Logo, company name

Description automatically generated

Risk Management Policy

G600 Governance Policies

April 2025

**Contents**

[1 Introduction 2](#_Toc155695103)

[2 Scope and Purpose 2](#_Toc155695104)

[3 Definitions 3](#_Toc155695105)

[4 Risk Identification 4](#_Toc155695106)

[5 Reporting Risk 7](#_Toc155695107)

[6 Risk Owners 8](#_Toc155695108)

[7 Risk Assessments 9](#_Toc155695109)

[8 Treating Risk 13](#_Toc155695110)

[9 Strategic Risk Register 14](#_Toc155695111)

[10 Monitoring 15](#_Toc155695112)

[11 Business Continuity and Risk Management 16](#_Toc155695113)

[12 Roles and Responsibilities 16](#_Toc155695114)

[13 Training and Compliance 18](#_Toc155695115)

[14 Communication and Dissemination 18](#_Toc155695116)

[15 EDI Impact Assessments 19](#_Toc155695117)

[16 Resources 19](#_Toc155695118)

[17 Version Control 19](#_Toc155695119)

1. Introduction
   1. MHA is committed to proactive risk management to protect the safety and wellbeing of all who are employed by, receive services from or are affected by MHA’s activities.
   2. MHA’s risk management culture aims to empower colleagues and volunteers to identify and report risks with the goal of creating a safer and more transparent environment. This depends on an open, just, and fair risk and safety aware culture whereby everyone feels confident and keen to identify and report risks, hazards, incidents, near misses and other concerns, with a view to reducing the likelihood of adverse events occurring and reducing the impact of such events if they do occur.
   3. MHA is regulated by the Charity Commission who provide regulatory guidance and advice to ensure that charities are accountable, well-run, and meet their legal obligations. MHA are required to report serious incidents relating to safeguarding and fraud to the Charity Commission who may ask for additional information or follow up on any reports to ensure that MHA is operating properly within the sector. MHA’s Operations and Audit and Risk Committees are also notified of any incidents reported to the Charity Commission.
2. Scope and Purpose
   1. MHA encourages a culture of responsible risk management practices that all colleagues and volunteers are expected to actively participate in, as well as contribute to the ongoing success of this policy. This policy applies to all MHA colleagues and volunteers (for the purpose of this policy, ‘colleagues’ refer to both those employed by MHA and volunteers from this point onwards).

* 1. This policy describes and clarifies MHA’s approach to risk management and associated assurance arrangements intended to cover the full range of MHA’s services and activities to help ensure:
  2. That people are enabled to live later life well.
  3. Thar care and support are of high quality, safe, effective, responsive, and person-centred.
  4. Effective strategic management and decision making.
  5. Robust operational and departmental management and leadership.
  6. Improved operational development and resilience.
  7. For managing clinical risk specifically, see the Clinical Risk Management Policy [CP010].

1. Definitions

| Term | Definition |
| --- | --- |
| **Business Continuity** | In relation to risk management, business continuity is the practice of ensuring critical operations can continue including service provisions in the face of disruption, disaster, or unforeseen events. |
| **Operational Risk** | Refers to non-strategic risk that relates to the day-to-day activities and processes within an organisation. This includes risks associated with internal operations that may impact on the immediate and ongoing operational aspects of the organisation. |
| **Radar** | Radar is the reporting software that MHA use to manage risk by identifying, tracking, and managing risks. Radar is used for (non-exhaustive):   * Incident reporting * Holding a register of risks * Rating risk * Escalation * Monitoring |
| **Risk** | Exposure to danger, harm, or loss. |
| **Risk Assessment** | The process of evaluation and prioritising risks to gain an understanding of the risk and develop risk control strategies. |
| **Risk Culture** | The collective attitudes, behaviours, and values embedded across the organisation that help to shape risk management. |
| **Risk Management** | Risk Management is the proactive identification, categorisation, and management of risk. MHA aims to reduce and manage the likelihood of risks materialising, and of their consequences when they do. |
| **Risk Owners** | An individual assigned the responsibility and accountability for managing a specific risk or group of risks. |
| **Risk Register** | A central list for recording organisational risks and information relating to identified risks. |
| **SugarCRM** | Database and incident reporting system for Communities and Volunteers. |
| **Strategic Risk** | Refers to the potential threats and uncertainties that may impact MHA’s long-term objectives and goals as an organisation. Strategic risk encompasses risks related to internal and external factors that can impact the overall direction and success of the organisation. |
| **Treating Risk** | The process of taking proactive measures to reduce the likelihood or impact of risks. Treating risk may involve tolerating, transferring, or mitigating risk using control measures. |

