Avon and Wiltshire NHS
Mental Health Partnership NHS Trust

Risk Management Policy

Board library reference	Document author	Assured by	Review cycle
P136	Head of Risk and Legal Services	Audit and Risk Committee	3 Years

This document is version controlled. The master copy is on Ourspace.

Once printed, this document could become out of date.

Check Ourspace for the latest version.

Contents

1. Introduction

Risk Management is the proactive identification, classification and control of issues that may affect the Trust's delivery of its objectives it is an integral part of management. Whilst Trust Board accepts that not all risks can be eliminated, it is committed to reducing its risks to an acceptable level wherever possible.

This policy sets out how the Trust will deliver Risk Management across the organisation. It sets out who does what and when.

2. Purpose or aim

This policy sets out the Trust's expectations for the management of risks to its objectives.

3. Scope

This policy covers management risks (risks to team and business objectives) and is not intended to cover clinical risks (risks specific to individual service users should not be recorded on risk registers which may be publically available). Further information on clinical risk assessment can be found on Ourspace

Management risks may impact upon service users, e.g. staff shortages but these risks are not specific to individual service users.

The policy applies to all internal staff of the Trust and, in particular, those who own a risk register.

4. Definitions

Risk	An uncertain event or set of events which, should it occur, will have an impact upon the achievement of objectives.
Risk Register	A record of the more serious (usually the highest scoring) risks within an area. In order to ensure focus on the most serious risks, risk registers should be proportionate and not an exhaustive list of all risks in an area.
Service	Usually a collection of teams operating as a group with a head of service, e.g. inpatients, community.
Team	A team may be a ward, clinic, department, service or hospital depending on the structure established within a locality.
Risk Owner	The team manager or director who is responsible for managing the risk. See Section 7.1.
Risk Assessor	The member of staff who is responsible for assessing the risk. This may not be the risk owner. A separate risk assessment policy is available here.
Risk Assessment	The evaluation of risk with regard to the severity and the likelihood of the risk event occurring.
Likelihood	Likelihood (or probability) is the chance of a risk materialising. Likelihood can range from rare to almost certain.
Severity	The extent of harm that would be caused should the risk materialise. This may range from minor to catastrophic. May also be known as the hazard.

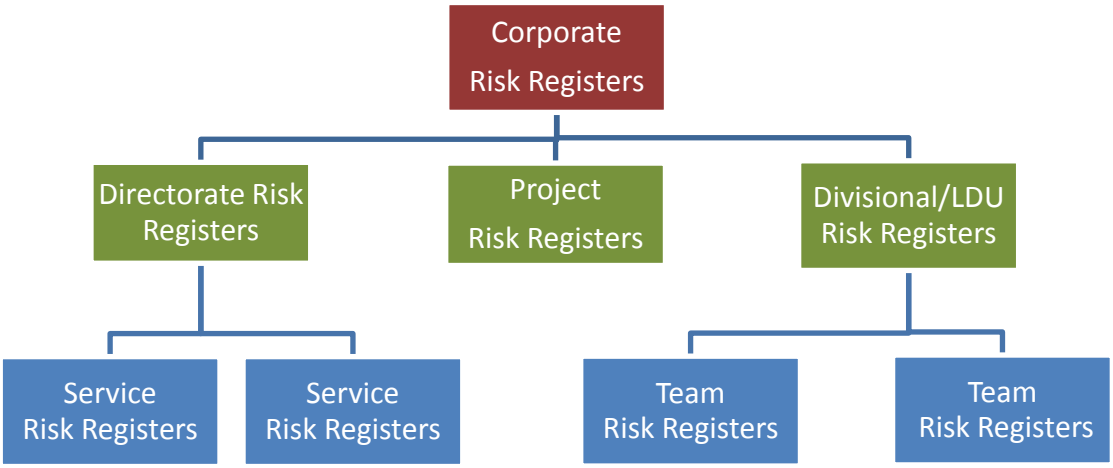
Controls	The mechanisms already in place to reduce the risk. For example policies, training, physical barriers. When actions are complete they may become then controls
Risk Mitigation	The action that can be taken to reduce the likelihood or severity of a risk.
Actions	What steps you will take to reduce or eliminate the risk.
Closed (risk)	If a risk has been eliminated entirely then it will be considered closed. Where a risk remains but all practical control measures are in place and the target risk score has been reached, this will be considered an accepted risk.
Accepted (risk)	Risks will only be deemed accepted if they meet the criteria of an accepted risk Red risks will not be accepted (see Section 9.3).
Escalation	The reporting of a risk to a manager or a management group at the next level of the management structure, e.g. team manager to operations manager/clinical lead, operations manager/clinical lead to Associate/clinical director, to the Executive Team. Ownership of the risk does not transfer upwards.
Risk Appetite	Describes the Trust's approach to risk management and appetite for taking risks as set out by Trust Board; it is a statement of intent from the organisation about the level of risk it is prepared to accept, tolerate, or be exposed to at any point in time.
Risk Management	All the processes involved in identifying, assessing, and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress.

