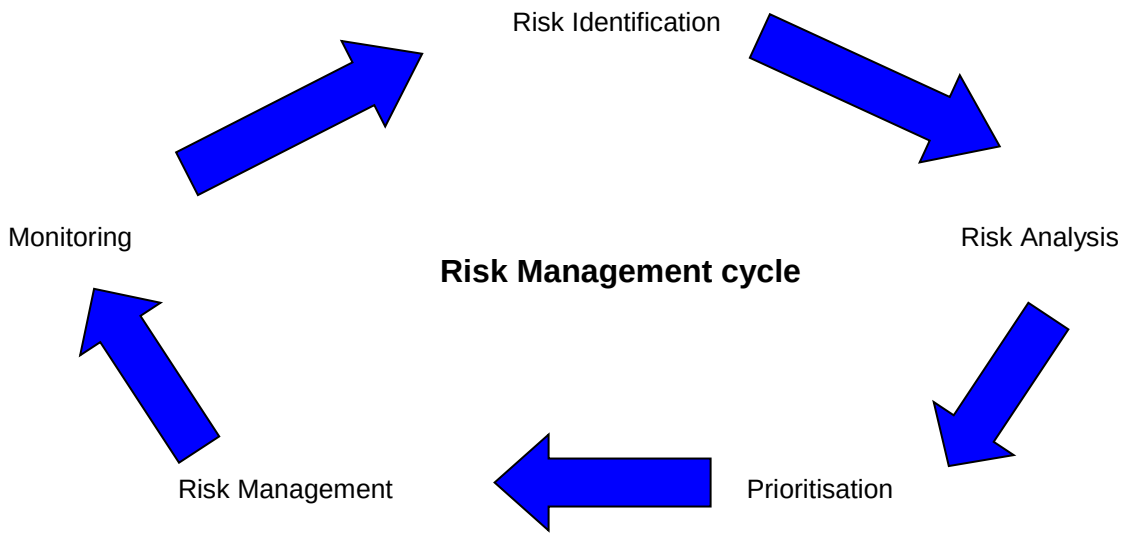
Risk Management Policy



Risk Management cycle

Last updated	August 2018	S:\Personnel\Policies - Restricted\Risk Management Policy.doc	Version:	3
Author	Crystina Woolley	1	Review Date:	July 2020

1. INTRODUCTION

1.1 General

This policy provides the framework to manage operational and business risk in the performance of Steps to Wok activities to meet the needs of both the companies' aims and objectives and charitable status.

1.2 Background

The Accounting and Reporting by Charities - Statement of Recommended Practice in 2000 the SORP introduced a new requirement into the trustees' Annual Report requiring trustees to report on Risk. The FRS 102 effective from 1 January 2015 states that "a description of the principal risks and uncertainties facing the charity and its subsidiary undertakings, as identified by the charity trustees, together with a summary of their plans and strategies for managing those risks".

The Charities (Accounts and Reports) Regulations updated November 2015 places a legal requirement on all charities preparing accounts currently with gross income of £500,000 or more. It states that the annual report must contain a statement confirming that the major risks to which the charity is exposed, as identified by the trustees, have been reviewed, and systems or procedures have been established to manage those risks.

Business Continuity Management ISO22301 specifies that "there shall be a defined, documented and appropriate method for risk assessment that will enable the organisation to understand the threats to and vulnerabilities of its critical activities and supporting resources, including those provided by suppliers and outsourced partners. The organisation shall understand the impact that would arise if an identified threat became an incident and caused a business disruption".

Quality Management ISO9001 states that

- risk based thinking is essential for achieving an effective quality management system
- that an organisation needs to plan and implement actions to address risk and opportunities
- addressing both risks and opportunities establishes a basis for increasing the effectiveness of the quality management system, achieving improved results and preventing negative effects

Environmental Management ISO14001 specifies that we determine the risks and opportunities, related to environmental aspects, compliance obligations and other issues identified that need to be addressed to:

- give assurance that the environmental management system can achieve its intended outcomes
- prevent or reduce undesired effects, including the potential for external environmental conditions to affect the organisation
- achieve continual improvement

1.3 Definitions

"Risk" is used to describe the uncertainty surrounding events and their outcomes that may have a significant effect, either enhancing or inhibiting:

- operational performance;
- achievement of aims and objectives; or
- meeting expectations of stakeholders

Risk is the effect of uncertainty and any such uncertainty can have **positive** or **negative** effects. A positive deviation arising from a risk can provide an **opportunity**, but not all positive effects of risk result in opportunities.

