Risk Management Policy

Last Updated: Sept 2024

Reviewer: Mireille Harris (Head of People)

Review Date: Sept 2026

Version: 1

Contents

Introduction

This policy provides the governance infrastructure to manage strategic and operational risk in the performance of Starting Point Recruitment activities to meet the needs of both the companies' aims and objectives.

Policy Statement

Starting Point Recruitment 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 The Board, CEO and Leadership Team to focus on the mitigation / treatment of risks that would prevent the business achieving its strategic and operational objectives.

Aims

In all activities undertaken by Starting Point Recruitment the following key business deliverables are expected:

- Achievement of 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.

Frameworks

Quality Management ISO9001 – accredited status with QMS

Risk based thinking is essential for achieving an effective quality management system. To conform we will ensure we plan and implement actions to address risk and opportunities. We will address both risks and opportunities; and establish a basis for increasing the effectiveness of the quality management system, achieving improved results, and preventing negative effects.

We comply with:

- Clause 4.4.1 f – address the risks and opportunities in accordance with requirements of 6.1
- Clause 6.1.1 – planning will consider the issues and requirements of the business activities to determine the risks and opportunities that need to be addressed to
    a) Give assurance for achievement of intended results
    b) Enhance desirable effects
    c) Prevent or reduce undesired effects
    d) Achieve improvement
- Clause 6.1.2 – actions will be agreed to address the risks and opportunities and evaluate the effectiveness of the actions. Actions shall be proportionate to the potential impact on conformity of services.

Business Continuity Management ISO22301 - comply with the principles

The standard 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".

Environmental Management ISO14001 - comply with the principles

The standard 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.

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.

Risk measurement is recorded using **"impact, probability and proximity"** on the RAID spreadsheet or an appropriate risk assessment form for specific responsibilities, roles or premises. A score is assigned for each of these, with a resulting risk rating score being the product of the three numbers. The rating populates the graph within the spreadsheet for a visual representation of risk.

Impact measures the consequences of exposure to a particular risk. Five levels of impact have been defined, as:

1	Insignificant	• Insignificant changes, re-planning may be required

2	Low – small delay	• Minimal impact on delivery • Small increased cost but absorbable • Low or no impact on contract requirements
3	Moderate - delay	• No financial impact or damage to reputation • Some inconvenience during incident
4	High – Substantial Delay	• Breach of contract as key deliverables not met • Breach of requirements or legislation such as H&S, safeguarding, info security, data protection, environmental • Loss of reputation • Loss of income • Impact to customer satisfaction score
5	Severe – inability to deliver	• Loss of a contract • Longer term loss of business • Significant costs to remedy • Closure

Probability and Proximity of risk measures combined determine the likelihood of a risk.

Probability classification have been defined as:

1	Very unlikely to occur
2	Less likely to occur
3	50/50 chance of occurring
4	More likely to occur than not
5	Certain

Proximity classification have been defined as:

1	Far in the future - Proximity of 1 year
2	Mid to long term - Proximity of 6 months
3	Mid to short term - Proximity of 3 months
4	Likely to be near future - Proximity of 1 month
5	Imminent – proximity of 1 week

Risk ratings are calculated by multiplying impact * probability * proximity

Minor = Green	Accept
Moderate = Yellow	Should be treated
Major = Amber	Should be treated – Urgently
Severe = Red	Must be treated

Risk Governance and Category

The CEO, Leadership Team and Extending Leadership Team will review and update their RAID spreadsheet 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 with legislation such as health and safety, environmental protection, GDPR, company law (the list is not exhaustive). In particular, the following activities will be undertaken:

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

Where appropriate, specialist advice may need to be considered in areas such as health & safety, fire, security, media/public relations, insurance, safety/critical systems and operations, disaster recovery.

Risk Category

A system of classification aligned with the Board structure is in development with an approach to encourage regular risk review where necessary.

Contract activities because of their intrinsic risks or from past experience, present particularly high-risk profiles and will require formal risk management activities to be undertaken.

Projects involving responsibility for:
1. Young people.
2. Expectant mothers.
3. Children or Vulnerable Adults.
4. Workers engaged in external, remote, off-site activities.
5. Where large scale capital investment is required.
6. Where the funding is output related and requires the use of sub-contractors.

Premises risk assessments including fire risk assessments and H&S requirements will be completed in accordance with the Health and Safety policy.

Establishing the Risk policy

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.

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, Vision, Values, Objectives 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, lessons learnt, corrective and preventive action plans.

- Our operating structure - e.g. use of branches, and subsidiary companies or use of Sub-Contractors
- of Business Continuity in terms of Governance, Finance, People, Premises, Technology, Stakeholders

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 RAID log populates a risk graph that illustrates the risk categories and the percentage of risks within each category.
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 RAID log, which is reviewed at least annually with the Board, annually as part of the Management Review and regularly by the Leadership Team.

Prioritisation and Strategy

The major risks identified are reported to the Board to ensure that appropriate action is being taken to appropriately mitigate and treat. 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 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.

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 leadership team 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.
- The Board consider and review the annual process.
- The Board are provided with relevant update information and inform the senior management of any changes required.