

Risk management policy and guide

Policy statement

Energy and Water Ombudsman Queensland (EWOQ) is committed to robust risk management practices to achieve its functions under the *Energy and Water Ombudsman Act 2006*, to satisfy its obligations as a statutory body and to act in accordance with the requirements of the *Financial Accountability Act 2009*.

EWOQ has taken an enterprise-wide approach to risk management.

It is EWOQ's policy to identify, assess, and manage all categories of risk in a proactive way, integrating risk management in the day-to-day running, monitoring, maintenance, and development of EWOQ. Risks are considered in all key strategic decisions and third-party relationships.

In implementing this Policy, EWOQ seeks to provide assurance to relevant stakeholders that the identification and management of risk plays a key role in the delivery of EWOQ's objectives, strategies and performance measures.

Our human rights obligations under the *Human Rights Act 2019* have been considered in this policy, and our decision making and actions respect, protect and promote those rights.

Scope

This Policy applies to all our employees (permanent, temporary or contract), assets and facilities. It incorporates the best practices of the international standard for risk management, *ISO31000:2018 Risk Management – Guidelines*, together with guidance from Queensland Treasury's *A Guide to Risk Management 2020* and aligns with the Queensland *Financial and Performance Management Standard (2019)*.

Purpose

EWOQ is committed to ensuring its employees understand the concept of risk management and its practical application to minimize risks to objectives and to identify opportunities. The principles and processes detailed in this document is collectively referred to as the Risk Management Policy.

Risk management framework

EWOQ's risk management framework is based on the principles of effective risk management contained within *ISO31000:2018 Risk Management – Guidelines*. We apply those principles by:

- Integrating risk management across all areas of EWOQ
- Practicing a coordinated approach for the management of risks
- Embedding consistent processes for the identification, assessment, evaluation and monitoring of risks
- Maintaining and regularly reviewing the EWOQ Risk Register
- Designing and implementing effective risk treatment plans for risks that have a residual risk level above our specified risk tolerance limits

- Efficiently and effectively assigning capabilities and resources to manage both opportunities and threats across EWOQ's functions
- Regularly monitoring the effectiveness of the Risk Management Framework

Governance and reporting

EWOQ has an Audit and Risk Management Committee (ARMC) that is engaged to provide independent advice and support to the Energy and Water Ombudsman (the Ombudsman) concerning EWOQ's risk, control and compliance frameworks, amongst other things. They will receive periodic reports on our strategic risk profile.

Members of our Executive Management Group (EMG) are the risk owners for EWOQ's strategic risks. They are responsible for the identification and management of those risks, as well as managing our operational risks where appropriate. Our Leadership Group (LG) supports the risk management role of the EMG and is responsible for the day-to-day management of risk where required. Risk owners are named in our risk register, and their risk responsibilities are included on their Performance Development Agreement Plan (PDAP). Risk owners are supported in their risk management function by a Risk Coordinator. All our team members have a responsibility to identify risk and to contribute to its management. Consequently, all team members should include their risk management role in their PDAP. Specific risk roles in EWOQ are at appendix A.

Risk statement

Risk appetite refers to the level of risk that EWOQ is prepared to pursue or retain to achieve our objectives. The EMG is responsible for determining the level of risk exposure considered acceptable. The risk appetite is reviewed by the EMG annually.

EWOQ will take considered risks where there is a high degree of confidence that controls are in place to minimise the likelihood of adverse consequences and where there is a high likelihood of capturing expected and considered benefits or opportunities.

EWOQ's lowest or no appetite is for risks associated with ethical behaviour, fraud and corruption, workplace health and safety, security of confidential and personal information as well as compliance with legislation and regulation. There is a low appetite for risks that negatively impact on high quality service delivery to our customers and stakeholders and that reduce public confidence in our service, areas in which we are highly risk averse. There is a low risk appetite for unmanaged risk.

Risk tolerance levels for specific risks and projects will be set by risk owners, and available on the risk register. Risk tolerance levels align with EWOQ's broader risk appetite.

Risk management process

The *risk management process* is a systematic way of applying policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk.

Figure 1 illustrates the process, as described in ISO31000: 2018. EWOQ manages risk in line with this process.

