RISK MANAGEMENT POLICY AND FRAMEWORK

Policy ID: HA/POL/DEMS

Author: Dr Ahmed Nasr

Owner: Performance and Accountability

Sign off: Dr Ahmed Nasr

Version: 3

Last updated: July 2024

Next review: End of July 2026

Risk Management Policy and Framework

1. About Human Appeal

Human Appeal (HA) is an international relief and development NGO, established in 1991 to relieve the suffering of those experiencing poverty, social injustice and natural disasters and to improve the quality of life of underprivileged communities through education, health, and social development. Human Appeal works both directly and with partners in 25 countries, carrying out emergency relief, short and long-term projects in orphan welfare, education, safe water, medical care, and income generation. We are committed to providing the highest quality service and support to our customers and essentially to our beneficiaries.

2. Risk Management Policy

Risks is defined as: The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

2.1. **Policy introduction and statement of intent**

Human Appeal will maintain a sound risk management system that will support good management and governance. The CEO, BoD members and the Trustees of Human Appeal are fully committed to ensuring the successful implementation of this policy and framework and promoting the culture of effective risk management across the organisation. The board will use the risk management framework outlined in this policy as a means to help achieve the aims defined in the organisational strategic plan as well as the business objectives.

Risk Management will form part of the organisation's decision-making, strategic, and operational planning.

2.2. Risk assessment will be conducted on all new projects and activities by the appropriate department managing the project to ensure that it is in line with Human Appeal's objectives and mission.
2.3. Any Risk or opportunities arising will be identified, analysed and reported at an appropriate level.
2.4. A Risk Register covering key strategic and departmental risks will be maintained and updated annually and more frequently where risks are known to be volatile.
2.5. Reports will be made to the Audit Committee and the CEO each quarter of continuing and emerging high concern risks and those where priority action is needed for better control.
2.6. Individual error and Serious Incident Reports will be required from individual staff where a reportable event is identified.

3. Aims and objectives

The Risk Management Policy and Framework supports the internal control systems of Human Appeal, enabling it to respond to operational, strategic and financial risks regardless of whether internally or externally driven. The aims and objectives of the policy and framework is to:

3.1. Confirm and communicate Human Appeal's commitment to Risk Management.
3.2. Ensure a consistent framework and protocol for determining appetite and tolerance of risk and managing it.
3.3. Assign responsibility to management and staff for risks within their control and provide a structured process for Risk to be considered, reported and acted upon throughout the Organisation.
3.4. Ensure the chances of adverse incidents, risks and complaints are minimised by effective risk identification, prioritisation, treatment and management.

3.5. Ensure a risk management framework is maintained, which provides assurance to the Board that strategic and operational risks are being managed.
3.6. Ensure risk associated with the health, safety & wellbeing of staff, fraud, project and programme management and information security are minimised.

4. Scope

The Human Appeal risk management policy and framework is intended for use by all its staff members, including contractors, consultants and suppliers. This document is applicable to all strategic and operational risks that Human Appeal could be exposed to, including information governance, programme and project risks. Additionally, the policy and framework is applicable in Human Appeal's regional offices and its overseas operations.

5. Distribution plan

5.1. This document is available to all staff via Human Appeal Intranet sites.
5.2. Notification of the documents will be included in the all staff bulletin, as well as through team meetings and staff induction.

6. Training

All staff will be provided with adequate training on risk management and their role and responsibilities in implementation.

7. Responsibility

This section will clearly outline the responsibilities and obligations of different stakeholders.

7.1. Risk owners

7.1.1. A risk owner is the responsible point of contact for an identified risk, who coordinates efforts to mitigate and manage the risk with various individuals who may also own parts of the risk. The responsibilities of the risk owner are to ensure that:

- Risks are identified, assessed, managed and monitored
- Risks are clearly articulated in risk registers
- Controls and treatment plans are in place to mitigate the risk to within risk appetite

7.2. The Audit Committee

7.2.1. Monitoring and reviewing in detail how effectively the key risks are being managed and how the overall risk management policy and process is operating.
7.2.2. Challenging the SMT and advising the board on overall risk appetite and tolerance of current exposures and future risk strategy.
7.2.3. Promoting the exchange and use of best practice techniques in risk management throughout the organisation.
7.2.4. Regular review of the highest level (corporate) risk register and the risk profile of the organisation, linked to the organisation's business model and strategy.

