# Risk Management Policy

**Policy Ref: CS8**

| | |
|---|---|
| **Prepared By** | Chief Executive |
| **Date of Review** | May 2021 |
| **Date of Next Review** | May 2024 |
| **Reviewed By** | PHA Board |

# 1 Introduction

1.1 All businesses are constantly faced with a multitude of risks. Within Partick Housing Association (PHA), and our subsidiary Partick Works Limited (PWL), we need to strike the correct balance between managing risk and potential reward. It is important to have an understanding of our risk appetite and the major risks associated with our business operations, so that we can manage them to our advantage.

1.2 Some risks are minor and therefore insignificant. Other risks have the potential to affect seriously our business's continued well-being. So it is important to understand the likelihood and potential impact of our risks and to take sensible, cost effective mitigation measures for those that are more significant.

1.3 We have a duty of care to our customers, staff, wider stakeholders and assets. We meet this duty by ensuring that risk management plays an integral part in the day-to-day management of our business, at both a strategic and operational level. Staff must understand the nature of the risks and accept responsibility for those associated with their area of control and authority so that they can provide assurance to Board members that such risks are managed effectively.

1.4 This policy describes PHA's approach to managing the risks inherent within our current and future activities and how we control and monitor these risks.

# 2 Aims and Objectives

2.1 Our aim is to manage our risk effectively to achieve the following objectives:

- A resilient business;
- Ability to achieve strategic objectives;
- Evidence-based decision making;
- Protection of reputation, financial resources and assets;
- Service and performance improvements;
- Ability to capitalise on business opportunities;
- Reduced overheads through smarter working – less remedial action or abortive works; and
- Fewer nasty surprises.

2.2 All business undertaken by PHA reflects our Group Corporate Plan, associated strategies, policies and service improvement plans. All risks therefore link back to the strategic themes of our business. Integrating risk management into the way that we deliver services is essential for the achievement of our vision, values and ambitions.

## 3 What is a Risk?

3.1 A ‘risk’ is essentially a potential future problem or opportunity. Every decision that we make or action that we take contains some element of risk.

3.2 Risks arise when the vulnerabilities in our systems, processes, facilities or resources are exploited by or exposed to threats. Examples might include the hacker who exploits the vulnerabilities in our IT security system, or a fire that starts due to an electrical fault and spreads because of weaknesses in our fire detection systems, errors made by inexperienced or insufficiently trained staff, or a whole host of other things.

3.3 The following table includes some examples of the possible risks that could affect PHA.

| | | |
|---|---|---|
| • Fire | • Flood | • Computer failure/ data loss |
| • Theft | • Bad debts | • Failure to exploit opportunities |
| • Workplace accidents | • Equipment failure | • Contractor failure |
| • Loss of key staff | • Power failure | • Fraud |
| • Interest rate fluctuations | • Human error | • Breach of contracts/ disputes |
| • Negative cash flow | • Pollution/ contamination | • Design defects |
| • Breach of regulation | • Litigation | • Vandalism |
| • Business failure | • Negative publicity | • Insolvency |

3.4 Risks can arise as a result of our own business activities or due to external factors such as legislation, market forces, the activities of others, or even the weather. They can be a product of the business environment, the natural environment, the political or economic climate or of human failings or errors.

3.5 Ultimately risk may impact on our business objectives or even threaten the business itself. Investing time and effort in managing our risks is an important investment and makes sound business sense. Effective risk management could be the difference between the survival and failure of our business.

3.6 It is not possible to create a completely risk-free environment, but we can manage risk effectively. We can identify risks, quantify them and once we understand what we are up against, we can make informed, considered decisions regarding what (if anything) to do about them.

## 4 Risk Management process

4.1 There are four stages to the risk management process, which are detailed in the diagram below


**Stage 1 – Identifying Risks**

4.2 Before we can take any meaningful action to address our risks we need to know what we are up against. So we need to identify the risks that we face. We must concentrate on the risks to the most important parts of our business or to its critical assets. These could include:

**Strategic Risk**, such as those associated with:

- Business planning and future direction;
- Achievement of strategic objectives;
- Business growth;
- Mergers, takeovers and alliances; or
- Litigation.

**Operational Risk**, such as those associated with:

- Service delivery;
- Financial/ commercial risks;
- Regulatory/ compliance risks;
- Health and safety risks;
- Personnel risks;
- Technology risks; or
- Project risks.

**Stage 2 – Assessing Risks**

4.3 Once we have identified our risks we need to assess them. We are most interested in those risks that we consider to be significant enough to do something about, so we need to separate these out. We do this by assessing the **likelihood** of the risk occurring and the **impact** if it does.

