Risk Management Strategy 2022 – 2025

At NHS Forth Valley we strive to be better every day.....

Written by	**Sara MacKenzie, Corporate Risk Manager**
Approved By	**Audit and Risk Committee**
Approval Date	**22nd June 2022**
Review Date	**31st March 2023**
Notes	**New 3 year strategy 2022 – 2025**

Contents

Foreword

Effective Risk Management is a fundamental cornerstone of good Corporate Governance and Internal Control and is an essential component in delivery of the Health Board's corporate objectives. This Risk Management Strategy has been written for and with staff and is intended to:

- Influence culture by helping staff better understand how to evaluate and take actions on all their risks to increase the probability of success whilst reducing the likelihood of failure.
- Ensure high conformity with applicable rules, regulatory regulations and mandatory obligations.
- Provide assurance to the Health Board, Integration Joint Boards and its Audit and Assurance Committees that risk management and internal control activities are proportionate, aligned, comprehensive, embedded and dynamic.
- Support decision making using a risk based approach.
- Adopt 'rules of engagement' whilst working in partnership with external stakeholders that are clear and unambiguous to support a culture of engagement and collaboration.

A good understanding and awareness of risks, based on the identification, assessment and mitigation processes as outlined in this Strategy, will enable the Health Board to successfully deliver the vision as set out in our Healthcare Strategy 2016-2021: 'Shaping the Future' and the Health Board's corporate objectives.

I want NHS Forth Valley to be a high performing Health Board. High performing organisations have good governance and management arrangements in place. I believe effective risk management is a key component of these arrangements. This Strategy aims to support a risk management culture that encourages us to be risk aware but not risk averse.

I want us to adopt good risk management behaviours and practice and this will requires all of us to be familiar with our systems, policies and processes and to be able to identify, assess and respond to risks within our operating environment. Training and support will available to staff to underpin this Strategy.

In summary, risk is unavoidable. It is an important part of life that allows us all to move forward and develop. Successful risk management is about ensuring that we have the correct level of control in place to provide sufficient protection from harm, without stifling our development. This Strategy sets out our approach to risk management and outlines the key objectives and responsibilities for the management of risk throughout our organisation.

This Strategy applies to all staff and contractors who work on our NHS owned sites. It will be distributed in electronic format and made accessible to all staff through the Health Board's staff intranet and internet sites. I believe we should not shy away from risk but instead seek to proactively manage it. This will allow us not only to meet the needs of today, but also be prepared to meet the future challenges of tomorrow.

Cathie Cowan
Cathie Cowan
Chief Executive

1. Introduction

The Risk Management Strategy sets out the principles and approaches to risk management which are to be followed throughout NHS Forth Valley. Its objective is to achieve a consistent and effective application of risk management and enable it to be embedded into all core processes, forming part of the day-to-day management activity of the organisation. Risk Management, when deployed effectively, should add value by supporting day-to-day activities as opposed to being seen as a separate, self-contained process and this Strategy supports this approach.

1.1. What is a Risk?

A risk can be defined as 'the effect of uncertainty on objectives' (*ISO31000)*. It is essentially any uncertain event which can have an impact upon the achievement of an organisation's objectives – either reducing the likelihood of achievement or stopping it altogether.

Not every perceived problem or adverse event is a risk. An important distinction must be made between what is a risk and what is an issue – or in other words, an uncertainty and a certainty. A risk is an event that may or may not happen. An issue or adverse event is something that is currently happening or has already happened. Issues and adverse events should therefore not be recorded and treated as risks – we want to adopt a proactive rather than reactive stance.

1.2. What is Risk Management?

Risk management is a systematic way of dealing with that uncertainty which involves the identification, analysis, control and monitoring of risk. Risk Management activities are designed to achieve the best possible outcomes and reduce the uncertainty. An effective system of risk management will draw together all types of risks and enable an interrelated view of the organisation's risk profile.

1.3. Why do we need Risk Management?

An effective system of risk management will deliver a range of outputs:

- Ensuring that decision making is informed and risk-based, to maximise the likelihood of achieving key strategic objectives and effective prioritisation of resources
- Ensuring compliance with legislation, regulations, and other mandatory obligations
- Providing assurance to internal and external governance groups that risks are being effectively controlled

- Supporting organisational resilience
- Raising awareness of the need for everyone to adopt consistent risk management behaviours and actions in our everyday business
- Empowering all staff to make sound judgements and decisions concerning the management of risk and risk taking – fostering a “risk aware” rather than “risk averse” culture
- Achievement of effective and efficient processes throughout the organisation
- Anticipating and responding to changing political, environmental, social, technology and legislative requirements and / or opportunities
- Preventing injury and / or harm, damage and losses.