5. Risk Registers

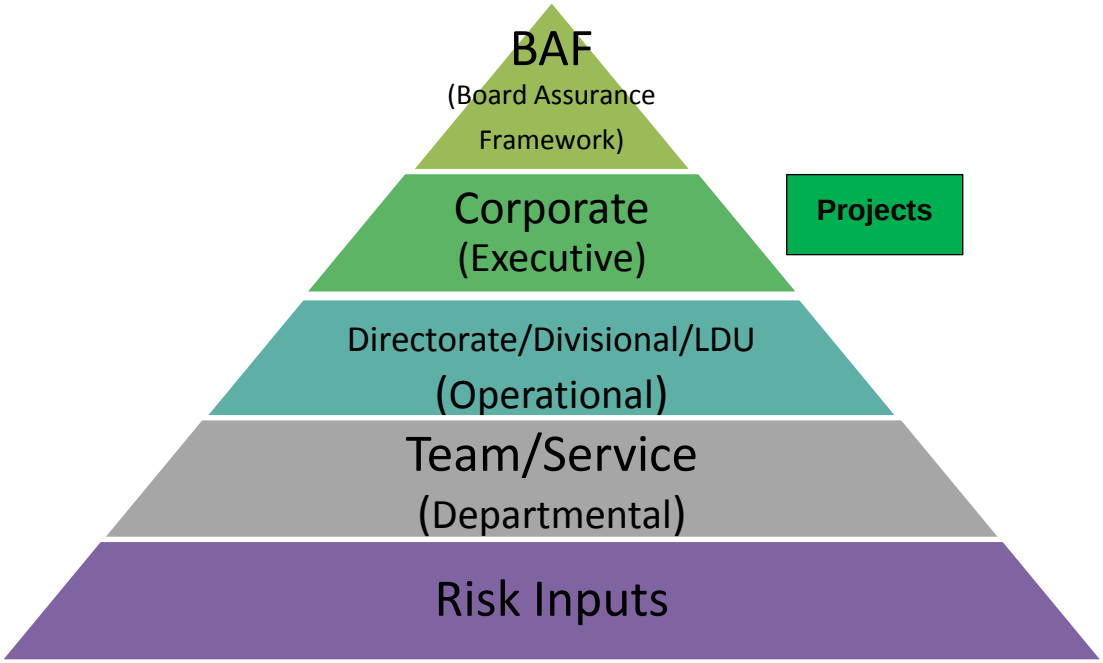
The Trust has one single risk register contained in RiskWeb. LDU and Directorate senior managers have agreed which of their teams require a risk register which are accessible via Ourspace This can be 'sliced' in different ways.

A User Guide for adding risks to RiskWeb is available on Ourspace here.

Each risk in RiskWeb will be assigned a risk level as shown below and follow these reporting lines:



The hierarchy of the risk register is shown below.



5.1 Minimum content of risk registers

Risk Registers will contain the following minimum dataset:

Date identified	When the risk was first identified
Risk description	"If [this event happens] then [this will be the consequence]" e.g. If we do not reduce our agency spend then the departmental budget will be in deficit.
Risk Owner	The owner of the risk will be the manager that owns the objective to which the risk relates to e.g. a risk of a financial deficit at year end will be owned by the manager responsible for balancing the budget.
Strategic Priority	Which strategic priority might the risk impact upon?
Current Score	What the risk is scored at now.
Controls	What processes do you have in place to control the risk e.g training, policy. Only include controls already in place. A plan is not a control.
Target Score	The score at which we would 'accept' the risk. A target risk score should be assigned to the risk which should be realistic.
Actions	Planned actions to further reduce the risk, see Section 8. Once complete, actions become controls.

In addition each risk should be reviewed regularly and all controls and progress noted. Risks are tagged with information on which management group or committee has oversight of the risk and which has ownership (where appropriate).

5.2 Corporate risk registers

The Corporate Risk Register contain risks to Trust objectives and each is owned by an Executive Director it comprises of three elements representing the Delivery Executive (Operations), the Clinical Executive (Medical and Nursing) and the Business Executive (Finance, HR etc.)

