مؤسسة زمزم
ZAMZAM
FOUNDATION

Risk Management Policy

TABLE OF CONTENT

1.0 INTRODUCTION

This policy and framework sets out Zamzam approach to managing risk to ensure it meets its overall objective to commission high quality and safe services. In addition, the adoption and embedding within the Organisation of an effective risk management policy and processes will ensure that the reputation of Zamzam is maintained and enhanced, and its resources are used effectively to reform services through innovation, large-scale prevention, improved quality and greater productivity.

1.2 Objective

The main objective of this policy is to ensure sustainable growth with stability and to promote a pro-active approach in reporting, evaluating and resolving risks associated with the business. In order to achieve the key objective, the policy establishes a structured and disciplined approach to Risk Management, including the development of the Risk Matrix, in order to guide decisions on risk related issues. The specific objectives of the Risk Management Policy are:

- To ensure that all the current and future material risk exposures of the Organisation are identified, assessed, quantified, appropriately mitigated and managed.
- To establish a framework for the Organisation risk management process and to ensure its implementation.
- To ensure systematic and uniform assessment of risks related with construction projects and operational power stations.
- To enable compliance with appropriate regulations, wherever applicable, through the adoption of best practices.
- To assure growth with financial stability

This policy applies to all employees and contractors of Zamzam. Managers at every level have an objective to ensure that risk management is a fundamental part of the approach to integrated governance. All staff at every level of the Organisation is required to recognize that risk management is their personal responsibility.

Independent contractors are responsible for ensuring compliance with relevant legislation and best practice guidelines and for the development and management of their own procedural documents. Independent contractors are required to demonstrate compliance with risk management processes which are compatible with this policy.

1.3 Definitions

The following terms are used in this document:

- Risk is the chance that something will happen that will have an impact on the achievement Zamzam objectives. It is measured in terms of likelihood (frequency or probability of the risk occurring) and severity (impact or magnitude of the effect of the risk occurring).
- Risk appetite/risk tolerance the organization’s unique attitude towards risk taking that in turn dictates the amount of risk that it considers is acceptable.
- Risk management is the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.
- Risk assessment is the process for identifying, analyzing, evaluating, controlling, monitoring and communicating risk.
- Residual risk the risk remaining after the risk response has been applied.
- Risk strategy defines the Organisation standpoint towards dealing with various risks associated with the business. It includes the Organisation decision on the risk tolerance levels, and acceptance, avoidance or transfer of risks faced by the Organisation.
- Risk Description Is a comprehensive collection of information about a particular risk recorded in a structured manner.
- Risk Register. A ‘Risk Register’ is a tool for recording the risks encountered at various locations and levels in a standardized format of Risk Description.

1.4 Types of risks

1. Compliance risks.
   Are those where the Organisation fails to meet its corporate and legal obligations. These include reporting, accounting, licensing, workplace relations, and work health and safety activities. Tolerance for compliance risks assessed as ‘high’ or ‘extreme’ is generally low. While organizations must comply with such obligations, with risk management controls in place the same risks may receive an assessment of ‘medium’ or ‘low’ and therefore may be considered valid.

2. Organizational risks.
   Are those where the Organisation fails to achieve objectives such as level of service delivery, standard of service delivery, or meeting stakeholder expectations. Consequences arising from such risks eventuating may include loss of reputation or high staff turnover.

3. Opportunity risk
   These risks arise from the pursuit of opportunities – ‘positive risks’ – that may enhance the Organisation in some way or allow it to more easily achieve its objectives. Such risks can be listed in an Opportunities Register (separate from the Risk Register). For these risks, consideration should be given to the potential gains for the Organisation as well as to the resources required to pursue the opportunities.

2.0 RISK MANAGEMENT FRAMEWORK

This policy sets out the Zamzam's risk management framework for how risk management will be implemented throughout the Organisation to support the realization of the strategic objectives.

This includes the processes and procedures adopted by Zamzam to identify, assess and appropriately manage risks and detailed roles and responsibilities for risk management.

In order to fulfil the objectives of this policy and lay a strong foundation for the development of an integrated risk management framework, the policy outlines the following guiding principles of Risk Management

- All decisions will be made with the prior information and acceptance of risk involved.
- The Risk Management Policy shall provide for the enhancement and protection from uncertainties and consequent losses.
- All employees shall be made aware of risks in their respective domains and their mitigation measures
- The risk mitigation measures adopted shall be effective in the long-term and to the extent possible be embedded in the activity of the Organisation.
- Risk tolerance levels will be regularly reviewed and decided upon depending on the change in Organisation strategy.
- The occurrence, progress and status of all risks will be promptly reported and appropriate actions be taken thereof.

