Risk Management Operational Procedure

Title: Risk Management Operational Procedure			
Date effective from:	05/04/2023	**Review date:**	05/04/2026
Approved by:	NHS Lothian Board		
Approval Date:	05/04/2023		
Author/s:	Quality & Safety Assurance Lead		
Policy Owner:	Associate Director for Quality Improvement & Safety		
Executive Lead:	NHS Lothian Medical Director		
Target Audience:	Managers / All NHSL Staff		
Supersedes:	Risk Management Operational Procedure v2.0 (June 2018)		
Keywords (min. 5):	Risk, Risk Management, Residual Risk, Governance, Register		

Version Control

Date	Author	Version/Page	Reason for change
June 2012	Associate Director of Quality & Safety	1.0	
May 2018	Quality & Safety Assurance Lead	1.1	Under review
June 2018	Quality & Safety Assurance Lead	2.0	Review Approved
December 2022	Quality & Safety Assurance Lead	2.6	Under review
April 2023	Quality & Safety Assurance Lead	3.0	Review Approved

Contents

1. **Executive Summary 3**
2. **Who is responsible for managing risk? 4**
3. **The Risk Register Hierarchy..... 5**
4. **Risk Register Process..... 7**
5. **Training & Support..... 15**
6. **Governance and Reporting Arrangements 15**
7. **Review of Procedure..... 16**

1. Executive Summary

1.1 This procedure has been prepared to support the implementation of the NHS Lothian Risk Management Policy, and ensure consistency of approach in risk management.

1.2 **Risk** is uncertainty of outcome, whether positive opportunity or negative threat, of actions and events. It is the combination of the likelihood and impact of the risk materialising.

1.3 Risk should always be related to some objective or purpose. A statement of risk should always contain:

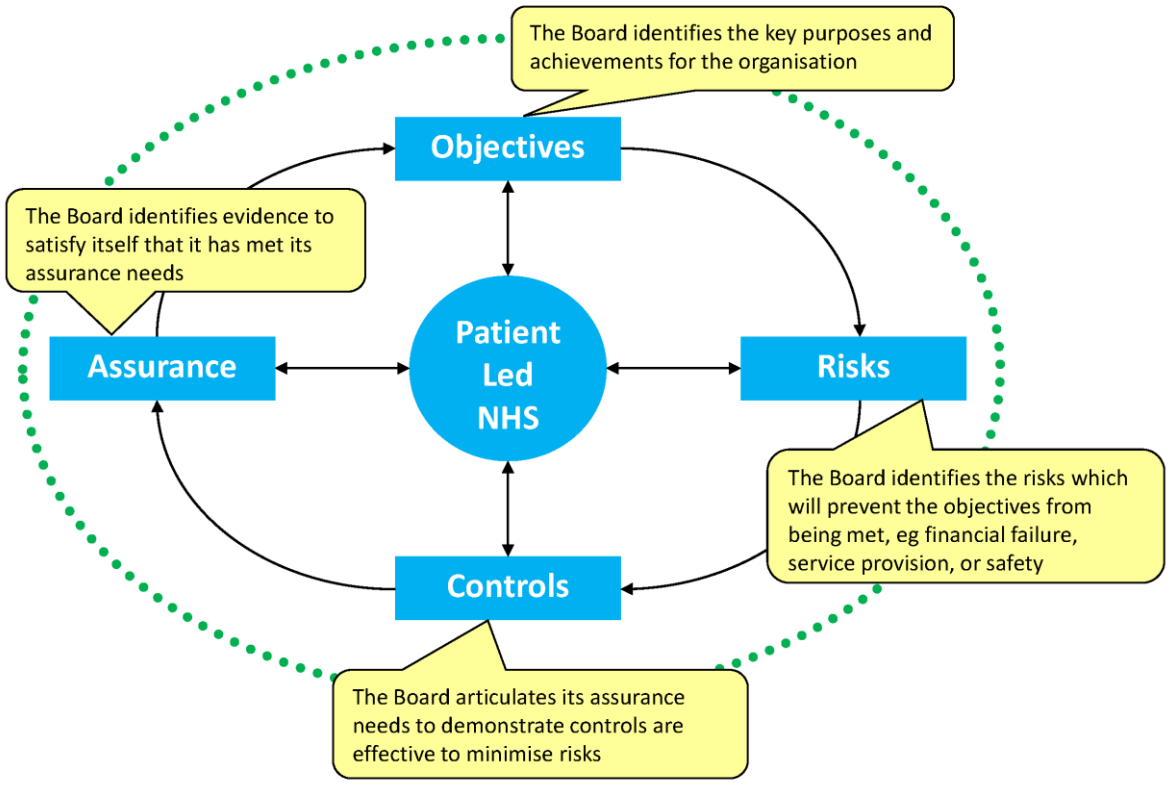
1. The cause of the impact on the objective, AND
2. The impact to the objective (i.e., the consequence of the risk)