5.3 Directorate and Divisional/LDU risk registers

Directorate (non-operational directorates) and Divisional risk registers feed into the executive risk registers that are defined by where they fall within the Trust.

These will be reviewed through directorate/Divisional meetings and informed by both operational and governance related issues.

Each Locality (LDU) in the Trust must have a risk register setting out how they will control any risks to achieving their objectives. As a minimum each locality will have a risk register for each major service they operate. Locality (LDU) risk registers feed into the Divisional risk registers.

5.4 Team/Service risk registers

Whilst a degree of flexibility is afforded to locality management to on how they define their teams, every team in the Trust that has objectives should have a risk register setting out how they will control any risks to achieving those objectives.

5.5 Project risk registers

Project risk registers are developed to help manage the risks associated with approved projects or initiatives. Project risk registers will have an executive lead and risks will be escalated to the executive's risk register, this would be the responsibility of the Programme Management Office lead.

6. How risks will be managed

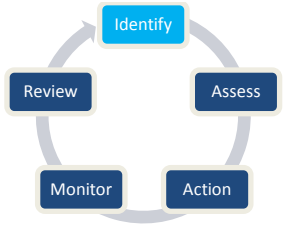
Figure 1 – Process for Managing Risk

Risk is managed through 5 key steps (see from Section 7 onwards):

- **Identification**: the initial task of acknowledging a risk in any particular area.
- **Assessment**: the proactive process of evaluation the risk and its impact and likelihood.
- **Action**: implement controls to mitigate the risk to potentially reduce the likelihood or severity of the risk event.

- **Monitoring**: to check risks are being reviewed regularly and that actions are being taken, that risk scores are being updated and progress notes are made.
- **Review**: to continually, and regularly, check the risk and associated controls to ensure the risk remains mitigated. This feeds back into the start of the cycle where unresolved or unexpected risks are identified and managed.

7. Risk Identification



7.1 Who can identify risks?

All staff can identify risks. Where staff are unable to eliminate the risk they should report it to their line manager. The responsibility for managing and recording those risks will lie with the manager of the of the team/service; and they are known as the “owner”

7.2 How to identify risks

Staff will identify risks proactively through:

- Proactive risk assessment - see the Risk Assessment Policy
- Incident reporting
- Review of complaints themes
- Business planning processes
- Project initiation
- External impacts, e.g. changes in the funding environment
- Line management reporting

This list is not intended to be exhaustive.

7.3 How to record a risk

Localities (LDUs) and support service departments will identify and report risks on RiskWeb. Actions will be identified and monitored through RiskWeb with a view of reducing the risk and achieving the targeted mitigated risk level. Guidance for using RiskWeb can be found on Ourspace and training is also available.

7.4 How to describe a risk

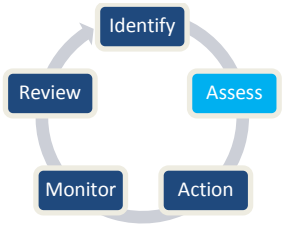
All risks are about potential future events. Therefore, it is useful to consider risk as an if/then sentence construction.

If… [this event occurs] then…[this will be the consequence]

e.g.

If *we do not reduce our agency spend* ***then*** *the departmental budget will be in deficit*

8. *If our estate is not maintained in safe condition then service users, staff and visitors experience will decline.*Assessing the risk



8.1 Policy statements

The Trust will assess all types of management risk using the same methodology.

Risks can be assessed by anyone in the Trust.

It is the responsibility of the manager to approve the risk assessment and to determine whether the risk should be entered on the team risk register.

Risk assessors will assess both the potential harm (severity) should a risk materialise and the likelihood of that harm occurring (likelihood).

8.2 Who owns the risk?

The owner of a risk is the person responsible for delivering the objective to which the risk relates. Risk ownership cannot be transferred from the owner of the objective that the risk relates to.

Actions taken to mitigate a risk may be delegated, but the ownership of the overall risk will remain with the person responsible for the objective.

Risk posed to a…	**Who owns the risk**
Trust objective	Executive Director
DIVISONAL/Locality/Directorate objective	Clinical Director (DIVISIONALs), Associate Director of Operations (DIVISIONAL), Operations Manager (LDU) or Clinical Lead (LDU), Head of Directorate (Directorate)
Service objective	Head of Service/Service manager/Modern Matron
Team objective	Team manager (e.g. ward manager)

8.3 Severity

Risk scoring is not an exact science, but should, wherever possible, be supported by evidence e.g. incident data, to make the assessment as objective as possible.

The **severity** of the possible outcome of a risk is assessed on a five point scale.

Tables for scoring risks within the 5 point scale in relation to specific risks is given in Appendix 1.

