ATRIUM GROUP

Risk Management Policy

Atrium Group
Risk Management Policy

Compliant with Scottish Housing Regulator's Regulatory Framework:	1.1, 1.2, 1.4, 1.5, 2.2, 2.3, 2.5, 3.1, 3.2, 3.3, 3.4, 3.5, 3.7, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 5.1, 6.7
Compliant with Legislation:	The Housing Scotland Act 2010 The Scottish Social Housing Charter
Compliant with Tenant Engagement and Empowerment Strategy:	Yes
Compliant with Equal Opportunities:	Yes
Compliant with Business Plan:	Yes
Tenants/customers consulted:	N/A
Date Approved	November 2024
Date for Next Review:	November 2027 or earlier if required by changes in legislation or guidance, or if the Governing Body sees fit
Responsible Officer:	Finance & IT Manager and Chief Executive
The Risk Management Policy has a direct link to the following Atrium policies and procedures:	Atrium's Rules and Standing Orders Board Role and Responsibilities Remits for Finance, Audit & Staffing, Housing & Community Services and Property Services Sub-Committees Scheme of Delegation Procurement Policy Financial Regulations Internal Financial Procedures

1. Introduction

Atrium Group (hereafter referred to as 'Atrium') has a statutory responsibility to manage risks as stated in the SHR's Regulatory Framework Standard 4: the governing body bases its decisions on good quality information and advice and identifies and mitigates risk to the organisation's purpose.

Risk management is the planned and systematic approach to identification, evaluation and mitigation of risks.

Atrium recognises the importance of adopting a corporate approach to risk management. In determining the policy, Atrium aims to:

- ensure an appropriate attitude to risk based on the group's current risk appetite;
- be fully aware of the key risks it faces, including potential opportunities;
- ensure appropriate actions and responses have been determined to each risk and are being operated in full; and
- promote a culture of awareness through effective communication and training

The purpose of this risk management policy is to set out Atrium's approach to Risk Management and how this will be monitored to ensure the achievement of our stated business and strategic aims and objectives.

2. Risk Management Aims and Objectives

The objectives of Atrium's Risk Management Policy are to:

- raise awareness of the need for risk management and promote a risk management culture throughout the organisation;
- minimise loss, disruption, damage, and injury, and reduce the cost of risk;
- inform decision-making by identifying risks and their likely impact;
- support strategic and operational management through enhanced managerial control;
- improve financial management by enhancing financial controls and reducing the risk of losses; and
- enhance customer service by minimising service disruption and improving the organisation's reputation.

3. Risk Management Strategy

Atrium Homes is committed to a proactive and comprehensive risk management strategy that integrates with our overall strategic and operational planning. Our approach involves a continuous risk management cycle of identification, assessment, management, monitoring, and modification. This ensures that risks are anticipated,

evaluated, and mitigated effectively. By embedding risk management into our culture, we empower all staff to identify and address risks promptly, supporting our mission to provide quality affordable homes and sustainable communities.

We utilise a robust framework of controls in which controls are linked to a live Risk Register. Regular reviews of the Risk Register ensure alignment with our risk appetite and regulatory requirements.

Our strategy emphasises the importance of training, communication, and stakeholder engagement, fostering an environment where risk awareness and management are integral to decision-making processes and everyday operations. This holistic approach enhances our ability to achieve our corporate objectives while safeguarding our organisation's assets, reputation, and long-term viability.