"Risk Management" is a systematic way of protecting the resources and income of the business against losses so that the aims and objectives of the company can be achieved without unnecessary interruption. It is the structured development and application of management culture, policy procedures and practices to the tasks of identifying, analysing, evaluating and controlling responding to risk.

"Risk assessment" is the systematic process of **risk identification, analysis and evaluation**

"Risk Appetite" is the total amount of risk that an organisation is prepared to accept, tolerate or be exposed to at any point in time.

Risks are measured in terms of **"impact and likelihood"**. A score is assigned for each of these, with a resulting risk score being the product of the two numbers. This risk score can then be used to rank risks.

"**Impact**" measures the consequences of exposure to a particular risk. For the Steps to Work classification, four levels of impact have been defined, as follows:

1	Low	• Minimal impact on delivery • No real impact / significance on Finance • Low or no impact on contract requirements
2	Moderate	• No financial impact or damage to reputation • Some inconvenience during incident
3	High	• Breach of contract • Breach of requirements such as H&S, safeguarding, info security, data protection, environmental • Loss of reputation • Loss of income • Impact to customer satisfaction score
4	Severe	• Loss of a contract • Longer term loss of business • Significant costs to remedy • Closure

The **"likelihood"** of risk measures how often a risk has the potential to occur. For Steps to Work, four levels of likelihood classification have been defined, as follows:

1	Low	Once every 2 - 5 years
2	Moderate	Once a year
3	High	Once per month
4	Severe	Every day/week

1.4 Aims

In all activities undertaken by Steps to Work the following key business deliverables are expected:

- Achievement a high level of customer satisfaction in all aspects of the services it provides.
- Development and enhancement of the company's reputation.
- Achievement of planned financial targets
- Maintenance and compliance with statutory and legal requirements
- Development of its employees.

1.5 Policy Statement

Steps to Work will develop and deploy appropriate strategies to identify, analyse and manage the risks associated with its service delivery with the following objectives:

- Ensure that decision-makers are given timely and objective information to aid decision making.
- To provide a safe, healthy and environmentally friendly environment to work in.
- Minimise financial and reputational losses and maximise opportunities
- To develop appropriate partnerships and working arrangements to maximise the opportunities for its target groups.
- Identify cost effective risk treatment options.

Risk management will not therefore be seen purely as a compliance issue or as being solely focused on the prevention of disaster / incident. The process will enable trustees to focus on the mitigation / treatment of risks that would prevent the charity achieving its strategic objectives.

2. PRINCIPLES

2.1 In all service areas managers will carry out risk assessments regularly, record the findings and take appropriate management actions in a timely fashion. Risk reviews will specifically address strategic and operational risks as well as risk by health and safety and environmental protection legislation. In particular the following activities will be undertaken:

1. Inter related contract and risk management processes;
2. Preparation of contingency plans for high risks;
3. Early identification of emerging risks and initiation of risk reduction or mitigation action.

Where appropriate, managers may need to consider specialist advice in areas such as health & safety, fire, security, media/public relations, insurance, safety/critical systems and operations, disaster recovery. The following contract activities, because of their intrinsic risks or from past experience, present particularly hig risk profiles and will require formal risk management activities to be undertaken.

Projects involving responsibility for:

1. Young people;
2. Workers engaged in external activities;
3. Where large scale capital investment is required;
4. Where the funding is output related and requires the use of sub contractors.

The key stages undertaken to establish, reduce and monitor risk have been identified as follows:

1. Establishing risk policy;
2. Risk Identification;
3. Risk Analysis;
4. Prioritisation;
5. Monitoring.

1. Establishing the Risk policy

Risk is an inherent feature of all activity and may arise from inaction as well as new initiatives. As a Charity we have differing exposures to risk arising from our activities and from our willingness to meet our objectives, we have different capacities to tolerate or absorb risk which need to be identified, documented and understood by all. Trustees and managers need to understand the organisations overall risk profile, i.e. the balance taken between higher and lower risk activities in order to inform the decision as to what level of risk we are prepared to accept. The trustees will then need to communicate to managers the boundaries and limits set by their policy to ensure a clear understanding of the risks that can be accepted and those that the trustees would consider unacceptable.

