St George Housing

RISK MANAGEMENT POLICY

SEPTEMBER 2023

Contents

RISK MANAGEMENT POLICY

1. INTRODUCTION

1.1 This risk management policy outlines St George Housing Association's (SGH) commitment to managing risk in an effective and appropriate manner to enable the achievement of its business plan objectives. It is supported by other polices such as our risk profile overview, risk register and summary risks document. A template risk register can be found at the end of this policy.

2. POLICY STATEMENT

2.1 SGH will adopt best practice in the identification, evaluation and control of risks, to ensure they are managed effectively.

This will include:

- Having a clear understanding about risk management at all levels within the organisation.
- The Board accepting responsibility for active risk management.
- The delegation of clearly defined responsibilities from the Board to the Chief Executive and senior staff.
- Annually reviewing the control environment and the effectiveness of internal controls.
- Highlighting risk implications in all Board reports.
- Carrying out programmes for change and improvement in internal processes that concentrate on areas with risks that have been assessed as most significant.
- Meeting the regulatory requirements including compliance with the Regulatory Standards.

3. REGULATORY FRAMEWORK

3.1 This policy complies with Regulator of Social Housing (RSH) Standards and has taken into account the following codes of practice:

3.2 ISO 31000 is an international standard for risk management that provides guidelines, principles, and a framework for implementing effective risk management practices across the organisation.

3.3 AS/NZS 4360:1999 is a globally recognised standard for risk measurement and management.

4. SCOPE AND OBJECTIVES

4.1 This policy applies to all of SGH's activities.

4.2 The objective of this policy is to set out our approach to risk management across SGH and the processes we have put in place to ensure there is an effective, proactive and integrated framework for identifying and managing risks, thereby ensuring that the following objectives are achieved:

- Creating a robust control environment that reduces negative impact to our business plan objectives.
- Ensuring cross-cutting and cumulative risks are understood and properly managed.
- Ensuring that opportunities are properly maximised through the control of risk.
- Supporting informed risk-taking that promotes business growth while recognising the risks associated with key decisions.
- Anticipating and responding to changing social, environmental and legislative requirements.
- Improving accountability, decision making, transparency and visibility
- Improving risk leadership/capabilities in managing risk.

5. RISK APPETITE

5.1 Risk appetite may be defined as the amount of risk that an organisation is prepared to accept at any point in time. Risk appetite will be set by the Board and expressed as watershed beyond which the organisation will not go.

5.2 SGH is prepared to take some risks to achieve its objectives. However, as a not-for-profit organisation it will not put social housing assets at risk in order to secure higher financial returns.

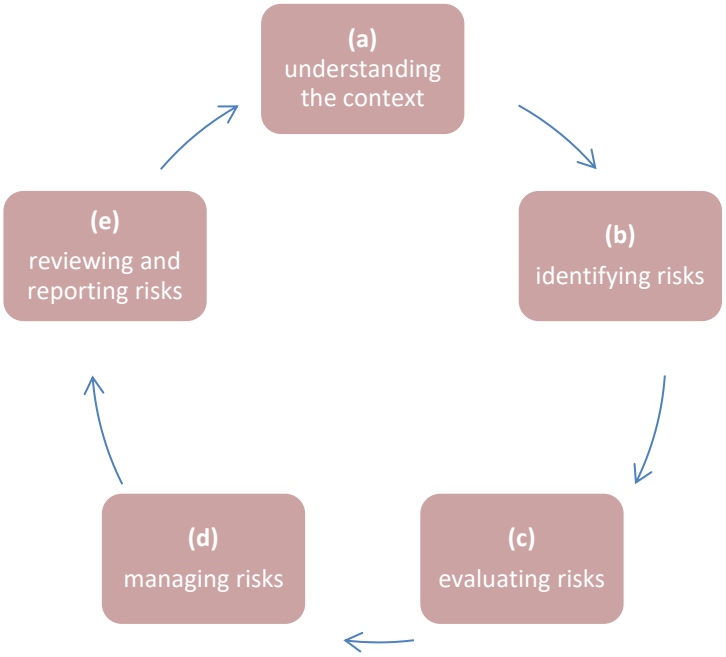
5.3 The Board will set the risk appetite and review it at least annually, usually as part of the annual business planning process, or as often as prevailing legislative or economic conditions dictate.