4. Roles and Responsibilities

Board	– Responsibility for strategic risk lies with the governing body. – Receive reports from the Finance, Audit & Staffing Sub-Committee. – Set the organisation's risk appetite and review annually. – Approve the risk management policy.
Finance, Audit & Staffing Sub-Committee	– Review the strategic risks under their responsibility on a quarterly basis and report to Board. – Review deep dives on strategic risks completed periodically and receive feedback from other sub-committees on strategic risks within their area. – Ensure the organisation has an effective risk management framework in place. This should include ensuring that an operational risk register is in place and operating effectively.
All Sub-Committees	– Responsibility for managing strategic risks under their remit and reporting to FASSC on any emerging risks and controls which will be put in place to mitigate the risks. – Review of the strategic risks under their remit should be completed quarterly.
Executive Management Team	– Lead a culture of risk management and awareness including ensuring that staff receive training on risk management. – Identify strategic risks and determine actions to manage strategic risks. – Monitor progress in managing strategic risks and report to Board monthly and relevant Sub-Committee quarterly. – Responsible for reviewing and managing operational risks, ensuring that the operational risk register is up to date and that corresponding controls are operating effectively.
Finance & IT Manager	– Continuously improve risk management policy, strategy and supporting framework. – Prepare and put in place risk management training.

All Staff	− All staff are responsible for identifying and managing risk. − Risk will be considered in all service delivery and project plans. − Implement risk mitigating actions as instructed and follow organisational processes and procedures.
Internal Audit	− Provide advice and guidance for consideration on the management of risk relating to the design, implementation and operation of systems, procedures and controls.

5. Risk Appetite

Atrium operates in a highly regulated and evolving environment and has requirements placed upon it by the Scottish Housing Regulator (SHR), OSCR, the Information Commissioner, the Scottish Public Sector Ombudsman, HMRC and Companies House.

This means that the risk framework and risk appetite require frequent review. Atrium will review its risk appetite annually unless required to review it more frequently.

Board and management make decisions within Atrium's strategic framework which includes the Business Plan, Vision, Mission, Values and Risk Appetite.

Our vision is that Atrium Homes is synonymous with quality affordable homes, sustainable communities and life chances for people.

We will achieve this by focussing on four elements which are inter-connected:

- Taking care of our Customers
- Taking care of our Housing
- Taking care of our Communities
- Taking care of the Business

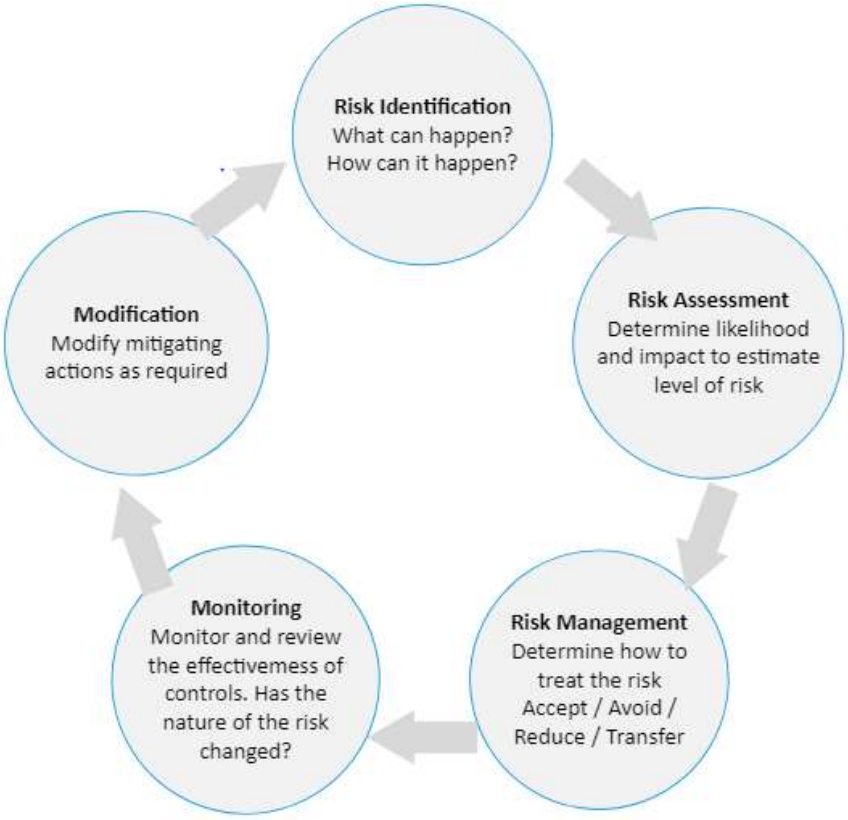
Tolerance for risk
Atrium has zero tolerance for activity which could result in failure to comply with relevant law and regulatory standards and a very low risk appetite for activities which could threaten the solvency, liquidity, reputation or long-term viability of the organisation.

