NHS
Wrightington, Wigan and
Leigh Teaching Hospitals
NHS Foundation Trust

| | |
|---|---|
| **STANDARD OPERATING PROCEDURE** | **Risk Management Process** |
| **SOP ID NUMBER** | **TW10-002 SOP 1** |
| **VERSION NUMBER** | **6** |
| **APPROVING COMMITTEE** | **Risk Management Group (RMG)** |
| **DATE THIS VERSION APPROVED** | **September 2021** |
| **RATIFYING COMMITTEE** | **PARG (Policy Approval and Ratification Group)** |
| **DATE THIS VERSION RATIFIED** | **November 2021** |
| **AUTHOR(S)**<br>(JOB TITLE) | **Head of Risk** |
| **DIVISION/DIRECTORATE** | **Corporate** |
| **ASSOCIATED TO WHICH POLICY?** | **TW10-002 Risk Management Framework**<br>**TW18-002 Risk Management Policy**<br>**TW10-007 Health and Safety Policy** |
| **CONSULTED WITH** | **RMG** |

| | |
|---|---|
| **DATES PREVIOUS VERSION(S) RATIFIED** | **Version 5: June 2018** |
| **DATE OF NEXT REVIEW** | **November 2024** |
| **MANAGER RESPONSIBLE FOR REVIEW (Job Title)** | **Director of Corporate Affairs** |

The WWL Way

**AT ALL TIMES, STAFF MUST TREAT EVERY INDIVIDUAL WITH RESPECT AND UPHOLD THEIR RIGHT TO PRIVACY AND DIGNITY**

## 1 INTRODUCTION

**1.1** This standard operating procedure details the overall approach for each stage of the process model (Fig.1). Throughout all stages of risk management effective communication and consultation should take place with internal and external partners, i.e., employees, patients/services users, commissioners, partners, other trusts, etc. This standard operating procedure is supported by a suite a Risk Guides which provide further detail and advice on the Risk Management process.

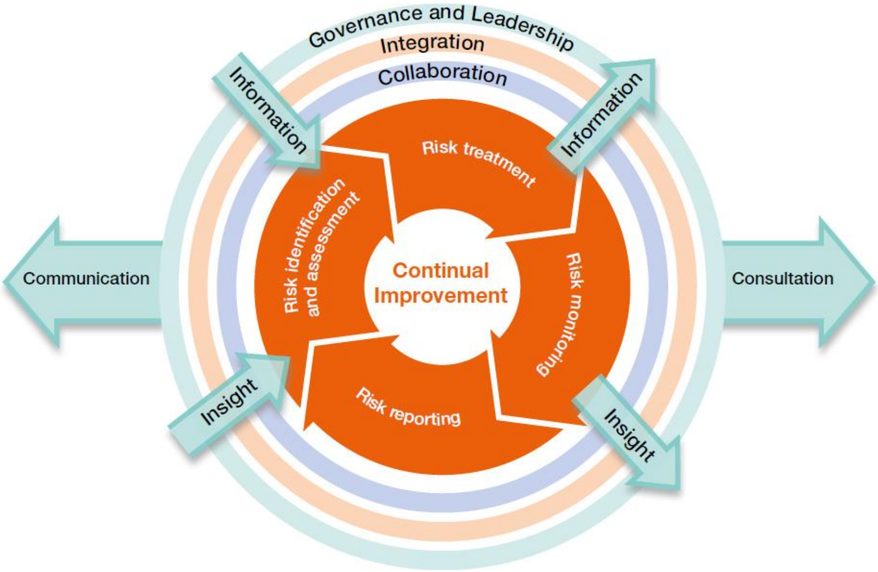


Fig.1 Risk Management Process (adapted from Gov: The Orange Book 2020 and ISO 31000:2018)

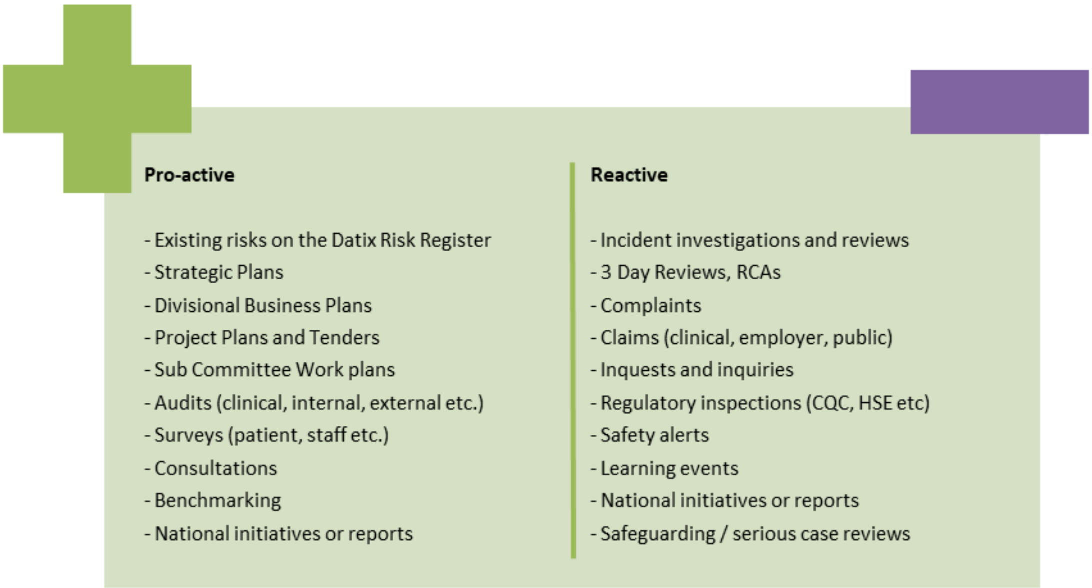
## 2. IDENTIFICATION OF RISK

2.1 The identification of risks will be undertaken at a strategic level and a local level**.** Strategic level risks, known as Board risks, are those that may have a positive or negative effect on achieving the trust's strategic objectives, which have been identified in the Strategic Plan. Strategic level risks are assessed, treated and managed by the Executive Management Team and are reported on the Board Assurance Framework and recorded as Board Risks on the Datix risk register.

