Risk management policy

January 2022

Document control

Document owner	Global Board
Document administrator	Director of Governance, Legal and Assurance
Document status	Approved
Date of last review	January 2022
Review period	2 years
Version number	4.0

Document amendment history

Version number	Date	Amendment summary	Approved by
1	November 2009	"Risk Management a New Framework" approved by Council. This framework replaced a risk register originally created under a previous strategic framework (2001 – 2003) that was not consistent with our new strategy developed in 2008. The new framework was in three parts a) a comprehensive list of all the significant risks faced by the organisation, b) from this a list of a dozen 'priority' risks for which management develop mitigation strategies and consider each quarter, and c) six 'top tier' risks (taken from the 12 priority ones) reviewed in detail quarterly. The priority risks are assessed and entered into a register or risk log, which has three parts; identification, assessment and mitigation/reporting.	Global Board
1.1	March 2016	Risk framework reviewed by Council. There were no substantive changes to the framework except to note that the six top tier risks element of the 2009 framework had been dropped and the risk process is the same for all twelve priority risks identified. It was noted that focusing the top level management and Council on a smaller number of critical risks allows far more in depth discussions about whether these are	Global Board

Version number	Date	Amendment summary	Approved by
		the right ones, and what activities to undertake to mitigate them. Each risk has an owner, responsible for the mitigation strategy. The dynamic nature of the process was recognised and the fact that priority risks change quite often.	
1.2	April 2018	Consolidation of the risk processes operating since 2009 into an overarching risk management policy.	Global Board
1.3	June 2020	Minor textual updates completed and reconfiguration of risk log by Risk Manager and approved by Director of Governance, Legal and Assurance (DGLA).	DGLA
1.4	Jan 2022	Minor textual changes - updated references, titles and Appendices IRM and Charity Commission Guidance updated to lates versions. Minor amendments approved by Director of Governance, Legal and Assurance (DGLA).	DGLA

Contents

Risk Management Policy 4

1. Policy Objective 4
2. Risk Governance 4
3. Principal Risk Identification 5
4. Assess Priority Risks 6
5. Risk Mitigation 6
6. Risk Monitoring and Review 6
7. Risk Communication and Reporting 7

Appendix 1: Charity Commission: Charities and Risk Management (CC26) 8

Appendix 2: Institute of Risk Management Guidance and FRC 8

Risk Management Policy

1. Policy Objective

Risk in this policy describes the uncertainty surrounding events and their outcomes that may have a significant impact, either enhancing or inhibiting, on any area of the charity's operations.

The Charity Commission strongly recommends that charities have a clear risk management policy and process (CC26 s.2.1). The charity should have a structured and proportionate approach to risk management that is appropriate for its size and complexity.

The objective of this policy is to provide guidance regarding the management of organisational risk to support the achievement of strategic objectives, protect beneficiaries, staff and business assets and ensure business operations and financial sustainability. The Policy objective is to provide a framework to:

- Define risk governance
- Identify principal risks
- Assess priority risks
- Develop mitigating strategies and actions
- Monitor and review risk activities
- Communicate and report risks

The policy design and section headers are in line with Charity Commission guidance, Charities and risk management (CC26)(2017), and UK corporate governance requirements, FRC risk guidance (2014).

2. Risk Governance

Role	Responsibility
Global Board	Trustees are required to identify and review the strategic, operational, regulatory, people, political and environmental risks to which the organisation is exposed and to assess the likelihood of such risks and the possible level of impact they would have. Trustees must be satisfied that risk management is embedded in the organisation and adequate systems are in place to monitor, manage and, where appropriate, mitigate Sightsavers' exposure to the major risks.
Audit Committee	Detailed review of priority risk log at every Audit Committee meeting.
Management Team	Review of key management reports, issues and actions at every management meeting. Discuss and decide as to whether priority risks need to be introduced, amended or replaced in light of external events or operational challenges.

Role	Responsibility
	Promote risk management processes throughout the organisation and encourage transparency in reporting and speedy issue and risk escalation.
Managers and Staff	Comply with risk management policy and processes and foster an environment where risks can be identified, escalated and mitigated.

3. Principal Risk Identification

Risk is embedded within the organisation and risk management is factored into business planning, performance management, audit and assurance, business continuity management and project management. All projects and countries look at risks specific to their particular context. Enterprise-wide risks that could have a major impact on Sightsavers as a whole are those reviewed by Council and management.

There are myriad enterprise risks to which Sightsavers is exposed. In 2009 the management team took time to identify a 'long list' of around fifty risks, split between six main categories:

- Financial
- Operational
- Legal and regulatory
- Political and environmental
- Strategic
- People

The purpose of introducing categories is to stimulate thinking and ensure that a comprehensive list of potential risks is developed.

Categorisation is not an exact science and there is some debate over whether people risks should be included separately and whether there should be a separate category for reputational risk. Our preferred approach on reputation is to mainstream it by ensuring that any mitigation strategy should include reputational elements arising from the underlying risk.

The long list of risks is reviewed periodically. From this list a subset of circa twelve 'priority risks' are chosen which are considered by management and trustees as particularly relevant and important at that point in time. These must have a high level of significance, and be relevant to the current operational challenges and external environment. Most link to an objective or objectives from our SIM card.

