Risk Management Policy and Procedure

CG04

Beware when using a printed version of this document. It may have been subsequently amended. Please check online for the latest version.

Applies to:	All NHS Resolution employees, Non-Executive Directors, contractors, secondees and consultants.
Version:	4
Date of ORG Review	25 September 2020
Date of SMT endorsement :	7 October 2020
Date of Audit and Risk Committee Endorsement	14 October 2020
Date of Board Approval	10 November 2020
Review date:	November 2023
Author:	Catherine O'Sullivan
Owner:	Joanne Evans

Contents

1. Introduction

1.1. This document sets out the governance structures in place to ensure that risks are managed and escalated through NHS Resolution as appropriate

1.2. Good risk management awareness and practice at all levels is a critical success factor for an organisation such as NHS Resolution. Risk is inherent in everything that we do. NHS Resolution will ensure that decisions made on behalf of the organisation are taken with consideration to the effective management of risks.

2. Aims

2.1. The aim of this Risk Management Policy and Procedure is to provide a supportive risk management framework that ensures:

- integration of risk management into activities across the organisation as well as policy making, planning and decision making processes;
- chances of adverse incidents, risks and complaints are minimised by effective risk identification, prioritisation, treatment and management
- a risk management framework is maintained, which provides assurance to the Board that strategic and operational risks are being managed
- risk management is an integral part of NHS Resolution culture and encourages learning from incident
- risk associated with the health, safety & wellbeing of staff, fraud, project and programme management and information security are minimised; and
- employees, reputation, finances and business continuity are protected through the process of risk identification, assessment, control and mitigation.

This policy represents a dynamic approach to the management of all risks.

3. Statement of intent

3.1. The Board intends to use the risk management processes outlined within this policy and Procedure as a means to help achieve the aims as set out in the organisational strategy as well as the business plan objectives. All identified risks will be required to:

- be recorded with a core minimum amount of information as set out in the procedure section;
- be assessed on the likelihood of the risk being realised and the level of impact should the risk be realised; and
- have an identified risk owner and treatment owners.

4. Who this policy applies to

4.1. This policy and procedure is intended for use by all NHS Resolution employees, Non-Executive Directors, contractors, secondees and consultants who carry out duties on behalf of NHS Resolution.

4.2. This document is applicable to all strategic and operational risks that NHS Resolution could be exposed to, including information governance, programme and project risks

4.3. **Distribution Plan**

- This document is available to all staff via NHS Resolution internet and intranet sites.
- Notification of the documents will be included in the all staff bulletin, as well as through team meetings and staff induction

4.4. **Training and Support**

- To support the implementation and embedding of this risk management policy and procedure NHS Resolution will ensure;
  - all employees are provided with training and tools specific to their role and ensure they can work in a safe manner;
  - new employees are provided with induction training and all employees provided with updated refresher training in health & safety, incorporating: the risk management, incident reporting and risk assessment process; fire and manual handling training and anti-fraud and bribery
  - employees and other workers have the knowledge, skills, support and access to expert advice necessary to implement the policies, procedures and guidance associated with this policy.

5. Roles and responsibilities

5.1. Each area of the business must undertake an ongoing robust assessment of risks and escalate risks through NHS Resolution governance and escalation route, as set out the procedure section;

5.2. It is the responsibility of all staff to maintain risk awareness, identifying and reporting risks as appropriate to their line manager and / or director

5.3. The table below sets out the responsibilities for risk management at NHS Resolution

Role	Responsibility
Risk Owner	A risk owner is the responsible point of contact for an identified risk, who coordinates efforts to mitigate and manage the risk with various individuals who may also own parts of the risk. The responsibilities of the risk owner are to ensure that: • Risks are identified, assessed, managed and monitored • Risks are clearly articulated in risk registers • •Controls and treatment plans are in place to mitigate the risk to within risk appetite
NHS Resolution Board	Executive and non-executive directors share responsibility for the success of the organisation including the effective management of risk and compliance with relevant legislation. In relation to risk management the Board is responsible for: • articulating the corporate objectives and success measures for the organisation; • protecting the reputation of the organisation; • providing leadership on the management of risk; • determining the risk appetite for the organisation; • ensuring the approach to risk management is consistently applied; • ensuring that assurances demonstrate that risk has been identified, assessed and all reasonable steps taken to manage it effectively and appropriately; • considering any risks that are outside of appetite and advice of ARC on remedial actions
Audit and Risk committee	Responsible on behalf of the Board for reviewing the adequacy and effectiveness of: • all risk and control related disclosure statements (in particular the Annual Governance Statement), prior to endorsement by the Board; • the underlying assurance processes that indicate the degree of achievement of corporate objectives and the effectiveness of the management of risks; and • risk related documents, policies and procedures • Review on a regular basis the strategic and high scoring corporate risks, controls and treatment plans (including overcontrols) and, in relation to those risks which are outside the risk appetite of the organisation, recommend appropriate action to the Board. • Escalate to the Board any matters of significance which require Board attention or approval