Zamzam's risk management reporting structure is set out in appendix 1.

2.1 <u>Risk assessment</u>

The process of Risk Assessment shall cover the following:

- Risk Identification and Categorization – the process of identifying the exposure to uncertainty classified as Strategic / Business / Operational.
- Risk Description – the method of systematically capturing and recording the identified risks in a structured format.

- Risk Estimation – the process for estimating the cost of likely impact either by quantitative, semi-quantitative or qualitative approach

Whenever risks to the achievement of Zamzam's objectives have been identified, it is important to assess the risk so that appropriate controls are put in place to eliminate the risk or mitigate its effect. To do this a standard risk matrix is used, details of which are provided at appendix 2*,* guidance on risk assessment and action.

Using this standardized tool will ensure that risk assessments are undertaken in a consistent manner using agreed definitions and evaluation criteria. This will allow for comparisons to be made between different risk types and for decisions to be made on the resources needed to mitigate the risk.

Risks are assessed in terms of the likelihood of occurrence/re-occurrence and the consequences of impact, using a standardized 5x5 risk matrix (see appendix 2). For each risk that is not adequately controlled, an action plan to reduce or eliminate the risk is required. The implementation of the action plan and residual risk assessment must be kept under review, to assess whether planned actions have reduced or eliminated the risk as expected.

2.2 Categories of risk

There are three categories of risk:

- **High** – the consequence of these risks could seriously impact upon the achievement of the organization's objectives, its financial stability and its reputation. Examples include loss of life, extended cessation or closure of a service, significant harm to a patient(s), loss of stakeholder confidence, failure to meet national targets and loss of financial stability.

- **Moderate** – these are significant risks that require prompt action. With a concerted effort and a challenging action plan, the risks could be realistically reduced within a realistic timescale through reasonably practical measures, such as reviewing working arrangements, purchase of small pieces of new equipment, raising staff/beneficiaries awareness etc.

- **Low**– these risks are deemed to be low level or minor risks which can be managed and monitored within the individual department, at operational level. These risks cause minimal or limited harm or concern.

Once the category of risk has been identified, this then needs to be entered onto the Zamzam's risk register.

Any risk that is identified through the risk assessment process (as well as the incident reporting system) and which Zamzam are required legally to report will be reported accordingly to the appropriate statutory body.

2.3 Identification of risks

As defined earlier, risks are events or conditions that may occur, and whose occurrence, if it does take place, has a harmful or negative impact on the achievement of the organization's business objectives.

Key characteristics by which risks can be identified are:

- Risks are adverse consequences of events or changed conditions
- Their occurrence may be identified by the happening of trigger events
- Their occurrence is uncertain and may have different extents of likelihood

Recognizing the kind of risks that company is/may be exposed to, risks will be classified broadly into the following categories:
Strategic Risk: include the range of external events and trends that can adversely impact the Organisation strategic growth trajectory and destroy stakeholder value.

Business Risk: include the risks associated specifically with the Organisation and having an adverse impact on the Organisation capability to execute activities critical for business growth, thereby affecting its near-term performance.

Operational Risk: are those risks which are associated with operational uncertainties like unpredictable changes in water levels, force majeure events like floods affecting operations, internal risks like attrition etc.

2.4 Managing risk

There are a number of ways in which risks can be managed, including:

- **Avoiding the risk** by not undertaking the activity generating the risk.
- **Eliminating the risk** where this is possible and cost effective through the use of control measures.
- **Reducing the risk** to an acceptable level if it can't be eliminated.
- **Transferring the risk** either fully or in part to another body – this may not always be possible if Zamzam retains statutory responsibility. An example would be insurance arrangements, e.g. the Litigation Authority, where the payment of premiums means that in the event of a claim arising, the authority bears the financial risk, or through contractual arrangements, partnerships or joint working where there is shared risk.

- **Monitoring of the risk** but taking no action, particularly where it is a relatively low risk or cannot be eliminated, reduced or transferred.

2.5 Risk appetite

Zamzam endeavors to reduce risks to the lowest possible level reasonably practicable. Where risks cannot reasonably be avoided, every effort will be made to mitigate the remaining risk. However there is the recognition that by understanding the organizations ‘risk appetite’, this will ensure Zamzam support a varied and diverse approach to commissioning, particularly for practices to work proactively to improve efficiency and value.

Risk appetite is the amount of risk that the Organisation is prepared to accept, tolerate or be exposed to at any point in time. It can be influenced by personal experience, political factors and external events. Risks need to be considered in terms of both **opportunities and threats** and should not be confined to money. They will also invariably impact on the capability of ZamZam, its performance and its reputation.

The governing body will set boundaries to guide staff on the limits of risk they are able accept to in the pursuit of achieving its organizational objectives. The governing body will set these limits annually and review them as appropriate.