The risk assessor should select the most appropriate heading and look at the definitions to determine the most appropriate score, i.e. select finance, impact on the safety of patients, staff or public (physical/psychological harm) etc.

N.B. This table is not intended to be exhaustive. Risk assessment is subjective and staff should not feel constrained by the definitions set out in the table.

8.4 Likelihood

Assessors should assess the likelihood of the event occurring.

For example, if an assessor rates the severity of a service user sustaining a fracture after a fall as a 4 (Major), it should be the likelihood of the fracture occurring that is assessed, not the likelihood of service users falling.

Appendix 1 provides a guide to decision making on likelihood.

8.5 Risk scoring

As a means of prioritising risks, the Trust has adopted the 5 x 5 scoring matrix as the means by which it will score risks based on the New Zealand/Australian model.

Severity (5) x Likelihood (5) = Risk score (25) All risks will be scored using the same 5 x 5 system and one matrix (see below).

[1] AS/NZS 4360 *Risk management (August 2015)*

Trust Board has set out its risk appetite in this policy and annual statement of risk appetite (see section 8.6 and 8.7).

The grading of risks will prompt the following actions:

- **Recording** – All yellow, amber and red risks will be recorded on a Risk Register (team, service, and locality, executive).
- **Accepting** – Whether a risk can be deemed accepted (see Section 9.3) will depend on risk grading. Red risks will never be 'accepted' by the Trust, yellow and amber risks may be accepted in the circumstances set out in Section 9.3.
- **Reporting** – Where a risk has been graded 12, this should be reported upwards, e.g. from a team manager to a service manager/ locality management, from locality management to the Divisional /executive. Any risks graded 12 or more will be considered for escalation. It should be noted that at each point of escalation the risk may also be downgraded. See examples in 8.8.
- **Review** – Red risks will be reviewed at least monthly (see section 11.2).

The current Risk Matrix is shown below (also refer to Appendix 1).

		Severity/Consequence				
		Negligible 1	**Minor 2**	**Moderate 3**	**Major 4**	**Catastrophic 5**
Likelihood / Probability of Recurrence	**Almost certain 5**	**5 Low**	**10 High**	**15 High**	**20 Extreme**	**25 Extreme**
	Likely 4	**4 Low**	**8 High**	**12 High**	**16 Extreme**	**20 Extreme**
	Possible 3	**3 Very low**	**6 Low**	**9 High**	**12 High**	**15 Extreme**
	Unlikely 2	**2 Very low**	**4 Low**	**6 Low**	8 **High**	**10 High**

	Rare 1	1 Very low	2 Very low	3 Very low	4 Low	5 High

8.6 Current Risk Appetite

The Board regularly reviews and approves its position on risk appetite. The appetite sets out the level of risk that the Trust is willing to accept. Managers throughout the Trust are expected to use this to guide their decision making.

The Trust's current overall risk appetite is defined as CAUTIOUS.

We are willing to accept some new low risks, while maintaining an overall preference for safe delivery options despite the probability of these having mostly restricted potential for reward/return.

8.7 Risk Appetite Statement

The risk appetite of the Trust is the decision on the appropriate exposure to risk it will accept in order to deliver its strategic objectives.

On an annual basis the Trust will publish its risk appetite statement as a separate document covering the overarching areas of:

- Risk to patients
- Financial risk
- Quality
- Organisational risk
- Reputational risk
- Opportunistic risk

The statement will also define the Board's appetite for each risk identified to the achievement of strategic objectives (those contained in the BAF) for the financial year in question.

Risks throughout the organisation should be managed within the Trust's risk appetite, or where this is exceeded, action taken to reduce the risk.

The Board determined that the Trust's risk appetite line is set at 12. Any risks rated at LDU/ Divisional level, at or above this level are reported to the relevant Board Sub-Committee and the Board on a quarterly basis. A risk score of 12 or above should therefore be treated as a trigger for a discussion as to whether the Trust is willing to accept this level of risk. These risks will also be reviewed monthly by the Executive Team.

A target risk rating should be set for all risks. This target (residual) risk rating is a means of expressing a target for the lowest acceptable (tolerated) level for that risk. When setting residual risk ratings, risk leads should consider what level of tolerated risk they are willing to retain. For some risks, the residual risk rating could be high, especially where the consequences are potentially severe or some elements of the risk lie outside the direct control of the Trust.

The Board will review the position on risk appetite at least annually against the new Trust strategic objectives and will produce an annual statement of risk appetite.

8.8 Upward Reporting (escalating risks)

Reporting risks

Risks are scored so that they can be prioritised for action. Risk management should be proportionate to the level of risk and the Trust will focus most resources on addressing red risks, followed by amber risks, then yellow and green risks.