1. Risk Identification
   1. **Identifying Operational Risk**
      1. Identifying and managing risk is something everyone on a daily basis, almost everything we do poses some kind of risk that we have to weigh up and manage before proceeding - for example, knowing the risk of crossing a busy road and not crossing until you can ensure it is safe to do so is effective risk management. Identifying and managing risks in the workplace should be as easy as safely crossing a busy road, by being aware of risk and integrating the management of risks into daily decision-making.
      2. Identifying operational risk is an ongoing process that requires input from all colleagues. Identifying operational risk can be done by:
   * Encouraging colleagues to actively report potential risks identified in their day-to-day work to their line management.
   * Engaging with colleagues to gather insights on potential risks they perceive whilst undergoing their daily duties.
   * Using insights taken from the wider industry to benchmark common and recurring operational risk to the organisations processes.
   * Conducting risk assessments to review various functions and sources of risk.
   * Using data from historical incidents to identify patterns and trends relating to operational disruption.
     1. Operational risk may become strategic risk depending on severity and potential disruption that could be caused to the organisation as a whole.
   1. **Identifying Strategic Risk**
      1. Identifying strategic risk involves recognising and assessing the threats and vulnerabilities that could impact on the organisations ability to achieve its long-term objectives and goals. Strategic risks are identified and managed by MHA’s executive and senior leadership. Methods for identifying strategic risks may be:
   * Using the organisations strategies to identify any factors that could impact or impede on the objectives and goals in place to meet the strategy.
   * Considering operational risks and their impact on the organisation as a whole.
   * Analysing internal and external factors that could affect the strategic position of the organisation.
   * Monitoring external factors such as industry trends, dynamics, regulatory changes, legislative changes, and economic shifts that could impact the organisation, including political changes and global events.
   * Developing scenarios that explore various events that could have an adverse impact on the organisation and assessing the risks associated with each scenario.
   * Identifying and researching new and upcoming trends such as digital changes that could disrupt the organisation of impact on the strategic direction of the organisation.
   * Assessing financial risks that could affect the organisations ability to execute strategy.
   * Using data trends taken from reports covering all service areas of the organisation.
   * Establishing an Audit and Risk Committee (ARC) to regularly review and assess the risks that the organisation faces.
   1. Each risk should be explored to identify how it potentially evolves through the organisation. The risk should be clearly defined and explained to facilitate further analysis. Risk registers for each department will provide an essential overview of any identified risk areas. Where appropriate risks are escalated from departmental risk registers to the ELT risk register which will be reviewed by ELT and reported to ARC.
   2. **Audit and Risk Committee (ARC)**
      1. The Audit and Risk Committee is a risk management group that has delegated authority to scrutinise the risk management processes put in place by the organisation and to seek assurance that the controls put in place are effective and to challenge the organisation when they are not. This check and challenge promote a better understanding of risk and facilitates the development of strategies for responding to identified risks.
      2. As part of its responsibility the Audit and Risk Committee reports any matters of concern to the Board, who have ultimate responsibility for ensuring risk of fraud is being managed appropriately
      3. The responsibility for reviewing systems, procedures, and control measures to reduce the risk of fraud in the organisation rests with the ELT who have overall responsibility for the management of the organisation. However, various managers and colleagues within the organisation will also be involved in the risk identification process reporting through their directorates to ELT.
   3. **Identifying Risk from Data and Reports**
      1. Identifying both operational and strategic risk can be done using data taken from reports and events such as:
   * Incident reporting and investigating
   * Internal and external audits/inspections and RA’s
   * Safety Alerts
   * Complaints and claims
   * Inquests
   * Whistleblowing
   * Horizon scanning (monitoring, analysing, and anticipating trends, opportunities, and external factors that may impact the organisations future).
2. Reporting Risk
   1. Reporting risks depends on the severity of the risk and who it may affect. For example, if a colleague comes across a water spillage, immediate action must be taken to treat the risk, this may include putting a wet floor sign out to ensure others are aware of the risk and can avoid the area whilst the risk is reported to the manager and action is taken to clean the spillage and make the area safe again. Assuming no incidents occurred relating to this risk, the manager may record the spillage and action taken to mitigate the risk without escalating the risk further to higher management for treating.