The governing body will set these limits based on whether the risk is:

- A threat: the level of exposure which is considered acceptable
- An opportunity: what the governing body is prepared to put ‘at risk’ in order to encourage innovation in creating changes.

2.6 Risk Description

A risk description helps in understanding the nature and quantum of risk and its likely impact and possible mitigation measures. Risk descriptions for each of the risks identified in the Risk Matrix are to be documented and recorded in a structured format in each area where the risk is identified. The suggested format is provided under the annexes.

2.7 Risk registers

- Zamzam maintains a risk register, which is a management tool used to provide it an overview of all significant ‘live’ risks facing the Organisation and the action being taken to reduce them. The risks included within the register are varied and cover the entirety of Zamzam activities, from health and safety risks to risks around the delivery of services and achieving financial balance. The register is used by managers to monitor and manage risks at all levels within the Organisation.

- Current and potential risks are recorded on the risk register and include actions and timescales identified to minimize such risks. The risk register is a log of risks that threaten the organization’s success in achieving its aims and objectives and is populated through the risk assessment and evaluation process.

- All risks will be managed by the risk management group as part of the director and senior team meetings. The risk management function will be overseen by the audit and risk committee to obtain assurances that there is an effective system operating across Zamzam. This approach provides greater focus on moderate and high-level risks which Zamzam faces and allows further challenge and scrutiny of actions taken to mitigate risks through the input of all directors and senior team members.

- Strategic risks will be monitored by the governing body on a six-monthly basis as part of the governing body assurance framework. In addition, the audit and risk committee will make recommendations to the governing body on any high risks that require a more detailed focus as appropriate.

- Risks categorized as low are reported on a low level risk register. Ongoing review and management of these risks will take place on a quarterly basis as part of the director and senior team meeting.

- A risk register standard operating procedure is available and provides further detail and advice on the completion of risk register. This is further supported by a robust training programme for all identified risk leads.

2.8 <u>Risk Materialization</u>

If a risk materializes whilst it is being managed through the risk register, it should be recorded as an incident. Management of risks and incidents is interdependent since risks can be identified through the monitoring of incident themes and trends. If a particular type of incident continues to occur, this is an indication that there is a risk that requires management through the risk register.

If a risk materializes whilst it is being managed through the risk register, it should be considered whether it needs removing from the risk register. Reasons for occurrence should be analysed and evidence established as to whether a trend of similar incidents exists, that need to be managed through the risk register. If the risk is certain to materialize again or has the potential to re-occur, the risk should remain on the risk register for on-going management in order to ensure that underlying causes are addressed. If there is no chance it could happen again, the risk should be closed with an explanation that the incident management process is being followed in order to invoke actions to deal with consequences. A risk materialization flowchart is attached at appendix 4.

The risk that has materialized should be recorded as an incident and Zamzam's incident management process should be followed.

Incident reports are reviewed at the executive and quality and safety committees as appropriate and this provides an opportunity for themes and trends to be picked up. The executive committee receives a report on a quarterly basis about non-clinical incidents and the quality and safety committee receive quality reports about clinical incidents reported by member practices. These reports may indicate that there is a strategic risk e.g. if a lot of practices are regularly reporting incidents around ambulance response times or referral problems. This is the most likely way that risks will be identified from incidents. It is highly unlikely that anything reported by Zamzam staff will become a risk e.g. information governance or health and safety incidents, although not impossible.

2.9 Assurance Framework

Zamzam is required to provide an annual assurance that they have robust systems in place across the Organisation to manage risk. This assurance comes in the form of an annual governance statement which must form part of the organization's statutory accounts and annual report.

In order to produce a proper report, the governing body must be able to demonstrate that they have been kept properly informed about the risks facing the Organisation and has received assurances that these risks are being managed in practice, including that gaps in controls intended to manage risks have been identified and action taken to address them. The governing body will be able to demonstrate that it has met this requirement through the establishment of a robust and formal assurance framework.

Together with this policy and the risk register, the assurance framework is the key document used by the governing body to monitor the position in relation to risk management, providing it with a sound understanding of not only the key risks facing the Organisation but also the action being taken to manage and reduce them.

The assurance framework is firmly connected to the organization's principal objectives as set by the governing body, and is a live document, maintained on an on-going basis. The assurance framework is monitored by the audit committee and governing body on a six monthly basis.

The assurance framework sets out:

- The organization's principal objectives;
- Any significant risks that may threaten the achievement of those objectives (detailed in the supporting strategic risk register);
- The key controls intended to manage these risks;
- The assurance available to demonstrate that controls are working effectively in practice to manage risks together with the source of that

assurance. Any areas where there are gaps in controls and/or assurances; and how the Organisation plans to take corrective action where gaps have been identified in either controls or the assurances available.