Effective risk management will be achieved by:

- Clearly defining roles, responsibilities and governance arrangements for individuals, teams and assurance committees within NHS Forth Valley
- Incorporating risk management in all Executive Leadership Team, Health Board, Integration Joint Board and Assurance Committee reports and when taking decisions
- Maintaining risk registers at all levels that are linked to the organisation’s strategic objectives
- Staff at all levels understanding risk management principles, and consistently applying them through their everyday activities, confidently identifying risks and taking actions to bring them down to an acceptable level for the organisation
- Monitoring and reviewing risk management arrangements on a regular basis
- Seeking assurance that controls relied on to mitigate risks are effective

2. Risk Architecture

The arrangements for communication, governance, reporting, roles and responsibilities forms the organisation's overarching risk architecture. Defining a consistent approach to how and where risk information is communicated is essential to developing a positive risk culture and to ensuring risk management is appropriately implemented to support NHS Forth Valley activities.

Risks, once identified, are captured on risk registers. Each Department and Specialty will hold a risk register for its area – these form the bottom level of risk registers. Overall there are four levels of risk register and an escalation route exists for risks that cannot be fully mitigated at the Department / Speciality level. This risk register hierarchy is detailed below.

Risk Register Hierarchy

Strategic Risk Register

Risks contained in the Strategic Risk Register (previously known as the Corporate Risk Register) are the high level risks that could impact the delivery of longer term strategic objectives of the organisation. Risks are not escalated/de-escalated from lower-level risk registers to the Strategic Risk Register. Instead, risk identification for the Strategic Risk Register is facilitated through twice yearly review and horizon scanning sessions led by the Executive Leadership Team.

Organisational Risk Register

Risks contained in the Organisational Risk Register are top level, cross cutting risks that present a significant short-medium term threat to multiple Directorates. Risks are escalated and de-escalated via the Directorate Risk Register(s).

Directorate Risk Registers

Each Directorate holds a risk register that contains a cut of the most significant risks from its component Departments / Specialties. Risks are escalated to the Directorate level via the individual Department / Specialty risk registers.

Department

Each Department and Specialty will hold a risk register for its area – these form the bottom level of risk registers.

2.1. Risk Escalation

Risk escalation is a process that ensures significant risks that cannot be managed by a local team, department or specialty are escalated appropriately following the risk register hierarchy and line management arrangements. The following questions should be asked when deciding whether to escalate a risk:

- Does the risk present a significant threat to the achievement of Government objectives and/or standards?
- Is the risk score assessed to be intolerable or beyond the organisation's risk appetite?
- Does the risk have a widespread impact beyond a local area, e.g. does it affect multiple Departments or Directorates or does it have dependencies on multiple Departments or Directorates to mitigate?
- Does the risk present a significant cost/decision making beyond the scope of the budget holder, or require change driven at an organisational level?

Risk score and organisational risk appetite should be key considerations when recommending risks for escalation.

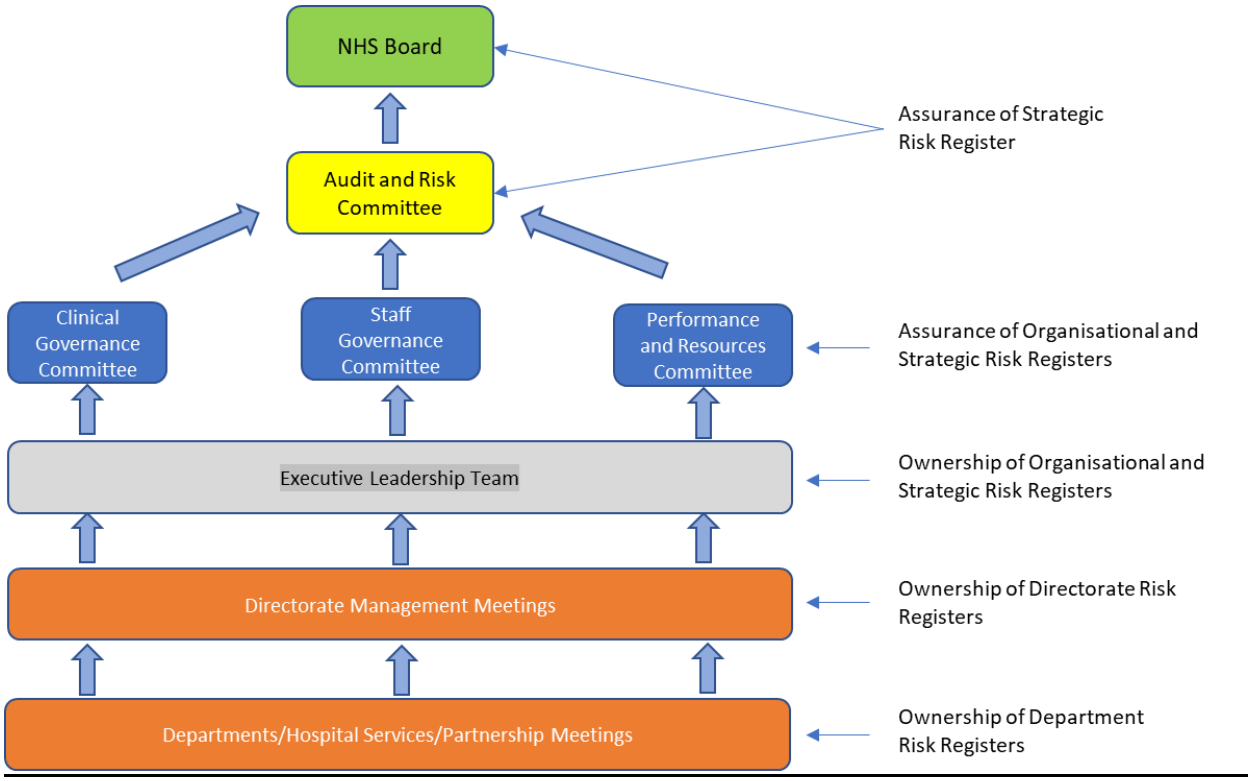
2.2. Governance & Reporting

The Board of NHS Forth Valley is corporately responsible for the Risk Management Strategy and for ensuring that significant risks are adequately controlled. To support the Board a number of formal committees have been established and are responsible for various aspects of risk management, principally these are the Audit and Risk, Performance & Resources, Clinical Governance and Staff Governance Committees. All Health Board Committees are responsible for providing assurance on the effective management of risks relevant to their area of responsibility. In addition, the Audit and Risk Committee has a responsibility for

overseeing the operation of the Risk Management Strategy, taking assurance from the Executive Leadership Team.

Diagram 1 illustrates NHS Forth Valley's risk management governance structure.

Diagram 1: Risk Management Governance Structure



2.3. Roles & Responsibilities

Risk Management Roles & Responsibilities
NHS Board
• Provide Oversight and Scrutiny of NHS Forth Valley's risk management arrangements to seek assurance on their effectiveness • Approve risk appetite within NHS Forth Valley
Chief Executive
• To have overall accountability for the management of risk across NHS Forth Valley

Executive Leadership Team

- Set risk appetite within NHS Forth Valley
- Ensure risk management processes are supported to provide them with adequate information and assurance related to strategic and organisational risks

Audit and Risk Committee

- To evaluate and recommend approval of the strategies and frameworks in respect of risk management to the NHS Board, and provide assurance on the effectiveness of the risk management arrangements, systems and processes
- To approve updates and provide direction in respect of risks held within the strategic and organisational risk registers
- To review the organisation's risk culture and maturity and direct action in pursuit of continuous improvement in this area
- To formally approve the strategic risk register for onward reporting to the NHS Board

Assurance Committees

- To ensure that an appropriate approach is in place to deal with risk management across the system working within the NHS Forth Valley Risk Management Strategy, and consider the assurance provided by the Executive Leadership Team and Senior Management regarding the effective management and escalation of risks

Executive and Non Executive Directors

- To ensure that risk management processes are providing appropriate information and assurances relating to risks in Directorates
- Promote the importance of risk management and foster a good risk culture within their area of responsibility
- Approve escalation of Directorate level risks where appropriate

Corporate Risk Manager

- Responsible for the implementation of the Risk Management Strategy
- Ensure risks are properly identified, understood and managed across all levels within the organisation
- Report on the organisation's risk profile at various levels to Directorates, Assurance and Audit Committees and NHS Board
- Periodically review the Risk Management Strategy and arrangements, identifying areas for potential improvement
- Drive an improving risk culture through risk education, awareness and embedding into day-to-day management

Risk Management Advisor

- Assist the Corporate Risk Manager with the development and implementation of the Risk Management Strategy
- Act as a key point of contact for Risk Management, providing expert advice and guidance and supporting the Directorates and Partnerships
- Assist the Corporate Risk Manager with reporting on the organisation's risk profile, providing Risk Management representation at various levels
- Support an improving risk culture through delivery of training, awareness and supporting Directorates and Partnerships to embed risk considerations into day-to-day management

Risk Owner

- Accountable for ensuring the effective management of a risk, and providing assurance that key controls are operating effectively

Risk Lead

- Responsible for managing a risk on a day-to-day basis, assessing the risk score and updating the management plan, reviewing the risk on a regular basis and identifying sources and levels of assurance regarding control effectiveness, to allow risk owners to provide assurance

Risk Champion

- Responsible within an individual speciality, department or Directorate area for maintaining lines of communication with the risk function, administering the risk register and co-ordinating all risk activities

Integrated Risk Management: Health & Social Care Partnerships

In order to ensure strong risk management partnership arrangements, it will be necessary to agree how some emerging risks have an impact on more than one partner at a strategic level. Risks will be discussed and agreed across partners, with particular focus on:

- Where the risk was first identified
- Date of identification
- Nature of emerging risk
- Impact areas (e.g. service delivery, performance, strategic commissioning intentions etc)
- Mitigation required

Risks with the potential to impact more than one partner will be identified for inclusion in one or more of the following risk registers:

- NHS Forth Valley Strategic Risk Register
- Clackmannanshire and Stirling IJB Strategic Risk Register
- Falkirk IJB Strategic Risk Register

Any such emerging risks will be submitted to the NHS Forth Valley Executive Leadership Team for approval to the Strategic Risk Register.

Operational risks will continue to be managed by partner bodies, with relevant risk specialists working together to ensure consistent practice, and that respective Risk Management strategies are aligned. The IJBs will also have a defined risk appetite acting as a trigger point for escalation. It is recognised that partners may not have the same appetite, however these variances will be taken into consideration when the risks are being managed and reported.

Reciprocal assurances on the operation of the Risk Management arrangements and of the adequacy and effectiveness of key controls will be provided to/from partners. Receipt/provision of assurance will be facilitated by risk specialists from partner bodies, who will attend regular meetings to discuss risks and provide relevant advice.

3. Risk Appetite

Utilising risk appetite principles can help the organisation identify and set appropriate thresholds for risks, whereby the Board establishes the level of risk impact they are willing and able to absorb in pursuit of objectives.

The delivery of public services can be inherently high risk and the concept of applying risk appetite can be challenging. However, the application of risk appetite, particularly in a resource-finite environment, is essential to avoid over or under management of risk. Deployed effectively, risk appetite can act as an enabler to the delivery of key services.

Risk Appetite:

The amount and type of risk we, as an organisation, are willing to seek or accept in the pursuit of our objectives.

Key considerations when applying risk appetite:

- It is not always possible to manage every risk down the minimum or most desirable level and maintain service delivery
- It is not always financially affordable or manageable to fully remove risk and uncertainty from decision making and service delivery
- Risk management is concerned with balancing risk and opportunity (or downside risk and upside risk)

When a risk increases to a point where it is no longer within appetite, it may initially fall within a range which is not desirable, but the organisation has the capacity to tolerate. This is known as the risk tolerance range.

Risk Tolerance:

The maximum level of risk the organisation can tolerate regarding each type of risk before it is significantly impacted.

If a risk is out of appetite and falls within the tolerance range, this indicates that close monitoring and corrective action is required to bring the risk back within appetite. A risk with a current score out with the tolerance range requires escalation and immediate corrective action.

There are benefits to the practical application of Risk Appetite:

- supports decision making (resources can be allocated to risks further away from the desired appetite level)
- allows further prioritisation (if you have several risks with the same score, mitigate those further from appetite first)
- subjectivity is taken away from the setting of target scores (the appetite range becomes the target score)

Risk appetite is also useful when budget setting or considering approval of business cases, such as those relating to innovation activity. Identifying associated risks and their appetite levels allows focus on activities which mitigate the risks furthest from the organisation's desired risk appetite/tolerance levels.

3.1. Risk Appetite Levels

There are four levels of risk appetite within NHS Forth Valley. Each risk category in the risk assessment matrix is assigned one of the risk appetite levels described below. The risk appetite levels and their application to each risk category is set and approved by the NHS Board. Risk appetite may vary depending on internal and external circumstances; therefore the levels will be reviewed on an annual basis.

Averse:

- Very little appetite for this type of risk
- Avoidance of risk and uncertainty is a key organisational objective
- Exceptional circumstances are required for any acceptance of risk

Cautious:

- Minimal appetite for this type of risk.
- Preference for ultra-safe delivery options that have a low degree of inherent risk and only reward limited potential.

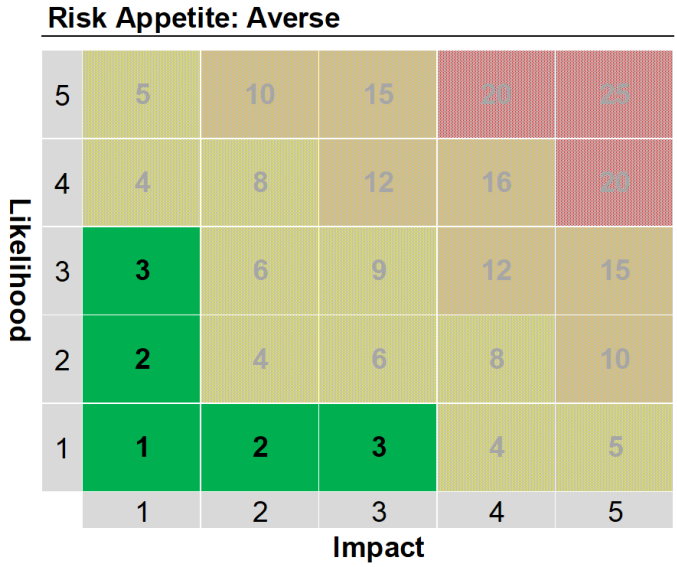
Moderate:

- Acceptance that a level of risk will be required to pursue objectives, or that a greater level of risk must be tolerated in this area.
- Preference for safe delivery options that have a low degree of inherent risk and may only have limited potential reward.

Open:

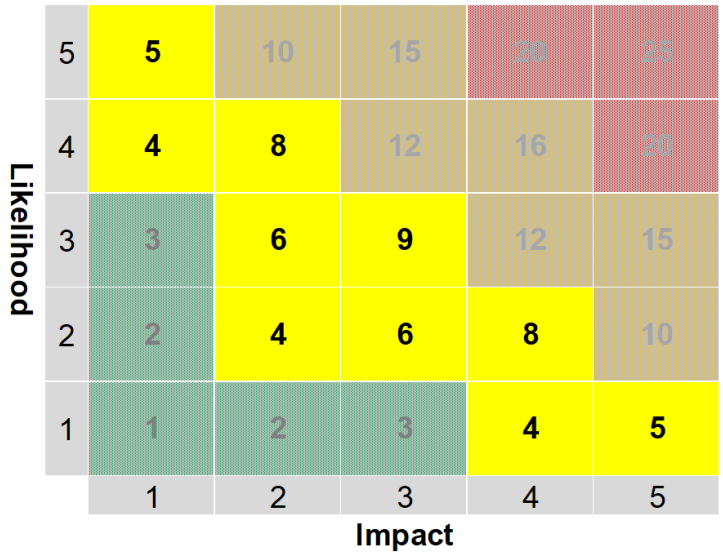
- Acceptance that risk must be more actively taken in the pursuit of transformation or that a high level of risk must be tolerated.
- Willing to consider all potential delivery options and choose the one most likely to result in successful delivery while also providing an acceptable level of reward (and Value for Money).
- Eager to be innovative and confident in setting high level of risk appetite as controls are robust.

Each risk appetite level correlates with risk score levels on our risk assessment matrix as shown below. Refer to the NHS Forth Valley Risk Appetite Statement for details on risk appetite levels for each risk category.



Demonstrates that if the risk appetite is 'Averse', a risk score of between 1-3 and the range of associated outcomes is within appetite

Risk Appetite: Cautious

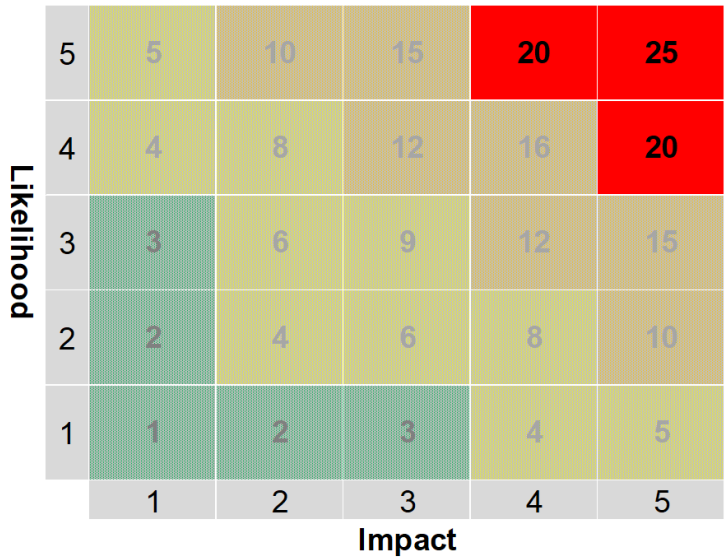


Demonstrates that if the risk appetite is 'Cautious', a risk score of between 4-9 and the range of associated outcomes is within appetite

Risk Appetite: Moderate

Demonstrates that if the risk appetite is 'Moderate', a risk score of between 10-16 and the range of associated outcomes is within appetite

