Risk Management Policy

Version: 4

Date: 05/07/2022

Document Control

Title	Risk Management Policy
Supersedes	Previous Version No. 3
Owner	Exec Team
Circulation/Distribution	All
Review Period	Annually

Version History

Next Review Date		05/07/2023		
Version	Date	Amendments	Author	Status
4	29/06/2021	Formatting into new Trust format	BO	Approved
4	05/07/2022	Formatting and Contents table	CEO	Approved
4	29/06/2023	None	CEO	Approved

Contents

DOCUMENT CONTROL 2

VERSION HISTORY 2

INTRODUCTION 4
WHAT IS RISK? 4
TYPES OF RISK 4
FIVE KEY QUESTIONS FOR THE BOARD 5
POTENTIAL RISK AREAS, THEIR IMPACT AND MITIGATION 6
RISK APPETITE 6
RISK SCORING MODEL 8
RISK IDENTIFICATION 8
RISK RECORDING AND ANALYSIS 8
RISK RESPONSE 9
RISK REVIEW, MONITORING AND REPORTING 9

Introduction

Risk management is a key component of sound corporate governance.

'The effective development and delivery of an organisation's strategic objectives, its ability to seize new opportunities and to ensure its own long-term survival depend on its identification, understanding of, and response to, the risks it faces,' says the Financial Reporting Council.

High profile scandals in private, public and third sectors, corporate failures, the banking crisis of 2008-2009, as well as increased globalisation, inter-connectedness and the fast pace of change in the business environment, have all focused more attention on the way boards handle risk management. There has been a step change in the need for boards to focus on risk in the last few years. Regulators have toughened their approach – all but the smallest companies in the UK must now prepare a 'strategic report' which includes a 'fair review of the company's business and a description of the principal risks and uncertainties facing the company.' For charities, the 'Statement of Recommended Practice' (SORP 2015) requires in the annual report from trustees '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'. Sector specific regulators from ESFA, OFSTED, the Information Commissioner, the Health & Safety Executive expect to see a proper risk management strategy.

As with all aspects of good governance, the effectiveness of risk management and internal control ultimately depends on the skills, knowledge and behaviour of those responsible for operating the system. The Board must set the desired values, ensure they are communicated, incentivise the desired behaviours, and sanction inappropriate behaviour.

What is risk?

A useful working definition is 'an event with the ability to impact (inhibit, enhance or cause doubt about) an organisation's mission, strategy, projects, routine operations, objectives, core processes, key dependencies and/or the delivery of stakeholder expectations.'

By taking a proactive approach to risk management, organisations should achieve positive benefits:

Operations should be more efficient because events that can cause disruption are identified in advance and actions taken to reduce the likelihood and containing the costs if they do occur.

Processes should be more effective because of the thought that is given to selecting processes and thinking about the risks involved in different alternatives.

Strategy should be more effective, because risks associated with different options will have been carefully analysed and better decisions reached, leading to better outcomes.

Types of risk

Risks break down into different types. Risk management practitioners classify risks into *hazard risks, control risks and opportunity risks*. In general terms, organisations seek to mitigate hazard risks, manage control risks and embrace opportunity risks.

Risks break down into categories:

Financial risks – (e.g. accuracy and timeliness of financial information, accurate accounting records, adequacy of cashflow, interest rates, exchange rates, investment returns).

Operational risks (machine failure, human errors, service quality, incorrect contract pricing, employment issues, health and safety, IT failures, data breaches, fraud and theft).

Environmental and external risks (reputation and adverse publicity, cyber-attacks, demographic trends, government policy, terrorism, extreme weather events, pandemics).

Compliance with laws and regulation – risk of legal claims, regulatory action, prosecution and fines for failure to comply with obligations.

The processes which boards use to consider risks were examined in some detail by the Financial Reporting Council (F&R) in 2011 and the Sharman Inquiry in 2012. The key areas of best practice recommended were:

The Board must first decide on its appetite and willingness to take on risk – this feeds into the organisation's culture, behaviour and values. Are the risks commensurate with the expected returns? An environment of excessive or ill-informed risk-taking could be fatal to the organisation's long-term future.

Risk management and internal control should be incorporated within the organisation's normal management and governance processes – not treated as a separate or one-off compliance exercise.

The Board must make a regular and robust assessment of the main risks to the organisation's business model, including ability to deliver its strategy, solvency, liquidity and long-term viability.

Once the risks have been identified, the Board should agree how they will be managed and mitigated. It should satisfy itself that the management and control systems are adequate and, in larger organisations, receive adequate formal assurances from managers, the risk and audit committee and external auditors. Regular reports should be coming to the board to provide this. Risk data should be captured from across the organisation: often front-line staff are the first to be aware of problems.