Green risks	Yellow risks	Amber risks	Red risks
Manage locally. No requirement to add to risk register	Add to the risk register	Add to risk register.	Add to risk register. Report to head of service or locality management

The ownership (responsibility) for a risk cannot be transferred (upwards/downwards or sideways) unless the objective to which the risk relates is also transferred.

Risks are not simply escalated up to the next level. Risks have to be accepted up and this does not mean that the original risk has moved or there is no need to manage it locally. Escalation is about informing the organisation and mobilising additional resources to mitigate the risk, particularly where the local resources are insufficient.

At team level, team managers should assess a risk to a team objective. Equally, locality risks should be assessed according to locality objectives and divisional risks according to divisional objectives etc.

Where a team risk has arisen that the risk owner is concerned might impact on a service objective, they will report it to the Service Manager. The risk will not be transferred upwards, instead the Service Manager will raise their own risk to their objective that may be scored differently and have different actions also considering other similar risks within the locality (thematic risks).

Any risk that transfers/escalates to the next level the owner needs to inform the Risk Management team so that that it can be link and thus reported against

Example 1

A risk of a team receiving a financial fine of £50k (4% of budget) may have a significant impact on the team's budget and may be rated red. This is then reported to the service manager. The service manager reviews that risk but decides that, as her other two teams are showing a surplus this risk won't impact upon her own objective for the service to deliver a surplus at year end. She therefore decides not to add a new risk to her risk register.

Example 2

Ward A, on doing a routine environmental assessment, identifies a tree that could prove a significant ligature risk. This risk is rated red and reported to the Service Manager. The service manager is concerned about this risk and has had reports from other wards about trees. As these risks threaten a service objective to keep service users safe, the service manager adds his own risk to the service risk register on the potential failures in the ligature assessment processes in the service.

The same risk may be a red at ward level, amber at locality level and yellow or green at Executive-level:

we will overspend by £50,000 at year end.	*Added to team risk register. Reported to Locality Manager.*	
If we are unable to restrict the use of FP10 pads then we will overspend by £50,000 at year end.	Locality Level (with a budget of (£6m p.a.) *Risk reviewed. No impact on locality objective to deliver a surplus. Not added to locality risk register. Not reported to the Executive. Remains a red risk on the team risk register.*	6
If we are unable to restrict the use of FP10 pads then we will overspend by £50,000 at year end.	Executive level (with a budget of £145m p.a.) *Not reported to the Executive. Not added to Executive Risk Register (unless this also occurred elsewhere and the cumulative effect became significant).*	4

The Trust may have risks that are rated 'red' on team risks registers that may not appear on Locality/Divisional or Directorate Registers.

Directors and Service Managers/Modern Matrons having reviewed the operational risk registers that sit within their services will identify risks that are to be escalated to the Corporate Risk Register. Escalation to the Corporate Risk Register will be based on the following criteria:

- the risk scores is equal to or higher than 12 or
- Directors or Service Managers/Modern Matrons have reported a thematic risk having identified a number of similar risks across the organisation e.g. workforce.

Directors can add corporate risks directly to the Corporate Risk Register even if the risk has not been reported on the operational risk register e.g. reduced number of trainee nurses going through university.

Directors are also responsible for rejecting any risks that are not deemed to be a corporate risk.

9. Take action

The following steps may be taken once a risk has been assessed.

- Stop the activity immediately
- Take action to reduce the risk
- Accept the risk

9.1 Stop the activity

The best way to prevent risks impacting upon our objectives is to stop the activity that gives rise to the risk. Where this is possible without impact upon the objectives of the Trust, this should be done as a first line of defence.

9.2 Take action

If it is not possible to stop the activity then action should be taken to mitigate the risk as far as is reasonably practical and cost-effective.

The law requires us to take all actions that are 'reasonably practicable' taking into account the potential severity of the outcome, the likelihood this will occur and our knowledge about ways of eliminating or minimising that risk.

Whilst risks should be owned by the manager responsible for the delivery of the objective to which the risk relates, the manager may delegate actions to another member of staff with their agreement.

Actions should be SMART (specific, measureable, achievable, realistic and time-bound) and should have a clear impact on the risk.

Once actions have been complete, they become controls, e.g. a plan to introduce a new training programme. Once the training is in place, this will become a control.

9.3 Accept the risk

The Trust Board accepts that not all risks to its objectives can be eliminated. However, where possible, it is committed to reducing risk to an acceptable level.