2.1.2 Tactical and operational level risks, known as corporate risks, are those which may have a positive or negative effect on achieving the trust's corporate objectives which have been identified in the divisional business plans, workforce plans, project plans/tenders, subcommittee workplans, operational plans/activities and local project plans. Corporate risks will be locally assessed, treated, managed and reported on the Datix risk register.

2.1.3 Every risk will have an identified risk lead and committee/sub group to oversee management of the risk. Where a division identifies a risk which impacts on the objectives of another service, or that sits jointly across several services or trust wide, discussion should take place between senior managers/Local Risk Management leads to identify a lead service and risk lead.

2.1.4 Risks can be externally or internally driven and identified from a number of pro-active and reactive sources as follows:



**Pro-active**

- Existing risks on the Datix Risk Register
- Strategic Plans
- Divisional Business Plans
- Project Plans and Tenders
- Sub Committee Work plans
- Audits (clinical, internal, external etc.)
- Surveys (patient, staff etc.)
- Consultations
- Benchmarking
- National initiatives or reports

**Reactive**

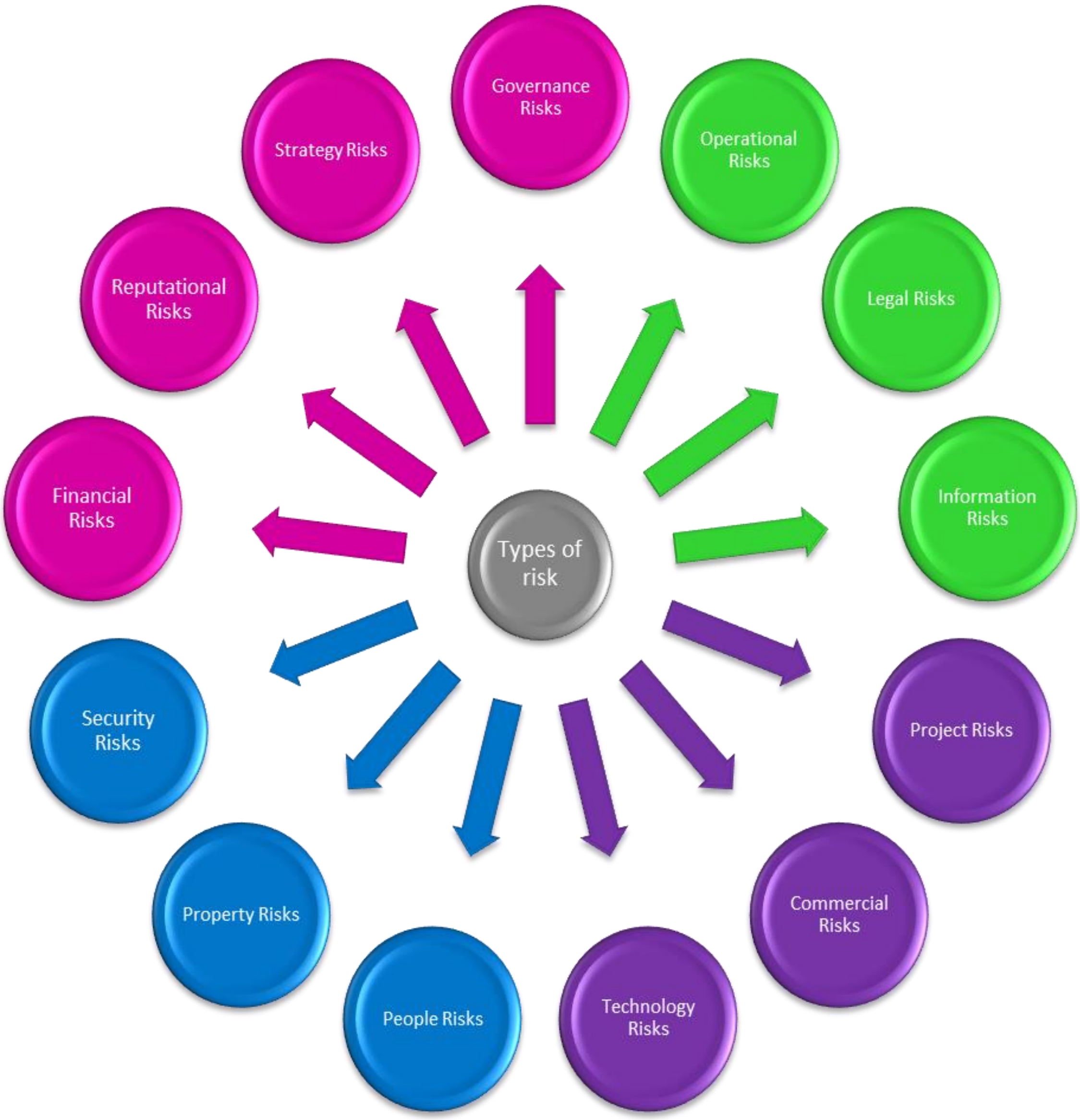
- Incident investigations and reviews
- 3 Day Reviews, RCAs
- Complaints
- Claims (clinical, employer, public)
- Inquests and inquiries
- Regulatory inspections (CQC, HSE etc)
- Safety alerts
- Learning events
- National initiatives or reports
- Safeguarding / serious case reviews

2.1.5 Consideration should be given to whether a risk or an issue has been identified before creating a new risk entry on the risk register. It may be more appropriate to escalate issues through the incident reporting system or the relevant helpdesk.