Role	Responsibility
Chief Executive officer	Responsible for: • ensuring that management processes fulfil the responsibilities for risk management; • ensuring that full support and commitment is provided and maintained in every activity relating to risk management; • planning for adequate staffing, finances and other resources, to ensure the management of those risks which may have an adverse impact on the staff, finances or stakeholders of NHS Resolution; • ensuring an appropriate corporate risk register is prepared and regularly updated and receives appropriate consideration; and, • ensuring that the governance statement, included in the annual reports and accounts, appropriately reflects the risk management processes in operation across NHS Resolution.
Director of Finance and Corporate planning	The Director of Finance is the executive director and Senior information risk owner (SIRO), designated as the accountable and responsible officer for implementing the system of internal control, including this Risk Management Policy. This responsibility extends to co-ordinating finance based reviews by internal audit and external agencies and action taken as a result.
Senior Management team (SMT)	NHS Resolution Senior Management team has responsibility for • on a quarterly basis undertake a review of the strategic and operational risk register to ensure they are current and review implementation of treatment plans, prior to submission to the Audit and Risk committee (ARC) • on a quarterly basis and SMT will assure ARC that risks are being reported and managed appropriately at local team level by receiving reports from the Operational Review Group
NHS Resolution directors and direct reports to CEO	Responsible for: • ensuring that risks are actively managed within their business areas; • owner and action owner of individual risks; • ensuring staff comply with all organisational policies and procedures and fulfil their responsibility for risk management by identifying, reporting, monitoring and managing risk; • leading the management of risk by devising short, medium and long-term plans to tackle identified risk, including the production of any mitigating action plans and; • escalation of risks from or to the operational and team risk registers, for consideration by the SMT for inclusion on the strategic risk register.

Role	Responsibility
Operations Risk Review Group	The Operations Risk Review Group is responsible for: • reviewing NHS Resolution team and Corporate Operational risk registers, including assurance on controls and, where appropriate, the treatment plans; • escalating risks in line with NHS Resolution risk policy and risk procedure and where there are risks that require SMT discussion, such as those that the group are unable to provide further treatment to reduce risk score; • reviewing risks that are common across the organisation for inclusion on the Corporate Operational risk register • reviewing updates on incident reporting and consider learning; and • reviewing updates on Health & Safety mandatory training and consider actions for improvement.
Information Governance Group	Responsible for: • overseeing the implementation of the Information Governance programme of work to ensure NHS Resolution achieves a satisfactory rating on the Information Governance Toolkit, as directed by NHS Resolution Senior Management Team. • reviewing information security risks and make recommendations to address issues to NHS Resolution Senior Management team; • reviewing information security risks that are common across the organisation for inclusion on the Corporate Operational risk register • ensuring NHS Resolution continues to meet its obligations as directed by the Cabinet Office, ICO, NHS Digital and the Department of Health • reviewing updates on Information Governance mandatory training and consider actions for improvement
Corporate Governance Team	The Corporate Governance team (CGT) is responsible for: • co-ordinating all risk based reviews and treatment plans taken as a result. • ensuring that appropriate reports are created from the Strategic, Corporate Operational, Team Risk Registers, incident reporting database and training records, and that these are presented to SMT, Operational Review and IG Groups on a no less than quarterly cycle. • the risk reports to include updates on risk position, risk treatment plans and implementation and escalated risks for SMT to consider • supporting SMT in submitting reports to the Audit & Risk Committee.