Risks can be accepted in the following circumstances:

- Risks rated 'red' will never be accepted. Red risks will be reviewed at least monthly.
- Risks rated 'amber' will only be accepted if the potential benefits in taking the risk significantly outweigh the risk.
- Risks rated 'green or yellow' can be accepted if they cannot be eliminated.

Risk owners are accountable for 'accepted' risks within their risk registers.

Accepted risks will be review at least annually to ensure controls remain effective.

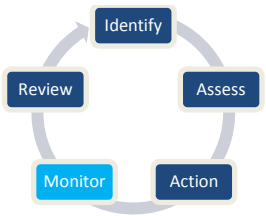
Risk owners are responsible for deciding that a risk can be accepted following the principles set out above.

9.4 Closing a risk

Risks will only be closed if the risk has been eliminated entirely.

More commonly, risks will not be eliminated entirely but the potential impact of the risk is mitigated to an acceptable level (see Section 9.3). These risks should not be closed on risk registers but instead marked as 'Accepted'.

10. Reporting and Monitoring



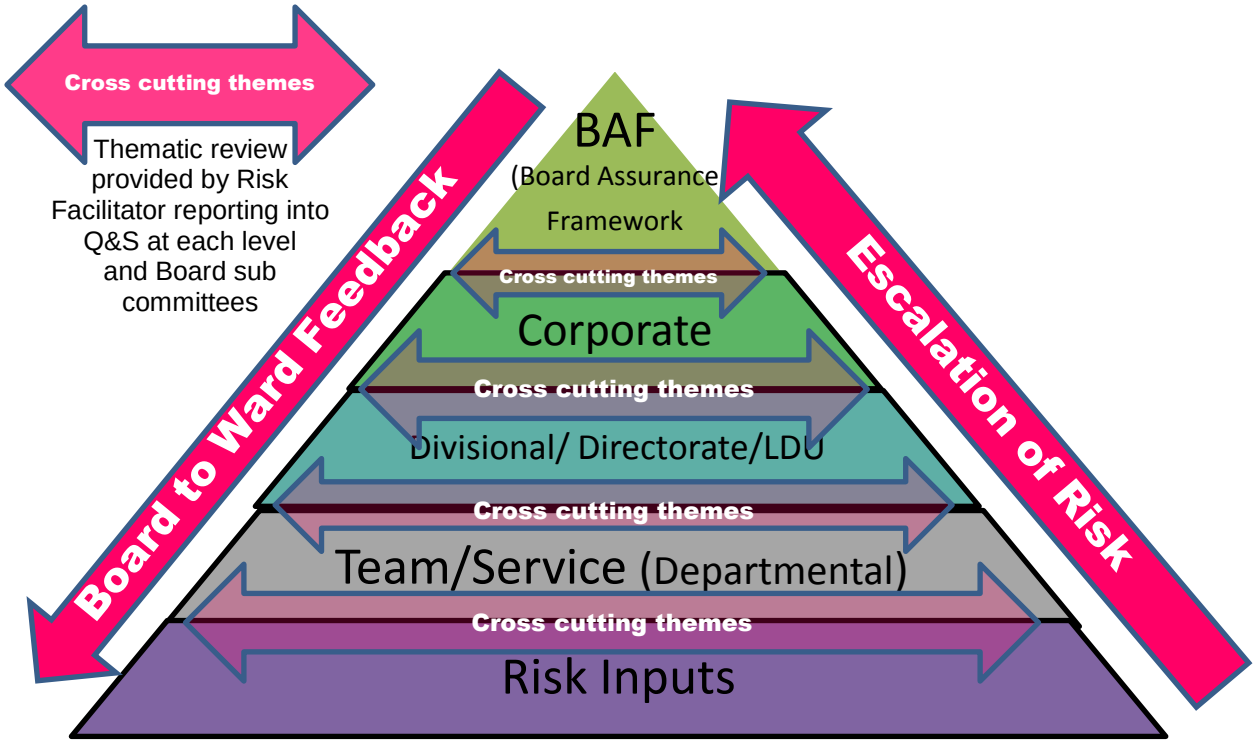
10.1 Monitoring Risks

This section describes the monthly process for reporting the operational and Corporate Risk Registers and the reporting of strategic risk reporting on the Board Assurance Framework (BAF). Table 1 presents a flow chart of how risk will be managed and reported.

10.2 Operational Risk

It is expected that the Director/Head of Service will monitor the operational risks that have been identified by their services to ensure that actions are happening to reduce the risk and also to consider whether any of their risks should be considered as a thematic risk and if similar risks are happening elsewhere in their services or the rest of the organisation.

Operational risks will be monitored through the normal performance management processes of the organisation, such as LDU Locality Group meetings and Operations Delivery Group meetings. The operational risk registers will be periodically reviewed by the Audit and Risk committee (A&R) and Quality and Standards committee (Q&S) as part of their deep dive assurance work (see diagram below).



10.3 Corporate Risk

Directors will be responsible for monitoring and reporting of all corporate risks.

The Risk Facilitator will be responsible for gatekeeping and quality checking new risks and ensuring that all risks are meeting expected standards and that actions are SMART.

Sub-committees of the Board will be responsible for monitoring the risks that relate to the sub-committee responsibilities. The Audit and Risk committee will have the responsibility for monitoring the Corporate Risk Register.

Corporate risks that impact on the strategic objectives may be raised for inclusion on the Board Assurance Framework (BAF).

In monitoring and reporting the Corporate Risk Register, Directors will establish whether any of the corporate risks could potentially affect the delivery of the Trust's strategic objectives if not mitigated. These would be recommended to the Board for inclusion on the Board Assurance Framework. Directors can also identify risks with strategic importance that do not originate from

the operational or Corporate Risk Registers if the risk in question is deemed to affect the Trust's ability to deliver its objectives.

The Board Assurance Framework describes the strategic objectives of the organisation and identifies the controls and assurance mechanisms that the Board will use to ensure that the strategic objectives are on course to be delivered. The reporting of strategic risks against the Board Assurance Framework will enable the Board to assess the impact of these risks on the strategic objectives and what additional actions and processes are required to ensure that the strategic risks are mitigated.

The Audit and Risk Committee will be responsible for reviewing the contents and controls of the Board Assurance Framework and providing assurance to the Board that the Board Assurance Framework is being managed appropriately.

New risks that are being recommended for inclusion on the Board Assurance Framework will be discussed at either the Audit and Risk Committee and/or Board.

10.4 Monthly timetable for reporting risk

The operational risk register will be updated as and when a risk has been identified or actions have been undertaken which reduce the status of the risk.

At the end of the first week of the month Directors and Heads of Service will be required to review their department's risks and identify any risks that need to be escalated to the Corporate Risk Register.

By the end of the second week of the month the Corporate Risk Register will have been reviewed and updated by the executive team in readiness for reporting to the Audit and Risk Committee and/or the Board. This review will identify any strategic risks that would affect the delivery of the strategic objectives

The Company Secretary will be responsible for adding any new strategic risks to the BAF or amending any previous risks following the executive review of the corporate and strategic risks. The Board Assurance Framework will be reported to the Audit and Risk Committee and the Board as per the committee and Board timetable.

10.5 Review of risk registers

Risk Register	Where reviewed	Frequency of review
Corporate	Trust Board	Quarterly
Corporate	Executive Team	At least eight times a year
Directorate/ Divisional Operational (LDU)	Directors Team Divisional /LDU meetings A&R Committee	At least eight times a year At least eight times a year One per meeting
Departmental (Team/service)	Team/service meetings	Monthly

The Head of Risk and Legal Services will keep risk registers under continual review via the RiskWeb system and issue reminders to risk owners to update their registers.

10.6 Trust Board review

The Director of Nursing and Quality will present a report to Trust Board summarising the Corporate Risk Register at least four times a year

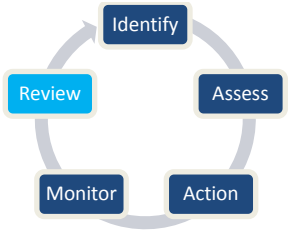
This report will contain, as a minimum:

- The top three risks (by score) on the Corporate Risk Register
- Any new risk added to the Corporate Risk Register
- All risks graded 'red' on the Corporate Risk Register
- Any significant changes (change of risk status, change of score) to risks contained in the Corporate Risk Register.

10.7 Locality risk registers

The Locality Risk Registers will be reviewed in full at the LDU Locality Group meetings and across the Operations Directorate at the Operations Delivery Group meeting.

11. Review



11.1 Purpose for reviewing of risks

Risks on the risk register are not a static record but need to be kept live and updated with progress, action and any changes in the risk. Completed actions may become controls. Each risk owner should review their risks periodically. The more significant the risk, the greater the scrutiny it should be subjected to and therefore should be reviewed frequently.

11.2 How frequently will risks be reviewed?

The following is a guide of how often risks should be reviewed by risk owners:

Green	At least annually
Yellow	At least six monthly
Amber	At least quarterly
Red	At least monthly

11.3 Accepted risks

Accepted risks will be reviewed at least annually to ensure controls remain effective but more often if these are not green rated risks. However if there is any change in the risk or the control then the risk should be reviewed at that point to determine if the risk control remains effective or if the risk has become unacceptable.