6. RISK MANAGEMENT GUIDANCE

6.1 This guidance aims to provide some best practice as to how risk management will function within SGH.

6.2 SGH'S risk management process follows the principles set out in the Risk Management Standard ISO 31000:2009. The 5 step process is as follows:

- Step 1: Establish the context
- Step 2: Identify risks
- Step 3: Evaluate risks
- Step 4: Treat/Manage risks
- Step 5: Report/Review Risks



7. STEP 1: ESTABLISHING THE CONTEXT

7.1 Context is very important in risk identification and management. It is important to consider required objectives, outcomes and goals when identify risks and risk actions.

7.2 Strategic objectives are documented in the strategic long-term and annual business plans. Annual plans also identify actions required in each area of the business.

7.3 Operational risks can be identified by operational teams in the context of the delivery of specialised functions or local services. Considering context will ensure that a resulting risk register is relevant and effective.

8. STEP 2: RISK IDENTIFICATION

8.1 Risk identification is the process of identifying risks which may impact on SGH's ability to achieve its objectives. The aim is to identify what, when, where, why and how events could prevent, degrade, delay or enhance achievement of objectives.

8.2 Risks can be identified from a number of sources including:

- Business planning
- Internal and external audit
- Complaints, adverse incidents and near misses
- Regulatory standards
- External review
- Risk assessment

8.3 There are many categories of risk including:

- Financial risk – threats to financial viability, loss of income, increased cost, fraud
- Strategic risk – threats to achieving business plan objectives
- Operational risk – threats to business continuity, security, contingency plans or of injury or death
- Legal risk – failure to adhere to statutory requirements, contractual disputes, civil action, criminal prosecution
- Reputational risk – adverse public/media comment, loss of tenant satisfaction/goodwill, partnership failure
- Regulatory risk – regulatory intervention, adverse public assessment
- Opportunity risk – loss of strategic, development or financial opportunity

Risk Descriptions

8.4 It is important that risk descriptions are both concise and contain sufficient information to allow a reader to understand the risk. The risk description should include:

- a summary of the cause of the risk ('as a result of')
- the circumstances in which the risk may occur ('we are unable to')
- a statement of the plausible reasonably impacts ('leading to').

8.5 Some examples of the descriptions above are detailed in the below table:

CAUSE	RISK	IMPACT
As a result of	**We are unable to**	**Leading to**
Failure of IT systems	Access tenant data	Service disruption
Poor compliance reporting	Meet our health & safety targets	Health & Safety non-compliance

c

8.6 When identifying risks, our risk identification process:

- Should identify risks that can be related back to our goals/ strategic high level outcomes
- Will name/describe the risk in negative terms e.g. 'loss of', 'failure of', 'ineffective', 'poor', 'failure of' etc;
- Will explain why it is a risk to our operations and identify the causes and consequences
- Is intended to focus on those risks most likely to occur or have a high impact, rather than trying to identify every possible risk
- Will assign clear responsibility for each risk to a risk manager (owner) who can monitor the risk and can take appropriate action
- Will not record any issues/risks that have already crystallised. However, a risk may be identified as a possible change in those existing circumstances.

8.7 Horizon scanning is the process of identifying, evaluating and managing changes in the risk environment, preferably before they manifest as a risk or become a threat to the Association. Issues identified through horizon scanning should link into and inform the business planning process. Horizon scanning can also identify positive areas for the Association to develop its business and services, taking opportunities where these arise.