Role	Responsibility
Heads of Service/Team Leaders	Responsible for: - participating (as appropriate) in the identification, assessment, planning and management of threats and opportunities; - keeping a record of the identified risks in a risk register; - undertaking a regular review of the risks on the risk register; and - escalating risks as appropriate and in accordance with risk management governance and escalation as set out in the risk procedure.
All Staff	Responsible for: - participating (as appropriate) in the identification, assessment, planning and management of threats and opportunities; - ensuring that they familiarise themselves and comply with the policies and procedures of NHS Resolution; and - undertaking and / or attending mandatory and other relevant training courses.
Internal Audit	The internal auditors are responsible for - agreeing (with the Audit Committee) a programme of audits which assess the exposures and adequacy of mitigation of the principal risks affecting the organisation. - the priorities contained in the internal audit programme should reflect the risk evaluation set out in the Strategic Risk Register. - ensuring the reports and advice produced inform the management of risk by directorates although responsibility remains with the relevant risk owners.

6. Risk appetite

6.1. ISO 31000 states Risk appetite is the amount and type of risk that an organisation is prepared to seek, accept or tolerate in pursuit of its objectives.

6.2. The Board has developed a risk appetite statement which forms part of NHS Resolution’s overall risk management strategy and will guide staff in their actions and ability to accept and manage risks.

6.3. The statement is reviewed at least annually by the Board

7. Risk Management framework

7.1. The organisational structure is supported by the Risk Management Framework. This enables NHS Resolution to monitor and address the strategic risks that would prevent the organisation achieving its strategic aims and business plan objectives, it sets out the controls (or ways the risks are being mitigated), and sources of assurance that those controls are effective. As well as setting out the treatment plans for those risks that require action to bring them within risk appetite where possible

7.2. Risks are linked to objectives and strategic aims, which exist at different levels:

7.2.1. Strategic risks – risks that affect NHS Resolution's ability to deliver the strategy or function as an organisation as a whole;

7.2.2. Corporate Operational Risks – risks that affect the delivery of NHS Resolution's business plan or common team risks that require a corporate response

7.2.3. Team risks - risks that are related to the delivery of departmental operations and objectives

7.2.4. Programmes and their project outcomes – risks associated with, usually, time limited activities and medium- to long-term delivery of benefits.

7.3. NHS Resolution maintains a strategic risk, corporate operational and local team risk registers. These registers record non-project risks.

7.4. All projects risks will be managed through the appropriate project boards with reporting and escalation through the change management governance process

8. Assuring implementation of this policy

8.1. The corporate governance team will be responsible for assuring the implementation of the policy and procedure. This will be through discussions with Directors, Deputy Directors and Heads of Service to consider the risk management processes and risk registers from their business areas on a quarterly basis.

8.2. The outcomes of the reviews will be reported to the Senior Management Team, Information Governance Group and Operations Risk Review Group for consideration and where required, further action taken to improve embedding risk management at NHS Resolution.

8.3. Internal audit will conduct audits as required to provide an independent assessment of the design of the risk management policy, processes and procedures and the extent to which they are applied across the organisation. The recommendations of the review will be reported to SMT and the Audit and Risk Committee.