Duties and responsibilities

The following table sets out the duties and responsibilities:

Governing Body	The governing body has delegated responsibility from members for setting the strategic context in which organizational process documents are developed, and for establishing a scheme of governance for the formal review and approval of such documents.
General Director	General Director has overall responsibility for the strategic direction and operational management, including ensuring Zamzam process documents comply with all legal, statutory and good practice guidance requirements. • Ensuring the implementation of an effective risk management framework, supporting risk management systems and internal control; • Continually promote risk management and demonstrate leadership, involvement and support; • Ensuring an appropriate committee structure is in place and developing the corporate governance and assurance framework; • Meeting all the statutory requirements and ensuring positive performance towards the achievement of the Zamzam strategic objectives; • Ensuring all directors and senior leads are appointed with managerial responsibility for risk management.
Finance and admin Manager	The Finance and admin manager has a responsibility for: • Providing expert professional advice to Zamzam governing body on the effective, efficient and economic use of Zamzam's allocation to remain within that allocation and identify risks to the delivery of required financial targets and duties. • Ensuring robust risk management and audit arrangements are in place to make appropriate use of the Zamzam's financial resources. • Ensuring appropriate arrangements are in order to identify risks and mitigating actions to the delivery of projects and resource releasing initiatives; • Incorporating risk management as a management technique within the financial performance management arrangements for the Organisation;

Head of audit department	The head of risk and audit is the lead for risk management and has a responsibility for: • Ensuring risk management systems are in place throughout the Zamzam, co-coordinating risk management in accordance with this policy; • Ensuring the assurance framework is regularly reviewed and updated; • Ensuring that there is an appropriate external review of Zamzam's risk management systems and that these are reported to the governing body; • Overseeing the management of risks as identified by the quality, safety and risk committee, ensuring risk action plans are put in place, regularly monitored and implemented; • Incorporating risk management as a management technique within the performance management arrangements for the Organisation; • Ensuring that systems are place for assuring the commissioning of high quality and safe services, and the on-going monitoring of the same; • Ensure incidents, claims and complaints are and managed used the appropriate procedures.
Audit and Risk Committee (ARC)	The ARC has overall responsibility for assuring the governing body that Zamzam has an effective system of internal control and risk management in place. The committee reviews the assurance framework and risk management systems and processes, which includes a review of the corporate risk register. It reports annually on its work in support of the annual governance statement, specifically commenting on the fitness for purpose of the governance and assurance arrangements, the extent to which it considers the application of risk management as a discipline to be embedded within the Organisation. The ARC has overall responsibility for risk management, including reviewing the risk registers.
Senior Leads	All senior leads have a responsibility to incorporate risk management within all aspects of their work and are responsible for ensuring the implementation of this policy by: • Demonstrating personal involvement and support for the promotion of risk management; • Ensuring staff under their management are aware of their risk management responsibilities in relation to this framework; • Setting personal objectives for risk management and monitoring their achievement; • Ensuring risk are identified, managed and mitigating actions are implemented in functions for which they are accountable; • Ensuring a risk register is established and maintained that relates to their area of responsibility, ensuring risks are escalated where they are of a strategic in nature; • Ensure incidents, claims and complaints are reported and managed used the appropriate procedures.

All Staff	All staff, including temporary and agency staff, are responsible for: • Complying with relevant process documents. Failure to comply may result in disciplinary action being taken • Co-operating with the development and implementation of policies and procedures and as part of their normal duties and responsibilities • Highlighting any changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and advising their line manager accordingly, that could impact on this framework • Identifying risks in relation to their working environment and role, and take appropriate action to assess them, take action and/or report them to their line manager • Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager • Attending training / awareness sessions as appropriate.
Senior governance	The senior governance manager and senior governance officer will provide risk management support and advice to Zamzam as part of a service line agreement.

3.0 RISK MANAGEMENT STEPS

3.1 Establishing the context.

The purpose of this step is to determine the scope for all risk management activities. This includes both the internal and external environments in which risks may occur: strategic, operational, financial, competitive, stakeholder, social, cultural and legal.

In this step you will need to:

- Confirm organizational objectives
- Identify stakeholders.
- Define risk assessment criteria

3.1.1 Confirm Organizational Objective.

Because risk is 'the effect of uncertainty on organizational objectives', you cannot begin to assess risk until you know exactly what an organization's objectives are. The first step is to confirm these objectives. They will have been established as part of Zamzam planning processes.

Broadly, the Risk Management Process is the whole set of activities to carry out to identify, assess, manage and monitor any risks to which your Organisation may be exposed.