9. STEP 3: EVALUATE RISK

9.1 When evaluating risk there are two prime areas of interest:

- How much of a detrimental effect could the risk have on the achievement of objectives – **impact**
- What is the probability of this happening – **likelihood**

9.2 Impact scores and guidance:

Score	Descriptor	Customers severely affected	Financial & Asset Loss	Health & Safety	Business interruption	Reputation & regulation
5	Catastrophic	>80%	>£15000 Complete asset loss	Multiple death; permanent disabilities	1 month	International news; regulatory intervention
4	Major	60-80%	<£15000 Significant asset loss	Single death; extensive injury	1 week	National news; regulatory engagement
3	Moderate	30-60%	<£3000 Major asset damage	Hospitalisation	4 days	Headline local article
2	Minor	5-30%	<£1000k Minor asset damage	Minor injury; medical treatment	1 day	Minor local article
1	Insignificant	<5%	<£250k No impact on assets	Minor injury; first aid	4 hours	No media coverage

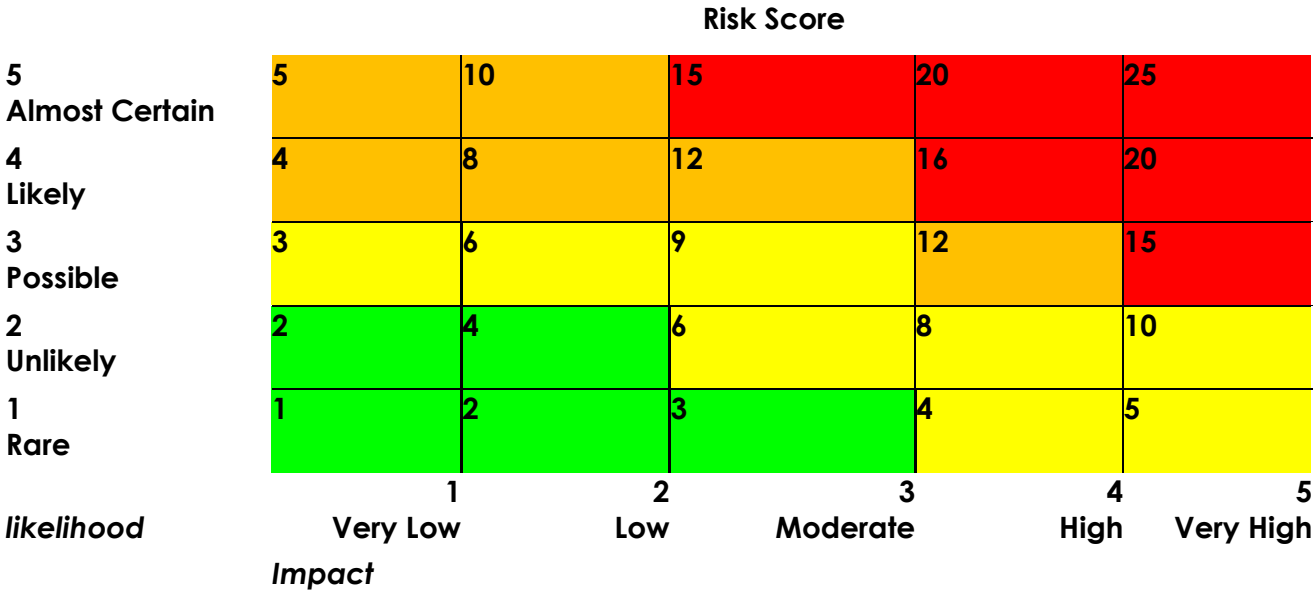
9.3 Likelihood scores and guidance

Score	Descriptor	How likely is it to happen?
5	Almost certain	>75%
4	Likely	51-75%
3	Possible	26-50%
2	Unlikely	10-25%
1	Rare	<10%

10. RISK PROFILE HEAT MAP

10.1 SGH uses a risk profile heat map to help identify and focus on the most significant risks.

10.2 The risk profile heat map clarifies the significance of risks and suggests priorities for addressing high risk exposures if these are not risks SGH is willing to tolerate. The "red zone" is high priority; "amber/yellow" is medium and "green" is low.