1.4 **Residual risk** is the exposure arising from a specific risk after action has been taken to manage it.

1.5 A **risk register** is simply an explicit record of identified residual risk, which should be used by management to take appropriate action to mitigate that risk.

1.6 The diagram below gives a high-level view of the system of corporate governance, and the part that risk management plays in it.

Figure 1 – Overall System of Corporate Governance



Source: adapted by NHS Lothian from Health Care Standards Unit, as referred to in the Oxford University Hospitals Foundation NHS Trust Assurance Strategy (September 2015)

1.7 If the systems of assurance within the organisation are designed properly, they can add value by reducing bureaucracy, and allowing the Board and senior management to confidently focus on the key matters which do require attention.

1.8 The design of the systems of assurance should reflect the strategic aim of making NHS Lothian a more data driven organisation.

1.9 You can find further information on corporate governance and assurance, and other information on the wider system of governance in the Board Members' Handbook on the Board's website.

1.10 When a risk has been identified, action must be taken to respond to it. The four options are:

1. **Treat:** Eliminate the risk completely or reduce it to the point where the risk is at an acceptable level.

2. **Tolerate:** Where the risk is unavoidable, formally conclude that the risk is of a type that any further action would be disproportionate to the level of risk exposure, and that the risk is therefore at an acceptable level.

3. **Transfer the Risk** e.g., insurance cover.

4. **Terminate the Activity** from which the risk derives.

1.11 An **internal control** is a measure put in place with the aim to mitigate risk. Internal controls will constrain risks but are unlikely to eliminate them entirely and every control will come at some type of cost. Management is expected to design and implement systems of internal control, and this procedure includes further detail on this subject.

2. Who is responsible for managing risk?

2.1 The simple answer is everyone. Every person through their daily duties contributes to the management of risks which are relevant to their activities.

2.2 The Board and its committees are not involved in operational management and delivery, but exercise oversight of the system of risk management in the organisation and receive reasonable assurance that the system supports the implementation of the Risk Management Policy. The Board and its committees require assurance from management (and other sources) to carry out their role in corporate governance.

2.3 Managers are responsible for managing risk and developing and implementing the detailed systems of internal control in their areas of responsibility. This effort should be aimed at delivering the Board's strategic objectives and improvement aims. If risks can be and are efficiently and effectively managed at a local level, it is less likely that more significant risks will develop throughout the organisation. Consequently, management need to assure themselves that those systems of internal control and risk management are operating as intended. If they successfully do so, they can efficiently provide assurance to a committee and the Board as and when required.

2.4 Risks should be managed at the lowest level possible in the organisation and aligned to operational management structures. The identification of and response to risk, and the development, maintenance and use of a local risk register should be a multi-disciplinary team effort. However, one person will be accountable at each level of the organisation for the co-ordination of the associated risk register.

2.5 The NHS Lothian Quality Department supports the whole organisation to develop and implement the system of risk management.

2.6 Two key roles within the process of risk management are the **risk owner** and the **risk handler.**

2.7 A risk owner is the named director or manager with overall responsibility for a particular risk, albeit the action points related to the management of the risk may be passed to other appropriate individual (risk handler).

2.8 The risk owner has overall responsibility for ensuring that:

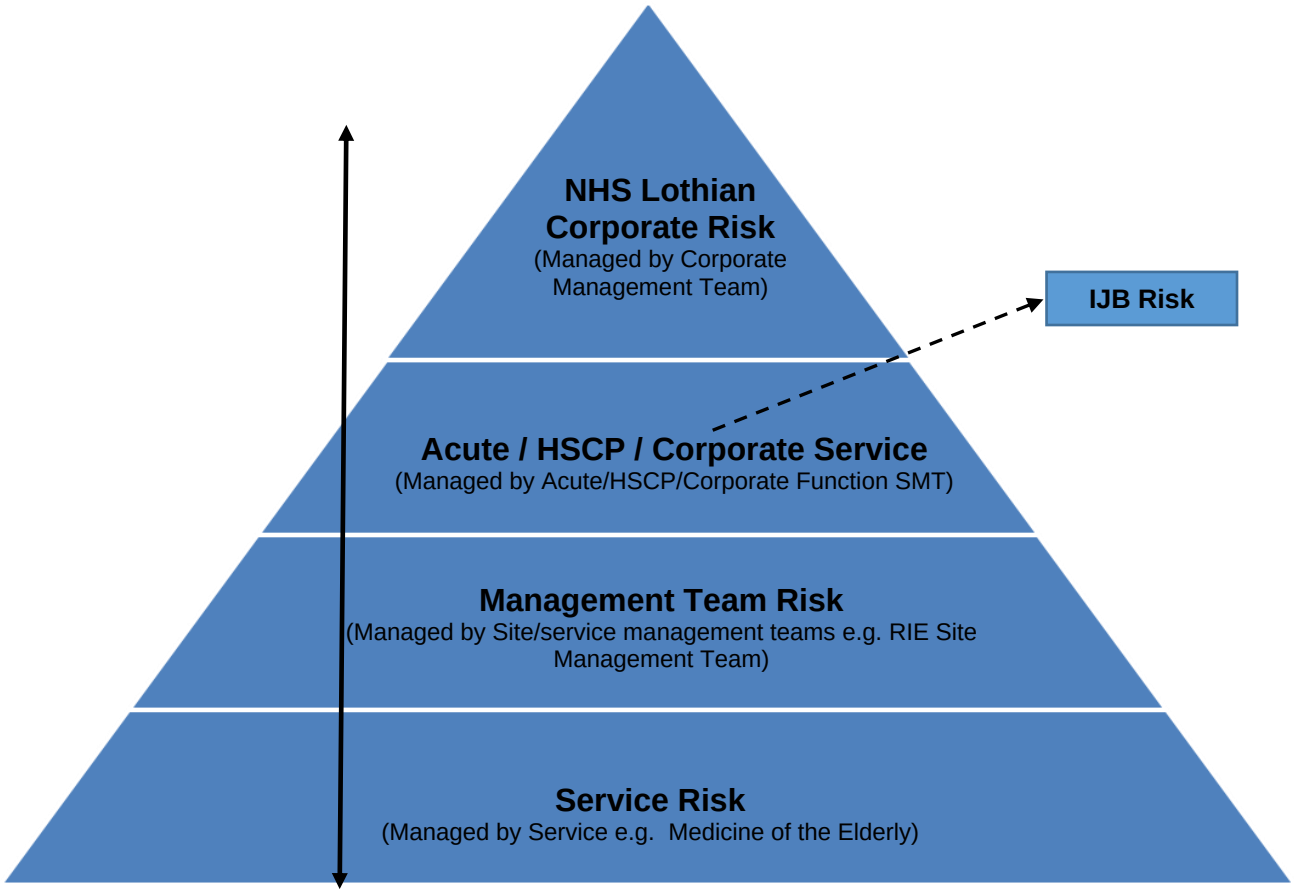
- risks are managed and analysed in accordance with the Risk Management Policy and Procedure
- risks and their supporting mitigation plans are evaluated and reviewed in a regular and timely manner and that progress against mitigation plans is maintained to support the management of risks
- they are assured that adequate and effective systems of internal control are in place
- provide a report on the management of a risk, should a management team or a Board committee require