4.4 Our vulnerability to any particular risk is a combination of the ***likelihood*** of the risk materialising and the ***impact*** if it does. When determining this, we use a simple scale shown below:

| Likelihood | Score | | Impact | Score |
|---|---|---|---|---|
| Almost Certain | 5 | | Catastrophic | 5 |
| Likely | 4 | | Major | 4 |
| Possible | 3 | | Moderate | 3 |
| Unlikely | 2 | | Minor | 2 |
| Rare | 1 | | Insignificant | 1 |

4.5 When considering likelihood this can be based upon statistical information or evidence, but generally it is an experienced and sensible assumption.

4.6 Following scoring, the likelihood and impact scores are multiplied together. For example if a risk was almost certain and the impact was catastrophic the score would be 5 x 5 = 25. This allows us to then consider which risks are significant enough to do something about, as shown within the matrix below.

| | | LIKELIHOOD | | | | |
|---|---|---|---|---|---|---|
| | | Rare (1) | Unlikely (2) | Possible (3) | Likely (4) | Almost Certain (5) |
| IMPACT | Insignificant (1) | **1** | **2** | **3** | **4** | **5** |
| | Minor (2) | **2** | **4** | **6** | **8** | **10** |
| | Moderate (3) | **3** | **6** | **9** | **12** | **15** |
| | Major (4) | **4** | **8** | **12** | **16** | **20** |
| | Catastrophic (5) | **5** | **10** | **15** | **20** | **25** |

**Overall Rating**

| Low | Medium | High |
|---|---|---|

4.7 The risk rating and traffic light colour coding (Red, Amber and Green – 'RAG') indicates the seriousness and priority for action for any given risks, and this is carried through to the Risk Registers.

4.8 Our Risk Registers detail the following key areas:

- Risk reference;
- Risk category;
- Description and Impact of Risk;
- Risk Owner;
- Inherent Likelihood;
- Inherent Impact;
- Total Inherent Risk Rating Before Mitigation;
- Mitigation/Control Measures;
- Residual Likelihood;
- Residual Impact;
- Total Residual Risk Rating After Mitigation;
- Assurance Level;
- Assurance and Quarterly Review Updates; and
- Last Updated.

4.9 We quantify risks both before and after mitigation, so that we can determine the effectiveness of the control measures in place. The 'pre mitigation' risk is always scored on the assumption that nothing has been done or been put in place as a starting point. This ensures consistency of scoring across the business.

**Stage 3 – Treating Risks**

4.10 Once we have assessed the various risks to our business we can then decide what to do about them. We can start to treat them by identifying and implementing possible 'mitigation' measures – i.e. methods of removing, reducing, controlling or recovering from adverse events. Having determined which mitigation measures we feel are sensible and cost effective and decided which ones we want to invest in, we must go ahead and implement them.

4.11 The responses to our various risks can broadly be divided into four categories, although some risks may cross over. Our ultimate aim is to select and implement measures that reduce the likelihood or impact (or both) to a level that PHA is prepared to accept.

| | | **LIKELIHOOD** | |
|---|---|---|---|
| | | Low | High |
| **IMPACT** | High | **Insure/ Contingency Plan** | **Reduce/ Transfer** |
| | Low | **Accept** | **Manage** |

- **<u>Accept</u>** ***(low likelihood and low impact)***

  If the likelihood is low and the impact is low, it may be a perfectly reasonable decision to do nothing and to accept certain risks. Also, the fact that many risks cannot be completely eliminated means that there is likely to be a level of residual risk remaining, even after implementing our mitigation measures. The ultimate aim of an effective risk management process is to reduce all of our risks to a level that we are willing to accept.

- **Manage** ***(high likelihood and low impact)***

  For risks with a low impact but a higher likelihood, a sensible approach might be to manage and control them, for instance by improving and documenting processes, by providing training or putting in place controls and procedures to monitor the situation.

- **Insure/Contingency Planning** ***(low likelihood and high impact)***

  If the likelihood is low but the impact is high (such as loss of operational capability, serious damage to our business, large financial losses or even complete failure), contingency plans should be developed. These are referred to within our Business Continuity Policy which seeks to ensure that our business critical functions or processes can continue to an acceptable level, perhaps emergency level, in the event of some sort of catastrophic disaster.

- **Reduce/transfer** ***(high likelihood and high impact)***

  For risks with a high likelihood and a high impact, risk reduction measures are absolutely essential. For instance, hazardous or dangerous procedures should be modified, monitored or outsourced to someone more qualified or better equipped to carry them out safely. This can also be achieved by taking out insurance for some areas, but consideration must be given to the non-financial aspects of the risks.

4.12 For risks that PHA is unable or unwilling to accept, there are numerous possible mitigation measures that we can consider within the categories above. These mitigation measures will vary depending upon the type of risk, its rating, the appetite for risk and budgets.

4.13 Once the mitigation measures have been identified, it is important that we manage the implementation of these properly. This is done through the management of risk registers, which summarise the risks and opportunities identified, along with likelihood and impact (before and after mitigation), mitigation measures, actions taken and the current status of these.

4.14 The risk registers are working documents and are regularly reviewed and updated. Within PHA we have a Strategic Risk Register along with an Operational Risk Register. There are also standalone risk registers for specific projects or pieces of work (e.g. every new housing supply project) that may feed into either the Strategic or Operational Risk registers.

**Stage 4 – Monitoring and Reviewing Risks**

4.15 The final stage in the risk management process includes us monitoring the effectiveness, or otherwise, of the controls that we put in place.

4.16 As well as reviewing the effectiveness of the risk control measures, and identifying changes or improvements to existing mitigation measures, regular monitoring and review ensures that new and emerging risks, changes to existing risks and new opportunities are identified and addressed appropriately. The risk review process for PHA is summarised below.

| What? | Who? | When? | How? |
|---|---|---|---|
| Strategic Risk Register | Board | Annually | Consideration of risk appetite, review mitigation measures, changes to scoring and new risks. |
| Strategic Risk Register | Audit & Risk Committee | Quarterly | Review system and ensure that being reviewed accordingly by Board and staff. |
| Strategic Risk Register | Leadership Team | Quarterly | Consideration of existing and new risks, re-scoring of risks, escalation and de-escalation of strategic/operational risks. |
| Operational Risk Registers | Chief Executive | Annually | Annual assurance of management systems to Board/Audit Committee. |
| Operational Risk Registers | Leadership Team | Monthly | Review of functional operational risk registers at monthly one-to-ones. |
| Operational Risk Registers | Management Team | Monthly | Review of functional operational risk registers. |
| Operational Risk Registers | Team Meetings | Quarterly | Review of functional operational risk registers. |
| Individual Activity Plans | All Staff | Annually | Creation of individual plans and identification of associated risks. Monitored at monthly one to ones. |

## 5 Risk appetite

5.1 PHA has a corporate 'risk appetite' which dictates the types and levels of risk that the organisation is willing to take or to accept. One of the key roles of the Board is to decide on the level of risk that the business is willing to take in seeking to take forward opportunities. It can be difficult to define the corporate risk appetite and put it into words, because it can be quite subjective and change depending upon factors such as the prevailing business environment, the timing, personal experiences, or professional (or emotional) judgment.

5.2 The way in which the Board determines its corporate risk appetite is through the review of its risk matrix at 4.6 above. The traffic light ratings set the boundaries for the level of risks and for these to be quantified and considered in more detail. Risk appetite will be considered within the context of the strategic objectives and outcomes set out within the Group Corporate Plan.

5.3 We will prepare a Risk Appetite Statement, which we will review and update annually to reflect any relevant changes in our corporate strategy or operating environment.

## 6 Risk awareness culture

6.1 Successful organisations embed risk management into their culture – where Board support is visible, where risks and associated mitigation measures are identified at all levels, where risk registers are maintained by the Leadership Team and Management Team and where risk management is seen by all employees as a normal part of the way they do their jobs. As a result various people within the organisation have various responsibilities:

**The Board**

- Agree and set the Risk Management Policy;
- Visibly support the risk management process;
- Set and communicate the organisation's risk appetite (acceptable levels of risk);
- Be aware of strategic risks facing the business; and
- Report to customers on the effectiveness of the risk management process in achieving the strategic objectives.

**Audit Committee**

- Monitor the effectiveness of the Risk Management Policy; and
- Seek assurance on the effectiveness of internal controls.

**Leadership Team**

- Establish a risk management process;
- Support and facilitate the risk management process;

- Report on the status of key risks and mitigation measures to the Board and Audit & Risk Committee as appropriate;
- Consider escalation and de-escalation of risks and reporting of these to the Board; and
- Ensure appropriate levels of awareness and involvement throughout the business.

**Management Team**

- Be aware of the risks within their particular function;
- Apply the risk management process to identify significant risks and implement or recommend mitigation measures;
- Manage risks on a day-to-day basis;
- Facilitate staff awareness; and
- Report on the status of risks and mitigation measures to the Leadership Team.

**All Staff**

- Understand role, responsibilities and accountabilities within the risk management process;
- Identify and rate risks and suggest possible mitigation measures through Individual and Team Activity Plans; and
- Report on the status of risks and mitigation measures to the Management Team and Leadership Team.

## 7 Policy review

7.1 This Policy will be reviewed every three years, or sooner if required.