7.2.5. To regularly review Human Appeal's approach to risk management and approve any changes to this.

7.3. **The CEO**

7.3.1. Ownership of the organisation's overall risk management policy, ensuring that the risk management policy is implemented throughout Human Appeal.
7.3.2. Ensuring that full support and commitment is provided and maintained in every activity relating to risk management.
7.3.3. Setting and instilling an appropriate risk culture across the organisation.
7.3.4. Defining the high level risk appetite of the organisation in liaison with BoD members.
7.3.5. Taking action in respect of any risks – or decisions in respect of risks – that have been escalated by management.
7.3.6. Holding management to account for complying with and operating the organisational risk management processes.
7.3.7. Ensuring that the governance statement, included in the annual reports and accounts, appropriately reflects the risk management processes in operation across.

7.4. **The Board (Executive Directors/Senior Management Team)**

UK Corporate Governance Code (FRC, 2012), states that:

'The board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems.'

The board will be responsible for:

7.4.1. Ensuring that the organisation has effective contingency plans for crises management.
7.4.2. Ensuring risk management is included in the development of plans, budgets and when considering strategic decisions.
7.4.3. Ensuring that risks are actively managed within their business areas.
7.4.4. Ensuring staff and management comply with all organisational policies and procedures and fulfil their responsibility for risk management by identifying, reporting, monitoring and managing risk.
7.4.5. Undertaking a review of the strategic and operational risk register on a quarterly basis to ensure they are current and review implementation of treatment plans, prior to submission to the Audit Committee.
7.4.6. Assuring the Audit Committee on a quarterly basis that risks are being reported and managed appropriately.

7.5. **Operational leads**

7.5.1. Taking the risk management policy and any procedures issued centrally and interpret them for use in their own operation.
7.5.2. Maintaining an up to date risk register for their respective department, ensuring that risks are regularly identified, evaluated and risk treatment is considered.
7.5.3. Involved in setting and communicating risk appetite or the level of risk the manager wants to take.
7.5.4. Deciding on the risk responses or strategies that they will employ to help realise opportunities or manage negative threats.
7.5.5. Playing a key role in the identification of threat and opportunity risks.
7.5.6. To implement adequate corrective action in responding to significant risks; to learn from previous mistakes and to ensure that crisis management plans are sufficiently robust to cope with high-level risk.

7.6. **Compliance**

The Compliance function will:

7.6.1. Maintain oversight, monitor and report on the status and progress of risks documented on the risk register on a daily basis to ensure risks are evaluated, reviewed and managed efficiently by the managers in their respective departments.
7.6.2. Reviewing risks that are common across the organisation for inclusion on Human Appeal corporate risk register (following discussion in the BoD).
7.6.3. Reviewing updates and cases on SIR cases and consider whether risks arising from those incidents should be included in the risk register.
7.6.4. Present relevant information relating to risk management in weekly BoD meeting
7.6.5. Provide regular and timely information to the Audit Committee on the status of Risks and their mitigation.

7.7. **Internal Audit**

7.7.1. Providing objective assurance that risk management processes and the systems of internal control are operating effectively.
7.7.2. Providing assurance that major business risks are being managed appropriately (reviewing the management of key risks).
7.7.3. Giving assurance that risks are correctly evaluated.
7.7.4. Evaluating the reporting of risks.
7.7.5. Coaching management in responding to risks.
7.7.6. Developing and maintaining the risk management framework.

7.8. **All staff**

Responsible for:

7.8.1. Participating (as appropriate) in the identification, assessment, planning and management of threats and opportunities.
7.8.2. Ensuring that they familiarise themselves and comply with the policies and procedures of Human Appeal.
7.8.3. Undertaking and / or attending mandatory and other relevant training courses.