2.1.6 Risk statements should be well defined with risk cause, uncertain event and impact identified. The context of the risks also needs to be considered.

2.1.7 Risk is a very broad term, and a number of different risk “categories” exist that should be considered, properly assessed and managed. The following chart highlights the common risk types, which have been identified within the Trust.

## 2.2 CATEGORIES OF RISK



2.2.1 Strategy risks – Risks arising from identifying and pursuing a strategy, which is poorly defined, is based on flawed or inaccurate data or fails to support the delivery of commitments, plans or objectives due to a changing macro-environment (e.g., political, economic, social, technological, environment and legislative change).

2.2.2 Governance risks – Risks arising from unclear plans, priorities, authorities and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance.

2.2.3 Operations risks – Risks arising from inadequate, poorly designed or ineffective/inefficient internal processes resulting in fraud, error, impaired customer service (quality and/or quantity of service), non-compliance and/or poor value for money.

2.2.4 Legal risks – Risks arising from a defective transaction, a claim being made (including a defence to a claim or a counterclaim) or some other legal event occurring that results in a liability or other loss, or a failure to take appropriate measures to meet legal or regulatory requirements or to protect assets (for example, intellectual property).

2.2.5 Property risks – Risks arising from property deficiencies or poorly designed or ineffective/ inefficient safety management resulting in non-compliance and/or harm and suffering to employees, contractors, service users or the public.

2.2.6 Financial risks – Risks arising from not managing finances in accordance with requirements and financial constraints resulting in poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting.

2.2.7 Commercial risks – Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, and /or failure to meet business requirements/objectives.

2.2.8 People risks – Risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviours, the unavailability of sufficient capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance.

2.2.9 Technology risks – Risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience.

2.2.10 Information risks – Risks arising from a failure to produce robust, suitable and appropriate data/information and to exploit data/information to its full potential.

2.2.11 Security risks – Risks arising from a failure to prevent unauthorised and/or inappropriate access to the estate and information, including cyber security and non-compliance with General Data Protection Regulation requirements.

2.2.12 Project/Programme risks – Risks that change programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits to time, cost and quality.

2.2.13 Reputational risks – Risks arising from adverse events, including ethical violations, a lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, leading to damages to reputation and or destruction of trust and relations.

2.2.14 Failure to manage risks in any of these categories may lead to financial, reputational, legal, regulatory, safety, security, environmental, employee, customer and operational impacts.

2.3 Good management practice should ensure that risks are identified from the above sources and are subsequently assessed and managed. All employees are responsible for raising, with their line manager and/or their Local Risk Management Lead, any concerns they have in relation to risks that have not been identified or appear not to be effectively managed.

## 3. ASSESSMENT OF RISKS

3.1 The assessment of a risk is undertaken by calculating the likelihood of the risk occurring and the impact if it did. This assessment is undertaken by scoring the likelihood and impact using the following tables, and then by multiplying the figures to obtain an overall risk level. The level of risk should be determined at three stages:

1) **Risk appetite** is the level of risk with which the trust **aims** to operate and is set annually by the Board as part of the strategic planning process.

2) The **current risk position** is the risk level at which the trust is currently operating. This level is tolerated by default, where cessation of activity is not an option. Risks are subject to management to drive activity into tolerance or appetite parameters.

3) **Risk tolerance** is the level of risk with which the trust is **willing** to operate, given current constraints. This level is set by the board as part of the strategic planning process.

3.1.1 The Trust has developed the following standard risk rating matrix to be applied across all risks (excluding clinical risk assessment). See appendix 3 for likelihood and impact descriptions.

**Calculating the Likelihood (probability):**

| Level | Descriptor |
|---|---|
| 1 | Rare |
| 2 | Unlikely |
| 3 | Possible |
| 4 | Likely |
| 5 | Almost Certain |

**Calculating the Impact on objectives:**

| Level | Descriptor |
|---|---|
| 1 | Insignificant |
| 2 | Minor |
| 3 | Moderate |
| 4 | Major |
| 5 | Critical |

**Calculating the overall Risk Level**

| | | **Impact:** | | | | |
|---|---|---|---|---|---|---|
| | | **Insignificant** | **Minor** | **Moder** | **Major** | **Critica** |
| **Likelihood:** | | 1 | 2 | 3 | 4 | 5 |
| **Certain** | 5 | 5x1 = 5 M | 5x2 = 10 H | 5x3 = 15 E | 5x4 = 20 E | 5x5 = 25 E |
| **Likely** | 4 | 4x1 = 4 M | 4x2 = 8 H | 4x3 = 12 H | 4x4 = 16 E | 4x5 = 20 E |
| **Possible** | 3 | 3x1 = 3 L | 3x2 = 6 M | 3x3 = 9 H | 3x4 = 12 H | 3x5 = 15 E |
| **Unlikely** | 2 | 2x1 = 2 L | 2x2 = 4 M | 2x3 = 6 M | 2x4 = 8 H | 2x5 = 10 H |
| **Rare** | 1 | 1x1 = 1 L | 1x2 = 2 L | 1x3 = 3 L | 1x4 = 4 M | 1x5 = 5 M |

| **Risk Score** | **Risk Rating** |
|---|---|
| 1 – 3 | Low Risk |
| 4 – 6 | Moderate Risk |
| 8 – 12 | High Risk |
| 15 - 25 | Extreme Risk |

3.1.2 Once the assessment of risk has been undertaken, an evaluation of the risk is required to be undertaken. The evaluation is to determine whether this risk level is within risk appetite or tolerable, or whether the risk requires further control measures to reduce its level, known as risk treatment. The evaluation process involves considering the level of risk and the time, cost and effort involved in reducing the risk rating further. The Datix record provides a section to record the financial cost of risk treatment.

