RUTLAND FIRST CIC

RISK MANAGEMENT POLICY AND PROCEDURES

Issued April 2022 Review April 2025

What is a Risk?

A Risk is an event or circumstance which may have a significant negative effect on an organisation or may affect its business negatively. A Risk may impact one or more of a number of areas which are referred to in more detail in Appendix 2. The Risk may restrict the ability of an organisation to achieve its objectives and may reduce future opportunities. Notwithstanding this, **risks are a normal aspect of any business**.

Further details regarding Risk and the most common risk categories can be found later in this paper under process and procedures. Types of risk can vary from business to business.

Commitment

As part of good corporate governance Rutland First CIC is fully committed to managing Risk within its control, in order to protect its business, employees and volunteers, protect assets, maintain and improve it services and ensure financial sustainability.

Rutland First CIC integrates the management of risk throughout all its activities and adopts an inclusive approach with employees and volunteers by encouraging a focal point for promoting risk management and ensuring that everyone understands their role in managing Risk and sharing good practices. **We aim to manage Risk better, but do not expect to eliminate it.**

Purpose and Scope

The purpose of this Risk Management Policy is to ensure everyone is aware of the risk management framework and to provide guidance regarding the management of Risk throughout all the activities of Rutland First CIC in order to support the achievement of corporate objectives. Active risk management will

- Protect the future of the organisation
- Maximise the potential for plans to be achieved
- Meet legal and compliance requirements
- Ensure that controls are effective

This policy applies to all Rutland First CIC's activities. It forms part of Rutland First CIC's governance framework and applies to all employees and volunteers who should ensure they are familiar with it.

Risk Governance

Below is an overview of the risk governance structure of Rutland First CIC. Each management level is responsible for being risk aware and managing Risk.

Rutland First CIC Board	Sets policy and defines risk appetite statement for specific risk areas. Provides oversight, acceptance and delegates management of (individual) risk.
Audit and Risk Committee	Defines and oversees the process of **risk** management; assures the integrity of the financial statements; oversees the effectiveness of the internal financial controls and the external and internal **audit** functions; reports to the Board;
Chairman	Drives culture of risk management and signs off on annual risk attestation
Chair of Audit and Risk Committee	Sets the committee's agenda, tone and work style; responsible for ensuring committee members understand the critical risks to the business, strategy and business model and works to develop and improve risk management policy; maintains Risk Register;
Senior Team	Ensure staff and volunteers in their areas comply with the risk management policy and foster a culture where risks can be identified and escalated
Staff and Volunteers	Comply with risk management policies and procedures
Internal Audit	Independently review the overall internal control framework, including risk management, and report findings to the Finance Officer and the Audit and Risk Committee

Process and Procedures

Rutland First encourages an open culture of risk management to ensure that all significant risks are identified and openly reported. This will ensure that risks are understood and mitigating action is prioritised accordingly.

Anyone may raise a risk issue which they believe they have identified and the issue will be heard by a senior Team member or the Chair of the Audit and Risk Committee, as appropriate. Where a potential significant risk is confirmed then the Risk Management Process will be followed.

Risk Management Process

The following key steps are involved in the risk management process:

- **I**dentify the risk
    - Identify risks to the business model
- **A**ssess the risk
    - Quantify potential impact
    - Determine likelihood of recurrence
    - Categorise according to overall risk score
- **M**anage the risk

    - Identify and implement risk mitigation
    - Identify key controls
- **M**onitor and review the risk
    - Monitor key controls
    - Use risk management tools
    - Report risk positions regularly
    - Report and assess incidents and risk events

Details of how to consider each step in this process and practical guidance can be found in Appendix 1.

Integration with other systems and processes

Risk management is factored into business strategy and planning, performance management, audit and assurance, business continuity planning and project management.

Risk reporting and the Risk Register

The purpose of risk reporting is to create awareness of key risks, improve accountability for the management of risk and the timely completion of risk treatment plans.