10.3 The 'gross risk score' is the rate the impact (I) or consequence of the risk happening and rate the likelihood (L) of the risk materialising before considering the effectiveness of SGH's systems of internal control. Multiply I x L and to calculate the risk score. Assign a colour using the risk profile heat map above.

11. STEP 4: TREAT/MANAGE RISKS

11.1 Not all risks can be dealt with in the same way. The '5 T's provide options for the management of risk:

- **Tolerate** – the likelihood and consequence of a particular risk happening is accepted.
- **Treat** – work is carried out to reduce the likelihood or consequence of the risk (this is the most common action).
- **Transfer** – shifting the responsibility or burden for loss to another party, e.g. the risk is insured against or subcontracted to another party.
- **Terminate** – an informed decision not to become involved in a risk situation, e.g. terminate the activity.
- **Take the opportunity** – actively taking the advantage, regarding the uncertainty as an opportunity to benefit.

11.2 In most cases the chosen option will be to treat the risk. When considering the action to take it is important to consider the cost associated with managing the risk, as this may have a bearing on the decision. The costs should be proportionate to the risk it is controlling. It is also important to consider whether the actions to manage the risk introduce new risks or affect other people or systems in ways that they need to be informed about.

Risk Management Controls

11.3 **Preventative Controls:** These are the steps taken to reduce the risk from occurring. The preventative control will usually act on the cause – not the risk.

11.4 **Recovery Controls:** These are steps taken to reduce the consequence or impact of the risk once it has crystallised.

11.5 Example of preventative and recovery controls:

Cause	Preventative controls	Risk	Recovery Controls	Impact of objectives
As a result of cyber attacks	Malware software	**We are unable to use our IT systems**	System data back-up	**Leading to system corruption and data loss**
As a result of high rent arrears	Income collection procedures	**We are unable to \meet our income targets**	Guaranteed rent insurance	**Leading to liquidity issues**

11.6 By identifying the CAUSE and IMPACT it becomes possible to identify preventative and recovery controls which in turn enables you to determine both the effectiveness and the cost of the control

11.7 Once preventative and recovery controls have been identified the risk score should be revaluated which should produce a lower 'Net' or 'Residual' risk.

11.8 The 'net' or 'residual' risk score is the rate the impact (I) or consequence of the risk happening and rate the likelihood (L) of the risk materialising after| considering the effectiveness of SGH's systems of internal control. Multiply I x L and to calculate the risk score. Assign a colour using the risk profile heat map above.

11.9 Contingency plans or management action plans should be developed and put in place for risks that have already occurred and cannot be prevented and risks that could materialise and are rated red or orange (extreme or high). Contingency plans should be recorded underneath the recovery controls on the register. Good risk management is about being risk aware and able to handle the risk, not risk averse.

11.10 A risk that has already occurred is no longer a risk but an issue. In other words, and issue is a risk that has already crystalised. The SGH risk management framework is designed to manage risk effectively in order eliminate or mitigate issues.

12. STEP 5: REPORT/REVIEW RISKS

12.1 Once a risk has been identified it should be recorded in a risk register. The SGH risk register has been designed to record risk and risk mitigation activity in a simplified manner that allows the monitoring of actions and aids decision-making.

12.2 Risk triggers should also be identified and recorded in the risk registers. Risk triggers are designed to provide early warning signs that a risk is becoming an issue.

12.3 The early warning indicators should be reviewed by the Board and SLT regularly to assess the proximity of these trigger points and/or if the future operating environment is becoming risker.

12.4 The Risk Register should be reviewed by the Board and the SLT regularly to ensure key risk remain relevant and risk scores appropriate.

12.5 All Board reports should evaluate if the reports content has any impact on SGH's current risk profile. This evaluation should be recorded in the report under the risk section. Any identified impact should be assessed against the risk register and any changes to the level of risk should be reported to the Board.