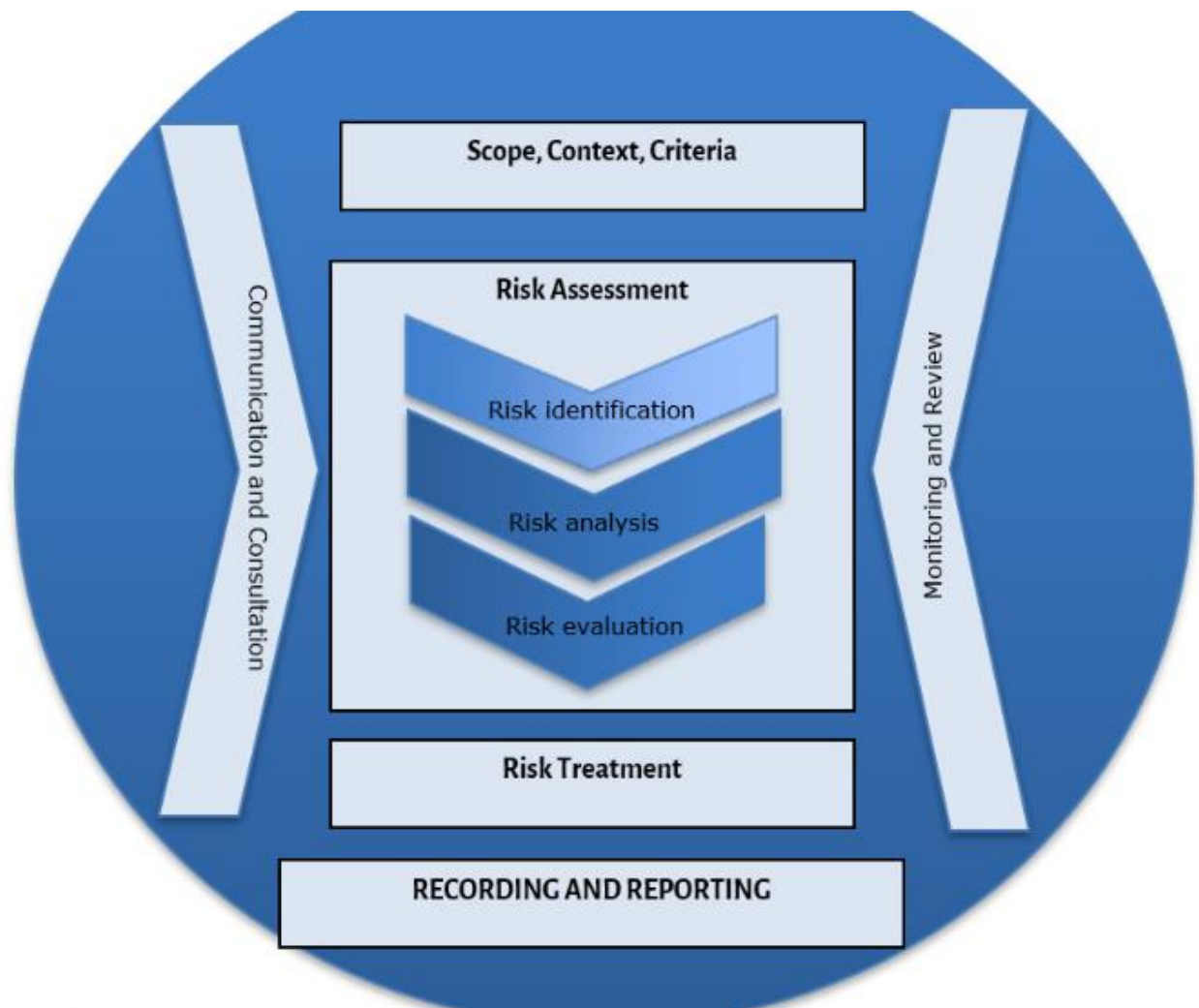


Figure 1 - Risk management process

Communication and consultation

Communication and consultation are continual activities across all stages of the risk management process. It assists stakeholders understand our risks and the reasons for decisions we make. We communicate about the management of our risks with key stakeholders including our ARMC, Scheme Participants, Government stakeholders, auditors and our team members

When considering risk, it is important to identify the stakeholders to that risk, and how we intend engaging with them. Key stakeholders in EWOQ's risks includes Advisory Council members, Scheme Participants, the Minister for the Department of Natural Resources Mines and Energy, EWOQ team members including the EMG and the LG.

A stakeholder engagement plan is a useful tool and recommended to assist with identifying and managing communication and consultation.

