RISK MANAGEMENT POLICY

Document Location	G:\CHS\Executive\1.3 ARMC meetings\Policies

Version	Date	Owner	Summary of Changes
4.0	20.09.2016	Business Manager	• Section 12 - description of risk appetite.

4.1	01.03.2022	Head of Strategy and Development	• Throughout document:
			  - include provision for the various types of risk registers used within CHS.
			  - General formatting
			• Section 6 – addition of the roles Business Support and Governance Lead and Programme Manager, and their responsibilities.
			• Section 7 – identification and definition of CHS risk registers.
			• Section 8 – addition of definition of risk types and appetites, addition of CHS escalation process and protocols, revision of monitoring and reporting and joint risk sections.
			• Section 9 – new section on assurances and mapping.
			• Appendix A – new appendix mapping risk management and escalation route within CHS
			• Appendix C – new appendix setting out risk scoring and tolerance levels
			• Appendix D – new appendix articulating risk management and reporting timelines

4.2	03.05.2023	Head of Strategy and Development	• Section 4- new section added to define the review period and approval process for the policy

Approvals	ARMC 30.08.2016 Board 20.09.2016 ARMC 10.05.2022

Date approved ARMC: 10 May 2022
Date for review by ARMC:

1. Introduction

1.1 The risk management policy states the objectives, CHS' approach to risk management, and defines the roles and responsibilities of the CHS Board, senior management team (SMT) and staff.

1.2 Risk can be a threat (downside) or an opportunity (upside).

1.2.1 A **threat** is an event or action that will adversely affect an organisation's ability to achieve its stated objectives and to successfully deliver approved strategies.

1.2.2 An **opportunity** is an event or action that will enhance the organisation's ability to achieve its objectives and deliver approved strategies.

2. Definitions

2.1 **Risk** - the possibility that an action, event or set of circumstances will adversely or beneficially affect an organisation's ability to achieve its objectives.

2.2 **Risk management** - the planned and systematic approach to identification, recording, monitoring, reporting on, and controlling of risk.

3. Scope of risk management policy

3.1 The risk management policy applies to all areas of CHS' activity including any services provided by a third party. It is not only concerned with strategic objectives but includes operational and programme/project management activity.

4. Review and approvals

4.1 The CHS Risk Management policy will be reviewed and approved by the Audit and Risk Committee every two years, or earlier if there is a process change which requires an amendment.

5. Policy objectives

5.1 The key objectives of the risk management policy are to:

5.1.1 increase confidence in our ability to achieve our objectives;

5.1.2 facilitate the identification, evaluation, and control of key risks and ensures that any residual risks are at an acceptable level;

5.1.3 integrate Risk Management into the operational and management practices and procedures of CHS to promote a culture of risk awareness;

5.1.4 support planning and performance reporting, ensuring strategic risks are monitored and escalated to mitigate any risks to our planned strategic objectives;

5.1.5   provide information to support the CHS' annual governance statement, as to the effectiveness of the arrangements for risk management and internal control mechanisms in practice.

6.   CHS' approach to risk management

6.1   The achievement of this policy requires the risk management process:

6.1.1   to form part of a robust corporate governance and management framework for assessing risks that evaluates both the likelihood of the risk being realised, and of the impact if the risk is realised. Risk assessment should be recorded in a way that demonstrates clearly the key stages of the process;

6.1.2   to assign ownership of risks to a senior officer and for the Board to approve the level of risk which CHS is prepared to tolerate (risk appetite); The Board of CHS have final accountability for risk management.

6.2   to provide a basis for the integration of risk management into the planning and performance framework allowing for Board, SMT, and staff to consider the   consequences of their decisions and actions from a risk management prospective;

6.3   to ensure that mitigating controls are in place to manage identified risks;

6.4   to ensure appropriate escalation routes for local/project risk registers;

6.5   to review regularly and monitor whether or not the risk profile is changing, to gain assurance that risk management is effective, and to identify when further   action is necessary;

6.6   to be supported by a programme of risk based internal audits; and

6.7   to ensure that risks are incorporated into area planning and escalated via the appropriate route.