Risks and associated control systems should be reviewed on a regular ongoing basis.

The organisation should report publicly and transparently to its stakeholders on the principal risks it faces, any material uncertainties and their review of the risk management and internal controls. Stakeholders should feel that the board has a visible role in governance and stewardship and that the Board is held accountable.

Five key questions for the Board

What are the top 5 actions the Board can take to ensure success?

Focus on the culture – is there an embedded commitment to risk management and control in your organisation? Does the board lead by example? There should be openness and creativity around risk issues.

The risk register and associated controls must be documented, understood, reviewed and disseminated regularly – not locked in a filing cabinet and dusted off once a year, or even less frequently.

There must be a process for monitoring and reviewing risk – adequate time must be scheduled at board meetings to consider risk issues and review whether the organisation has the skills and capacity and tools to manage risks effectively. The board should focus its attention on the top ten areas identified with highest risk score.

The Board must be alert to new and emerging risks through horizon-scanning and recent events (such as cyber-attacks, social media, pandemics, demographic changes, terrorism).

Report on the Board's activities in examining and reviewing risks so that stakeholders can gain assurance that the board is discharging its duties and form a balanced, clear and informed view of the organisation's prospects.

Potential risk areas, their impact and mitigation

The nature of activities, funding base, reserves and structures will expose charities to differing areas of risk and levels of exposure. The Trustee Directors of The Sovereign Trust have considered the main areas of risk that the organisation could be exposed to. Illustrative examples of potential impact are given, as well as examples of controls or action that will be taken to mitigate the risk or impact. Some risks fall into more than one category.

The risks are classified as follows:

Compliance

Financial

Governance

People

Reputation

Strategic

The risks are scored and colour coded accordingly (Red, Amber, Yellow and Green). Those marked in red are the areas of highest risk which need to be monitored most closely.

Risk Appetite

6.1 Defining Risk Appetite

Risk appetite is the level of exposure the Trust is willing to accept in pursuit of its strategy and objectives. Without a defined appetite the Trust would be run with insufficient guidance on the levels of risk that are acceptable or the boundaries in which to operate. This could also result in parts of the Trust not seizing important opportunities, due to a perception of the need to be risk averse. Although the Trust must aim to meet the risk appetite, there will be occasions when a risk has to be accepted or tolerated outside the appetite level.

The appetite for risk can be shown diagrammatically in Figure 1:

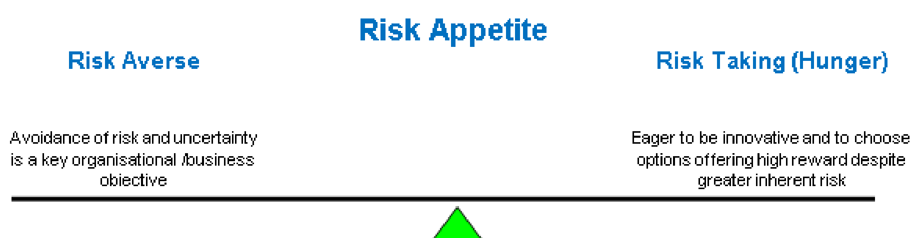


Figure 1 Risk Appetite

In both extreme cases, the risk management process is equally important; to ensure that there are either controls in place at one extreme or there are contingencies in place at the other. So, there will inevitably be a balance between being risk averse and risk taking which will be affected by a number of factors including:

aims/objectives;

stakeholders;

business environment;

risk profile;

the impact if the risk occurs;

the likelihood of occurrence;

“risk velocity” i.e. the time for the impact to happen or the time to recover from the impact.

Risk appetite is therefore expressed in the same terms as those used in assessing risk. Where it differs is that it is a conceptual target position against which actual individual risks can be compared against.

The appetite should not be static and will potentially move or shift depending on the circumstances at the time i.e. the occurrence of a significant risk, the “risk velocity”, the large cumulative effect of moderate level risks or an emerging risk may reduce the appetite.