2. Risk Identification

This is the creative element of risk analysis and is a process that requires careful consideration and is best done by involving those with a detailed knowledge of the organisation's workings. In order to establish the "Risks" faced by the company we have considered:

- The companies Mission, Objectives, Values and strategy;
- The nature and scale of our activities;
- The success factors that need to be achieved;
- External factors that might affect the us such as legislation and regulation, and our reputation with our major funding partners;
- Past experience, mistakes and problems that we have faced;
- Our operating structure - e.g. use of branches, and subsidiary companies (Starting Point Recruitment) our use of sub contractors;
- Requirements of Business Continuity in terms of People, Premises, Technology, Information and Resources/Utilities

3. Risk Analysis and Evaluation

Identified risks need to be put into perspective in terms of the potential severity of impact and likelihood of their occurrence. Analysing and categorising risk assists us in prioritising and filtering the risks identified and establishing further action (if any) required and at what level as a strategy to mitigate / treat the risk or accept the risk. Our methodology is to consider each identified risk and decide for each the likelihood of it occurring and the severity of the impact of its occurrence on the organisation.

This will result in an effective mapping of risks onto a chart, such as that shown below.

Following the classification of risk, the score assigned to each risk is then used to determine how it should be treated. Levels have been defined that classify risk as:

- **LOW**: Can be automatically accepted Score 1 - 3
- **MODERATE**: Should be treated Score 4 - 7
- **HIGH**: Should be treated – urgently Score 8 - 12
- **SEVERE:** Must Be Treated or activity terminated Score 13 - 16

	Likelihood	Low	Moderate	High	Severe
Impact		1	2	3	4
Severe	4	4	8	12	16
High	3	3	6	9	12
Moderate	2	2	4	6	8
Low	1	1	2	3	4

Key:							
	Acceptable		Should Be Treated		Should Be Treated - urgently		Must Be Treated

This approach attempts to map risk as a function of the likelihood of an undesirable outcome and the impact that an undesirable outcome will have on the organisations ability to achieve operational objectives. This process will enable the trustees to identify those risks which fall into the major/(severe) risk category identified by the SORP statement.

Risks are recorded on the risk register, which is reviewed at least annual as part of the Management Review or whenever any significant contract changes occur. The risk register is accessible to all staff on the shared drive in pdf format.

4. Prioritisation and Strategy

The major risks identified need the trustees to ensure that appropriate action is being taken to ensure that these are mitigated. This review must include establishing the adequacy of controls already in place. For each of the risks identified, trustees will need to consider any additional action that needs to be taken to mitigate the risk, either by lessening the likelihood of the event occurring, or lessening its impact if it does. This could include the following actions:

- The risk may need to be avoided by that activity (e.g. stopping work with on a particular contract or with a sub contractor);
- The risk could be transferred to a third party (e.g. a trading subsidiary, outsourcing or other contractual arrangements with third parties);
- The risk could be shared with others (e.g. a joint venture project);
- The charity's exposure to the risk can be limited (e.g. establishment of reserves against loss of income, forward contracts, phased commitment to projects);

- The risk can be reduced or eliminated by establishing or improving control procedures (e.g. internal financial controls, controls on recruitment, personnel policies);
- The risk may need to be insured against;
- The risk may be accepted as being unlikely to occur and/or of low impact and therefore will just be reviewed annually.

.

Once each risk has been identified and evaluated, we can draw up a plan for any action that needs to be taken. This action plan and the implementation of appropriate systems or procedures allows the trustees to make a positive statement as to risk mitigation / treatment reducing the " gross level" of risk identified to a "net level" of risk that remains after appropriate action is taken and scheduled in the risk register for future monitoring. Strategy is focused on ensuring critical services can continue within their recovery time objective (RTO), thus ensuring that the Maximum Tolerable Period of Disruption (MTPD) is not met thereby creating a satisfactory recovery from any incident.

5. Monitoring and assessment

Effective risk management extends beyond simply setting out systems and procedures. The process needs to be ongoing to ensure new risks are addressed as they arise and also cyclical to establish how previously identified risks may have changed. Risk management is not a one-off event and should be seen as a process that will require monitoring and assessment. Staff and managers need to take responsibility for implementation. There needs to be communication with staff at all levels to ensure responsibilities are understood and embedded into the culture of the organisation.

It is therefore inherent upon the trustees and senior managers to ensure that:-

- New risks are properly reported and evaluated;
- Risk aspects of significant new projects are considered as part of project appraisals;
- Any significant failures of control systems are properly reported and actioned;
- There is an adequate level of understanding of individual responsibilities for both implementation and monitoring of the control systems;
- Any further actions required are identified;
- Trustees consider and review the annual process;
- Trustees are provided with relevant update information and inform the senior management of any changes required.