7.   Roles and responsibilities

7.1   Role of the Board

7.1.1   the Board has overall responsibility for the system of internal control and for overseeing risk management within CHS and approving the annual governance statement. The Board will seek regular assurance from the Audit and Risk Management Committee (ARMC) that the system is functioning effectively;

7.1.2   overseeing the work of the senior management team, ensuring that all strategic and operational risks have been identified, and that important risk and control issues have not been overlooked;

7.1.3   influencing the culture of risk management, sharing experience and good practice;

3

7.1.4   setting appropriate policies on internal control;

7.1.5   determining the level of risk (risk appetite) which CHS is prepared to tolerate;

7.1.6   approving decisions affecting CHS' risk profile or exposure;

7.1.7   annually reviewing the risk management policy.

7.2   Role of the Audit and Risk Management Committee (ARMC)

7.2.1   The Audit Committee advises the Board and/or Accountable Officer on the strategic processes for risk, control and governance. This includes advising on the adequacy of assurances needed by the Accountable Officer that suitable controls and risk management processes are in place.

7.2.2   The overall risk management structure and escalation routes are attached at Appendix A.

7.3   Role of the National Convener/Chief Executive

7.3.1   As Accountable Officer, the National Convener/Chief Executive has overall executive responsibility for risk management arrangements within CHS, leading the risk management processes and ensuring that responsibilities delegated to other senior managers and staff at all levels within CHS are discharged in an effective manner. The National Convener/Chief Executive is also responsible for signing the Governance Statement for inclusion in the Annual Accounts.

7.4   Role of the Senior Management Team

Senior Management Team has responsibility for:

7.4.1   undertaking a formal review of the Strategic and Operational Risk Registers on a quarterly basis and to consider any other issues from a risk management perspective as they arise by including risk management reporting as a standing item on the agenda for SMT meetings;

7.4.2   developing and reviewing operational risk registers for the service areas under their control and to review on an ongoing basis;

7.4.3   Make a decision on strategic and operational risks raised via quarterly review.

7.5   The Depute Chief Executive has responsibility for:

7.5.1   developing and implementing policies on risk management and internal control;

4

7.5.2 identifying, assessing and developing action plans to mitigate the most significant risks faced by CHS;

7.5.3 facilitating an annual review of the effectiveness of the system of internal control and reporting to the Audit and Risk Management Committee.

7.6 The Business Operations and Governance Lead

7.6.1 the day to day operation of CHS' risk management arrangements;

7.6.2 engaging with business leads, senior managers, and programme manager to ensure risk registers are regularly reviewed and escalation routes followed;

7.6.3 coordination and review of the assurance map within the risk register;

7.6.4 regular reporting to the SMT, Audit and Risk Management Committee and Board on strategic risks and controls.

7.7 Role of the Programme Manager

7.7.1 Engaging with Project Managers and Leads to ensure Project risk registers are developed at project initiation phase, and reviewed regularly thought the project life cycle.

7.7.2 Review project risks with the Business Operations and Governance Lead monthly following escalations routes as required and moving/reporting risk appropriately.

7.8 Role of employees

7.8.1 CHS' employees should have the necessary knowledge, skills, information and authority to establish, operate and monitor the system of internal control and be responsible for managing risks as an integral element of their job, as well as updating risk registers and following appropriate routes of escalation.

7.9 Role of Audit

7.9.1 Internal audit will prepare an annual work plan which is risk based for approval by ARMC. It will be focused on the significant strategic and operational risks, as identified by management.

7.9.2 External audit provide feedback to the ARMC on the operation of internal controls as part of the annual audit.

8. **Risk registers**

Date approved ARMC: 10 May 2022
Date for review by ARMC:

8.1 The **Strategic risk** register is linked to the Business plan and assess risk events which could affect the attainment of our business objectives and strategic goals. Strategic risk represents disruption often determined by business plan performance, business objectives, and overall business strategy.

8.2 The **Operational risk** register assess our operational, day to day business activities and our ability to execute our business plan and statutory duties. Operational risk management is critical to remove roadblocks to the execution of strategic plans.

8.3 **Project** risk registers are an integral part of the project initiation and life cycle. The project risk register records any uncertain event or condition that, if it occurs, has a positive or negative effect on one or more project objectives.

8.4 **Department/local** risk registers or **issues lists** are not a requirement in all areas but may be used to identify the most significant risks that pose a threat to the department meeting its service delivery objectives. Where a department identifies a significant operational risk this should be escalated at organisational level via the appropriate escalation routes.

9. Risk Management Procedures

The key elements of the risk management procedures are set out below and more information on risk register management is provided in [Appendix B].