11.4 Unforeseen risks

An unforeseen risk may be created as a consequence of another risk treatment, and therefore may need to be treated as a risk in its own right with its own controls. In reviewing a risk it is important to determine if any risks have been created in treating the original risk.

11.5 Robustness of control

This is the responsibility of the "owner" of the risk; team manager (e.g. ward manager), the Quality Lead/Operations Manager and Associate/Clinical Directors and the Executive directors to ensure that the risk is updated with progress and actions/controls that are in place to manage the risk are effective and efficient. It is only then that the risk can either be "Accepted" or "Closed".

12. Audit

Internal Audit will undertake an audit on compliance with this policy at least once every two years.

The Audit and Risk Committee assures Trust Board as to the integrity and efficiency of the management of risk. To fulfil this function, the committee will receive a report from the Risk Facilitator on the Corporate Risk Register and Board Assurance Framework at least four times a year. It will review in detail one LDU risk register at each meeting and will receive the Internal Audit report on risk management.

13. Roles and Responsibilities

The responsibilities of the Trust Board, its Committees, second management groups, are the responsibility of the Director of Nursing & Quality as the lead Executive Director for risk. The Director of Nursing and Quality is responsible for preparing reports on risk for the Trust Board and its committees (including the Audit and Risk Committee).

13.1 Executive Team

The Executive Team will review new corporate risks at every meeting and the Corporate Risk Register monthly.

13.2 Executive Directors, Clinical Directors, Associate Directors, Quality Leads, Heads of Service Operations Managers and Team Managers

All managers are responsible for identifying, communicating, and managing the risks to their objectives in accordance with this policy.

13.3 Head of Risk Management and Legal Services

The Head Risk Management and Legal Services is responsible for the day to day management of the Corporate Risk Register and providing support to users of the system. He/she is also responsible for providing support to the Director of Nursing and Quality in providing reports on risk management.

13.4 Risk Management Facilitator

The Risk Management Facilitator will provide support to the Head of Risk and Legal Services on all risk matters.

13.5 All Employees and Contractors

All employees and contractors are expected to act in accordance with the Trust's approach to risk management, take a risk management approach to their own work, and take responsibility for the management of the risks they own.

14. Training

The Trust requires that risk management training should be mandatory requirement for all managers, as a commitment to Trust positive appetite to risk. This will be provided through six risk management-training sessions for managers every year plus ad-hoc training will be provided by the Risk Management Team on the use of the RiskWeb system for compiling risk registers

The risk team delivers specialised training in relation to risk management in a health and safety context. Please contact the Risk Facilitator for more information.

14.1 Learning and development

The Learning and Development department will maintain records of risk management training and follow up non-attendees to assure there is consistent attendance where needed.

Information on all training available can be accessed via the Learning and Development team.

15. Associated Policies and Strategies

The policy also directly relates to the policies below:

- Incident Policy
- Risk Assessment Policy
- Claims Handling Policy
- Being Open policy
- Whistleblowing Policy

16. References

This policy has been informed by:

- HM Treasury's Orange Book
- NHS Resolution
- The Healthy NHS Board: Principles for Good Governance

17. Appendices

Appendix 1 – Risk Scoring Tables

Version History

Version	Date	Revision description	Editor	Status
1.0	13 February 2014	Creation of new policy in draft to replace Risk Management Strategy Policy and comply with Trust policy requirements. Approved by Audit and Risk Committee.	Corporate Governance and Risk Manager	Approved
1.1	21 April 2015	Extension to review date approved by Audit and Risk Committee to 30 August 2015	Head of Corporate Governance	Approved
1.2	12 February 2016	Policy expiry extended by Audit and Risk Committee	Head of Corporate Governance	Approved
1.3	6 April 2016	Comprehensive re-write to support the new Risk Management Strategy	Head of Risk and Legal Services	Draft
2.0	15 April 2016	Comments incorporated. Revised policy approved at the Audit and Risk Committee	Head of Risk and Legal Services	Approved
3.0	27 Sept 2017	Approved by the Trust Board	Head of Health, Safety and Risk	Approved
3.1	26 Oct 2017	Administrative revisions to risk diagrams and charts	Head of Health, Safety and Risk	Approved
4.0	11 Dec 2018	Administrative revisions in line with the Trust re-organization and a requirement that risk management training becomes mandatory for line managers	Risk Facilitator/ Head of Risk and Legal Services	Approved
4.1	8 March 2019	Administrative revisions in line with the Trust re-organization	Head of Risk and Legal Services	Approved by audit & Risk committee March