3.1.2 Identify Stakeholder

Part of the context for risk is stakeholders – those with whom an Organisation consults, communicates and interacts. Developing a list of stakeholders generally assists in determining what risk information is communicated to whom, and who should be consulted on which risk issues. This process will also help inform Zamzam initial and ongoing consultation and communication processes.

3.1.3 Define Risk Assessment Criteria

Define criteria against which the significance of a risk can be evaluated. These criteria should reflect Zamzam objectives, values and resources, and should be consistent with this Policy. Some criteria will necessarily be imposed by, or derived from, legal and regulatory requirements and any other requirements Zamzam subscribes to.

Factors to consider when defining risk assessment criteria include the following:

- The nature and types of causes and consequences that can occur and how they will be measured.
- How 'likelihood' will be defined.
- The timeframe(s) of the likelihood and/or consequence(s).
- How the level of riskis to be determined.

- The views of stakeholders.
- The level at which risk becomes acceptable or tolerable.

Whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered. Once you've defined and documented the risk assessment criteria, don't forget to review them on a regular basis. They may need to be amended or refined as the Organisation evolves and/or as the external environment changes.

3.2 Risk assessment

Having established the context, you can now begin the process of assessing the potential risks. There are 3 stages:

- Risk identification
- Risk analysis
- Risk evaluation

3.2.1 Risk Identification

The purpose of this step is to identify all of the risks Zamzam may be exposed to, as well as their sources and causes, their potential consequences and areas of impact, and any risk management controls already in place. As the process is going on, the information gathered shall be entered into the Risk Register. By the end, a comprehensive list of risks and controls are maintained.

It is important that all potential risks are identified in this step. Any risk overlooked here will not be captured in the subsequent analysis and evaluation stages:

There are three tasks:

- Identify categories of risk
- Identify risks
- Identify existing risk management controls.

3.2.2 Risk Evaluation

The purpose of this step is to list risks in order of priority for action. The list will show which risks need treatment and which don't; and those requiring treatment, which are the most urgent. There are three stages:

- Develop escalation and retention guidelines
- Evaluate risks
- Escalate risks

3.3 Risk treatment

The purpose of this step is to identify and implement the most appropriate means to mitigate risks deemed to be at an unacceptable level. These risk treatments, in effect, will become new risk management controls or will augment existing controls.

There are four stages:

- Identify risk treatment options
- Select the most suitable risk treatment option(s)
- Develop risk treatment plans
- Implement and review risk treatments

3.4 Communication and consultation process.

In all steps of the Risk Management Process is to ensure that the appropriate stakeholders (external and internal) are consulted and/or informed about what's going on. There is need also to develop plans and mechanisms for doing this at an early stage.

Effective communication (e.g. reports) will ensure that those responsible for implementing the Process, as well as other relevant stakeholders, understand the basis on which decisions are made and the reasons why particular actions are required. It will also support and encourage accountability for ownership of risks.

A consultative approach will yield more successful outcomes by helping to engage managers and staff in the Risk Management Process and to integrate risk management into the organization.

Monitor and review the ongoing process.

Risk management must be responsive to change – both within the Organisation and in the external environment. Therefore, the activities of monitoring and reviewing must be ongoing, and are integral to every step in the Risk Management Process.

Conducting ongoing monitoring activities, we recommend a formal review and reporting mechanisms are set up. These mechanisms are a requirement of good governance, provide the management team with regular and up-to-date information on risks, risk treatment plans and any issues arising, and assure the Board that risks are being managed in line with this Policy and Framework.

3.5 Implementation.

3.5.1 Policies

- This policy will be available to all staff for use and be available. It will also be available from the head of risk and audit, senior governance manager and all line managers.

- All directors and managers are responsible for ensuring that relevant staff within their own teams and directorates have read and understood this document and are competent to carry out their duties in accordance with the procedures described.

- Zamzam has adopted a standardized approach for the assessment and analysis of all risks encountered in the Organisation and which is set out in this framework. The implementation of this policy is supported through the completion of the risk register and the reporting arrangements to the various committees of Zamzam. Directors and senior leads are also responsible for ensuring the policy is implemented in their areas of responsibility and compliance may be monitored through the audit programme set by the governing body.

- The governing body has a duty to assure itself that the Organisation has properly identified the risks it faces and that it has processes and controls in place to mitigate those risks and the impact they have on the Organisation and its stakeholders. The governing body discharges this duty as follows:

  - Identifies risks to achievement of its strategic objectives.
  - Identifies risks associated with transitional arrangements.
  - Monitors these via the assurance framework.
  - Ensures that there is a structure in place for the effective management of risk through Zamzam.
  - Approves and reviews strategies for risk management on an annual basis.
  - Receives regular reports from the relevant quality and safety committee identifying significant clinical risks and mitigating actions.
  - Receives regular reports from the relevant quality and safety committee on significant risks to delivering financial balance and the delivery of the quality, innovation, productivity and prevention programme.
  - Demonstrates leadership, active involvement and support risk management.