9.1 **Risk registers** – the format for all CHS risk registers is based on the standard, internationally recognised, format which is prescribed for all risk registers across Scottish Government as reviewed with BDO in 2018. The content is in Excel format and allows information to be filtered for flexible reading and reporting.

9.2 **Risk types** – it is helpful to categorise risks to ensure consistency in the process of identification, monitoring, and reporting of key risks. The table below identifies the 5 risk types CHS uses to categorise risk and gives examples of how they may be applied. It is important to note that some risks may fall under more than one type, e.g., a financial risk which results in an inability to pay a supplier could pose a reputational as well as operational risk.

9.3 **Risk appetite** – The key to achieving effective risk management is determining the level of risk which CHS is prepared to tolerate. The table below defines the 5 key types of risk appetite CHS may want to assign to a particular risk. In practice, risk appetite is considered when updating a risk entry on the risk register. Risk appetite is often reflected in how a risk impact is scored; while consideration is given to scores

6

before and after existing mitigations, the tolerable risk status is also determined taking into account the status for that particular risk.

9.4 **Risk tolerance** - CHS has identified the residual scoring level of a risk it is willing to tolerate, mitigate, transfer, orr terminate. Tolerance levels, actions, and scoring structure are noted at Appendix C.

Appetite	Descriptions
Averse	Avoidance of risk and uncertainty in achievement of key deliverables or initiatives is paramount. Activities undertaken will only be those considered to carry virtually no inherent risk.
Minimalist	Predilection to undertake activities considered to be very safe in the achievement of key deliverables or initiatives. Activities will only be taken where they have a low degree of inherent risk. The associated potential for reward / pursuit of opportunity is not a key driver in selecting activities.
Cautious	Willing to accept / tolerate a degree of risk in selecting which activities to undertake to achieve key deliverables or initiatives, where we have identified scope to achieve significant reward and/or realise an opportunity. Activities undertaken may carry a high degree of inherent risk that is deemed controllable to a large extent.
Open	Undertake activities by seeking to achieve a balance between a high likelihood of successful delivery and a high degree of reward and value for money. Activities themselves may potentially hold a high degree of residual risk.
Hungry	Eager to be innovative and choose activities that focus on maximising opportunities and offer potentially very high reward, even if these activities carry a very high residual risk.

9.5 **Risk Category** – CHS allocates risks to 5 standard categories: Strategic, Operational, Reputational, Partnership, and Financial. The table below provides more detail on the definitions of these 5 key types of risks, how they may be applied, and our potential risk appetites across the categories:

Risk Category	Description	CHS Appetite
Strategic	Any risk which affects, or is created by our strategic objectives and business plan. Strategic risks are generally reported via the strategic risk register and categorised based on their area within the CHS Business Plan.	Open Cautious
Operational	Any risks to the delivery of day to day operations and fulfilment of our statutory duties. This can include but is not limited to: H&S, IT, loss of systems, HR/People management, volunteer numbers and management, recruitment, training,	Open Cautious
Reputational	Any risk refers with the potential for negative publicity, public perception or uncontrollable events which have an adverse impact on our reputation.	Open Cautious
Partnership	Any risk where there is a dependency or inter dependency on a partner organisation to deliver all or part of the objective.	Open Cautious
Financial	Any risk with a financial implication which would result in a loss of funds or an inability to fulfil financial obligations. These include, but are not limited to: financial reporting, auditing, valuation, market, liquidity, and credit risks.	Open Cautious

9.6 **Risk identification** – Risk identification should be undertaken as an integral part of the corporate and business planning process and must also be done at the initiation of any new project or initiative. In every case, risk identification should be ongoing and risks should be prioritised in relation to objectives. It is the responsibility of all members of project groups and teams to identify risks. A workshop approach is likely to be most effective allowing individuals within the group/team to work together and look beyond their areas of responsibility. When defining the impact of risks, care should be taken to differentiate between the impacts that may arise and the risks themselves, and to avoid stating risks that do not impact on objectives. The risk description should encompass both the possible cause and the impact to the objective which might arise. It is advised to use a risk register and, if appropriate, exception reports during the duration of the project or initiative.

9.7 **Risk assessment** – a numerical value between 1 and 5 is given to the two key measures of risk – Impact and Likelihood. Definitions for these measures are provided in [Appendix C.](#)

Risk assessment should be recorded in a way that demonstrates clearly the key stages of the process and facilitates identification of risk priorities (in particular to identify the most significant risk issues with which senior management should concern themselves):
- capture the reasons for decisions made about what is and is not tolerable exposure;
- facilitate recording of the way in which it is decided to address risk;
- allow all those concerned with risk management to see the overall risk profile and how their areas of particular responsibility fit into it; and
- facilitate review and monitoring of risks.