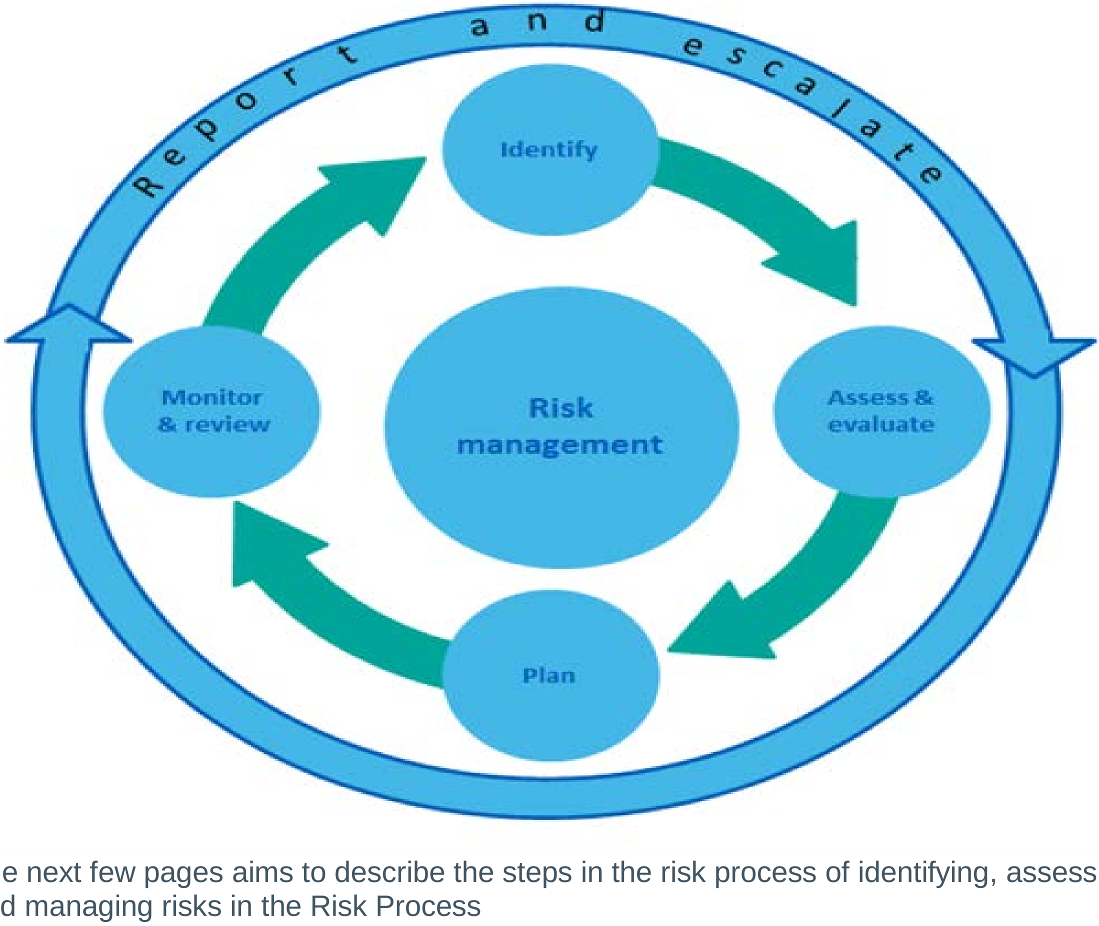
8.4. The Audit and Risk Committee oversee the establishment and maintenance of an effective system of assurance on risk management through approval of the risk management policy, regular reporting on the management of strategic and risks and progress updates against audit recommendations.

9. Equality impact assessment

As part of its development, this policy and its impact on equality have been reviewed in consultation with trade union and other employee representatives in line with NHS Resolution's Equal Opportunities Policy and the public sector equality duty. The purpose of the assessment is to minimise and if possible remove any disproportionate impact on employees and service users in relation to the protected characteristics: race, sex, disability, age, sexual orientation, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity. No detriment was identified.

10. Risk Management Procedure

Risk management is central to the strategic management of NHS Resolution. It provides a systematic process for identifying risks attached to new and current business activities.



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

10.1. Identify - Risk identification

When identifying a risk consideration should be given to what could pose a potential threat (or opportunity) to assets of the organisation.

Assets can be considered as:

- Information assets as identified on the asset register
- Business processes, objectives and KPI’s
- Our staff

Risk, incidents and issues can often get confused and a useful way of remembering the difference is;

- **Risks** are things that **might happen** and stop us achieving objectives, or otherwise impact on the success of the organisation

- **Incidents/issues** are things that **have happened**, were not planned and require management action, must be reported as appropriate and where required in line with the Incident Reporting Policy and Procedure
  - Once identified, the risk needs to be described clearly to ensure the risk is understood.
  - Once identified and described the risk should be added to the risk register and scored.
  - Guidance on how to write a risk to identify the cause, the event and the effect can be found in **Appendix A**.

Recording risks - The risk register

- The risk register provides a framework where risks that may be a threat (or opportunity) to the achievement of objectives are to be recorded.
- NHS Resolution has in place registers for team, corporate operational and strategic risks.
- The team and corporate operational risk registers must contain:

Risk ID	Risk title	Risk response
Date raised	Risk description	Treatment plan
Business area	Risk owner	Treatment owner
Risk category	Inherent risk	Date by
Risk type	Key controls	Target risk
Raised by	Current risk	

Guidance for completing the risk register can be found at Appendix A.

10.2. Assess and evaluate - Risk assessment and evaluation

A risk assessment is a qualitative or quantitative evaluation of the nature and magnitude of the risk. The assessment is completed by scoring the likelihood of the risk occurring and the impact should it occur Appendix B sets out NHS Resolution’s scoring matrix which are based on a scale of 1 - 5 and the risk rating matrix which gives the scoring a RAG status. The risk evaluation involves making a decision about what should be done with the risk.