8. The risk management framework

Human Appeal has established a risk management structure which will enable the organisation to monitor and address the strategic risks that would prevent the organisation achieving its aims and objectives as well as setting out the treatment plans for those risks that require action to bring them within risk appetite where possible.

8.1. Risks are linked to the key strategic objectives and aims which exist at different levels.
8.1.1. Strategic risks are risks that affect Human Appeal's ability to deliver the strategy or function as an organisation as a whole
8.1.2. Operational risks – risks that affect the delivery of Human Appeal's business plan or common department risks that require a corporate response
8.1.3. department risks – risks that are related to the delivery of departmental operations and objectives
8.1.4. Programmes and their project outcomes – risks associated with, usually, time limited activities and medium- to long-term delivery of benefits
8.1.5. Human Appeal maintains a strategic risk register, a departmental risk register and a programme risk register.

8.2. The strategic risk register is subject regular review at the BoD
8.2.1. All project risks will be managed by the appropriate departments relevant to the project. Reporting and escalation will be through the Board.

9. The procedure

Risk management is central to the strategic management of Human Appeal. It provides a systematic process for identifying risks attached to new and current business activities. The diagram below describes the process that Human Appeal has adopted to manage risks.

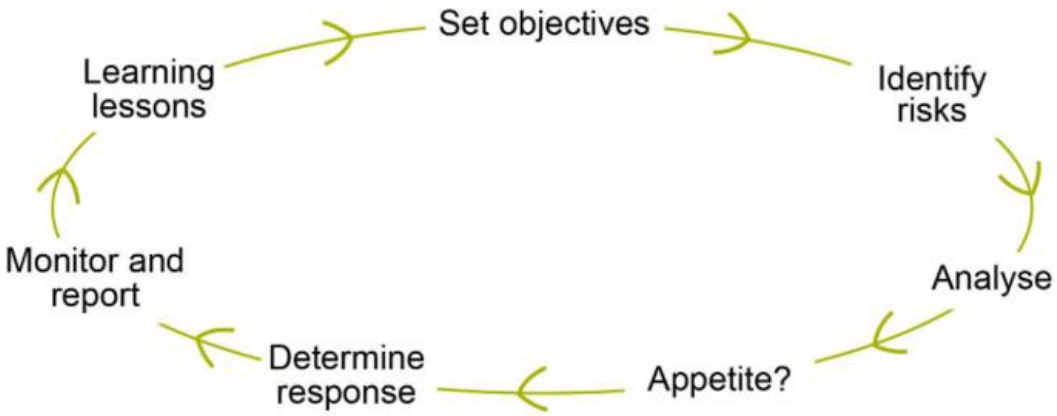


Figure 1 - generic risk management process

The next few pages aims to describe the steps in the risk process of identifying, assessing and managing risks in the Risk Process.

9.1. **Setting objectives**

Risks can only be identified, assessed and prioritised in relation to objectives. The starting point for risk management is business objectives. These objectives can be long term, high level and strategic in nature, and apply to the whole organisation; or they may be short term and operational, and apply to business units, teams, and business processes.

9.1.1. Objecting setting will be an integral process which will link top level corporate planning to business activities and operations.
9.1.2. Key strategic objectives will be set following meetings and discussions between top management through organised planning day.
9.1.3. Every business unit, departments, team and individual must have objectives
9.1.4. Every objective will be clearly and effectively defined and described in order to identify risks to the achievement of objectives.
9.1.5. Objective setting will involve a process of discussion and agreement between those setting the objective and those who are to deliver.
9.1.6. Once agreed, the objectives will be documented for the purposes clarification and referral.

9.2. **Identifying risks**

In order to manage risk, an organisation needs to know what risks it faces. Therefore, risk identification is the first formal step in developing the organisation's risk profile or risk register, the complete list of risks identified by management that may impact upon the achievement of the organisation's objectives.

9.2.1 Recording risks – Human Appeal will maintain an up to date strategic risk register which will be subject to regular review at the BoD meeting. The strategic risk register will be used to record new risks and update existing ones.