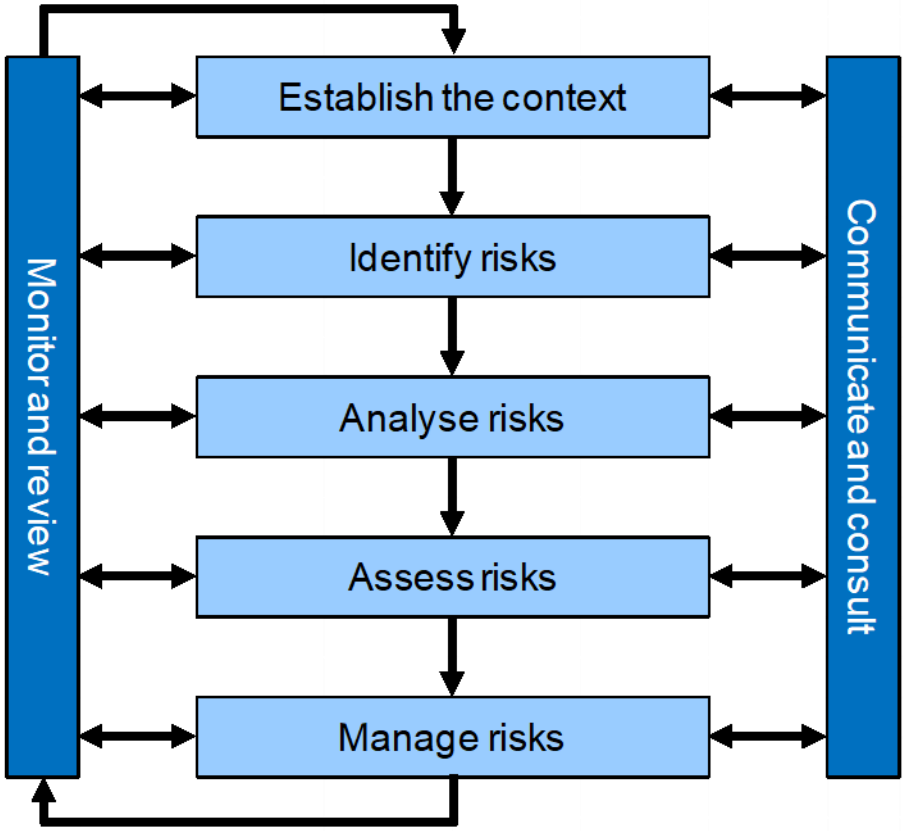
Risk Appetite: Open



Demonstrates that if the risk appetite is 'Open', a risk score of between 20-25 and the range of associated outcomes is within appetite

4. Approach to Risk Management

4.1. Risk Management Process – ISO31000



The above diagram demonstrates the whole process and cycle of risk management under the international standard ISO 31000.

The standard as outlined above makes clear that risk management is a dynamic process, with frequent review of existing risks and monitoring of the environment necessary to ensure the risks captured represent the current profile of the organisation.

Continual communication of risks within the organisation is essential to allow for informed decision-making. Communication to the Health Board and other stakeholders is also imperative to allow effective scrutiny and provide assurance that our risk profile is being effectively managed. It is also imperative to consult with and receive information from other departments within the organisation and our stakeholders to inform the management of our risks.

4.2. Step 1: Establish Context

The purpose of establishing context is to customise the risk management process, enabling effective risk analysis and appropriate risk treatment. In order to identify risks, we need to understand what we are assessing risk *against.* We must set risks within the context of the team, specialty, department and overall organisation. In addition, we need to recognise the internal and external drivers that could create risk.

Risks should be set against what we are trying to achieve as an organisation – our strategic objectives. In this stage it is important to ensure there is a common understanding of what those objectives mean at a team, specialty, department and organisational level in order that risk identification is not based on an inconsistent set of assumptions.

4.3. Step 2: Identify Risks

Once a clear, common set of objectives are agreed, the next step of the process is to identify potential risks that will prevent us from achieving them.

A range of techniques can be used for risk identification. Some prompts to consider:

- What might impact on your ability to deliver your objectives
- What does our performance data tell you?
- What do our audit and scrutiny reports and external reviews tell us?
- Do you have experience in this area? Do you know or do you need to involve others?
- Should you involve partners or specialists in your risk identification?
- Lessons learned – what happened before?

Risk can be identified in a multitude of ways, through focused identification sessions or as a product of other work:

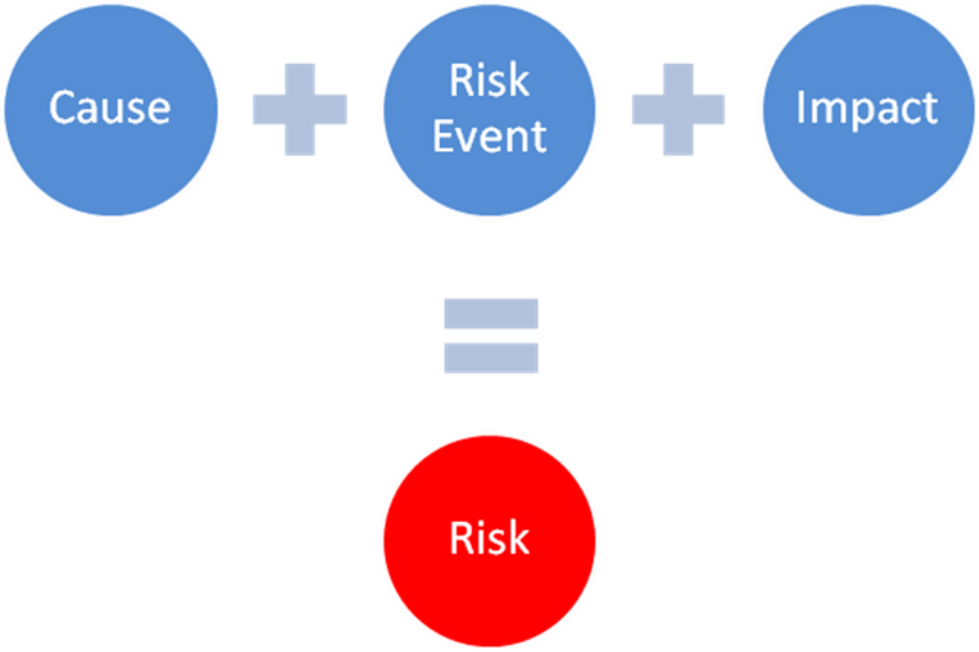
Focused Identification Methods	Other Identification Opportunities
• Risk Identification Workshops • Risk Questionnaires • Review & refresh of existing risk registers • Interviews	• Horizon scanning • Board meetings / working groups / management meetings • Audit & scrutiny reports • Performance data • Risk Management training