3.6 **Training**

The General Director (supported by the head of risk and audit) will ensure that the necessary training or education needs and methods needed to implement this policy and supporting procedure(s) are identified and resourced as required. This may include identification of external training providers or development of an internal training process.

Regular training is key to the successful implementation of this policy and embedding a culture of risk management in the Organisation. Through a robust training and education programme staff will have the opportunity to develop more detailed knowledge and appreciation of the role of risk management. This will be offered through regular staff induction, mandatory training sessions and risk management training.

3.7 Documentation

Other policies

This policy is also supported by the incident reporting and management policy.

3.8 Dissemination, monitoring and review and archiving

Dissemination

The policy will be available to all staff

Monitoring and review

The Audit and Risk Committee (on behalf of the governing body) will ensure the policy is reviewed on a bi-annual basis Staff who become aware of any change which may affect a policy should advise their line manager as soon as possible. The governing body will then consider the need to review the policy or procedure outside of the agreed timescale for revision. For ease of reference for reviewers or approval bodies, changes should be noted in the 'document history' table on the front page of this document.

Note: If the review consists of a change to an appendix or procedure document, approval may be given by the sponsor director and a revised document may be issued. Review to the main body of the policy must always follow the original approval process.

Archiving

The head of risk and audit will ensure that archived copies of superseded policy documents are retained in accordance.

4.0 APPENDICES

4.1 Appendix 1: Guidance for Risk Assessment and Action

1. Risk Assessment

The following steps are intended to help guide staff when undertaking an assessment of a risk.

Step 1: determine the consequence score

Use the tables below when completing a risk assessment, either when an incident has occurred or if the consequence of potential risks is being considered.

Choose the most appropriate domain for the identified risk from the left hand side of the table. Then work along the columns in same row to assess the severity of the risk on the scale of 1 to 5 to determine the consequence score, which is the number given at the top of the column.

Note: consequence will either be negligible, minor, moderate, major or catastrophic.

Table 1: consequence score

	Consequence score (severity levels) and examples of descriptors				
	1	**2**	**3**	**4**	**5**
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Impact on the safety of patients, staff or public (physical/psychological harm)	Minimal injury requiring no/minimal intervention or treatment. No time off work	Minor injury or illness, requiring minor intervention Requiring time off work for >3 days Increase in length of hospital stay by 1-3 days	Moderate injury requiring professional intervention Requiring time off work for 4-14 days Increase in length of hospital stay by 4-15 days RIDDOR/agency reportable incident An event which impacts on a small number of patients	Major injury leading to long-term incapacity/disability Requiring time off work for >14 days Increase in length of hospital stay by >15 days Mismanagement of patient care with long-term effects	Incident leading to death Multiple permanent injuries or irreversible health effects An event which impacts on a large number of patients

Quality/complaints/audit	Peripheral element of treatment or service suboptimal Informal complaint/inquiry	Overall treatment or service suboptimal Formal complaint (stage 1) Local resolution Single failure to meet internal standards Minor implications for patient safety if unresolved Reduced performance rating if unresolved	Treatment or service has significantly reduced effectiveness Formal complaint (stage 2) complaint Local resolution (with potential to go to independent review) Repeated failure to meet internal standards Major patient safety implications if findings are not acted on	Non-compliance with national standards with significant risk to patients if unresolved Multiple complaints/ independent review Low performance rating Critical report	Totally unacceptable level or quality of treatment/service Gross failure of patient safety if findings not acted on Inquest/ombudsman inquiry Gross failure to meet national standards
Human resources/ organizational development/staffing/ competence	Short-term low staffing level that temporarily reduces service quality (< 1 day)	Low staffing level that reduces the service quality	Late delivery of key objective/ service due to lack of staff Unsafe staffing level or competence (>1 day) Low staff morale Poor staff attendance for mandatory/key training	Uncertain delivery of key objective/service due to lack of staff Unsafe staffing level or competence (>5 days) Loss of key staff Very low staff morale No staff attending mandatory/ key training	Non-delivery of key objective/service due to lack of staff Ongoing unsafe staffing levels or competence Loss of several key staff No staff attending mandatory training /key training on an ongoing basis
Statutory duty/ inspections	No or minimal impact or breech of guidance/ statutory duty	Breech of statutory legislation Reduced performance rating if unresolved	Single breech in statutory duty Challenging external recommendations/ improvement notice	Enforcement action Multiple breeches in statutory duty Improvement notices Low performance rating Critical report	Multiple breeches in statutory duty Prosecution Complete systems change required Zero performance rating Severely critical report
Adverse publicity/ reputation	Rumors Potential for public concern	Local media coverage – short-term reduction in public confidence Elements of public expectation not being met	Local media coverage – long-term reduction in public confidence	National media coverage with <3 days service well below reasonable public expectation	National media coverage with >3 days service well below reasonable public expectation. MP concerned (questions in the House) Total loss of public confidence