Once risks have been assessed, the risk priorities for CHS will emerge. The less acceptable the exposure in respect of a risk, the higher the priority which should be given to addressing it. The highest priority risks (the key risks) should be given regular attention at the highest level of the organisation and in partnership with key stakeholders and partners e.g. consideration of joint CHS/SCRA risks.

9.8 **Controls** – the activities that CHS conducts with the purpose of reducing the likelihood/ impact of a risk occurring. Activities should be recorded and any new controls to be put in place should be proportional to the risk. Some form of cost benefit analysis might be required to ensure the control action represents value for money in relation to the risk being controlled e.g. cost, feasibility, probability and the potential impact.

8

9.9   **Risk review, escalation, and reporting** – CHS has implemented a structured risk review and reporting process, the timeline of which is located at <ins>Appendix E</ins>.

9.9.1   Risks are identified and assessed as part of the business and corporate planning process, regular review and discussion of current business activities, and at project initiation stage by the project manager(s). Depending on their nature, risks are and recorded in either Issues lists, Project, Strategic, or Operational risk registers.

9.9.2   Project risk registers are regularly reviewed during project meetings as a standing agenda item. Any significant risk movements or changes are presented to SMT via monthly project reporting/risk reporting.

9.9.3   The Business Operations and Governance Lead reviews operational and project level risks monthly and reports to SMT. Operational risks are reviewed in consultation with risk owners, project risks are reviewed in consultation with the Programme Manager. Any variations to scoring, tolerance, or other significant changes (such as new or closed risks) are formally reported at the SMT monthly meeting where decisions will be made to move significant risks to the strategic register if the threat cannot be managed within the project/operational setting, or has become so significant as to pose a threat to strategic objectives.

9.9.4   When used, departmental or local risk registers/issues lists are compiled and reviewed at departmental/team meetings. The risk interrogation template at <ins>Appendix F</ins> should provide the basis of this review and should be completed whenever a risk is identified. The matrix at <ins>Appendix D</ins> is used as a simple mechanism to increase visibility of risks and assist management decision making. The process of risk identification and management requires a commitment from the senior management team and other risk owners.

9.9.5   Any significant risks are highlighted to the Business Operations and Governance Lead at monthly risk review. The Business and Operations Lead will determine if the risk should be added to the operational or strategic risk registers and follow monthly reporting and escalation procedures accordingly.

9.9.6   Where risks cannot be satisfactorily managed locally, or where they are above scores as set out in the acceptable tolerance levels, they will be escalated for possible entry onto the strategic or operational risk registers. It is critical to emphasise that the risk management system

cannot rely on escalation through the risk register process alone. Senior management, through individual managers and directors, and through the operational group management structure, have a key role in helping to manage and find solutions to risk issues at all levels of the organisation.

9.9.7   Strategic risks are reviewed quarterly by SMT and Senior Managers and recorded in the Strategic Risk Register. Significant risks where there is a 4 point (or greater) difference between the residual score and the tolerance level are reported to ARMC quarterly. The full Strategic Risk Register is also reviewed by ARMC annually.

9.10   **Joint risks** – CHS has a number of significant partners without whom it will not be possible to achieve its objectives. It is the responsibility of the manager attending partnership meetings to raise any shared risks inherited by partnership work and ensure they are accurately reflected in the appropriate CHS risk register.
Children's Hearings Scotland and SCRA hold regular liaison meetings and any joint risks would be highlighted at joint Board meetings.

10.   Assurance

10.1   Assurance Mapping
The March 2018 Scottish Government Audit and Assurance Committee Handbook encourages organisations to 'define their assurance needs, map their various sources of assurance and develop an integrated approach to assurance which will secure best value for the public purse and embed best practice principles within their organisation'.
CHS optimise their assurance framework by inclusion within the operational and strategic risk registers in order to provide the Board awareness of the assurances available and any possible gaps.

10.2   CHS adopts a "three lines of defence" model for the assessment of risk assurance. In this model, the three lines of defence consist of a) frontline staff and policy/procedure, b) Oversight and Governance and c) Independent Review/Audit. The model provides confidence over the adequacy and effectiveness of the risk controls and is reviewed in line with risk register review and reporting.