Scope, context, criteria

This is an initial part of the risk management process and is applied for all levels of risk: strategic, operational and project. An understanding of the external and internal factors that influence activities and operations will assist in the risk identification process. This part of the risk management process will only need to be repeated when there are significant changes to the internal and external environment, organisational operations or implementation of a new project. Regular and systematic

monitoring of the environment is important to identify such changes. An environmental scan is conducted regularly by EWOQ to identify potential changes in the context in which we operate.

External environment:

An understanding of the environment in which EWOQ operates is essential to identify potential risks to our objectives. A scan of the business, industry, social, economic, technological and political environment is undertaken regularly for risk identification purposes.

Internal environment:

EWOQ's vision is to provide Queenslanders with an independent and effective way of resolving disputes with their energy and water suppliers. To help us achieve our vision, strategic objectives have been identified under the categories of Service, Customer, Connections and People (see the EWOQ Strategic Plan 2020-2023 on our website).

Additional internal factors which are considered in understanding our internal environment include EWOQ's organisational structure and capabilities, changes to resources, policies or processes, and understanding stakeholder objectives and priorities.

Criteria:

The criteria that we use to assess our risk is developed by the EMG. It includes our risk appetite statement, consequence table, likelihood table, risk matrix and management actions table.

Risk assessment

Risk identification:

A risk is defined in ISO31000:2018 as 'the effect of uncertainty on objectives'. The risk event is something that has a potential future impact on our objectives. The identification of possible risk events allows EWOQ to prepare for uncertainty and better position itself to meet strategic objectives.

There are many activities and processes that EWOQ undertakes to identify risks to its objectives. These include: critically analyzing strategic plans, workshopping scenarios, conducting environmental scans, reviewing media coverage, analyzing proposed legislative changes, conducting post-event analyses, and discussions with industry stakeholders.

Describing risk focusses on the potential event that is likely to impact our objectives. For simplicity, it should not include a cause or impact statement, as there are likely to be many causes and impacts. Those elements will be included in the risk register as a result of analysis of the risk event. The description of the risk is agreed in consultation with EMG members.

In describing risks, avoid:

- stating impacts which may arise as being the risks themselves
- including risks which do not impact on objectives
- including risks which are simply the converse of the objectives

Example: 'Cyber-crime' would not be described in the risk register as a risk. Instead, a better description would be 'loss of confidential information'. One of the causes is that EWOQ might be the target for cybercrime/systems hacking, but there will be other causes such as ineffective system security. The key consequence is to our Service objective but may impact other strategic objectives as well.

Risks are recorded in the risk register according to their category, which assists reporting.

Example: A strategic risk is numbered in the risk register as S1, another strategic risk would be numbered S2. An operational risk would be number O1, then O2 and so on.

A comprehensive list of our current organisation's risks is found in the EWOQ Risk Register.

Risk analysis:

Analysis of risk is conducted to identify the causes of the risk, the likelihood that the risk will occur and impacts of the risk on objectives should the risk come to fruition. Included in the analysis is an assessment of the effectiveness of current controls in either reducing the likelihood that the risk event will occur, and/or reducing its impact on our objectives.

Current risk rating¹:

The current risk rating is arrived at by conducting a risk analysis using the steps below:

1. Clearly state the relevant strategic or business objective
2. Identify key strategies designed to achieve that objective
3. Identify the risk events that may occur that will potentially prevent the strategy being effective, which puts achieving the objective in jeopardy
4. Analyse one risk event at a time. For each risk event:
 - 4.1. conduct a root cause analysis – ask what cause(s) might lead to the risk event occurring
 - 4.2. identify the current controls in place that target the cause(s) and reduce the likelihood that the risk event might occur
 - 4.3. assess the effectiveness of those controls (use the control effectiveness rating table at appendix B). Evidence to support the effectiveness rating should be available and noted
 - 4.4. identify the impacts on our objectives should the risk event occur
 - 4.5. identify the current controls in place that aim to reduce the impacts on our objectives and assess their effectiveness (per c. above)
5. Calculate a current risk rating. This is done by applying a likelihood rating (see the table at appendix C) which takes into account the effectiveness of current controls to reduce the likelihood of the risk occurring; and a consequence rating taking into account the effectiveness of current controls in reducing the impact of the risk on stated objectives (see the consequence table at appendix D).

There are many tools available to conduct the analysis, but a bow-tie analysis is commonly used in EWOQ. A template to assist risk analysis is available in the sharedrive.

To allow consistent risk rating, EWOQ employees are required to use the consequence criteria at appendix D, and likelihood table at appendix C. The risk rating is devised using the risk matrix at appendix E.

Risk evaluation:

The purpose of risk evaluation is to assist management make defensible decisions regarding resource allocation.

The risk rating arrived at during the analysis stage is compared with the risk tolerance for that risk. If the risk rating is above tolerance, resources should be applied for additional treatment to reduce the risk to within tolerance. Where a risk is rated at or below tolerance, there is generally no need to apply additional resources to managing the risk. Instead, the risk manager should monitor the risk to ensure it remains within tolerance.

¹ Note the use of 'current risk rating' in this document as opposed to 'inherent risk rating' used in some Guides. Inherent risk considers the risk rating in the absence of controls. The EWOQ environment will always have a level of controls in place, so it is more practical to consider the risk rating considering the effectiveness of current controls in place.

The EWOQ Risk Register records the current risk rating and the associated risk tolerance. This highlights those risks where the risk is above tolerance and should be the subject of a treatment strategy.

Risk treatment

The purpose of risk treatment is to reduce the risk to within tolerance. When selecting risk treatment options, consideration should be given to the values, perceptions and potential involvement of key stakeholders, along with the most appropriate ways of communicating and consulting with those parties.

Table 1 shows four options for treating risk.

Treatment option	Definition
Accept	Accept the potential benefit or gain or burden of loss from a risk. In this case, the risk tolerance should be adjusted to bring the tolerance in line with the risk rating. Monitoring of the risk should take place to ensure the risk level is still acceptable.
Avoid	An informed decision not to be involved, or to withdraw from an activity in order not to be exposed to a particular risk.
Control	Apply a risk treatment that reduces the likelihood and/or consequence of the risk occurring.
Transfer	Spread the risk amongst other parties. This can be achieved through taking out insurance or other contracts, such as with the Queensland Government's Corporate Administration Agency (CAA)

Table 1: Treatment options

Risk treatment strategies should be the subject of a quarterly review. This is to assure the EMG that the strategy is being effective in achieving its planned outcomes. Regular monitoring of the treatment strategy by the Risk Owner also allows swift changes to be made to the strategy if it is found to be ineffective. Outcomes of reviews of treatment strategies should be reported to the EMG on a quarterly basis by the Risk Owner. Risk Owners should note that treatment strategies can also introduce new risks that may need to be managed.

In EWOQ, risk treatment strategies are developed using the template stored in the sharedrive. Risk owners are responsible for developing and implementing treatment strategies for their allocated risks. For strategic risks rated above tolerance, treatment strategies are discussed and approved by the EMG.

The progress of treatment strategies for all strategic risks rated above tolerance should be reported quarterly to the EMG. For other risks, Risk Owners should report progress quarterly at the LG. A risk treatment progress report template is available in the sharedrive.

A treatment strategy should be designed to be completed within one year. This ties in with resource planning. Once the treatment strategy is complete the treatment status is changed on the risk register to 'complete'. If new controls originating from the treatment strategy will be maintained and included as 'business as usual' they are moved on the risk register to the 'controls' section. If the risk is still rated above tolerance, a new treatment strategy is developed, and new resourcing allocated. The new treatment strategy will be included in the risk register and the status would be changed to 'in progress'.

When a treatment strategy has been completed and the residual risk rating is at or below tolerance, the risk status should be changed to 'monitor'. This allows the Risk Owner to continue to monitor the environment for any changes that may raise the risk rating. A risk may be closed on the risk register if the EMG considers it is obsolete and no longer poses a threat (or opportunity) to EWOQ's objectives.

Residual risk rating

The residual risk rating is assessed after considering the likely effectiveness of proposed treatment strategies designed to reduce the current risk rating.

The assumption is that treatment strategies are to be implemented as designed and would be fully effective. Given that assumption, the remaining consequence and likelihood of the risk is calculated and recorded on the risk register as the residual risk rating. The same consequence and likelihood tables and risk matrix are used to calculate the residual risk rating.

The regular review of the treatment strategy confirms whether the residual risk rating will be achieved.