Business objectives/ projects	Insignificant cost increase/ schedule slippage	<5 per cent over project budget Schedule slippage	5–10 per cent over project budget Schedule slippage	Non-compliance with national 10–25 per cent over project budget Schedule slippage Key objectives not met	Incident leading >25 per cent over project budget Schedule slippage Key objectives not met
Finance including claims	Small loss Risk of claim remote	Loss of 0.1–0.25 per cent of budget Claim less than £10,000	Loss of 0.25–0.5 per cent of budget Claim(s) between £10,000 and £100,000	Uncertain delivery of key objective/Loss of 0.5–1.0 per cent of budget Claim(s) between £100,000 and £1 million Purchasers failing to pay on time	Non-delivery of key objective/ Loss of >1 per cent of budget Failure to meet specification/ slippage Loss of contract / payment by results Claim(s) >£1 million
Service/business interruption **Environmental impact**	Loss/interruption of >1 hour Minimal or no impact on the environment	Loss/interruption of >8 hours Minor impact on environment	Loss/interruption of >1 day Moderate impact on environment	Loss/interruption of >1 week Major impact on environment	Permanent loss of service or facility Catastrophic impact on environment

Step 2: determine the likelihood score

Now determine what is the likelihood of the impact occurring. The frequency based score is appropriate in most circumstances and is easier to identify. It should be used whenever it is possible to identify a frequency. The frequency based score will either be classed as rare, unlikely, possible, likely or almost certain.

Table 2: Likelihood Score

Likelihood score	**1**	**2**	**3**	**4**	**5**
Descriptor	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost certain**
Frequency How often might it/does it happen	This will probably never happen/recur	Do not expect it to happen/recur but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur but it is not a persisting issue	Will undoubtedly happen/recur, possibly frequently

Step 3: assigning a risk rating

Now apply the consequence and likelihood ratings to give you a risk rating for each of the risks you have identified. Calculate the risk score the risk multiplying the consequence by the likelihood: C (consequence) x L (likelihood) = R (risk score)

Table 3: risk assessment matrix, scoring = consequence x likelihood (C x L)

	Likelihood score				
Consequence score	**1**	**2**	**3**	**4**	**5**
	Rare	**Unlikely**	**Possible**	**Likely**	**Almost 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 Negligible	1	2	3	4	5

For grading risk, the scores obtained from the risk matrix are assigned grades as follows:

Green	1 – 9	Low Risk
Amber	10 – 12	Moderate Risk
Red	15 - 25	High Risk

Step 4: control measures

Consider the control measures that will be put into place to mitigate the risk. Identify and record any gaps in controls**.**

Step 5: assessing the effectiveness of control(s)

For each of the risks (and especially extreme and high risks) identify the controls that are in place. For example, in an operational setting and where an incident may have occurred, the controls may take the form of a policy, guideline, procedure or process, etc. For risks that have been identified as preventing achievement of organizational objectives then the control is likely to be a management action plan.

Review the control(s) for each of the risks and apply the following criteria: *Table 4: Assessing the effectiveness of control(s)*

Satisfactory:	Controls are strong and operating properly, providing a reasonable level of assurance that objectives are being delivered.
Some Weaknesses:	Some control weaknesses/inefficiencies have been identified. Although these are not considered to present a serious risk exposure, improvements are required to provide reasonable assurance that objectives will be delivered.
Weak:	Controls do not meet any acceptable standard, as many weaknesses/inefficiencies exist. Controls do not provide reasonable assurance that objectives will be achieved.

Step 6: determine the risk type

The risk type should be specified into one of the following categories:

- strategic
- operational

Step 7: align to organizational objective

The risk should be aligned to the organizational objective it could/will impact on. Zamzam organizational objectives are:

CO1 - Ensure Zamzam meets its public accountability duties
CO2 - Maintain financial control and performance targets
CO3 - Maintain and improve the quality and safety of Zamzam commissioned services
CO4 - Ensure Zamzam involves beneficiaries in commissioning and reforming services
CO5 - Identify and deliver Zamzam strategic priorities
CO6 - Develop Zamzam localities

Step 8: developing an action plan

An action plan must be developed for all risks with a score of 15 or above. However, it is useful to develop an action plan regardless of risk score in order to record progress on control measures and who is responsible for carrying them out.