3.1.3 Risks scoring 15 or above are escalated to the RMC and considered for inclusion in the BAF every quarter. The trust's willingness to accept a risk above the tolerance level will depend on which of the corporate objectives is at risk and the positive or negative impact that the risk would have on objectives, should it materialise. Therefore, the risk evaluation referred to above must be completed by managers with sufficient knowledge and authority.

3.1.4 To enable the Trust to make an informed decision on accepting levels of risk the table below identifies those managers and groups that should be involved in deciding if a risk level is acceptable. The framework below does not include the management of strategic risks that feature on the Board Assurance Framework (BAF).

| **Risk Score Awarded** | **Risk Owner** | **Decision to accept risk** | **Risk Register** |
|---|---|---|---|
| 1-8 | Ward / Department Manager | Divisional Risk Review Panel | Corporate |
| 9-12 | Directorate Managers / Heads of Nursing and/or Service | Divisional Quality Executive Committee | Corporate |
| 15-25 | Divisional Director of Performance (or equivalent Head of Service) in association with the Ward / Department Manager | Risk and Management Committee (RMC) | Corporate |

## 4. TREATMENT OF RISKS

4.1 Risk treatment is the process of applying further control measures to eliminate, reduce or mitigate the risk.

Details of each response can be found in the following table:

| **Response** | **Description** |
|---|---|
| Terminate the Risk | A risk maybe outside the trust's risk appetite or tolerance and the trust does not have the ability to introduce additional controls to reduce likelihood and/or impact of the risk therefore there is no other option than to terminate the activity generating the risk. |
| Treat the Risk | Risks need additional treatments (controls) to reduce the likelihood and/or impact levels.<br>This response is most likely where the risk has been identified as a high risk due to the likelihood and impact levels and the trust can introduce further controls that will reduce the likelihood and/or the impact of a risk. |
| Transfer the Risk | Risks are shared (e.g., through an insurer). Some service delivery risks can also be transferred to a partner or contractor by way of a formal contract or written agreement.<br>Some aspects of risk however cannot be transferred, for example those that have a reputational impact. |
| Tolerate the Risk | Retaining the risk by informed decision. The controls in place reduce the likelihood and impact levels to an acceptable level (within appetite or tolerance) the introduction of additional controls would be cost-benefit prohibitive. It is therefore decided to *tolerate* the risk. |
| Take the opportunity | Taking or increasing the risk to pursue an opportunity. |

The Datix risk record should be used to record any identified gaps in controls.

4.1.1 For each additional control measure a person responsible and a target date must be identified through the actions section in the Datix risk record. The following table provides guidelines on suitable timeframes based on the risk level:

| **Risk Rating** | **Risk Score** | **Recommended timeframe for actions** |
|---|---|---|
| **Low Risk** | 1 – 3 | 6-12 months |
| **Moderate Risk** | 4 – 6 | 3-6 months |
| **High Risk** | 8 – 12 | 1 month |
| **Extreme Risk** | 15 – 25 | Immediate |

## 5. ASSURANCES

5.1 The trust will identify and implement appropriate controls to manage the risks identified. It will also implement processes to give assurance that these controls are working effectively. Divisional Risk Leads will attend the Risk Management Committee on a regular basis to confirm their approach to risk identification and risk management.

5.1.1 There are a number of internal and external assurance mechanisms that may be used to inform and reduce the level of risk exposure.  These include but are not limited to the following:

| **Internal examples** | **External examples** |
|---|---|
| Performance reports | Internal Audit |
| Management accounts | External Audit |
| Managing committees and functions:<br>• Health, Safety and Wellbeing<br>• Safeguarding<br>• Audit Committee<br>• Executive Management Team<br>• Risk Management Committee<br>• Quality Governance Committee | CQC reviews and ratings |
| | Monitor reviews and ratings |
| | CCG and NHSE/I reviews |
| | HMRC |

5.1.2 Once risk treatments have been implemented and embedded fully as control measures; the risk is rescored using the same matrix as originally used but considering these additional measures to calculate a new “current risk level” rating. The ‘current risk level’ should now be as low as reasonably practicable. A decision on whether further risk treatment is required will be dependent upon the risk score versus the risk appetite and risk tolerance.