Atrium will consider some risk with regard to growth and in particular development of new housing. Atrium continues to take a cautious approach to risk and has therefore planned to commit only to modest costs for site investigation and consultant input to establish the viability of new build sites within the current Business Plan.

Atrium uses key performance indicators, a compliance matrix, financial planning, stress / sensitivity testing, performance monitoring and the code of conduct to ensure compliance with the risk appetite.

6. Risk Management Methodology

The key stages of the risk management cycle are shown below.



Step 1 Risk Identification:

Risk identification is the first step in the risk management process. It involves recognising and understanding potential hazards that could adversely affect the organisation's objectives. The Executive Management Team (EMT) will lead the identification of both strategic and operational risks. This process includes:

- Strategic Reviews: Conducted during annual planning sessions, considering long-term objectives and external factors (e.g., political, economic, socio-demographic, technological, legislative, environmental, and competitive factors).
- Operational Reviews: Conducted regularly by the management team and staff to identify risks affecting daily operations (e.g. financial management, compliance, IT systems, physical security, and service delivery).
- Employee Input: Encouraging all staff to be risk-aware and report any emerging or observed risks to their line managers or directly to the EMT. This promotes a culture of proactive risk management.
- Stakeholder Engagement: Engaging with tenants, partners, and other stakeholders to identify external risks and opportunities.
- Environment Scanning: Monitoring changes in the regulatory, economic, and competitive environment to identify new or evolving risks.

EMT leads the identification of strategic and operational risks, incorporating them into all strategic or operational reviews and business planning processes. All staff are encouraged to be risk-aware and report any emerging risks.

Step 2 Risk Assessment:
Identified risks are assessed and added to the risk register, considering:

- Likelihood: The probability of an event occurring.
- Impact: The potential severity of the consequences.

Risks are scored based on likelihood and impact, resulting in inherent, residual, and target risk scores. The scores populate a risk matrix to determine priority.

Once risks have been identified, they are assessed to determine their potential likelihood and impact. This assessment helps prioritise risks and determine appropriate management actions.

Likelihood and Impact Scoring: Each risk is evaluated based on its likelihood of occurrence and potential impact.

- **Likelihood**: The probability of a risk event occurring, scored on a scale from 1 (rare) to 5 (almost certain).
- **Impact**: The severity of the consequences if the risk event occurs, scored on a scale from 1 (negligible) to 5 (catastrophic).

Likelihood Score	Description	Indicative Guidelines
5	Almost Certain	Event expected to occur; has occurred and will continue without action
4	Likely	Reasonable to expect event to occur; has occurred in the past
3	Possible	Little likelihood of occurring; external influences may affect controls
2	Unlikely	Risk probably won't materialise soon, but should be prepared for
1	Rare	Not expected to occur, but possible in exceptional circumstances

Impact Score	Description	Indicative Guidelines
5	Catastrophic	Urgent action needed; significant ongoing adverse impact; regulatory attention
4	Major	Action needed; major loss or disruption; regulatory scrutiny
3	Moderate	Requires attention by EMT; financial loss could affect Business Plan
2	Minor	Can be managed day-to-day; short-term operational impact
1	Negligible	Minor operational impact; no external publicity risk

Risk Scoring: Calculating a numerical risk score by multiplying the likelihood and impact scores (Inherent Risk Score). This score helps prioritise risks on the risk register.

Residual Risk: Evaluating the risk after existing controls and mitigating actions are applied. This involves reassessing the likelihood and impact considering the effectiveness of current controls (Residual Risk Score).