References:
HM Treasury, "The Orange Book Management of Risk – Concepts and Principles", Crown Copyright, 2004, 18453204411;
Scottish Government, "Our Approach to Risk Management", 2011;
Scottish Government, "Scottish Public Finance Manual", 2011
SCRA, "Risk Management Policy", 2009/2022;
AIRMIC, ALARM, IRM "A Risk Management Standard", 2002;
Scottish Government Audit and Assurance Committee Handbook, 2018

Risk Management and Escalation Structure

Project Managers
- *Individual project level risk register and management*
- *Consider and review own risks monthly*

Senior Managers/Leads
- *Own and manage risks on operational/project/local risk registers in relation to their areas of work*
- *Consider and review own risks monthly*

Monthly meetings with BOGL to review risk and update register (s)

Programme Manager
- *Owns programme risks*
- *Reports on programme risks to SMT*
- *Considers risk escalation from individual project registers to strategic, or operational*
- *Reviews project risks with project managers monthly*

Business Operations and Governance Lead (BOGL)
- *Considers and reviews operational/local risks with risk holders and reports to SMT*
- *Maintains operational and strategic risk registers and reports to SMT monthly*
- *Reviews Programme risk reporting and considers escalations to SMT and other registers.*

Monthly review of risk register (s) and reporting to SMT

Monthly report reviewed by SMT on risk changes and consideration of risk escalations. Quarterly review of strategic risk register.

Senior Management Team
- *Owns strategic and operational risk registers and considers risks escalated from local/project risk registers*
- *Reviews Operational and Strategic Risk registers quarterly*
- *Reviews risk reports monthly*

Audit & Risk Committee
CHS Board
- *Sets strategic direction and policy for Risk Management and Governance*
- *Has overall responsibility for the system of internal control and for overseeing risk management*
- *Reviews regular reports to gain assurance on Risk Management*

Quarterly report and review of high level strategic risks. Annual review of policy and full strategic register.

Date approved A   ay 2022
Date for   by ARMC:

Risk Register Management

Register Column	Column description and information requirements for Risk Registers
A	Risk number.
B	Risk Category e.g. Financial, Joint, Operational, Strategic, Reputational, etc.
C	Risk Title and Description. A statement of a risk should encompass both the possible cause and the impact to the objective which might arise. Care should be taken to avoid confusion between the impacts that may arise and the risks themselves, and to avoid stating risks that do not impact on objectives; equally care should be taken to avoid defining risks as simply the converse of the objectives. A statement of a risk should encompass both the possible cause and the impact to the objective which might arise.
D	Select Risk Owner, main CHS contact with primary responsibility for business area.
E	Gross score. The impact multiplied by the likelihood of the event taking place **before** any action has been taken to manage it (see Appendix C)
F	Describe current mitigating actions in place to bring risk to acceptable and justifiable level. Columns N through P are the "three lines of defence" for assurance of the mitigating factors. (See section 9 of this policy for more detail)
G	The effectiveness of the controls i.e. Effective, partially effective, ineffective.
H	Residual score. The impact multiplied by the likelihood of the event taking place **After** the identified controls are in place (see Appendix C)
I	Change since last review. Report change of score, if new or edited risk since last review cycle.
J	Risk Appetite. The level of risk prepared to accept in pursuit of objectives, before additional action is deemed necessary to reduce the risk. (see section 8.3 of this policy for more detail)
K	Tolerance level. The exposure scoring (inherent risk) arising from a specific risk **before** action has been taken to manage it. The colour would relate to the organisational risk appetite and tolerance, i.e. RED 20-25, Orange 12-20 , Yellow 6-12, and Green 1-6
L	Additional actions. Describe additional mitigating actions needed to bring risk to acceptable and justifiable level. Columns N through P are the "three lines of defence" for assurance of the mitigating factors. (See section 9 of this policy for more detail)
M	Action owner and deadline for completion of additional actions.
O	1st Line Assurance. Local Processes, Controls and Monitoring i.e. policy, procedures, staff skills and competencies, internal compliance, training, etc. that provide assurance the mitigating actions are effective controls.
P	2nd Line Assurances. Oversight of Functions, processes, controls and monitoring ie. governance polices, strategic planning, KPI reporting, SMT review, Board and subcommittee reivew, etc., that provide assurance the mitigating actions are effective controls.
Q	3rd Line Assurance. Independent Assurance i.e. Joint/Partner Boards, internal/external audit, legal advice, external accreditations, etc., that provide assurance the mitigating actions are effective controls.
S-U	Summary assurance map assessment. Using a RAG status, assess the effectiveness of assurances and identifies areas in need of improvement/grater assurance. This can be used to create an action plan to improve assurances and create more robust mitigating factors.