2.9 The risk handler typically undertakes the detailed work on the particular risk, and reports to the risk owner on that work.

3. The Risk Register Hierarchy

3.1 Risk registers exist at all levels of the organisation in line with operational management structures (see Figure 2 below).

Figure 2 – Risk Register Hierarchy



3.2 Risks should be recorded on the Risk Management Information System (Datix), where all the information required can be entered (see Guidance on Recording and Reviewing Risks on Datix.)

3.3 We should ensure that the risks are in the right level to be managed appropriately and effectively. Escalation can be up or down. Please refer to NHS Lothian's Risk Escalation Flowchart.

3.4 The Corporate Risk Register contains strategic risks which compromise the delivery of NHS Lothian objectives as well as operational risks which cannot be managed at a lower level and/or have an impact across the system.

3.5 Divisional risk registers must have a local process in place for management. Risks at this level may also reflect or contribute to management of risks on the Corporate Risk Register – examples (Acute and West Lothian HSCP).

3.6 Ward/Department Risk Assessments General Risk Assessment Form may be held in Ward/Departmental Health, Safety and Risk Folders rather than on Datix. For further advice please refer to the NHS Lothian Health & Safety intranet pages.

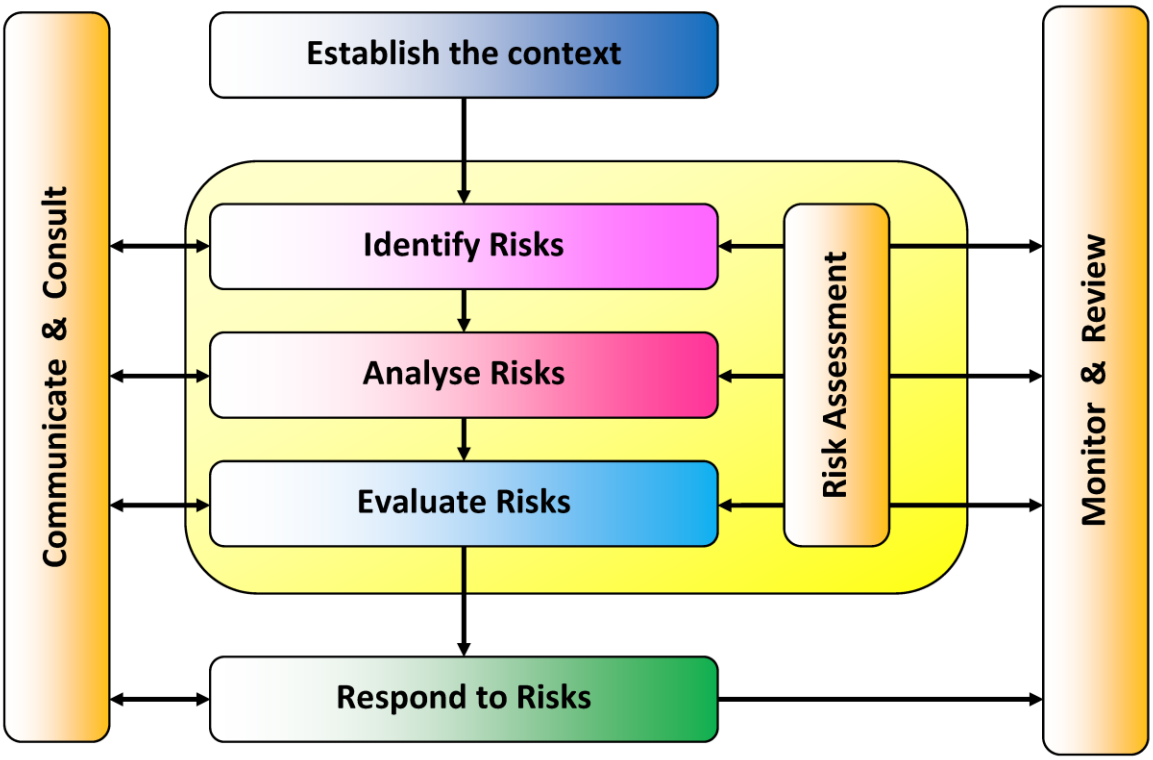
3.7 Risks associated with specific projects will be held on individual project risk registers and managed as part of the overall management of the project.

3.8 Risks associated with business cases and proposals must be explicitly identified and assessed and included in any papers presented to management groups or Board committees seeking agreement.

4. Risk Register Process

4.1 The steps to identify and respond to risks are summarised at Figure 3 below:

Figure 3



Establish the context

4.2 Risks may be generated through a range of mechanisms, though will ultimately relate either directly or indirectly to the achievement of NHS Lothian objectives, objectives specifically defined for your service, or area of responsibility. Risks may relate to a specific objective or may be generic, for example, related to patient safety, quality, and experience which will affect delivery of several objectives.

Risk Assessment → **Identify Risks**

4.3 It is essential that all risks are clearly defined. If you define your risks properly, you will have a better understanding of what they are and are more likely to identify appropriate actions that will successfully attend to those risks. It is also helpful to consider whether a concern is really a risk, as opposed to an issue or problem as outlined in Table 1 below.

Table 1

Issue	Problem	Risk
A matter of concern or contention	A matter that is difficult to manage and can create a dilemma	A known escalating matter or an emerging unexpected event
Management on a day-to-day basis and can be resolved	Senior management decisions are required to support day-to-day management with action planning to manage safely and effectively	Requires a quantification of the risk, level of risk recording of mitigating controls and actions to be taken for improvement and subsequent monitoring of the effectiveness of the controls and actions

4.4 Risk identification should be a team effort. It is good practice to purposely identify risks which will impact on several objectives or assurance needs. Its potential impact may vary in relation to different objectives. (It is possible that a single treatment may adequately address the risk in relation to more than one objective).

4.5 **How to express a risk**

A risk should have two elements:

1) **What can happen** which will have an impact on achieving an objective or assurance need (the cause) refer to Figure 1

2) The **impact on the objective or assurance need** (the consequence).

What you should **not** do when expressing risk is:

a) State risks which are simply the converse of the objectives.
b) State impacts which may arise as risks themselves.

Illustration

Objective: to travel by train from A to B for a meeting at a certain time	
Failure to get to from A to B in time for the meeting.	X This is simply the converse of the objective.
Being late and missing the meeting.	X This is a statement of the impact of the risk, not the risk itself.
There is no buffet on the train, so I get hungry	X This does not affect the achievement of the objective.
Missing the train causes me to be late and miss the meeting.	✓ This is a risk which can be controlled by getting to the station in plenty of time.
Severe weather prevents the train from running and me from getting to the meeting.	✓ This is a risk which cannot be controlled; however, you can make a contingency plan. You could alternatively "terminate the activity" and not make the journey and instead use tele- or video-conferencing.

A helpful discipline in articulating a risk is to think of three elements:

'There is a risk that ....'
What event could happen that creates uncertainty as to the achievement of the stated objective or assurance need?

'Because ...'

Why and/or how could the event occur? The risk will often occur because something changes e.g., a new target, a new piece of legislation, a gap in assurance identified by a committee or performance below expectation highlighted through the performance management system

'Leading to ...'
What would the consequence be if the event occurred?

Specific Examples of Risks for the NHS

There is a risk that the Board has to reduce or cease certain services in order to live within resources **because** our overall costs in providing services are increasing at a faster rate than growth in our income, **which can lead to** poorer health outcomes.

There is a risk that smokers who do wish to quit are unaware of the support that is available to them, **because of** ineffective communication of services **leading to** low uptake and successful quits.

There is a risk that prospective mothers are not aware of the benefits of breastfeeding, **because** of inadequate funding of resources for promotion, **leading to** the rate of breastfeeding being lower than it could be, and missed opportunity for positive health outcomes.

There is a risk that surgical services are unable to staff the on-call rota **because** there is a shortage of surgeons **leading to** poor patient experience and increased waiting times with potential deterioration in conditions, as well as unsustainable extra workload for the surgeons.

There is a risk that the Board does not treat patients in a timely manner **due to** a combination of demand significantly exceeding capacity for specific specialties and suboptimal use of available capacity, **leading** to compromised patient safety.

4.6 Once you have created a list of risks, review them, and look for some which may state similar risks, or may need reworded.

4.7 Finally, decide, what is the main objective or assurance need that will be compromised should the risk materialise? This function provides the organisation with the opportunity to group risks against specific objectives and assess what risks are likely to impede their delivery.

Risk Assessment → Analyse Risks

4.8 **Identify the System of Internal Control**

For each identified risk you should be aiming to have assurance that those internal controls are in place and operating effectively so that the associated objective(s)/ assurance needs are being achieved. In identifying the current controls it can be helpful to consider the four types:

1. DIRECTIVE

These are designed to ensure a particular outcome is achieved. Directive controls are typically expressed in a policy or procedure, describing broadly and setting out what is required to happen. They are not in themselves effective in managing risk and providing assurance unless there is a corresponding suite of preventative and detective controls in place.

Examples:

- Require staff to wear protective equipment when doing certain tasks.
- Require staff to have completed a qualification or have cleared a check before being employed
- Require staff to have completed a particular training before being allowed to carry out a particular activity without supervision.

2. PREVENTATIVE

Preventative controls are designed to prevent undesirable outcomes. They are measures which design out risk and, if they operate correctly, should ensure that the right thing does happen. This is the strongest type of internal control.

Examples:

- Upon appointment the employee is automatically issued with the required protective equipment. There is a supervisory check to ensure the equipment is available for use before an activity, and the activity will not start unless this is the case.
- An employee is required to provide documentary evidence of qualifications before a job offer can be made.
- A PVG check must be undertaken before a job offer can be made.
- A person (who is independent from the person who approved an order) has to confirm that the goods or services have definitely been received before any payment is made to the supplier.

3. DETECTIVE

Detective controls will alert management to when an undesirable outcome has happened. As they only operate after the event, they are not as useful at managing risk as preventative controls.

Examples:

- A system of spot observation checks can confirm whether or not employees

are indeed using their protective equipment in practice.

- All employees are required to and know how to report all adverse events.
- A monthly check against the NMC database will identify whether current employees have up-to-date registration.
- A stock check will identify whether we have all the stock that we think we should through our stock records.

Managers are advised to explore opportunities to use the reporting capability within existing systems as these can automatically provide information that will allow you to monitor the operation of key controls, e.g. Tableau, finance reports, TRAK, DATIX.

4. CORRECTIVE

These are measures that can be put in place to correct undesirable outcomes after they have happened. They provide a way to allow for some recovery of any loss or damage.

Examples:

- The design of terms within a contract to allow for the recovery of any overpayments.
- The use of insurance policies that will provide compensation should certain insured events happen.
- The development of business continuity plans and disaster recovery plans, to help the organisation respond to an event that it could not control.

4.9 Evaluating the controls

The next stage is to evaluate the controls so that you can identify any unmanaged risk. To do this, you must consider the adequacy of the controls that are already in place either to reduce the likelihood of the risk materialising or to reduce the impact if it does materialise. Consideration should be given to both the design of the control and implementation. For each risk, select from the list below how best to describe the adequacy of controls.

Satisfactory	**All controls are working and can be demonstrated through measurement** **Examples** Sustained improvement in performance Consistent reduction in adverse events/complaints Compliance audits with relevant procedures demonstrate positive results.
Some weaknesses	**Improvement can be demonstrated however not at optimal level.** **Examples** Early indication of improved performance but still variable month on month Reduction in adverse event/complaints around one aspect of the

	risk Compliance audits with relevant procedures demonstrate positive results for some staff groups but not others.
Weak	**The controls in place have not made much difference and the level of risk cannot be reduced** **Examples** No or occasional improvement in performance No reduction in adverse events/complaints Compliance audits with relevant procedures demonstrate poor results for all staff groups.
Unknown	**The current controls are not known and further work is required to identify the current situation**

Risk Assessment → **Evaluate Risks**

4.10 Once you have established the adequacy of controls, apply a risk grade.

The grading tool used in NHS Lothian measures risks according to the following formula:

Likelihood x Impact = Risk

This is done by considering the likelihood of the risk and the most likely consequence (bearing in mind the controls that are in place). Each description of likelihood and consequence has an assigned line on the risk matrix. The risk grade is given taking account of the controls and other preventative measures that are in place and provides you with the **residual** or current risk grade. Please refer to NHS Lothian Risk Matrices.

The resulting value will inform prioritisation and place the risk into one of 4 categories:

Risk Grade		Risk Level
Very High	Red	20-25
High	Amber	10-16
Medium	Yellow	4-9
Low	Green	1-3

4.11 When evaluating the risks, it is important to also think about and record the target risk grading that you wish to set for the risk – this is the level of risk that the organisation will deem acceptable.

NB If a risk has been identified with an extreme impact but a rare likelihood of happening, this could be a business continuity risk and should be escalated to the attention of the Resilience Team rather than being recorded on the risk register.

Respond to Risks

4.12 Now that the risk has been identified and analysed, any gaps or opportunities for improvement in the adequacy of controls should be addressed through a risk mitigation plan.

4.13 Action must be taken to either:

	PROCESS	TREATMENT
Tolerate	The current risk is either acceptable or tolerable i.e. the risk is currently managed to an acceptable level	Periodically reassess to ensure the risk and controls have not changed. (See section 4.17)
Treat	The level of current risk is not tolerable, it is too high. Additional action should be taken to reduce the likelihood and/or impact of the risk occurring	Consider which additional controls are required to better manage the risk and develop a risk mitigation plan. The cost and effectiveness of additional controls should be balanced against the potential consequences of the risk crystallising
Transfer	Management of the risk should be either be fully transferred e.g. to an insurer	Identify how the risk can be transferred. Consider the consequences of transferring the risk to a third party and what new risks may arise
Terminate	Consider whether this risk can be eliminated by ceasing to carry out the activity	If the underlying activity giving rise to the risk cannot be terminated, then apply the action to **Treat**

4.14 All actions in risk mitigation plans should be **SMART**, i.e.:

- **Specific** – target a specific aspect for improvement/action
- **Measurable** – quantify or at least suggest an indicator of progress
- **Assigned** – specify who will make it happen
- **Realistic** – ensure that it can realistically be achieved, given available resources
- **Time Bound** – specify when the result(s) can be achieved.

4.15 Risk Actions should be reviewed regularly, and updates provided. They should detail progress against agreed actions to date. If there is a failure to make progress on an action, consider if there are any new actions required.

4.16 When an action is completed, it will become a control and the controls should be updated to reflect this.

Monitor & Review

4.17 A review of the risk register should be carried out by the relevant manager (see Section 2 for Roles and Responsibilities) at least every 3 months at the appropriate level, although individual risks, depending on their grade, may be reviewed more frequently. New risks and escalation of risks should be considered at this point.

The main elements when reviewing a risk are:

- Cause of risk
- Controls in place and have any actions resulted in new controls
- Adequacy of controls
- Risk grade and level
- Action plan to address any gaps in adequacy of control
- Escalation

Refer to Level of Risk and Review for further information regarding review of risk.

4.18 It is important that a clear measurement framework is in place for each risk to assess the effectiveness of the risk mitigation plan on the adequacy of controls as set out in 4.7 above.

4.19 It may be necessary to escalate the risk to a higher level of management if:

- all local actions required to reduce the risk have been exhausted at your level of management, e.g., you do not have the necessary resources or authority
- controls are maximum and agreement is required regarding acceptance of the residual risk.

Note that by escalating a risk:

- its description may change i.e., the same risk may be described and assessed differently, according to differing objectives and perspectives at different management levels.

Please refer to the NHS Lothian's Risk Escalation Flowchart.

4.20 A risk may have been managed to a reasonable/tolerable level but because the cause is still present, the risk should not be closed. It should be reviewed regularly to consider:

- Whether there are any new innovations or reasonable newly available actions to further mitigate the risk
- If the controls are effective, due consideration being given to other data such as incidents, complaints, concerns, claims
- If the existing risk assessment requires a review.

In such instances, one action, for example to carry out a review of the 3 bullet points given above, in 3 months is sufficient.

Closing risks

4.21 A risk can be closed in the following circumstances:

- The situation or set of circumstances that gave rise to the risk being recorded is totally removed. An example could be a piece of outdated equipment that presented a level of risk has been replaced or a particular procedure is no longer carried out

- The controls and preventative measures enable the risk to be graded medium or low and there is sufficient assurance regarding the effectiveness of the controls.

4.22 It **may not** be appropriate to close a risk in the following circumstance:

- The organisation has deemed that the controls and preventative measures will be tolerated, but the risk grade remains high or very high. These risks should be reviewed as on a regular basis to monitor effectiveness of controls.

Communicate & Consult

4.23 The Board and/or relevant senior management teams must be periodically informed of the key risks of the organisation and factor this into its decision making. This will ensure that the adequacy and effectiveness of the controls and assurances identified in the risk register are routinely considered. This must include measures to address gaps in controls and assurances through monitoring of risk mitigation plans, identifying any further measures NHS Lothian should take to manage its key risks.

4.24 All the senior management teams must have an explicit process in place for managing and reviewing risks within their own area (see example Acute services, West Lothian HSCP).

4.25 A standard paper format should be used when reporting risks to committees and management groups.

5. Training & Support

5.1 The NHS Lothian Quality Department provides training and support on developing and maintaining a risk register, including recording on DATIX which includes running workshops for management teams if requested.

5.2 For DATIX training and support contact: Datix Helpdesk – datixhelp@nhslothian.scot.nhs.uk Tel: 0131 537 8561, (Ext 88561)

5.3 The Health & Safety Department provides risk assessment training on task based or environmental based risks.

6. Governance and Reporting Arrangements

6.1 Each senior management team requires to have explicit processes in place for regular reporting and review of risk registers (see example Acute services process).

6.2 The Corporate Management Team review the corporate risk register and make recommendations to the Board for consideration at every Board meeting. (Corporate Risk Register Process.)

6.3 All corporate risks will be presented to the relevant Board committee for assurance at least annually. (Corporate Risk Register Process.)

6.4 The Corporate Management Team considers divisional high / very high risks every 6 months to assess the requirement of any risks to be escalated to the Corporate Risk Register. (Corporate Risk Register Process.)

6.5 The Corporate Risk Register is considered at every Board meeting, Audit and Risk & Healthcare Governance Committees. (Corporate Risk Register Process.)

7. Review of Procedure

7.1 The procedure will be continuously reviewed by the Quality Directorate with a formal review carried out every 3 years.