can be found below. This table explains the further actions required at each level of risk when the **inherent** risk falls into one of these categories:

Key	Score	Action	Escalation Procedure
Severe	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. Will be recorded on the corporate risk register.

<b>Major</b>	15-20	Unacceptable level of risk exposure which requires constant active monitoring as well as measures to be put in place to reduce exposure.	LET to be notified immediately. Relevant Director to advise CEO as soon as possible. LET will advise Management Committee in line with reporting procedures at next possible Management Committee and Audit and Compliance Sub-Committee Meeting. This will be recorded on the corporate risk register.
<b>Moderate</b>	6-14	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.  LET advised through Operational Risk Maps and Corporate Risk Map reviews at LET meetings. If the risk scores a 12 or above and is of key strategic importance these risks may be included in the corporate risk register. LET will agree this at their review meeting.  Management Committee will not be notified of Moderate risks.
<b>Minor</b>	1-5	Acceptable level of risk subject to regular passive monitoring measures.	Managers to add and monitor risks through Operational Risk Maps. LET advised through Operational Risk Maps reviews with Heads of Service.

6.12. Through the corporate risk register LET 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.

6.13. The Management Committee will focus on monitoring those strategic risks with a score of 15 or more on a monthly basis. The Audit and Compliance Committee will review and monitor the whole Corporate risk register on a quarterly basis. All Operational risks are reviewed at LET Risk Meetings as well as regular 1-2-1s and team meetings.

## 7. Training & Induction

7.1. Management Committee training on Risk Management will form part of their annual refresher update. Training will be provided as and when required on any changes to the Risk Management software.

7.2. LET and Heads of Service will have an annual internal refresher session on this policy and supporting procedure document. This will be delivered by the policy champion. Training will be provided as and when required on any changes to the Risk Management software.

7.3. Any new members of LET, Heads of Service or Team Managers will have a session with the policy champion on this policy and our procedures in line with the new start induction programme. This includes any existing members of staff who are seconded or promoted to new roles.

- 7.4. All staff will have ongoing updates on Risk Management as part of team meetings, where Risk is discussed as a standing item on the agenda.

## 8. Equality & Human Rights

- 8.1. Loreburn aims to ensure that equality, fairness, dignity and respect are central to the way we work and how we treat our customers. We support diversity and uphold equal opportunities in all areas of our work as an employer and service provider.
- 8.2. Loreburn will not discriminate against tenants, staff, visitors, suppliers or others based on their age, sex, sexual orientation, race, disability, religion or belief, marital status, pregnancy and maternity or gender reassignment (collectively referred to as 'protected characteristics' in the Equality Act 2010).

## 9. Responsibilities Chart

- 9.1. The chart below illustrates the responsibilities of all staff in relation to this policy:

Responsibilities	Board/ CEO	Audit & Compliance	LET	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			✓			
Hold quarterly Operational Risk review meetings			✓	✓		
Maintain live Operational Risk Maps with monthly review as minimum					✓	
Escalate new or increased risks to LET 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 H A has a robust understanding and application of risk management policy		✓	✓		✓	
Ensure effective and clear communication with key stakeholders including customers			✓			
Working with P&C arrange appropriate training				✓	✓	
Ensure policy is reviewed annually or as necessary				✓		

## 10. Policy Review

- 10.1. The Policy Champion is the Director of Finance & Corporate Services.
- 10.2. The Policy Champion is responsible for completing the Health and Safety Assessment and Equality, Diversity and Inclusion Assessment Checklist.
- 10.3. This policy will be reviewed by the Policy Champion every 2 years or sooner as required due to legislative or substantive change.

## Policy Assessment Checklist

### Health & Safety Assessment

**Does this policy have the potential to affect:**

Lone Working	Yes
Safety and/or wellbeing of staff	Yes
Safety and/or wellbeing of customers	Yes
<b>Have the above items been considered in the preparation of this policy?</b>	Yes

**Comments:**

### Equality, Diversity & Inclusion Assessment

**Does this policy have the potential to affect:**

Staff's rights to equal opportunities	No
Tenants' / Customer's rights to equal opportunities	No
Tenants' / Customer's ability to access to homes and/or services	No
<b>Have the above items been considered in the preparation of this policy?</b>	Yes

**Comments:**

### Agile Working Assessment

**Agile working requirements have been considered and addressed in the preparation of this policy:** Yes