



Unit 6B (5) Hopton Industrial Estate, Devizes, Wiltshire, SN10 2EU

Tel: 01380720722/720200

www.kfr.co.uk

Charity Registration No. 1056649

Company Registration No. 3213883

RISK POLICY

1. Purpose

- 1.1. Every company carries risk across a wide variety of activities, from strategic risks to operational risks. Good company management requires that all risks are identified, analysed and monitored to ensure that a company understands its risk exposure and acts accordingly.
- 1.2. Risk management should be proportionate and appropriate, depending on the size and extent of the company, whilst maintaining the integrity of a viable risk framework.
- 1.3. The role of risk management is summarised in Appendix 1.
- 1.4. KFR takes the management of risk seriously. This policy sets out KFR's approach to risk management and introduces the company's risk taxonomy.

2. Approach

- 2.1. KFR's approach to risk management is formed around four risk pillars or groups of risks, also known as Level One risks. These are Operational Risks, Business and Strategic Risks, Funding and P&L Risks and Regulatory Risks.
- 2.2. Each pillar, or Level One risk, is broken down into its component risks (Level Two risks), with some of those risks being further broken down (Level Three risks).
- 2.3. All risks are owned by the most senior executive, currently the company's General Manager, who is accountable for the operational effectiveness of the risk framework. The General Manager has the authority to delegate responsibility for the management of groups of risks, or indeed individual risks, to a member of the supervisory team. Accountability, however, always remains with the General Manager.
- 2.4. Practical support is provided by the trustee board to the General Manager through each risk pillar being oversighted by a trustee, who, at least annually, reviews the pillar and confirms to the trustee board that the risks in the pillar are relevant, and appropriately described and scored, and that the risk controls are being observed. The trustee may propose changes to the content of the pillar.

3. The Risk Taxonomy

- 3.1. The risk taxonomy is maintained by an individual trustee, currently the Chair of Trustees, in an Excel spreadsheet. The taxonomy is updated after each pillar review.

- 3.2. The Level Two risks in the pillars are as follows:
 - 3.2.1. Business and Strategic Risks: Planning, Strategic, Legal, Fraud, Key Persons, Business Continuity, Organisational, Premises, and Technology
 - 3.2.2. Funding and P&L Risks: Income Source, Market Source, Gross Margin (budgeted surplus/deficit), and Competitor Impact
 - 3.2.3. Operational Risks: Colleagues, Information Security, Financial Management, Delivery, Vulnerable Adults, and Health and Safety
 - 3.2.4. Regulatory Risks: Charity Commission Compliance, Companies House Compliance, Environmental Regulations, Audit Regulations, and HMRC
- 3.3. Each pillar is analysed across four headings:
 - 3.3.1. Risks – a short Title for each Level One, Two and Three risk; and a description of that risk
 - 3.3.2. Scores – Likelihood, Impact and Total scores:
 - 3.3.2.1. Likelihood is scored from 1 to 4 representing remote / low / medium / high risk
 - 3.3.2.2. Impact is also scored from 1 to 4 representing insignificant / low / medium / high risk
 - 3.3.2.3. The Likelihood score is multiplied by the Impact score to get a ‘heat’ score – Appendix 2 shows the heat map
 - 3.3.3. Controls – Monitoring, Mitigations and Trigger (the Trigger Point is how we recognise that a risk has been breached)
 - 3.3.4. Reviews – Review Cycle (in months), Last Review (month of board meeting) and Next Review
- 3.4. A breached risk is no longer a risk but has crystallised into an issue that has to be managed.

4. Policy Review Cycle

- 4.1. This policy must be reviewed at least once every five years to ensure it is up to date and relevant.

Appendix 1

The Role of Risk Management



Effective risk management requires the following:

- The identification of all risks that could impact the company
- A detailed analysis of the principal risks, along with options for action should a risk event or risk breach occur
- An understanding of the minor risks, along with options to prevent a minor risk becoming a major risk event/breach through the consequences of inadequate or no action
- A set of trigger points, monitors and controls that facilitate the earliest possible identification of a risk breach
- Data that speak to the controls

Appendix 2

The Heat Map

The Likelihood multiplied by the Impact scores determine where a risk is placed on the heat map

GREEN	Total scores of 1 and 2
YELLOW	Total scores of 3 and 4
AMBER	Total scores of 6, 8 and 9
RED	Total scores of 12 and 16