13. ROLES AND RESPONSIBILITIES

13.1 The Board

- Determine strategic approach to risk and set risk appetite
- Establish the structure for risk management
- Understand the most significant risks
- Gain assurance on the mitigation of risk and control the overall level of risk exposure.
- Review the risk management policy, strategy and framework
- Review risk on a quarterly basis
- Gain assurance on detailed risk management activity and the effectiveness of SGH's risk management activity.
- Confirmation statement on SGH's internal control environment in the annual accounts

13.2 CEO/SLT

- Build a risk aware culture within SGH
- Collectively own the corporate risk register and individually own key risk that fall under their specialism or area of oversight.
- Agree risk management performance targets
- Ensure implementation of risk mitigation strategies
- Identify and report changed circumstances / risks
- Develops the risk management policy and keep it up to date
- Documents the internal risk policies and structures
- Co-ordinate the risk management (and internal control) activities
- Compile risk information and prepares reports for the Board

- Individual members of staff/service delivery partners
- Understand, accept and implement risk management processes
- Comply with SGH's policies and procedures
- Report inefficient, unnecessary or unworkable controls
- Report loss events and near miss incidents

14. TRAINING

14.1 The training of staff is an integral part of SGH's approach to risk management. All new staff will be provided with risk management training. All Board members will receive annual risk management training in the format of a risk management awareness seminar co-ordinated by the Director of Governance.

15. EQUALITY IMPACT ASSESSMENT

15.1 In writing this policy we have carried out assessment to ensure that we are considering, equality, diversity and inclusion. Our assessments did not indicate that any group had been adversely impacted by our approach to risk management.

15.2 To request copies of these assessments, please contact info@stgeorgehousijng.co.uk

16. RELATED INTERNAL POLICIES

16.1 List all related internal policies

- Health & Safety policies
- Complaints Policy
- Whistle Blowing Policy
- Data Protection and GDPR Policy
- Business Continuity Policy and Plan
- Risk Appetite Statement
- Risk Profile Overview

17. CONSULTATION

17.1 This policy will be reviewed in consultation with staff.

18. REVIEW AND APPROVAL

18.1 This policy will be reviewed at least every two years or as required to take into account changes in legislation.

Responsible officer: Director of Governance
Policy Author: Director of Governance
Policy version: V1
Date of Board Approval: September 2023
Date the next review is due: September 2025

19. DEFINITIONS

Assurance	**External evidence that risks are being effectively managed Assurance provides confidence, evidence and certainty to the Board and management that what needs to be happening is actually happening in practice.**
Control(s)	Actions in place to manage the risk to reduce the likelihood and / or consequence of that risk.
Internal Control	A method of restraint or check used to ensure that systems and processes operate as intended and in doing so mitigate risks to the Association. Controls are the result of robust planning and good direction by management. If a control is not working effectively then it is not a control.
Gross Risk	the level of risk before any control activities are applied.
Impact	The potential consequence if the adverse effect occurs because of the hazard.
Likelihood	the chance or possibility of something happening.
Net Risk	The current risk 'left over' after controls, actions or contingency plans have been put in place.
Risk	The chance of something happening that will have an adverse impact on the achievement of SGH's objectives and the delivery of good quality and safe services.
Risk Appetite	The level of risk the SGH Board is prepared to accept, tolerate or be exposed to at any point in time.
Risk Capacity	Maximum level of risk to which the Association should be exposed, having regard to the financial and other resources available.
Risk Management	All the processes involved in identifying, assessing and judging risks, assigning ownership, taking actions to mitigate and anticipate them, and monitoring and reviewing progress'.
Risk Maturity	The overall quality of the risk management framework.
Risk Owner	The individual who is responsible for the management and control of all aspects of individual risks. This is not necessarily the same as the action owner, as actions may be delegated.
Risk Profile	The overall exposure of the Association to risks (or a given level of the organisation).
Risk Rating	The total risk score worked out by identifying the consequence and likelihood scores and cross referencing the scores on the risk matrix.
Risk Register	The tool for recording identified risks and monitoring actions and plans against them.
Risk Tolerance	The boundaries of risk taking outside of which SGH is not prepared to venture in the pursuit of its objectives.