Date approved ARMC: 10 May 2022
Date for review by ARMC:

Risk Scoring and tolerance

Impact and Likelihood Scoring

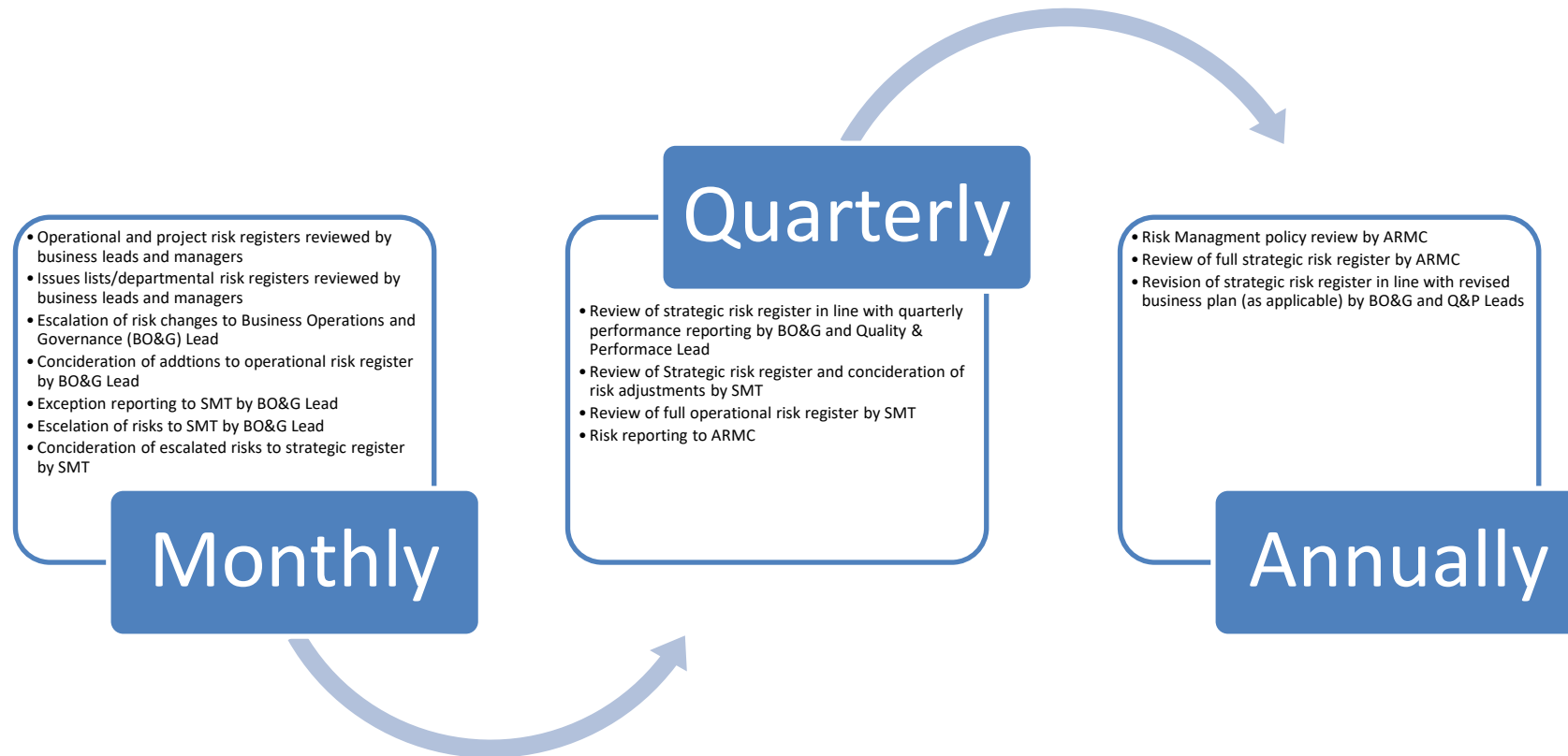| IMPACT		LIKELIHOOD				
		Rare The event will only incur in exceptional circumstances	**Unlikely** The event is not expected to occur	**Possible** The event might occur at some time	**Likely** The event will probably occur at least once	**Almost Certain** The event will occur in most circumstances
Multiplier		1	2	3	4	5
Severe Catastrophic effect on service provision	5	5	10	15	20	25
Major Significant impact on the achievement of the objective or service provision	4	4	8	12	16	20
Moderate Low impact on achievement of the objective or service provision	3	3	6	9	12	15
Minor Little impact on achievement of the objective or service provision	2	2	4	6	8	10
Insignificant No impact on achievement of the objective or service provision	1	1	2	3	4	5