Step 9: Frequency of review

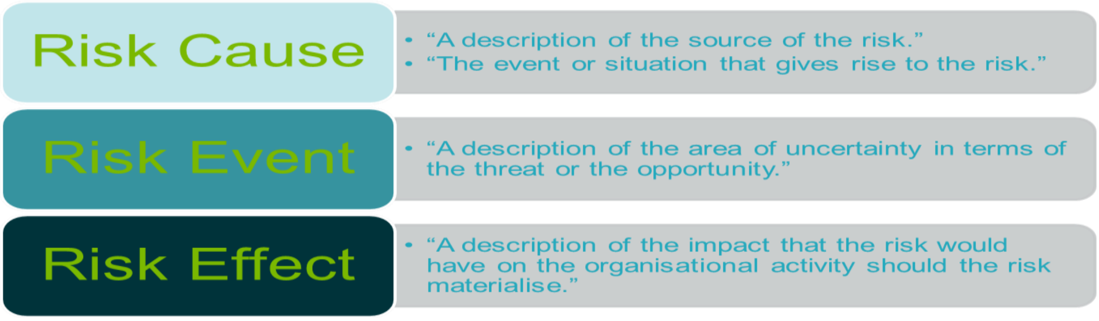
The frequency of review should also be specified as this will need to be added to 'Review Details' section by choosing the appropriate option from the drop down list.

Step 10: Residual risk rating

Taking into account the initial risk rating and the assessment of the effectiveness of the control together, you can now assess the residual risk that needs to be managed. The consequence and likelihood ratings should be applied, as in table 3 above

Please remember when describing to include the risk cause, event and effect. There is a mandatory field within the system for you to complete.

.



Risk Cause

- "A description of the source of the risk."
- "The event or situation that gives rise to the risk."

Risk Event

- "A description of the area of uncertainty in terms of the threat or the opportunity."

Risk Effect

- "A description of the impact that the risk would have on the organisational activity should the risk materialise."

Risk Cause: As a result of…. (The trigger)

Risk Event: There is a risk that…. (What might happen)?

Risk Effect: Which will result in…? (The impact on the achievement of objectives).

4.2 Appendix 2: Risk management action guide

Where risks have been identified and scored, the following escalation arrangements should be used. The table below provides a suggested action guide for the management of a risk.

Table 5: The table below provides a suggested action guide for the management of a risk

Risk Rating	**RAG Rating**	**Action**	**Assurance Flows**	**Level of Authority**
15 -25	High Risk	Proactive review and oversight by Audit and Risk Committee (ARC). Proactive management by Risk Management Group (as part of director and senior team) Significant probability that major/catastrophic harm will occur if control measures are not implemented. **URGENT/IMMEDIATE** action required. Director may consider limiting or halting activity.	ARC with ongoing assurance to Governing Body	Director attention

10-12	Moderate Risk	Proactive review and management Exception reporting and oversight to ARC where necessary. Unacceptable level of risk exposure which requires constant monitoring and controls. High probability of harm if control measures are not implemented.	ARC with ongoing assurance to Governing Body	Director attention
1-9	Low Risk	Proactive review and management by risk	Assurance provided to ARC	
		Management group (as of the director and senior team) at operational level. Regular monitoring of low level risks. The majority of control measures are in place and severity of harm low. Actions managed within the day to day working of the Organisation.	Through regular monitoring of low level risks.	

4.3 Appendix 3: Zamzam New Risk Form

Risk Register – New Risk Form					
Risk Ref *Leave blank*	Date Identified	Responsible Director *Name and job title*		Risk Owner *Name and job title*	
Risk Details					
Directorate		Frequency of Review	Source of Risk		Risk Type
Description of Risk					
Risk Cause					
Risk Event					
Risk Effect					
Initial Risk Assessment Matrix *(please circle)*					
	Likelihoodscore				
Consequence score	1	2	3	4	5
	Rare	Unlikely	Possible	Likely	Almost 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 Negligible	1	2	3	4	5

Initial risk rating:	

Controls

Control Details	Assurances on Controls (Progress/Evidence)	Effectiveness of Controls	Gaps in Control

Actions

Action Details	Responsibility / Lead	Target Date

Residual Risk Assessment Matrix *(please circle)*

	Likelihood score				
Consequence score	**1**	**2**	**3**	**4**	**5**
	Rare	**Unlikely**	**Possible**	**Likely**	**Almost 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 Negligible	1	2	3	4	5

Residual risk rating score:	

Form Completed By

Name	Job Title	Contact Details

Approved to add to risk register?	□ **Yes** □ **No**

Completed forms should be returned by email to: