Uppingham Homes CLT

Risk Management Policy

1. Introduction

1.1 Risks are a normal aspect of any business. A risk is a potential impact which may affect the business negatively. It may have a financial, health or reputational impact. It may limit the ability of The Society to achieve its objectives. It may reduce future opportunities or restrict the ability to achieve objectives. Anything that may have a significant negative impact on the organisation can be considered as a risk.

1.2 Uppingham Homes CLT ('The Society') considers the active management of Risk to be an essential management practice.

1.3 The Board will actively:

- identify risks to its business model
- quantify their potential impact
- determine the likelihood of occurrence
- categorise identified risks according to their overall risk score
- manage these risks
- identify and implement risk mitigation
- identify key controls
- monitor key controls
- use risk management tools
- report risk positions regularly
- report and assess incidents and risk events

1.4 The purpose of active risk management is to:

- protect the future of the organisation
- maximise the potential for plans to be achieved
- meet legal and compliance requirements
- ensure that controls are effective

2. Identifying Risks to The Society

2.1 Uppingham Homes CLT seeks to identify and openly report all significant risks to ensure that risks are understood and so that mitigating action is prioritised accordingly. This is achieved by maintaining a register of significant risks which is reviewed at least quarterly by the Board and also updated when a new significant risk is identified.

2.2 For each risk identified on The Register of Significant Risks ('Risk Register') information is recorded to allow for the quantification of risk and where relevant, the mitigants, controls, ownership and actions taking place to manage the risk.

2.3 The Board will define, from time to time, a formal risk appetite statement in connection with specific risk areas as part of its approach to general risk mitigation.

3. Quantifying Impact, Determining Likelihood and Deriving Risk Scores

3.1 The impact of a risk will be assessed against a banded points scale which will be clearly indicated on the Risk Register. The scale will take account of the size and reserves of the organisation, reflecting the fact that a small impact can have a significant effect on a small organisation.

3.2 A Gross Risk Score will be derived from the combined Impact and Likelihood of the risk and the score will determine the overall seriousness of the risk which will be RAG (Red: Amber : Green) rated. The break-points for RAG rating will be clearly identified on the Risk Register.

3.3 Mitigations will typically either reduce the likelihood of a risk impact or reduce the impact should a risk event occur.

3.4 If mitigations are already in place, these will be noted in the Risk Register and a Net Risk Score will be calculated based on the scenario for that risk assuming that the mitigating actions or mitigating controls are effective.

4. Managing Risks

4.1 A board director will be appointed with responsibility for maintaining the Risk Register.

4.2 For Low Gross Risks (RAG=Green) no further action will be required other than recording on the Risk Register.

4.3 For High Gross Risks (RAG=Red) and Medium Gross Risks (RAG=Amber), a specific board member will be identified as the owner of the risk and mitigating actions and mitigating controls will be identified and noted in the Risk Register.

R4.4 For each High Risk, where possible, early warning indicators will be developed to give the Board the earliest possible indication of an incident.

4.5 Key Controls are defined as those controls which need to be effective to reduce the level of risk (from Gross to Net) to be within the risk appetite of The Society.

4.6 A register of key controls will be kept with a testing frequency identified. A board member will be identified as responsible for the independent testing of the key control. When a control is tested it will be assessed as E/N/I (Effective, Needs Improvement or Ineffective). For Needs Improvement or Ineffective, an action plan will be agreed and implemented.

5. Reputation Risk Management

5.1 The Society considers it important to manage the reputation of the organisation and be aware of events which impact positively and negatively on that reputation. The Society will, through its management processes, seek to maintain a positive reputation and will actively manage risks which might negatively affect that reputation.

6. Incident Management and Risk Events

6.1 An incident is defined as any major issue occurring which was, or could have been, identified as a significant risk to The Society. (A low impact realisation of a risk would be termed a “risk event” rather than an incident).

6.2 Incidents will be reported to board members by email within 24 hours of them occurring.

6.3 An incident report will be prepared by the relevant board member and will be reviewed at the next convenient board meeting. The report will include a description of the circumstances, the root cause, the impact on the organisation, any failures of controls leading up to the incident and recommendations for restorative and preventative actions.

6.4 Risk events will be recorded and reported to the Board on a regular basis subject to a materiality level set from time to time.

7. 1 in 100 Year Assessment

7.1 The Society will develop a set of negatively impacting scenarios that are likely only to happen rarely (typically once in 100 years) and will develop high level response plans to ensure that the organisation is prepared for responses to such events.   These will include assessments and high level plans for such incidents as fire, flood, serious criminal damage, rioting, loss of life.