   2. Depending on the risk, Managers may escalate the concern to the relevant responsible individual within that Directorate.
   3. Strategic risk is usually identified centrally by MHA’s executive and senior leadership teams. If colleagues have concerns relating to strategic risk, they should report this to their manager for escalation.
   4. **Unforeseen Incident Reporting**
      1. For the reporting and management of incidents, serious incidents, adverse events, or near misses refer to:
   * Incident Response and Escalation Policy
3. Risk Owners
   1. Risk owners lead on the management and monitoring of risk. For operational risk, this is likely to be the home or scheme manager, area manager, regional director, or team manager (depending on the risk). In all cases, the local manager in the home, scheme, or team, is responsible for actioning control measures the risk owner has put in place whether they are the risk owner or not.
   2. **Strategic Risk Owners**
      1. Strategic risk owners lead on the management and monitoring of strategic risk(s). Depending on the severity of the risk, strategic risk owners may be department managers, Senior Leadership Team (SLT) members, or Executive Leadership Team (ELT) members.
      2. Strategic risk owners are responsible for identifying the risks relevant to their role and department or team. For ELT, the risk usually poses a threat to MHA as a whole or is rated as severe. Once the risks have been identified and agreed by MHA, risk owners use Radar to report the risk and rate it’s significance to MHA including the potential impact of the risk and the likelihood of it occurring. They determine the significance of the risk, it’s consequences to individuals, groups of people, services, or the organisation as a whole. The risk owner must then develop and implement strategies to treat the risk, this may involve contingency plans, or preventative action to reduce the risk. Risk owners must continually monitor the risks and regularly report on the status and management of the risk, which could be the relevant ELT member (depending on the risk). This includes any changes to the plans, or to the risk itself. In some cases, the owner must escalate the risk if it is beyond their control.
4. Risk Assessments
   1. Once a risk has been identified, it can be assessed in terms for potential impact and likelihood of occurrence, as well as categorising risks based on severity and probability.
   2. Risk assessments should identify the hazards, potential harm, existing control measures, level of risk (rating), additional control measures required, residual risk (rating), responsible person, and target completion dates. Using this, an action plan can be developed to help treat the risk, this should include remedial action details, responsible person, and completion dates.
   3. The risk assessment should be reviewed regularly to confirm that it is still valid, to update any changes to the plan, add new controls, and identify any significant changes in the assessment. A further review date should be set.
   4. During the review of the assessment, the assessor should consider the following questions:
   * The controls in place to treat the risks identified – are they designed and operating effectively?
   * The consequences of the risk which remain and are these acceptable in the course of MHA’s activities?
   * The benefits and opportunities which may be presented by the risk.
   * The threats posed by the risk should it be untreated, or control failure occurs
   1. For more information on risk assessments and completing risk assessments, refer to the Risk Assessment Policy.
   2. **Operational Risk Ratings**
      1. The level of risk and residual risk in terms of probability and severity should be rated in the assessment based on the following scale:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Severity** | | | | | | |
| **Probability** |  | **1 Trivial** | **2 Minor** | **3 Serious** | **4 Major** | **5 Fatal** |
| **5 Certain** | 5 | 10 | 15 | 20 | 25 |
| **4 Likely** | 4 | 8 | 12 | 16 | 20 |
| **3 Possible** | 3 | 6 | 9 | 12 | 15 |
| **2 Remote** | 2 | 4 | 6 | 8 | 10 |
| **1 Improbable** | 1 | 2 | 3 | 4 | 5 |
| **Level of risk** | | **Action and Timescale** | | | | |
| **High** | | You should not start work until the risk has been reduced. You may have to set aside considerable resources to reduce the risk. If the risk involves work in progress, you should take urgent action. If it is not possible to reduce the risk even with unlimited resources, you must stop all work. | | | | |
| **Medium** | | You must try to reduce the risk but should carefully measure the cost of prevention. You should use measures to reduce the risk within a defined time period. If the medium risk is associated with extremely harmful consequences, you may need to carry out another assessment to identify more precisely the likelihood of harm. This will help you decide whether you need to use improved control measures. | | | | |
| **Low** | | You don’t need to act or keep documentary records. Monitoring is necessary to make sure that the controls are still effective. | | | | |