It includes determining appropriate controls and or treatments for the risk, and what level of risk can be tolerated within the organisations risk appetite.

- A **Control** is an **existing** strategy and process currently in place such as systems, policies, procedures, standard business processes, practices.
- A **Treatment** is an **additional** strategy/activity we need to develop and implement should the risk level be unacceptable after controls are applied.

Following the evaluation consideration on what to do with the risk is taken; this is the risk response;

Risk Response	
Terminate	Where an activity or system gives rise to significant risk to NHS Resolution the activity will be carried out differently or ended hence risk is no longer relevant.
Tolerate	Where it is considered that nothing more can be done at a reasonable cost to reduce the risk or the risk is low.
Treat	This is where action can be taken to reduce the impact or the likelihood of the risk identified
Transfer	NHS Resolution is a member of the Liabilities to Third Parties Scheme and Property Expenses Scheme administered by NHS Resolution. This membership transfers some financial risk to these risk pooling schemes.

10.3. Plan – Treatment plan

Where it has been considered the risk requires further action to reduce the likelihood and/or impact of a threat or maximize the likelihood of opportunities a risk treatment plan should be devised.

The treatment plan must have an owner; it should be specific to the risk and SMART (specific, measurable, attainable, relevant and time bound) to evidence how the risk score can be reduced.

10.4. Monitor and review

The implementation of the risk treatment plan must be kept under review along with the risk score to measure its effectiveness; if the treatment is not reducing the risk a new treatment plan should be considered.

Once a treatment plan has been implemented the risk will be re-assessed and rescored and that treatment plan will become a control

Reviews of the risk registers and the treatment plans will be carried out in discussion with Directors and Heads of Service as well as at the Information Governance and Operational review groups. Escalated risks and associated will be treatments reported and reviewed by Senior Management team at least quarterly

10.5. Report and escalate

Reporting

The Corporate operational and strategic risk registers are an integral part of the system of internal control and define the highest priority risks which may impact on NHS Resolution's ability to deliver its objectives

SMT will receive updates on the team risk registers through sub group reports and Director updates, and will review the corporate operational and strategic risk registers at least quarterly.

The Strategic risk register and reports from the corporate operational risk register enables the Board and the Audit and Risk committee to be assured of management of the risks.

SMT with support from the Corporate Governance team will manage the Strategic and Corporate Operational risks on behalf of the Board.

Escalating

The table Risk Escalation and Responsibilities in Appendix D sets out the process for how risks can be escalated for inclusion on the Corporate Operational and Strategic risk registers. It is recommended that at each level Amber and Red risks are escalated.

11. Other relevant approved documents

All documents listed within the Policy Register are relevant to the risk management process, as these are in themselves risk management mechanisms; those of particular relevance are:

HR10	Disciplinary Policy and Procedure
CG11	Incident Reporting Policy and Procedure
ITFA04	Health, Safety & Wellbeing Policy

12. Document Control

Date	Author	Version	Reason for Change
17.04.18	Catherine O’Sullivan	Draft V1.0	Updated aims to align to strategy
			Updated Board Assurance section
			Updated roles and responsibilities as agreed with Chair and ARC chair
			Changed the risk framework illustration to match that in the ARA
			Updated risk categories to reflect GDPR.
25.04.18	Catherine O’Sullivan	Draft V2.0	Merged the Risk policy and Procedure into one document
25.04.18	Catherine O’Sullivan	Draft V2.0	Approved by SMT
10.05.18	ARC	Draft V2.0	Approved by ARC
July 2018	Board	Final V3.0	Approved by Board
18.09.20	Catherine O’Sullivan	Draft V4.0	Updated: Removed strategic aims and inserted link to strategy Inserted link to business plan Removed assurance framework to reflect the risk management framework Added the explanation on strategic, corporate operational, team and project risks Included statement on how project risks will be managed Updated impact table of the risk matrix to remove PESTLE following feedback from colleagues stating it was difficult to follow Updated escalation table to include project risk process Updated escalation table to include ARC reporting to the Board

14.10.20	ARC	Draft V4.2	ARC reviewed and made suggested changes ARC endorsed for Board approval
15.10.20	Catherine O'Sullivan	Draft V4.3	Incorporated ARC suggestions: • Moved the roles and responsibilities table up to section 5 of the policy, so it is no longer an appendix • Included a statement in the table on Risk Owner • Updated the risk appetite statement to reflect ARC's point ' ISO 31000 states Risk appetite is the amount and type of risk that an organisation is prepared to seek, accept or tolerate in **pursuit of its objectives'**
10.11.20	Board Review	Draft V4.4	Board Review
16.11.20	Catherine O'Sullivan	Final V4.0	Approved for publication