The Risk Management function facilitates risk identification workshops with Departments to direct an in-depth review of new or emerging risks.

It is important to note that just because a risk cannot be fully mitigated by the organisation alone does not mean that it should not be captured. If the risk exists to the organisation, then it should be captured, managed as far as practicable and then monitored. Ongoing management of the risk may well be in conjunction with partner agencies or influence can be exerted over those capable of mitigating the risk to within an acceptable level.

4.4. Step 3: Analyse Risks

Once a risk has been identified it must be described in a certain way in order to effectively understand, manage and mitigate it. The risk description should contain three essential components:



These three components can be included within the description as follows:

"If [insert cause here], there is a risk that

[a certain event that may happen], resulting in

[describe impact this will have if it manifests]"

An example of an effective risk description might be:

If there is insufficient in external funding and continued uncertainty over our cost base there is a risk that NHS FV will be unable to achieve financial sustainability, resulting in Scottish Government intervention and a detrimental impact on service delivery.

Without understanding the underlying causes of the risk and all the potential impacts, it would be very difficult to design and implement effective controls.

4.5. Step 4: Assess Risks

The assessment, or scoring, of risk allows for prioritisation by severity. Determining the likelihood and impact of a risk and utilising a standardised assessment criteria to assign a

score based on these factors allows us to understand and prioritise which risks to mitigate first. Three scores must be assigned to cover the full trajectory and lifespan of the risk:

Untreated Score

This is the inherent risk score, that is the score with no controls applied. This score represents the "worst case scenario" for the risk. If there were no controls, mitigation or contingency plans in place, how likely is it the risk would materialise and what would the impact be?

Current Score

Considering any controls that are currently in place to manage the risk, how does the risk score compare to the untreated score? This is the current score. Current risk score is assessed on a regular basis to establish the effectiveness of the controls applied to the risk. It is also the current score that is the key indicator used to determine if the risk should be considered for escalation.

Target Score

The target risk score is the optimum position for the risk. Once all controls have been adequately implemented, what will the residual risk score be? Target risk scores should reflect the organisation's risk appetite and align with the amount and type of risk NHS Forth Valley is willing to accept (refer to section 3 on Risk Appetite). Risk controls should be designed to actively reduce the risk score towards the target level.

Risk Assessment Matrix

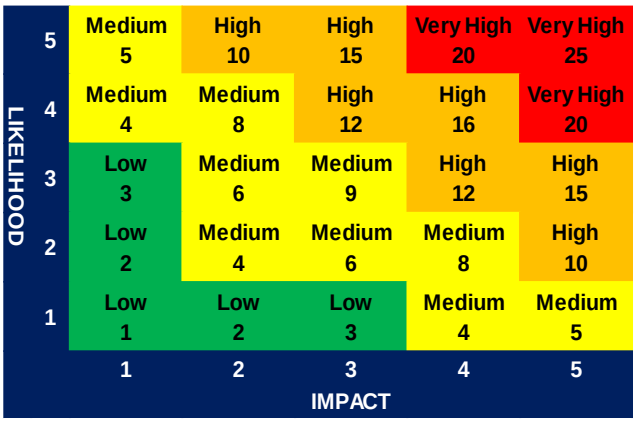
The risk assessment matrix is a 5x5 scoring mechanism which will identify a score between 1 (1x1) at the lowest and 25 (5x5) at the highest possible score.

When utilising the impact criteria on the assessment matrix, a score must be applied for every category of impact applicable to that risk. For example, one risk may have a financial impact, an impact to patient experience and reputational/public confidence implications. The impact category with the highest scoring criteria will identify the overall impact score for that risk.

Assessment of likelihood is considered on a sliding scale from 1 to 5, with 1 representing 'very unlikely' and 5 'very likely.'

Once both scores have been identified, they are multiplied giving the overall score at *untreated, current* and *target* levels.

The risk assessment matrix is summarised below, and a full copy included at Appendix B.



Categorisation

All risks, once identified, must be categorised into one of the recognised impact categories in order to understand the overall risk profile for the organisation. Categorisation of a risk is based upon the impact score, with the impact category which has the highest scoring criteria for that particular risk determining the risk category.