Risk Tolerance

Risk rating	Net risk assessment	Risk tolerance response
Very High	20-25	Rating: Unacceptable level of risk exposure that requires immediate termination, transfer or mitigation Reporting: To Accountable Officer/ Audit Committee for upward reporting to Board
High	12-20	Rating: Unacceptable level of risk which requires controls to terminate, transfer, or mitigation to reduce exposure Reporting: consideration should be given as to whether High risks should be escalated to Senior Management/Executive (Scores between 10 - 14: No / scores between 15 - 19 Yes)
Medium	9-14	Rating: Acceptable level of risk exposure subject to regular active monitoring which may be tolerated or treated with minor mitigation. Reporting: Lead/Manager
Low	1-6	Rating: Acceptable level of risk based on the operation of normal controls. In some cases it may be acceptable for no mitigating action to be taken e.g. net risk< 4 Reporting: Lead/Manager

Example Risk Impact Definitions

Description	Financial	Injury or Illness	Asset Loss	Business Continuity	Reputational	Corporate Objectives	Regulatory & Legal
Insignificant	<£50k	Minor injury, or illness, first aid, no days lost	Minor damage to single asset	<0.5 days	Minor media interest	<2.5% variance	Act or omission resulting in legal or regulatory breach causing insignificant impact loss (as categorised in other impact categories)
Minor	£50k – 100K	Minor injury, or illness, medical treatment, days lost	Minor damage to multiple assets	0.5>1 day	Headline media interest	2.5-5% variance	As above - causing minor loss
Moderate	£0.1>0.25 m	Moderate injury, medical treatment, hospitalisation, <14 days lost, RIDDOR reportable	Major damage to single or multiple assets	1>7 days	Headline media interest causing public embarrassment	5-10% variance	As above - causing moderate loss
Major	£0.25m> 0.5m	Single death, extensive injuries, long-term illness (>14 days)	Significant loss of assets	7>30 days	Short-term media campaign	10-25% variance	As above - causing major loss
Severe	>£0.5m	Multiple deaths or severe disabilities	Complete loss of assets	>30 days	Sustained media campaign/ lobbying	>25% variance	As above - causing catastrophic loss and Legal or regulatory supervision

Risk Management and Reporting Timelines

Monthly

- Operational and project risk registers reviewed by business leads and managers
- Issues lists/departmental risk registers reviewed by business leads and managers
- Escalation of risk changes to Business Operations and Governance (BO&G) Lead
- Concideration of addtions to operational risk register by BO&G Lead
- Exception reporting to SMT by BO&G Lead
- Escelation of risks to SMT by BO&G Lead
- Concideration of escalated risks to strategic register by SMT

Quarterly

- Review of strategic risk register in line with quarterly performance reporting by BO&G and Quality & Performace Lead
- Review of Strategic risk register and concideration of risk adjustments by SMT
- Review of full operational risk register by SMT
- Risk reporting to ARMC

Annually

- Risk Managment policy review by ARMC
- Review of full strategic risk register by ARMC
- Revision of strategic risk register in line with revised business plan (as applicable) by BO&G and Q&P Leads

Date approved ARMC: 10 May 2022
Date for review by ARMC:

Risk Interrogation Questionnaire

1. What are the key elements of the risk?

2. On what basis have you decided of the initial risk score?

3. What actions are in place/planned and what is the expected impact of each action in mitigating the risk?

4. Will the risk be fully mitigated within the resources currently available?

5. If no to question 4, what more could be done and what further resources are required?

6. What corporate action, if any, is necessary?

7. Who needs to know about the risk and the mitigation plans?

8. What additional evidence is there that the risk is under control?

9. What is the timetable for reviewing the progress of mitigating the risk?

10. On what basis have you decided on the target risk score?