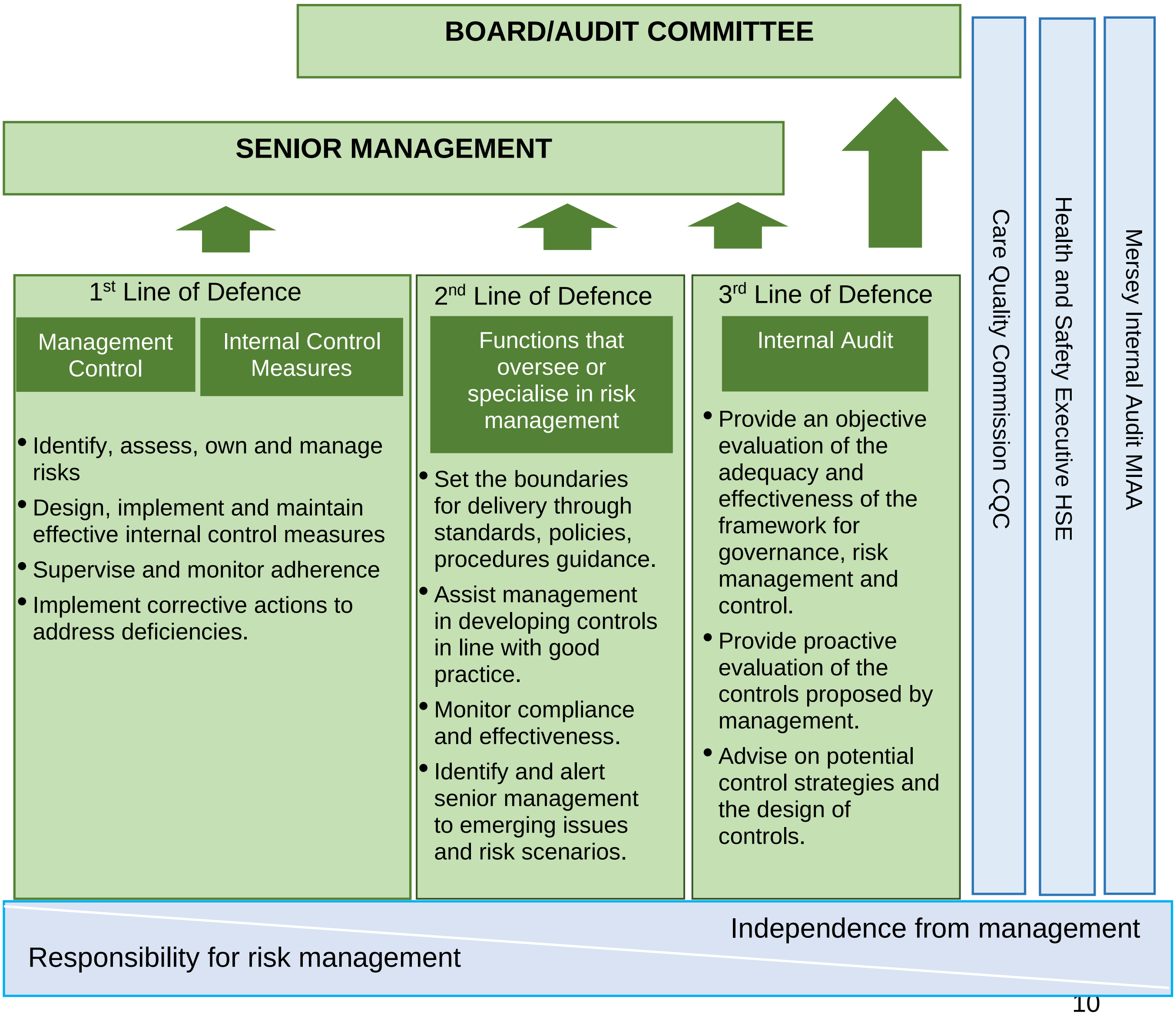
## 6. MONITORING AND REVIEWING RISKS

6.1 All risks should be given a review date based on their level of risk, but not normally greater than annually. It is important to note that progress against any actions to implement further control measures must be monitored.

6.1.1 The arrangements for monitoring the progress of actions relating to risk treatment should be recorded in the assurance section of the Datix risk record. Any identified gaps in assurances should also be recorded in the Datix risk record along with further treatment, if required, in the actions section to address the gaps in the assurances.

6.1.2 Heads of Operations/Associate Directors must ensure within their divisional/department that a process exists to review new risks and manage ongoing risks – this may be by establishing a local risk management group or by having risk management as a standing item for divisional/department management team meetings.

6.1.3 The Director of Corporate Affairs and Head of Risk will review Board risks and update the Board Assurance Framework every quarter.



**BOARD/AUDIT COMMITTEE**

**SENIOR MANAGEMENT**

1st Line of Defence

Management Control

Internal Control Measures

- Identify, assess, own and manage risks
- Design, implement and maintain effective internal control measures
- Supervise and monitor adherence
- Implement corrective actions to address deficiencies.

2nd Line of Defence

Functions that oversee or specialise in risk management

- Set the boundaries for delivery through standards, policies, procedures guidance.
- Assist management in developing controls in line with good practice.
- Monitor compliance and effectiveness.
- Identify and alert senior management to emerging issues and risk scenarios.

3rd Line of Defence

Internal Audit

- Provide an objective evaluation of the adequacy and effectiveness of the framework for governance, risk management and control.
- Provide proactive evaluation of the controls proposed by management.
- Advise on potential control strategies and the design of controls.

Care Quality Commission CQC

Health and Safety Executive HSE

Mersey Internal Audit MIAA

Independence from management

Responsibility for risk management

### 6.2 First Line of defence

Under the “first line of defence”, management have primary ownership, responsibility and accountability for identifying, assessing and managing risks. Their activities create and/or manage the risks that can facilitate or prevent the trust’s objectives from being achieved.

The first line ‘own’ the risks and are responsible for execution of the trust’s response to those risks through executing internal controls on a day-to-day basis and for implementing corrective actions to address deficiencies. Through a cascading responsibility structure, managers design, operate and improve processes, policies, procedures, activities, devices, practices, or other conditions and/or actions that maintain and/or modify risks and supervise effective execution. There should be adequate managerial and supervisory controls in place to ensure compliance and to highlight control breakdown, variations in or inadequate processes and unexpected events, supported by routine performance and compliance information.