9.2.2 Every department will maintain a local risk register (or departmental risk register) to record risks relevant to their functions. The local risk register must be reviewed and update at regular intervals

9.2.3 The risk register must contain the following information:

Risk ID or ref	Risk Title	Risk response
Risk description	Treatment or action plan (mitigation)	Risk owner
Date raised/created	Treatment owner	Risk category
Raised by	Key controls	Risk rating
Department or business area	progress notes	Status
Date of next review		

See appendix 2, risk register guidance.

9.3. **Assessing and evaluating impact and likelihood**

This will involve determining the probability (or likelihood) and the consequences (or impacts) of the risks occurring. Analysis also involves taking a more detailed look at the risks to understand them better.

9.3.1. The assessment will be completed by scoring the likelihood of the risk occurring and impact should it occur.

9.3.2. Appendix 4 shows Human Appeal's scoring matrix which are based on a scale of 1-5 and the risk rating matrix which gives the scoring a RAG (red, amber, green) status.

9.3.3. The risk evaluation will involve making a decision about what should be done with the risk. It includes determining appropriate controls and or treatments for the risk, and what level of risk can be tolerated within Human appeal's risk appetite.

9.3.4. A control is an existing strategy and process currently in place such as systems, policies, procedures, standard business processes, practices, procedures, standard business processes, and practices.

9.3.5. A treatment is an additional strategy/activity we need to develop and implement should the risk level be unacceptable after controls are applied.

9.4. **Risk response and treatment plan**

Having identified, analysed and evaluated the risks, it should then possible to determine the risk responses. There are a number of ways an organisation can respond to risk as set out in the illustration.

9.4.1 Risk responses will be evaluated to ensure they do in fact manage the risks down to the level required.

9.4.2 The remaining 'residual' risk will be assessed. It should be in line with the target residual risk.

9.4.3 If it is reasonable, no further action is required. If it is still excessive, Human Appeal will consider what further responses it will put in place (or not).

9.4.4 Human Appeal will take the following approaches in responding to risk:

- **Terminate (or avoidance)** – Where an activity or system gives rise to significant risk to Human Appeal the activity will be carried out differently or ended hence risk is no longer relevant.
- **Tolerate** - Where it is considered that nothing more can be done at a reasonable cost to reduce the risk or the risk is low.
- **Treat** - This is where action can be taken to reduce the impact or the likelihood of the risk identified.
- **Transfer** – depending on the nature and circumstances of the risks Human Appeal will consider the option of sharing, transferring (e.g. insurance) or outsourcing to third parties (contracting).

9.5. **Monitoring and reporting on risk**

Monitoring is an essential management action in respect of any system, process or activity. Human Appeal will monitor its risk management activities to:

- assess whether or not the risks are changing
- provide assurance that risk management is effective
- identify when further action is necessary

9.5.1 The organisational strategic and the departmental risk will be reviewed and discussed at the weekly BoD meeting and on a quarterly basis in the Audit Committee (AC) meeting.
9.5.2 Status and updates will be provided on the relevant risks.
9.5.3 If the treatment is not reducing the risk a new treatment plan should be considered.
9.5.4 All departments must engage and corporate on the monitoring and reporting of risks.
9.5.5 Updates on the departmental risks must be prepared to be presented at the quarterly AC meetings
9.5.6 The strategic risk register and reports from the operational risk register enables the Board and the AC to be assured of management of the risks
9.5.7 New or emerging risks will be discussed and if relevant, it will be added on the risk register.
9.5.8 Escalation measures will be determined where risks are not being addressed or there are significant delays in taking action to reduce or eliminate risks.

10. Policy Review

This policy will be reviewed on a bi-annual basis to ensure continuing appropriateness.

Appendix 1 – Definition of risk

Institute	Definition
Institute of Internal Auditors – UK and Ireland (2009)	*'. . .the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.'*
The Institute of Risk Management (2008)	*'Risk can be defined as the combination of the probability of an event and its consequences. In all types of undertaking, there is the potential for events and consequences that constitute opportunities for benefit (upside) or threats to success (downside)'*
HM Treasury (UK) (2004, p. 49)	*' . . .uncertainty of outcome, whether positive opportunity or negative threat, of actions and events. It is the combination of likelihood and impact, including perceived importance'.*
Department of Finance (Ireland) (2004, p. 6)	*' . . .a possible loss or other adverse consequence that has the potential to interfere with a Department's ability to achieve its objectives and fulfil its mission'.*
Office of Government Commerce (UK) (2007, p. 156)	*'. . .an uncertain event or set of events that, should it occur, will have an effect on the achievement of objectives. A risk is measured by a combination of the probability of a perceived threat or opportunity occurring and the magnitude of its impact on objectives'.*
ISO 31000 (2009)	*'The effect of uncertainty on objectives'.*

Appendix 2 – Risk register guidance

Risk register heading	Guide
Risk ID	A unique identifier in a numbering system assigned to a risk. The identifier should be used for reference or for cross-reference Date raised Enables us to see how long a risk has been on the risk register for
Business area	Identifies the team the risk affects Risk category This allows us to identify sources of risk.
Risk type	This will be Strategic, Corporate Operational or Team; this field enables risks to be filtered and reported through the internal processes
Raised by	It is good practice to have a name of who raised the risk to enable further clarification or discussion
Risk title	Short title/description of the risk - No more than 10 words
Risk description	Describe the risk event, the cause and the effect. The risk should be articulated clearly and concisely. When wording the risk it is helpful to think about it in three parts and write it using the following phrasing: There is a risk that … This is caused by… Which w/could lead to an impact/effect on …
Risk owner	Should include initials of the person who owns the risk
Inherent risk	Risk impact, likelihood and total score if there were no controls in place to manage the risk
Key controls	Existing strategy and process currently in place such as systems, policies, procedures, standard business processes, practices. A risk may have more than one control
Current risk	Risk impact, likelihood and total score with the controls in place to manage the risk
Risk response	Terminate, tolerate, treat or transfer the risk

Treatment plan	Additional strategy/activity needed to develop and implement should the risk level be unacceptable after controls are applied. There may be more than one treatment plan for a risk
Treatment owner	Should include the names of those responsible for completing the treatment plan(s)
Date by Each	Treatment plan should have a completion date set
Target risk	The risk we aim to get to with controls on place and completing the treatment plan
Progress note	Update on progress
Status	Is the action Complete, ongoing, open

Appendix 3 – Examples for judging impacts when assessing risks

Impact scores				
1 Insignificant	**2 Minor**	**3 Moderate**	**4 Major**	**5 Catastrophic**
• Brief disruption to service delivery • IT services not available for less than 2 hours • Data loss isolated to one or a very small group of people affected • Financial implications are negligible • Short-term low staffing level that temporarily reduces service quality (< one day) • Minimal Injury to staff/visitors etc. • Minimal impact on the quality or timeliness of a project • No impact on reputation	• Some disruption to service delivery of up to 24 hours • IT services not available for up to 8 hours • Small to medium group of people affected by data loss • Some financial implications £50 - £1M • Low staffing level that reduces service quality (up to 48 hours) • Minor reportable injury not requiring RIDDOR report • Some impact on the quality or timeliness of a project • Slight impact on reputation	• Disruption to service delivery of up to 48 hours • IT services not available for up to 48 hours • Large group of people affected by data loss • Moderate financial implications £1-5 million • Late delivery of key objective/ service due to lack of staff • RIDDOR reportable incident • Impact on timeliness of a project, but not quality • Limited damage to reputation	• Unable to deliver services for more than one month • IT services not available for more than one week • Significant group of people affected by data loss • More than 2 ICO fines received in a year due to data breach • High financial implications £5- 15 million • Uncertain delivery of key objective/service due to lack of staff • Major injury/ illness. Might affect more than one person. • Possible enforcement action by HSE • Impact on delivery and quality of programme of projects • Loss of credibility and confidence in Human Appeal • Adverse national press interest. • Independent external enquiry	• Permanent inability to deliver services • IT services not available for over one month • Very high financial implications (>£15 million) • Uncertain delivery of key objective/service due to lack of staff • Loss of Life / Major incident which is more than likely as a result of negligence or which could lead to prosecution. • Loss of credibility and confidence in Human Appeal • Adverse national press interest. • Independent external enquiry • Major public enquiry • Brand tarnished to the extent that re-branding may be necessary