Determining the Risk Appetite

The risk appetite for the Trust is determined by the Board and on a day to day basis is endorsed by the SLT. Based on the business objectives, the key determinants for appetite levels within the Trust are:

Compliance impacts (Legal and Regulatory)

Financial impacts

Governance impacts

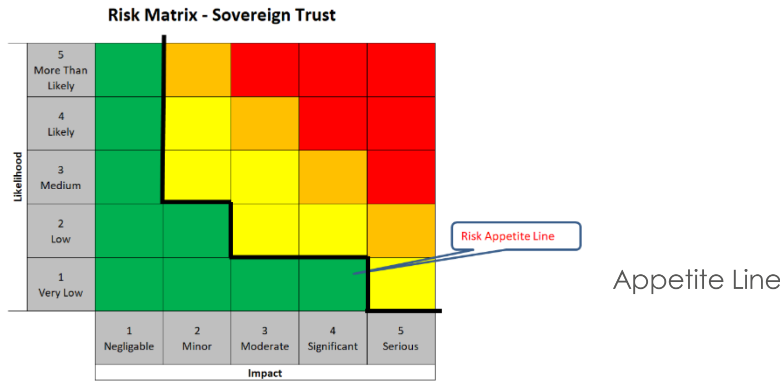
Health, safety, environmental and people (including teaching) impacts

Reputational impacts

Strategic impacts

For each impact area the Trust determines whether or not it is willing to operate when the likelihood of the impact materialising on a scale of 1 to 5 by following a stepped approach. The decision is made considering the existing business and external educational environment.

Figure 2 Risk



Appetite Line

Risk Scoring Model

The Trust's Risk Model seeks to articulate risks in a common format, i.e.:

"There is a risk that undesirable will happen, leading to consequences, because of trigger or compounding factors."

In the model, likelihood and impact are given a score from 1 to 5, and the resulting product of these two ratings used to score and rank the risks. In the first instance, the 'uncontrolled' risk score is calculated. It is then considered if any controls already exist to reduce the risk and if any are in place, a "controlled" risk score is calculated. If the risk requires increased control, then once appropriate actions are taken, the same methodology can be used to determine the resulting, reduced 'controlled' risk score.

The key to conducting a reliable risk assessment is the accuracy of the input data and so every effort shall be made to validate the data used in all risk assessments. The risk scoring for the six areas considered in the model and likelihood criteria are defined in Appendix A.

The scoring matrix is used by the Trust and senior management to continually review business risks, their mitigating action(s) and controls, and to ensure that risks are managed in priority order.

Risk Identification

Risks can be identified by anyone within the Trust and passed through to the respective SLT member. Through the SLT, risks will be defined and recorded by the Chief Finance Officer in the Trust Risk Register.

Risk Recording and Analysis

The Risk Register identifies the 'risk lead', i.e. the person responsible for managing and reporting on a particular risk and the 'risk oversight' i.e. the person or committee who will monitor the risk.

Risks associated with individual projects may be maintained separately by the respective part of the Trust. However, any risks deemed to be of sufficient weighting will be included within the Trust Risk Register.

Risk analysis involves developing an understanding of the risk, considering the causes and sources of risk, the consequences and likelihood. Having identified the risk, it shall be scored following the standard scoring format described in the risk scoring model in section 7 above.

1Risk Evaluation and Escalation

Risk evaluation involves comparing the level of risk found during the analysis process with the set risk criteria, context or appetite. Based on this comparison, the response to the risk can be considered which will address any conflicting interests that may arise; escalating if necessary to the identified SLT member or Trust Board member.

The output of the evaluation shall confirm if a particular risk can be:

Accepted (Tolerated)

Managed (Treated)

Avoided (Transferred e.g. to a third party)

Removed (Terminated)

Whilst a risk may be deemed acceptable, it may still be kept open on the risk register if it is a risk that needs to be kept visible and not overlooked.

The risk score, analysis and evaluation shall determine how each risk, if appropriate, is initially escalated:

Any risks scoring 20 or over should be raised with the CEO within 24 hours. The CEO will also determine if there should be any additional on-going reporting requirement over and above that detailed below.

Risks scoring 15 and above shall be routinely reported to the Board

Any new or closed risks shall be considered by the Finance, Risk and Audit Committee (F&R) and reported to the Board.

Risk Response

The Chief Finance Officer provides a routine update on risk status to the F&R. This comprises new and closed risks along with high scoring risks and an associated commentary. The F&R is then able to review these risks for acceptability and alignment with the risk appetite.

Where an unacceptable risk has been identified, the SLT or Board member with the lead for this risk, shall manage and implement suitable strategies through planning, design, investment, processes, tasks and behaviours in order to mitigate the consequences of this particular risk.

Risk Review, Monitoring and Reporting

Risks are monitored by the F&R through regular termly use of the Risk Register. The normal route for this is by means of regular updates, managed by the Chief Finance Officer, whereby risks are considered, updates provided on mitigating actions and risk coverage checked as being appropriate.

The reports provided by the Chief Finance Officer consists of two parts:

A report containing a high-level overview of the key risks, together with information on any risk related developments (e.g. workshop activity, key mitigation).

A report containing a summary of the key risks (those scoring 10 and above) showing any together with a summary of risks opened and closed in the month.