Target Risk: The desired level of risk that the organisation aims to achieve, reflecting its risk appetite.

Step 3 Risk Management:

The three main strategies for managing risk are:

1. Risk Mitigation: Implementing controls, policies, procedures, and other actions to reduce the likelihood and / or impact of risks. Examples include:
   - *Preventive Controls*: Implementing safeguards to prevent risk events (e.g., security systems, training programs).
   - *Detective Controls*: Establishing mechanisms to detect risk events when they occur (e.g., audits, monitoring systems).
   - *Corrective Controls*: Developing response plans to manage risk events after they occur (e.g., contingency plans, incident response teams).
2. Risk Transfer: Shifting the risk to another organisation through outsourcing, contracting, or insurance. This approach is useful for risks that can be managed more effectively by third parties.
3. Risk Avoidance: Opting not to engage in activities that are too risky and too costly to mitigate or insure against. This might involve discontinuing certain operations or projects that pose unacceptable risks.

Severe and high risks require immediate action plans, while medium risks require monitoring. Low risks are accepted without additional plans.

Risk management involves taking actions to minimise the likelihood of risk events occurring and / or reducing their impact if they do occur.

Step 4 Risk Monitoring:
The strategic risk register is reviewed quarterly by the EMT and Sub-Committees with relevant updates communicated to FASSC and the Board. The strategic risk register is considered at each Board meeting to provide Board with an opportunity to identify changing or emerging strategic risks outwith the Sub-Committee meeting cycles.

Effective risk management requires continuous monitoring to ensure that controls and mitigating actions are effective and that new risks are identified promptly. The monitoring process includes:

- **Quarterly Reviews**: The EMT and Sub-Committees review the risk register quarterly, assessing the effectiveness of risk management actions and controls, and identifying any new or emerging risks.
- **Reporting**: The strategic risk register is presented to FASSC quarterly, along with any severe risks and updates on the strategic risk register. Operational risk registers are reviewed by the EMT.
- **Performance Metrics**: Utilising key performance indicators (KPIs), compliance matrices, financial planning, stress testing, and performance monitoring to track compliance with the risk appetite and the effectiveness of risk management strategies.

See Appendix 1

Step 5 Risk Modification:
Risk scores and management actions are continuously modified based on ongoing assessment and emerging conditions.

Risk management is an ongoing process that requires regular adjustments based on monitoring outcomes. Modifications include:

- **Updating Risk Scores:** Revising likelihood and impact scores based on the latest information and the effectiveness of current controls.
- **Adjusting Controls**: Implementing new controls or modifying existing ones to address any gaps or weaknesses identified during monitoring.
- **Continuous Improvement:** Ensuring the risk management cycle of identification, assessment, management, monitoring, and modification is continuous and responsive to changing conditions.

7. Training and Communication

Training in risk management methodology is provided to all staff, who are encouraged to highlight risks to their line managers. Board members are also given risk management training. Regular communication ensures a culture of risk awareness.

8. Confidentiality and Data Protection

Confidential information is used solely for its intended purpose, stored securely, accessed only by authorised persons, and disposed of in accordance with the General Data Protection Regulations.

Appendix 1 - Risk Assessment Matrix

RISK MATRIX		Impact				
		Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Catastropic (5)
Likelihood	Almost Certain (5)	5	10	15	20	25
	Likely (4)	4	8	12	16	20
	Possible (3)	3	6	9	12	15
	Unlikely (2)	2	4	6	8	10
	Rare (1)	1	2	3	4	5

Severe	Risks which can have a catastrophic effect on operations and may result in significant financial loss or service disruption e.g. a major fire in the office
High	Risks which have a noriceable effect on services, organisational resources or reputation
Medium	Risks which have a noticeable effect on services and may have an adverse financial result e.g. short term IT system failure
Low	Risks where consequences are not severe and any associated loss is immaterial, e.g. minor incidents of vandalism