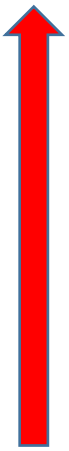
This is not intended as a comprehensive list

Appendix 4 – Scoring and rating matrix

Likelihood Score	1	2	3	4	5
Descriptor	**Rare**	**Unlikely**	**Possible**	**Likely**	**Certain**
Frequency	Not expected to happen for years	Expected to occur at least once in the year	Expected to occur up to once a month)	Expected to occur at least weekly	This type of event will happen frequently

Impact	Likelihood				
	1 Rare	2 Unlikely	3 Possible	4 Likely	5 Certain
5 Catastrophic	5	10	15	20	25
4 Major	4	8	12	16	20
3 Moderate	3	6	9	12	15
2 Minor	2	4	6	8	10
1 Insignificant	1	2	3	4	5

Appendix 5 – Risk escalation and responsibility

Risk score	Risk response	Action	By whom	Escalation
High risk	**Treat/transfer/terminate**			
15-20	Risks deemed as high require a systems approach to identify the root causes of the risk and thereby help choose an appropriate risk response. Where it is not possible to terminate or transfer the risk a treatment plan will be in place	• Corporate Operational risk register reviewed by SMT to consider escalation to Strategic Risk Register • SMT review Strategic risk Register for addition or removal of risks and recommend to the AC • AC review strategic and top corporate operational risks • AC to report risks by exception or of significance to the Board	AC CEO BoD Compliance	
Moderate risk	**Treat**			
8-12	Risks deemed as moderate to high will require a treatment plan in line with the risk appetite. Those risks where it is deemed no further treatment	• Risk register discussed in BoD • Risks identified as amber and red will be discussed to determine whether to	CEO Directors SMT Compliance	

	can reduce the risk will be reviewed regularly to assess impact on the organisation	include it in the corporate risk register • Amber and red risks and associated treatment plans reviewed BoD		
Low risk	**Tolerate**			
1-6	Risks graded as 1-6 either require no action or can be managed through local action or by an appropriate person or department.	•Risk is identified •Risk added to team risk register •Action to reduce risk where necessary is considered •Risk register discussed at team meetings • Project risks discussed with project team	All staff	

Appendix 6 - Glossary

Risk: The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

Opportunity: An uncertain event that would have a favourable impact on objectives or benefits if it occurred.

Likelihood: Is the measure of the probability that the threat or opportunity will happen, including a consideration of the frequency with which this may arise.

Impact: Is the result of a particular threat or opportunity should it actually occur.

Risk management: A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organisation's objectives.

Risk appetite: The level of risk that an organisation is willing to accept.

Risk responses: The means by which an organisation elects to manage individual risks.

Risk assessment: The overall process of risk identification, risk analysis and risk evaluation.

Risk identification: The process of determining which events might occur to affect the objectives of the organisation and their root causes.

Risk analysis: The systematic use of available information to determine the likelihood of specified events occurring and the magnitude of their consequences ie their impact.

Risk evaluation: The process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria.

Inherent (gross) risk: Evaluation of risk before management undertakes any action or initiates any risk responses.

Retained (net) risk: The evaluation of risk after management action and risk responses.

Assurance: Evidence that risks are being effectively managed (e.g. planned or received audit reviews and assurance map).

Control(s): Existing strategies and processes currently in place such as systems, policies, procedures, standard business processes and practices to manage the likelihood or impact of a risk Practices.

Corporate Operational risk register: A record of the risks identified through internal processes that will impact on Human Appeal's business objectives or major programmes.

Current Risk: Risk impact, likelihood and total score with the controls in place to manage the risk.

Gaps in controls or assurances: Where an additional system or process is needed, or evidence of effective management of the risk is lacking.

Incident/ issue: A relevant event that has happened was not planned and requires management action and must be reported as appropriate.

Operational risks: A risk or risks that have the potential to impact on the delivery of business, project or programme objectives. Operational risks are managed locally within departments and significant operational risks are escalated, where appropriate, to SMT via the internal reporting process.