* 1. **Strategic Risk Ratings (Scores)**
     1. Strategic risks are scored on their severity and likelihood of occurrence. The risk owner scores the risk on the based on the following tables for consequence (severity) and likelihood):

| **Consequence (Severity)** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Descriptor** | **1 Insignificant** | **2 Minor** | **3 Moderate** | **4 Major** | **5 Catastrophic** |
| Harm (Physical & Mental) \*If you are risk scoring a near miss, choose the most likely descriptor | Insignificant harm (not requiring first aid) | Minor harm or illness (first aid or other treatment required) | Serious harm or illness (requires hospital / paramedic treatment) | Major harm, or long-term incapacity / disability / illness (e.g., loss of limb or ongoing mental health issues) | Death(s) or major permanent incapacity (physical or mental health) |
| Objectives / Projects | Insignificant cost increase / schedule slippage. Barely noticeable reduction in scope or quality | < 5% over budget / schedule slippage. Minor reduction in quality or scope | 5 - 10% over budget / schedule slippage. Reduction in scope or quality requiring client approval | 10 - 25% over budget / schedule slippage. Does not meet secondary objective(s) | > 25% over budget / schedule slippage. Does not meet primary objective(s) |
| Service / Business Interruption | ss / interruption less than 1 hour |  | ss / interruption less than 1 hour |  | ss / interruption less than 1 hour |
| Financial | Low organisational financial loss; less than £10k | Minor organisational financial loss; between £10k-£100k | Moderate organisational financial loss: between £100k-£500k | Major organisational financial loss +£500k | Significant financial loss +£1m |
| Adverse Publicity / Reputation | Localised rumours specific to MHA services | Local Media interest (short term) | Local Media interest (long term) | National Media interest less than 3 days. Local MP concern | National Media interest more than 3 days. National MP concern (questions in the House) |
| Risk Register Only - Human Resources / Organisational Development | Sort term low staffing level temporarily reduces service quality - less than 1 day | Ongoing low staffing level reduces service quality | Late delivery of key objective / service due to lack of staff (recruitment, retention, or sickness). Minor error due to insufficient training. Ongoing unsafe staffing level(s) | Uncertain delivery of key objective / service due to lack of staff (recruitment, retention, or sickness). Serious error due to insufficient training | Non delivery of key objective / service due to lack of staff. Very high turnover. Critical error due to insufficient training |
| **Likelihood** | | | | | |
| **Descriptor** | **1 Rare** | **2 Unlikely** | **3 Possible** | **4 Likely** | **5 Almost Certain** |
| Frequency | Not expected to recur in the next 12 months | Expected to recur at least annually | Expected to recur at least every 6 months | Expected to recur at least monthly | Expected to recur at least weekly |