### 6.3 Second line of defence

The second line of defence consists of functions and activities that monitor and facilitate the implementation of effective risk management practices and facilitate the reporting of adequate risk related information up and down the organisation. The second line should support management by bringing expertise, process excellence, and monitoring alongside the first line to help ensure that risk is effectively managed.

The second line should have a defined and proportionate approach to ensure requirements are applied effectively and appropriately. This would typically include compliance assessments or reviews carried out to determine that standards

In addition to professional standards, functional standards guide people working in and with the UK government. They exist to create a coherent and mutually understood way of doing business across organisational boundaries, and to provide a stable basis for assurance, risk management, and capability improvement. expectations, policy and/or regulatory considerations are being met in line with expectations across the organisation.

### 6.4 Third line of defence

Internal audits form the trust’s “third line of defence”. An independent internal audit function will, through a risk-based approach to its work, provide an objective evaluation of how effectively the trust assesses and manages its risks, including the design and operation of the “first and second lines of defence”. It should encompass all elements of the risk management framework and should include in its potential scope all risk and control activities. Internal audit may also provide assurance over the management of cross-organisational risks and support the sharing of good practice between organisations, subject to considering the privacy and confidentiality of information.

### 6.5 External assurance

Sitting outside of the trust’s own risk management framework and the three lines of defence, are a range of other sources of assurance that support the trust’s understanding and assessment of its management of risks and its operation of controls, including the Care Quality Commission and the Health and Safety Executive.

### 6.6 Coordination, cooperation and communication

The lines of defence have a common objective: to help the trust achieve its objectives with effective management of risks. They often deal with the same risk and control issues. The accounting officer and the board will clearly communicate their expectation that information be shared and activities co-ordinated across each of the 'lines' where this does not diminish the effectiveness or objectivity of any of those involved.

## 7. RECORDING OF RISKS

7.1 Risks are recorded on different forms across the trust relating to how they are identified. For example, on a risk assessment form or an audit report. The Risk Register exists to provide an integrated tool for recording strategic and divisional risks that may create uncertainty on meeting the trust's objectives, allowing effective monitoring and reporting of risk. However, not all risks need to be recorded on the Risk Register. Please see below for guidance:

a. Risks identified through a risk assessment tool should be recorded on the standard template and in accordance with the relevant policy/procedure, for example the Clinical Risk Policy, Fire Safety Policy or Health and Safety Risk Assessment Procedure. Where the risk is deemed to be high, i.e., scored 8 or over and have the potential to affect achievement of objectives, the risk should **also** then be recorded on the Datix Risk Register.

b. Risks identified through another source, i.e., inspection/audit, should be recorded on the appropriate form/template and in accordance with the relevant policy/procedure. For example, an audit would have an action plan. Where the risk is deemed to be high, i.e., scored 8 or over, and have the potential to affect achievement of objectives, the risk should be recorded onto the Datix Risk Register.

c. Clinical risks relating specifically to an individual patient or service user should be recorded within the patients care records only.

## 8 HUMAN RIGHTS ACT

Implications of the Human Rights Act have been taken into account in the formulation of this policy and they have, where appropriate, been fully reflected in its wording.

## 9 ACCESSIBILITY STATEMENT

This document can be made available in a range of alternative formats e.g., large print, Braille and audio cd. For more details, please contact the HR Department on 0194277(3766) or email equalityanddiversity@wwl.nhs.uk

**Appendix 1**

| | | |
|---|---|---|
| Risk Register Template | **Risk Title:** | |

| | |
|---|---|
| **Division:** | |
| **Div/Directorate:** | |
| **Speciality:** | |
| **Does this risk have an impact outside of the Division which it originated? Yes/No** | |
| **Date of Risk Assessment:** | |
| **Risk Lead:** | |

| **Step One: Risk Identification** |
|---|
| **Risk Statement:** *There is a risk that: (uncertain event) may happen, due to: (root cause) resulting in (impact on achieving objectives).* |
| **Supporting information:** *(Optional) Provide further supporting information about the risk cause and impact.* |

| | | |
|---|---|---|
| **Opportunity or Threat:** *Does the risk present an opportunity or threat to achieving the trust's objectives? Delete as appropriate*<br>Opportunity / Threat / Both | **Risk Type:** *Delete as appropriate. H&S risks scoring 6 and under should be recorded on the appropriate H&S form.*<br>Board Assurance Framework Risk / Corporate Risk | **Principal objective:** *Delete as appropriate*<br>Patient / People / Performance / Partnerships |
| **Local Reference:** (if applicable) | **Lead Committee / Subgroup:** | **Risk Category:** *Delete as appropriate*<br>Adverse Publicity / Contracts & Demand / Estates / Financial Duties / Governance/ Information / Performance Targets/ Quality of Services / Regulatory Standards / Staff Capacity & Capability / Staff Engagement / Strategy / Technology / Transformation |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Step Two: Risk Analysis** | | | | | | | |
| Current Risk Score: *Take into account controls and assurances already in place.* | | | | | | | |
| Likelihood: (1 to 5) | | **x** | Impact: (1 to 5) | | **=** | Risk Rating: (5 to 25) | |
| List existing controls:<br>● | | | | | | | |
| Gaps in existing controls:<br>● | | | | | | | |
| List existing assurances:<br>● | | | | | | | |
| Gaps in assurances:<br>● | | | | | | | |

## Step Three: Risk Evaluation

**Overall assurance level:** *Delete as appropriate*

Low / Medium / High

Risk Target / Appetite Score: *Risk target score that we are aiming for to achieve our objectives.*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Likelihood:<br>(1 to 5) | | **x** | Impact: (1 to 5) | | **=** | Risk Rating:<br>(5 to 25) | |