Recording and reporting

The EWOQ risk register records all key risks by category. This one repository provides visibility of risks across the organisation, avoids duplication of risks and allows for flexibility should the organisation's structure change. The risk register clearly states the Risk Owners, current risk rating, residual risk rating and status of treatment plans.

The risk register is the key tool used to report the status of our risks. It is accessible by all team members, but only risk owners and their delegates and the Risk Coordinator have access to edit the register. This assures the integrity of the risk register.

Exception reporting from the register is provided to the ARMC quarterly, the EMG quarterly and the LG monthly. Reporting is facilitated by the Risk Coordinator in consultation with Risk Owners.

Monitor and review

Risk owners must regularly monitor the allocated risks and review them at least annually. This includes an assessment of any changes in the internal or external environment that might impact the risk, as well as an evaluation of the effectiveness of controls and treatment strategies.

Where risks are above tolerance and a treatment strategy is in progress, Risk Owners should review the risk quarterly. This is to assess whether the treatment is likely to reduce the risk rating to within tolerance, and to allow timely changes to the treatment strategy to improve effectiveness.

Any changes to risk rating should be recorded on the risk register and reported as above.

Continual improvement of the framework

EWOQ is committed to a review of the Risk Management Framework at least every two (2) years to ensure that risk management is effective and continues to support its performance.

This will be informed by periodic reviews facilitated by the Risk Coordinator at the request of the Ombudsman and will cover:

- Evaluation of the effectiveness and alignment of this Risk Management Policy with risk management contemporary best practice
- Evaluation of the degree to which activities stated in this Policy are undertaken
- Review of the completeness and currency of the EWOQ risk register
- Assessment of the awareness of team members in relation to their risk management responsibilities (e.g. through surveys)

- Review of training and development needs of managers and team members in relation to their risk management responsibilities

The Ombudsman will provide results of the review to the ARMC who will evaluate EWOQ's performance in relation to risk management.

Legislation and standards

- *Energy and Water Ombudsman Act 2006*
- *Financial Accountability Act 2009*
- International Standard ISO31000:2018 – Risk Management - Guidelines
- A guide to risk management 2020 – Queensland Treasury
- Financial and Performance Management Standard 2019
- *Human Rights Act 2019*

Approval

Approved by the Energy and Water Ombudsman and effective from the date endorsed.



Name: Jane Pires

Energy and Water Ombudsman

Date: 15/09/2020

Appendix A – Risk roles and responsibilities

Who	Risk responsibilities
Audit and Risk Management Committee (ARMC)	<ul style="list-style-type: none"> Responsible to the Ombudsman for the assurance of organisational risk management process, compliance and performance Review significant risks (i.e. those rated 'High') to assure they are being managed effectively Provide oversight of the management of risks across EWOQ Monitor EWOQ's risk profile
Energy and Water Ombudsman	<ul style="list-style-type: none"> Conduct a review of the Risk Management Framework at least every two years to assure an effective Framework
Executive Management Group (EMG)	<ul style="list-style-type: none"> Develop risk appetite statement and review it annually Develop consequence and likelihood ratings tables used to assess risk and review annually Develop the management actions table Manage the communication of risk across EWOQ Monitor EWOQ's risk profile Identify strategic risks and allocate to a risk owner Approve risk treatments and allocate resources for treatment of strategic risks Approve tolerance levels for specific risks in line with the risk appetite statement
Leadership Group (LG)	<ul style="list-style-type: none"> Identify business/project risks and assist risk owners in the management of those risks Support risk owners report effectiveness of controls Ensure team members within their area of control have adequate training in risk management and contribute to EWOQ's risk management processes. Provide risk management information when requested to the Ombudsman or EMG. Report on the implementation of risk control measures and treatment plans within their area of responsibility.
Risk owners	<ul style="list-style-type: none"> Responsible for the management and ongoing review of assigned risks as detailed in the EWOQ risk register Develop risk assessments and present to the EMG and the LG Recommend tolerance levels for their assigned risks to the EMG

	<ul style="list-style-type: none"> • Develop and implement risk treatment plans to reduce risk ratings to tolerance levels • Assess effectiveness of controls and report annually to the EMG • Review effectiveness of treatment strategies and report to the LG and EMG • Update, review and maintain the risk register for their assigned risks
Team members	<ul style="list-style-type: none"> • Report potential new or emerging risks to their nominated Manager • Adhere to processes detailed in this Risk Management Policy and Guide • Implement and report on allocated risk control actions as required • Participate in risk assessments as required
Risk Coordinator	<ul style="list-style-type: none"> • Co-ordinate and deliver training in risk management regularly and as required • Facilitate risk management workshops with EMG and LG for risk identification particularly during the strategic and business planning process • Work with Risk Owners to maintain the EWOQ risk register • Report on and provide risk management information to the EMG and the LG • Liaise with, and assist Internal and External auditors to ensure audits of the risk management framework are conducted efficiently