1. Treating Risk
   1. Treating risk may include control measures that help to avoid or reduce the risk and its consequences. Treating risk may involve tolerating, transferring, or mitigating risk using control measures.
   2. Measures for treating risk must be monitored on a regular basis, the frequency of which depends on the severity and likelihood of the risk.
   3. Monitoring how well control measures are working at treating risk can help to identify whether a new assessment needs to be completed to amend the risk rating and amend the control measures to reflect this.
   4. Strategies for responding to risk generally fall into one of the following categories:
   * Risk retention – choosing and accepting small risks.
   * Risk avoidance – cessation of certain activities to avoid the risk occurring.
   * Risk reduction – implementing effective controls and procedures.
   * Risk transfer – contractual transfer of risk i.e., transferring risks to insurers.
2. Strategic Risk Register
   1. **Strategic Risk Register**
      1. Risks that affect MHA as a whole are considered as ‘Strategic Risks.’ Strategic risks are record these type of risks on a centralised risk register within Radar. The risk register includes the following information about the risks:
   * Reference
   * Category
   * Description
   * Owner
   * Risk Identified Date
   * Impact of Risk
   * Last Review Date
   * Next Review Date
   * Status (compliant, planned, pending, or overdue)
   * Original Score
   * Current Score
   * Risk Controls
   * Attachments
   * Links
   * Comments
   * History
   1. **Strategic Risk Categories**
      1. MHA’s risk register categories are an amalgamation of the most serious risks that the organisation faces. These include:
   * IT, Data and Digital Capability
   * Change Management
   * People (Capacity & Engagement)
   * Financial Resilience
   * External Environment
   * Reputation and Brand
   1. **Strategic Risk Controls**
      1. MHA’s risk controls in Radar include a description of the action to be taken, the adequacy of this action in treating the risk, assurance this will provide, and the status of the control being implemented. Each control also has an ‘owner’ which may be someone the overall risk owner has delegated the individual control to. Each control also has its own due date and review date.
   2. **Strategic Risk Appetite**
      1. The strategic risks in Radar are assigned a response status as to whether they need to be treated, tolerated, transferred, or mitigated, this comes from the risk appetite which refers to the levels of acceptable risk. MHA’s risk appetite considers factors such as tolerance, financial capacity, regulatory requirements, and strategic goals. The risk appetite helps to prioritise risks further and to establish boundaries in decision making regarding the risk and it’s controls.
3. Monitoring
   1. The risk owner for both operational and strategic risk must ensure that recorded risks are robustly and routinely monitored and updated on a regular basis depending on the risk’s rating, or sooner if there is a change in circumstance or the risk itself.

Strategic Risk Monitoring

* + 1. The relevant ELT member must provide oversight, support, and guidance to the risk owner (unless they are the risk owner) in all stages of risk management including the approval of an escalation and closure process for risks.
    2. On a monthly basis, a risk register report is provided to the Executive Leadership Team to review the strategic risks that MHA face. This report includes matters for consideration such as:
  + New strategic risks that have been identified and their ratings.
  + Strategic risks that have been removed from the risk register.
  + Strategic risks that have an increase or decrease in risk rating.
  + Consideration of all other strategic risks where there has been no movement.
  + Consideration of the strategic risk register to establish if there are any newly emerging risks which need to be captured.
  + Monitoring of the use of Radar and SugarCRM (communities). This could include details on which users have been activated, reviewed their risks, and the number of risks assigned to each individual.

1. Business Continuity and Risk Management
   1. For business continuity, refer to Business Continuity and Emergency Policy. Business continuity is a subset of risk management that focuses on maintaining critical operations and services during and after disruptive events (example events may include a cyberattack, pandemic, gas leak). Business continuity and risk management assist in minimising disruption and protect the organisations reputation and enhances sustainability.
2. Roles and Responsibilities