Risk Tolerance Score: *Risk target score that we are willing to accept given current constraints.*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Likelihood:<br>(1 to 5) | | **x** | Impact: (1 to 5) | | **=** | Risk Rating:<br>(5 to 25) | |

**Risk Treatment:** *Delete as appropriate*

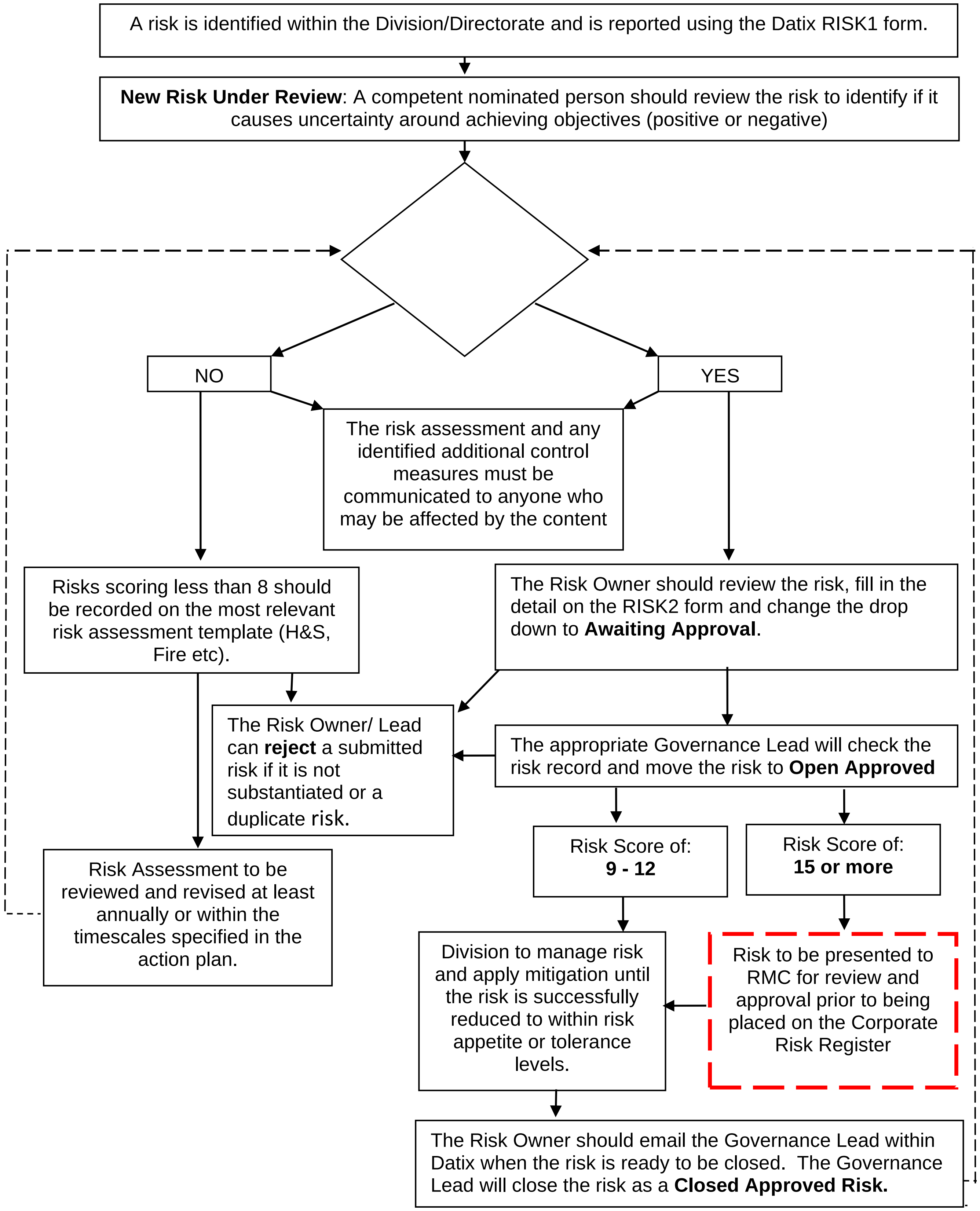
Take the opportunity / Terminate (stop the activity) / Tolerate (accept the risk) / Transfer / Treat (reduce the risk)

| **Step Four: Risk Treatment** | | | |
|---|---|---|---|
| Further actions required to address gaps in controls and assurances: | Nominated person for action: | Date action to be completed by: | Priority (High / Medium /Low) |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| **Step Five: Monitor and Review** | | | |
|---|---|---|---|
| **Date Risk Opened:** | | **Review Date:** *When was the risk reviewed?* | |
| **Next Risk Review:** *When is the risk due for its next review?* | | **Approval Status:** *Delete as appropriate* | New risk under review /<br>Awaiting approval /<br>Open Approved Risk /<br>Open Board Risk /<br>Closed Approved Risk /<br>Rejected |

## Appendix 2 Risk Management and Escalation Process

The flowchart below describes the process for managing and escalating a risk within the Division/ Directorate.



A risk is identified within the Division/Directorate and is reported using the Datix RISK1 form.

**New Risk Under Review**: A competent nominated person should review the risk to identify if it causes uncertainty around achieving objectives (positive or negative)

The risk assessment and any identified additional control measures must be communicated to anyone who may be affected by the content

Risks scoring less than 8 should be recorded on the most relevant risk assessment template (H&S, Fire etc).

The Risk Owner should review the risk, fill in the detail on the RISK2 form and change the drop down to **Awaiting Approval**.