Appendix B – Control effectiveness rating table

Control effectiveness	Description
Effective	The control design meets the control objective and the control is operating the majority of the time
Partly effective	The control design meets the control objective and the control is normally operational but occasionally is not applied when it should be, or not as intended
Ineffective	The control design does not meet the control objective, and/or the control is not applied or is applied incorrectly

Appendix C – Likelihood table

Rating	Probability of risk occurring	Descriptor ²
Almost Certain	>90%	Is expected to occur, or occurs in most circumstances Less than 10% of the critical controls associated with the risk are rated as either Effective or Partly Effective. Without control improvement, it is almost certain that the risk will eventuate at some point in time.
Likely	60-90%	Will probably occur, or occur in many circumstances 10-40% of the critical controls associated with the risk are rated as either Effective or Partly Effective. Without control improvement, it is more likely than not that the risk will eventuate.
Possible	30-60%	May occur, or may occur from time to time 40-70% of the critical controls associated with the risk are rated as either Effective or Partly Effective and, if there is no improvement the risk may eventuate.
Unlikely	10-30%	Could occur at some time 70-90% of the critical controls associated with the risk are rated as either Effective or Partly Effective. The strength of this control environment means that it is more than likely that the risk eventuating would be caused by external factors not known to EWOQ.
Rare	<10%	Could occur at rare times 90% or more of the critical controls associated with the risk are rated as either Effective or Partly Effective. The strength of this control environment means that, if this risk eventuates, it is most likely a result of external circumstances outside of the control of EWOQ.

² Additional descriptors extracted from Paladin risk management services; www.paladinrisk.com.au

Appendix D– Consequence criteria table

	Categories				
Impact level	Customer	Finance	People	Compliance	Reputation
Critical	<i>The risk has the potential to stop EWOQ operating.</i>				
Major	<i>Significant impact on business outcomes, requiring major resource commitment to rectify. May result in change to organisational structure.</i>				
Moderate	<i>Some impact on business outcomes, perhaps some disruption of services and require a change in allocation of resources. The impact could be rectified within 3-6 months.</i>				
Minor	<i>Minor disruption to business as usual. The business will recover in up to 3 months.</i>				
Insignificant	<i>Very minor disruption in business as usual which is recoverable without redirection of resources and within a month.</i>				

Appendix E – Risk matrix

RISK MATRIX	Consequence				
	Insignificant	Minor	Moderate	Major	Critical
Likelihood					
Rare	LOW Accept the risk Routine management	LOW Accept the risk Routine management	LOW Accept the risk Routine management	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review
Unlikely	LOW Accept the risk Routine management	LOW Accept the risk Routine management	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review
Possible	LOW Accept the risk Routine management	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review	HIGH Quarterly senior management review
Likely	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review	HIGH Quarterly senior management review	EXTREME Monthly senior management review
Almost certain	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review	EXTREME Monthly senior management review	EXTREME Monthly senior management review

Appendix F – Management actions table

Risk rating	Required action to reduce residual rating to within tolerance
Critical	<ul style="list-style-type: none"> • Immediate action by EWO • Treatments designed by Risk Owner for EMG approval, and implemented • Regular monitoring of treatment plan effectiveness by Risk Owner and reported to the EMG • Audit and Risk Committee informed
High	<ul style="list-style-type: none"> • Immediate action by EMG • Treatments designed by Risk Owner for EMG approval, and implemented • Regular monitoring of treatment plan effectiveness by Risk Owner and reported to the EMG • Audit and Risk Committee informed
Medium	<ul style="list-style-type: none"> • Immediate action by Risk Owner • Treatments designed by Risk Owner for EMG approval, and implemented • Regular monitoring of treatment plan effectiveness by Risk Owner and reported to the LG
Low	<ul style="list-style-type: none"> • Risk to be managed through business-as-usual processes and monitored for changes in risk profile • Reporting of changes to risk profile to LG and EMG