| Role | Responsibilities |
| --- | --- |
| **All Colleagues and Volunteers** | All MHA colleagues and volunteers share the responsibility for risk management in identifying and reporting all risks as quickly as possible to local management. |
| **Local Managers** | Responsible for the risk identified in their area. |
| **Internal Audit** | Ensure that risk management processes are effective and compliant with relevant regulations and best practices. |
| **Senior Leadership Team (SLT) and Department Heads.** | MHA’s Senior Leadership Team (SLT) have responsibility to ensure that the risks in their assigned area (e.g., department / location) are identified and actively managed and are responsible for updating of risk management records and relaying changes to their ELT representative on a monthly or more frequent basis where the risk level is ‘high,’ to contribute the risk management process. |
| **Executive Leadership Team (ELT)** | Executive Leadership Team (ELT) have overall responsibility for ensuring risks are managed effectively, and for providing assurance to the Board in this regard, for each area of identified significant risk. |
| **Chief Executive Officer (CEO)** | Responsible for ensuring that ELT are focused on strategic risks that could prevent the organisation achieving its strategic objectives. |
| **Operational Committee** | To scrutinise the risk management processes put in place by the organisation and to seek assurance that the controls put in place are effective and to challenge the organisation when they are not in relation to operational risks such as risks relating to people and property. |
| **Finance and Capital Expenditure Committee** | To scrutinise the risk management processes put in place by the organisation and to seek assurance that the controls put in place are effective and to challenge the organisation when they are not in relation to financial related risk. |
| **Audit and Risk Committee (ARC)** | To scrutinise the risk management processes put in place by the organisation and to seek assurance that the controls put in place are effective and to challenge the organisation when they are not. |
| **Board of Trustees** | The Board are responsible for setting the risk appetite for the organisation in line with the strategic objectives and the risks that have been identified. The Board scrutinises and mitigations put in place to gain assurance they are effective. |

1. Training and Compliance
   1. MHA’s online learning platform the Learning Zone provides the following courses on risk management:
   * Risk Assessment (Statutory)
   * Risk Assessment in the Home (MHA Mandatory)
   * H&S Risk Management (Statutory)
   * Risk and Safety Management for Senior Leaders
   1. Compliance is assessed through the learning zone, RADAR and SugarCRM reporting, as well as direct observation, monitoring, and supervision of our colleagues.
   2. **Regulatory and Statutory Compliance**
   3. MHA’s risk management process complies to regulatory and statutory requirements for ensuring the safety and wellbeing of those who use MHA services, colleagues, volunteers, and all others who engage with MHA. This includes.
2. Communication and Dissemination
   1. This policy is disseminated and implemented within all MHA services through MHA’s channels of communication.
   2. Each colleague’s line manager must ensure that all teams are aware of their roles, responsibilities.
   3. This policy will be available to the people we support and their representatives in alternate formats, as required.
   4. Any review of this policy will include consultation with our colleagues, review of support planning, incident reports, quality audits and feedback from other agencies.
   5. Queries and issues relating to this policy should be referred to the Standards and Policy Team [policies@mha.org.uk](mailto:policies@mha.org.uk)
3. EDI Impact Assessments
   1. Equality, Diversity, and Impact Assessment to be confirmed.
4. Resources
   * Clinical Risk Management Policy
   * Risk Assessment Policy
   * Business Continuity and Emergency Policy
   * Incident Response and Escalation Policy
5. Version Control

| Version | Version Date | Revision Description / Summary of Changes | Author | Next Review Date |
| --- | --- | --- | --- | --- |
| 4 | January 2024 | * Regular compliance review. * Policy updated to reflect MHA’s approach to risk management, previously the policy focused on financial risk management. * Version reviewed by Head of H&S, Head of Quality Assurance, and the Head of Quality Improvement. | * General Counsel / Company Secretary * Standards and Policy Manager | January 2027 |
| 5 | March 2024 | * Addition of content relating to the Charity Commission. * Resource list updated. | * General Counsel / Company Secretary * Standards and Policy Manager | January 2027 |
| 6 | June 2024 | * Amended policy references due to new Incident Response and Escalation policy | Head of Standards and Policy | January 2027 |
| 7 | April 2025 | * Included reference to Communities reporting on SugarCRM * Advised by CRM systems manager | Head of Standards and Policy | January 2027 |