2020 Changes to the Policy and Procedure

Section	Page	Changes
3. Statement of Intent	4	Removed strategic aims and inserted link to our 2022 strategy Approval date updated
3. Statement of Intent	4	Inserted link to business plan risk management supports the delivery of our objectives set out in the document
5. Roles and Responsibilities	5	Moved the roles and responsibilities table up to section 5 of the policy, so it is no longer an appendix. (ARC request) Added a statement in the table on Risk Owner responsibilities (ARC request)
6. Risk Appetite	9	Updated the risk appetite statement to reflect ARC's suggestion that of adding the words 'In pursuit of its objectives: ' ISO 31000 states Risk appetite is the amount and type of risk that an organisation is prepared to seek, accept or tolerate **in pursuit of its objectives'**
7. Risk Management Framework	10	Removed the assurance framework diagram and updated the text to reflect the risk management framework
7. Risk Management Framework	10	Added an explanation on strategic, corporate operational, team and project risks as they form the risk management framework
7. Risk Management Framework	10	Included statement on how project risks will be managed
Appendix B- Risk matrix and risk categories	20	Updated impact table of the risk matrix to remove PESTLE following feedback from colleagues stating it was difficult to follow. The list is more concise now, but note as stated in the document they are illustrative examples and not intended to be a comprehensive list.
Appendix D – risk escalation	22	Updated escalation table to include project risk process
Appendix D – risk escalation	22	Updated escalation table to include ARC reporting to the Board

Appendix A

Risk register guidance

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

The strategic risk register requires further information in relation to assurances:

Movement since last risk register	This indicates any change in the current risk score in the form of an arrow. ↑ indicates an increase in the level of risk**;** ↓ is an improvement in position and therefore a reduction in the level of risk. Where there is no change in the level of risk this is indicated by ↔.
Assurance on controls	This should include internal assurance / evidence (e.g. Board reporting, sub- committee governance) and external assurance / evidence (e.g. planned or received audits or reviews) that the risk is being effectively managed.
Gaps in control	Where an additional system or process is needed, or evidence of effective management of the risk is lacking.

It is important to note that risk registers are subject to Freedom of Information (FOI) requests, therefore care should be taken with the wording of the risk.

Appendix B

Risk matrix and risk categories

Impacts: This table gives illustrative examples to enable managers to judge the scale of impact in a consistent way when assessing risks. It is not intended as a comprehensive list.

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

This table sets out the likelihood scores for the risk occurring:

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

This table sets out the RAG status for the risk:

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

Appendix C

Risk categories and potential sources of risk

Best practice in risk identification requires the categorisation of risks. Each risk/opportunity identified can be classified into one of the risk categories that define business activity. If a risk has aspects that relate to more than one category, the predominant category is recorded on the risk register

Risk considerations	Risk category	Examples of sources to consider	
Risks that may relate to the delivery of services Internal and external factors impacting on the core operations of the organisation	**Service Delivery & Planning**	• Organisational Change • External Pressures • Communication • Outsourced Services • Departmental guidelines • Legal liabilities • Organisational Change • Customer Satisfaction • Value of service • Failure to deliver key programmes or-projects	• Human & Financial Resources • Information Governance • Business Continuity • Market Awareness • DH Directions • Market Awareness • Evaluation and feedback • Legal liabilities
Risks that relate to the resources used by the organisation to accomplish its objective	**Information Technology**	• Information Governance • Business continuity and disaster response • Cyber attack • Records management	• Contractors • Outsourced services • Separate NHS Resolution and NCAS networks • Advancement in technology
	Human Resource Management	• Recruitment and allocation of resources • Staff recognition & dispute resolution	• Workforce and succession planning • Policies & Procedures
	Finance	• Financial management • Legislative & industry requirements	• Government austerity cuts • Policies and procedures • Legal liabilities
Risks that originate from the requirements to comply with a regulatory framework for data protection, policies, directives or legal agreements	**GDPR (General Data Protection Regulations)**	• Records management • Data Transfer • DPA/ FOIA Compliance • Cyber Attack • Outsourced services • Contractual agreements • IG incidents	• Business continuity and disaster response • Disposal/ destruction of data • Data storage • Information security