The Risk Owner/ Lead can **reject** a submitted risk if it is not substantiated or a duplicate risk.

The appropriate Governance Lead will check the risk record and move the risk to **Open Approved**

Risk Assessment to be reviewed and revised at least annually or within the timescales specified in the action plan.

Risk Score of: **9 - 12**

Risk Score of: **15 or more**

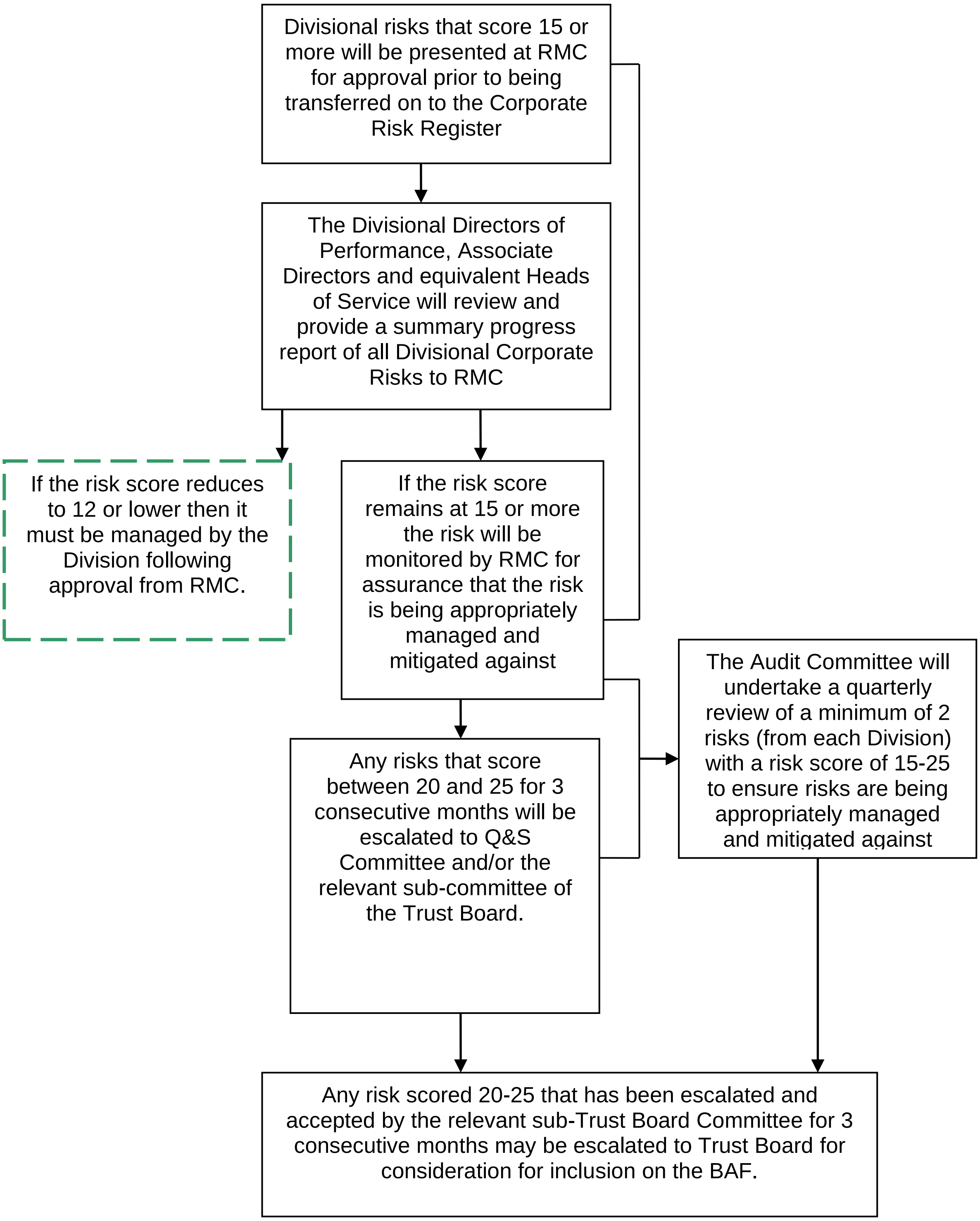
Division to manage risk and apply mitigation until the risk is successfully reduced to within risk appetite or tolerance levels.

Risk to be presented to RMC for review and approval prior to being placed on the Corporate Risk Register

The Risk Owner should email the Governance Lead within Datix when the risk is ready to be closed. The Governance Lead will close the risk as a **Closed Approved Risk.**

## Appendix 3 The Corporate Risk Management and Escalation Process

The flowchart below describes the process for managing and escalating risk within the organisation:



Divisional risks that score 15 or more will be presented at RMC for approval prior to being transferred on to the Corporate Risk Register

The Divisional Directors of Performance, Associate Directors and equivalent Heads of Service will review and provide a summary progress report of all Divisional Corporate Risks to RMC

If the risk score reduces to 12 or lower then it must be managed by the Division following approval from RMC.

If the risk score remains at 15 or more the risk will be monitored by RMC for assurance that the risk is being appropriately managed and mitigated against

The Audit Committee will undertake a quarterly review of a minimum of 2 risks (from each Division) with a risk score of 15-25 to ensure risks are being appropriately managed and mitigated against

Any risks that score between 20 and 25 for 3 consecutive months will be escalated to Q&S Committee and/or the relevant sub-committee of the Trust Board.

Any risk scored 20-25 that has been escalated and accepted by the relevant sub-Trust Board Committee for 3 consecutive months may be escalated to Trust Board for consideration for inclusion on the BAF.