We will maintain a register of significant risks (Risk Register) which is reviewed [quarterly] by the Board. It will be updated when a new significant risk is identified. The Risk Register will be maintained by the Chair of Audit and Risk Committee

Risks can be grouped into categories of risk and should be included in the risk register and in risk reporting. The 7 key categories are described at Appendix 2.

Statement of Risk Appetite

Risk appetite is the amount of risk that we are willing to tolerate for example, whilst implementing a project. It should be both qualitative and quantitive. As part of its approach to risk mitigation, the Board will agree a set of risk appetite statements that address key risk areas and specific areas of operation of our business. Periodically the Board should review and update these statements. Key to developing these statements is to understand our strategic goals and objectives.

Appendix 1

How much risk?

We must decide on how much risk we are prepared to take in our business. Some risks may be critical to our success; however, exposing our business to the wrong types of risk may be harmful.

The most common business risk categories are:

- strategic –decisions concerning our business' objectives
- compliance –the need to comply with laws, regulations, standards and codes of practice
- financial –financial transactions, systems and structure of our business
- operational –our operational, planning/forecasting and administrative procedures
- environmental –external events that the business has little control over such as unfavourable weather or economic conditions
- reputational –the character or goodwill of the business.

Others include health and safety, project, equipment, security, technology, stakeholder management and service delivery.

For each risk identified on the risk register we record the quantification of risk and where relevant the mitigants, controls, ownership and actions taking place to manage the risk.

1. Identify the risk

Undertake a review of our business to identify potential risks. Some useful techniques for identifying risks are:

- Evaluate each function in our business and identify anything that could have a negative impact on our business.
- Review our records such as safety incidents or complaints to identify previous issues.
- Consider any external risks that could impact on our business.
- Brainstorm with the entire team.

Ask ourselves 'what if':

- we lost power?
- our premises were damaged or not accessible?
- our suppliers went out of business?
- there was a natural disaster in our area?
- one of our key team members resigned or was injured at work?
- our computer system was hacked?

- our business documents were destroyed?
- others?

2. Assess the risk

We can assess each identified risk by establishing the significant level (seriousness) and then RAG rating the result:

- the likelihood (frequency) of it occurring
- the impact (consequence) of it occurring

The level of risk is calculated using this formula:
Level of risk (Gross Risk Score) = likelihood x impact

The resultant RAG will have break points which define the level at which the Gross Risk Score changes colour between red, amber and green.

Low Gross Risk – RAG Green – no further action required other than recording on the register

Medium and High Gross Risk -RAG Amber and RAG Red - require a specific Board member to be identified as the risk owner and mitigating actions and controls will be identified and noted in the Risk Register.

To determine the likelihood and impact of each risk it is useful to identify how each risk is currently controlled. Controls may include:

- elimination
- substitution
- financial controls
- administrative controls
- others?

3. Manage the risk

Managing risks involves developing cost effective options to deal with them including:

- Avoiding the risk - change our business process, equipment or material to achieve a similar outcome but with less risk.
- Reducing the risk – if a risk can't be avoided then reduce its likelihood and impact. This could include staff training, documenting procedures and policies, complying with legislation, maintaining equipment, practicing emergency procedures, keeping records safely secured and contingency planning.

- Transferring the risk – transfer some or all of the risk to another party through contracting, insurance, partnerships or JVs.
- Accepting the risk – this may be our only option if we want to continue doing business in a particular way.

Assess the Net Risk in a similar way to the Gross Risk and score accordingly.

Low Net Risk – RAG Green – no further action required other than recording on the Risk Register

Medium and High Net Risk – key mitigating controls which reduce the level of risk need to be defined and effective and within the risk appetite.

A Key Controls register should be kept and a testing frequency applied to each control. A board member will be responsible for independent testing of key controls.

Early warning indicators should be developed for High Risk items to ensure the Board has the earliest possible indication of an incident.