This list is not conclusive & indicates only some examples of potential sources of risk

Appendix D

Risk escalation and responsibility

Risk Score	Risk Response	Action	By Whom	Escalation
High Risk	Treat/Transfer/Terminate			
15-25	Risks deemed as high require a systems approach to identify the root causes of the risk and thereby help choose an appropriate risk response. Where it is not possible to terminate or transfer the risk a treatment plan will be in place	• Corprate Operational risk register reviewed by SMT to consider escalation to Strategic Risk Register • SMT review Strategic risk Register for addition or removal of risks and recommend to the ARC • ARC review strategic and top corporate operational risks • ARC to report risks by exception or of significance to the Board	• SMT • ARC • Board	↑
Moderate Risk	Treat			
8-12	Risks deemed as moderate to high will require a treatment plan in line with the risk appetite. Those risks where it is deemed no further treatment can reduce the risk will be reviwed regulalry to assess impact on the organisation	• Risk register discussed with Director/Deputy Direcor/Head of Service • Risks identifed as amber and red reported to the Opertaions Review/Information Governance Groups for inclusion on the Corporate Operational Risk Register • Amber and red risks and associated treatment plans reviwed by ORG/IG and reported to SMT • SMT review report from ORG and Directors • Project risks discussed at relevant project board and CMG where required • Where projects have been identified as a treatment plan impacts on their delivery to be discussed at ORG/SMT	Directors and CEO direct Reports ORG/IG SMT Project Boards CMG	↑
Low Risk	Tolerate			

1-6	Risks graded as 1-6 either require no action or can be managed through local action or by an appropriate person or department.	• Risk is identified • Risk added to team risk register • Action to reduce risk where necessary is considered • Risk register discussed at team meetings • Project risks discussed with project team	All staff	

Appendix E

Glossary: Common terms used in risk management

Assurance	Evidence that risks are being effectively managed (e.g. planned or received audit reviews and assurance map).
Control(s)	Existing strategies and processes currently in place such as systems, policies, procedures, standard business processes and practices to manage the likelihood or impact of a risk Practices.
Corporate Operational risk register	A record of the risks identified through internal processes that will impact on NHS Resolution’s business objectives or major programmes.
Current Risk	Risk impact, likelihood and total score with the controls in place to manage the risk
Gaps in controls or assurances	Where an additional system or process is needed, or evidence of effective management of the risk is lacking.
Impact	Is the result of a particular threat or opportunity should it actually occur.
Incident/ issue	A relevant event that has happened was not planned and requires management action and must be reported as appropriate and where required in line with the **Incident Reporting Policy and Procedure**
Inherent Risk	The risk score where there are no controls in place to manage the risk
Likelihood	Is the measure of the probability that the threat or opportunity will happen, including a consideration of the frequency with which this may arise.
Operational risks	A risk or risks that have the potential to impact on the delivery of business, project or programme objectives. Operational risks are managed locally within teams and significant operational risks are escalated, where appropriate, to SMT via the internal reporting process
Opportunity	An uncertain event that would have a favourable impact on objectives or benefits if it occurred.
Risk	A risk is an uncertain event or set of events that, should it occur, will have an effect on the achievement of business, project or programme objectives. A risk can be a threat or an opportunity.
Risk Appetite	The phrase used to describe where NHS Resolution considers itself to be on the spectrum ranging from willingness to take or accept risk through to an unwillingness or aversion to taking some risks.
Risk Assessment	The process used to evaluate the risk and to determine whether controls are adequate or more should be done to mitigate the risk within the organisations risk appetite

Risk Management	The systematic application of management policies, procedures and practices to the task of identifying, analysing, assessing, treating and monitoring risk.
Target Risk	The risk we aim to get to with controls on place and completing the treatment plan
Team Risk Register	A record of the risks identified through internal processes that will impact on the delivery of team objectives and / or plans.
Threat	An uncertain event that could have a negative impact on the delivery of objectives or benefits, should it occur
Treatment Plan	Is a plan for additional strategies/activities we need to develop and implement should the risk level be unacceptable after controls are applied. A treatment plan should be specific to the risk and SMART (Specific, Measurable, Attainable, Relevant and Time bound) to evidence how the risk score can be reduced.
Strategic Risk Register	A record of the risks identified that will impact on NHS Resolution's strategic objectives or have significant impact on the organisation ability to deliver.