This process replaced a risk log which was far more 'comprehensive' but which had become nothing more than a tick box exercise. Focusing senior management and Council on a smaller number of critical risks means we are able to have far more in-depth discussions about whether these are the correct principal risks, and what we should be doing to mitigate them. Each principal risk is entered into a risk log; it is dated, summarised, categorised, assigned an owner, and linked to specific SIM card objectives.

Priority risks change quite often, we recently brought in cyber security, media crisis given the assertive external environment that charities face, and full consideration of safeguarding matters when developing risk mitigation strategies.

4. Assess Priority Risks

Each priority risk is entered on the risk log. The risk is assessed by considering the following dimensions:

- Risk appetite (high, medium, medium/low, low)
- Significance of the risk (scale of 1-5 where 5 is the most significant)
- Probability of risk occurrence (scale of 1-5 where 5 is the most probable)
- Description of worst-case outcome including a financial quantification if appropriate

In addition, 'direction of travel' is also noted, whether we think that overall the impact of the risk has stayed static since previous review or is changing for better or worse.

5. Risk Mitigation

Each risk has an owner responsible for the mitigation strategy. The key elements of the mitigation strategy are noted on the risk log with summary associated comments. In addition, if a risk has been delegated to a specific Standing Committee of the Global Board this is also captured.

A key element of our approach is to capture 'RAG' status which relates to our progress on mitigating the risk rather than on 'retained risk'. Our view has been that this is far more useful as it indicates what management should be focusing on rather than simply ranking risks post mitigation. Red means the strategy is not yet finalised (or can mean that the current strategy has not been found to be adequate to mitigate so we are 'back to the drawing board'), Amber means we have a strategy but have not yet fully implemented it, and Green means we have taken all the actions we think are required.

It is designed to be a dynamic process, both in terms of considering what the top risks are and looking at strategies to mitigate them. These strategies provide the foundation for developing our key operational and financial processes such as Safeguarding, Reserves, Investment and Treasury Management policies.

6. Risk Monitoring and Review

The Global Board is ultimately responsible for the system of risk management and internal control and through the Audit Committee reviews the effectiveness of this system.

Every year the Global Board considers in depth the nature and extent of the principal risks that Sightsavers is willing to take to achieve its strategic objectives. For each principal risk, risk appetite is assessed to balance opportunities for business development and growth in areas of potentially higher risk, whilst maintaining reputation and reasonable levels of broad stakeholder support.

The Audit Committee reviews the risk log at each meeting.

Review of key management reports, issues and actions is done at every monthly management meeting. There are discussions to decide as to whether priority risks need to be introduced, amended or replaced in light of external events or operational challenges. It is an accountability of senior management to promote risk management processes throughout

the organisation and encourage transparency in reporting and speedy issue and risk escalation.

Priority risks are reviewed regularly by the Director of Governance, Legal and Assurance, the Internal Audit Manager and the Controller of Governance and Assurance and considered when developing the annual internal audit plan and key risk focus. Key risks are also assessed and referenced in the development of the audit approach for each individual internal audit review.

In addition, the risk list is reviewed in depth by senior management prior to each Audit Committee and annual review of risks by the Global Board.

7. Risk Communication and Reporting

Trustees are required to report on the adequacy of the risk management framework under Charities SORP - Accounting and Reporting by Charities: Statement of Recommended Practice applicable to charities preparing their accounts in accordance with the Financial Reporting Standard applicable in the UK and Republic of Ireland (FRS 102) (effective 1 January 2015)

As well as a risk systems adequacy statement, a description of each priority risk is published by trustees in the annual report.

Risk management is factored into business planning, performance management, audit and assurance, business continuity management and project management and monitoring. All projects and countries look at risks specific to their particular context. Project risk logs are published on the programme portal alongside other relevant documentation.

Partner risk processes inclusive of safeguarding and financial control elements are assessed as a core element of partner due diligence. If their policy/processes are deficient we will either not work with them or where it is deemed essential that Sightsavers do partner, policies will be developed as part of the early stages of the partnership, led by the due diligence process. These should include child safeguarding and risk management elements and partners could use our policies as a foundation, adapted to the legislation of the relevant country.

This Risk Management policy is published on its Sightsavers' website alongside other key policies such as Safeguarding and Programme Partnership.

Appendix 1: Charity Commission: Charities and Risk Management (CC26)

https://www.gov.uk/government/publications/charities-and-risk-management-cc26

Appendix 2: Institute of Risk Management Guidance and FRC

https://www.theirm.org/join-our-community/special-interest-groups/charities/

https://www.theirm.org/media/3296897/0926-IRM-Risk-Appetite-12-10-17-v2.pdf

https://www.frc.org.uk/getattachment/d672c107-b1fb-4051-84b0-f5b83a1b93f6/Guidance-on-Risk-Management-Internal-Control-and-Related-Reporting.pdf

The documents contained in the links above summarise UK Corporate Governance Code requirements and notes selected company approaches to designing and implementing risk appetite statements, and provide guidance on creating, embedding and further developing risk management frameworks

We work with partners in low and middle income countries to eliminate avoidable blindness and promote equal opportunities for people with disabilities.

www.sightsavers.org

www.sightsavers.org

Registered charity numbers 207544 and SC038110

Sightsavers