4. Monitor and review

We should regularly monitor and review our risk management plan and ensure the control measures and insurance cover is adequate. We should discuss our risk management plan with our insurer to check our coverage as this may affect our attitude to some of the partly-mitigated risks we might wish to accept.

Appendix 2

TYPES OF BUSINESS RISK WE MAY WISH TO PLAN FOR

Accept, But Plan

Although we will never be able to completely eliminate business risk, proactively planning for it can help. Awareness is key in helping you save money and time whilst protecting the trust, reputation, and client/grantee base we have worked so hard to achieve.

1. Economic Risk

The economy is constantly changing as the markets fluctuate. Some positive changes are good for the economy, which lead to booming purchase environments, whilst negative events can reduce sales. It's important to watch changes and trends to potentially identify and plan for an economic downturn.

To counteract economic risk, we should save as much money as possible to maintain a steady flow. Also, we should operate with a lean budget with low overhead through all economic cycles as part of our business plan.

2. Compliance Risk

We face an abundance of laws and regulations to comply with. For example, recent data protection and payment processing compliance could impact how we handle certain aspects of our operation. Staying well versed in applicable laws both state and local agencies can help minimise compliance risks.

If we rely on all our income from one or two grantees, our financial risk could be significant if one or both no longer provide any money. We need to start marketing our capabilities and services to diversify our base so the loss of one won't devastate our bottom line.

Non-compliance may result in significant fines and penalties. We should remain vigilant in tracking compliance by regularly reviewing government and other information and seeking assistance from consultants who specialise in compliance, if necessary.

3. Security and Fraud Risk

As online and mobile channels are used more and more to share personal data, there are also greater opportunities for hacking. News stories about data breaches, identity theft and payment fraud illustrate how this type of risk is growing for businesses.

Not only does this risk impact trust and reputation, but a company is also financially liable for any data breaches or fraud. To achieve effective enterprise risk management, we should focus on security solutions, fraud detection tools and employee and volunteer education about how to detect any potential issues.

4. Financial Risk

Making adjustments to our business plan will help us avoid harming cash flow or creating an unexpected loss. By relying on all our income from one or two sources, our financial risk could be significant if one or both no longer support us. Marketing to diversify our base is key so that the loss of one won't devastate our bottom line.

5. Reputation Risk

There has always been the risk that an unhappy customer, product failure, negative press or lawsuit can adversely impact a company's brand reputation. However, social media has amplified the speed and scope of reputation risk. Just one negative tweet or bad review can decrease our following and cause future income to be pulled.

To prepare for this risk, we should leverage reputation management strategies to regularly monitor what others are saying about us online and offline. We should be ready to respond to comments and help address any concerns immediately. We should keep quality top of mind and avoid product failures that can also damage our reputation.

6. Operational Risk

This business risk can happen internally, externally or involve a combination of factors. Something could unexpectedly happen that causes us to lose business continuity.

That unexpected event could be a natural disaster or fire that damages or destroys your physical business. Or, it might involve a server outage caused by technical problems, people, or power cut. Many operational risks are also people-related. An employee or volunteer might make mistakes that cost time and money.

Whether it's a people or process failure, these operational risks can adversely impact your business in terms of money, time and reputation. We should address each of these potential operational risks through training and a business continuity plan. Both tactics provide a way to think about what could go wrong and establish a backup system or proactive measures to ensure operations aren't affected.

7. Competition (or Comfort) Risk

A company may be aware that there is always some competition in their sector, it's easy to miss out on what companies are offering that may appeal to our customers.

In this case, the company risk involves a company leader becoming so comfortable with their success and the status quo that they don't look for ways to pivot or make continual improvements. Increasing competition combined with an unwillingness to change may result in a loss of customers.

Enterprise risk management means a company must continually reassess their performance, refine their strategy, and maintain strong, interactive relationships with their audience and

customers. Additionally, it's important to keep an eye on the competition by regularly researching how they use online and social media channels.