For example, a risk scoring a 3 for impact in Patient Experience but scoring a 5 in Finance will categorise that risk as Finance overall. Risk categories are outlined in the risk assessment matrix:

- Patient Experience
- Objectives / Project
- Injury / Illness (physical and psychological) to patient / staff / visitors
- Complaints / claims
- Service / Business interruption
- Staffing and competence
- Financial (including damage / loss / theft / fraud)
- Inspection / audit
- Public Confidence

Where more than one category has the same impact score, select the category which has the lower risk appetite level. For example, if Patient Experience and Finance both score 5, but Patient Experience has an averse appetite but Finance has a cautious appetite, select Patient Experience. If both categories have the same risk appetite level, use professional judgement.

4.6. Step 5: Manage Risks

The purpose of this step is to select and implement the appropriate action to respond to the risk. There are four broad ways we can respond to risk, known as the 4 Ts:

- Tolerate: this is the decision to accept the risk at its current level (usually after treatment). The ability to do anything may be limited, or the cost of taking action may be disproportionate to the benefit gained. Generally, it is risks that are within appetite that are tolerated.

- Treat: this is the decision to retain the activity or process creating the risk and to take action to implement risk controls that reduce either the likelihood of the risk occurring or minimising the impact. Risks which are out of appetite or tolerance will have to be treated.
- Transfer: this is the decision to transfer the impact of the risk either in full, or in part, to a third party. The most common form of risk transfer is insurance.
- Terminate: this is the decision to stop doing the activity associated with the risk. This may not always be possible and may create risks elsewhere as a result.

Risk Controls

Risk controls are management measures put in place to effectively manage a risk to within acceptable levels (i.e. to target score range). It is essential that the controls put in place to manage a risk are effective. The identification of effective controls is the most important part of the whole risk management process as without this element we would simply be identifying risks and doing nothing to manage them.

To assess whether the controls we identify are or will be effective, it is important to consider the following:

- What do you already have in place to manage the cause and / or impact of the risk? e.g. policies, procedures, projects, training courses, business continuity plans etc
- Do they work and what evidence do you have of the effectiveness? A policy which is in place but never complied with is not an effective one.
- Are there any gaps in your controls?
- Do you have all the information that you need about this risk or do you need to find out more?
- What more should you do?
- If several activities are required to manage the risk, how will you prioritise these?
- Are these controls within the remit of your department? If not, you will need to liaise with stakeholders to ensure that appropriate controls are put in place.

If you implement the controls you have identified, will this manage the risk to within acceptable levels for that risk category? If the answer is no, further controls are required. There are two main types of control measure that can be put in place to manage a risk:

- *Preventative Controls:* These are mitigating actions which will work to control the cause of the risk and prevent it happening in the first place
- *Contingency Controls:* These are actions that can be put in place to reduce the impact of the risk if it does materialise. Contingency controls are often aligned to the business continuity plans of an organisation.

As an example, consider fire safety measures. Segregation of flammable materials and sources of ignition is a control which prevents the risk of fire. Smoke detectors, sprinkler systems and fire evacuation plans are contingency controls should the risk of fire materialise.

If a risk has been effectively analysed (see section 4.4), it will be much easier to identify appropriate preventative and/or contingency controls.

4.7. Monitor and Review

Risk Review

Once the process of identifying, analysing and assessing a risk are complete, it is imperative that it is subject to regular review. Ongoing management and review of a risk is the most important part of the process, as maintaining or reducing the risk score to within an acceptable level assures the overall management of the organisation's risk profile.

Required risk review timescales are outlined below:

Very High (20-25)	Monthly
High (10-16)	Monthly
Medium (4-9)	Quarterly
Low (1-3)	Quarterly

During a risk review, the risk score must be re-assessed. If it is identified that the risk continues to exist, the list of current controls and further controls required must be checked and added to where necessary. On the basis of progress with controls and an assessment of the risk environment (i.e. are there any significant changes to the internal/external context), a re-assessment of the current score must be made using the risk assessment matrix. This will show whether the risk is decreasing, increasing or remaining static. Depending on its escalation level, a change to risk score will be reported at the appropriate assurance committee.

Review of the Risk Management Process

In addition to review of the risks themselves, the Risk Management team also reviews the whole system of risk management – are the right risks being escalated at the right time? Are the tools we provide sufficient to allow staff to effectively identify, analyse, assess and manage their risks? This enables learning and improvement and ensures that risk management adds value to the organisation's activities.

Assurance

A fundamental component of any risk management framework is the expert and objective assessment of risk controls to ensure they are well designed and operate effectively. Implementing a process to critically review risk controls provides the Board with assurance on the effective management of key strategic risks. To facilitate the provision of assurance, NHS Forth Valley utilises the "three lines of defence" model.

Operating as the first line, operational management has ownership, responsibility and accountability for directly assessing, controlling and mitigating risks, understanding what the

key controls are, and how effectively and consistently those controls are operating, in order to provide assurance to the Board. The second line is provided by governance/compliance functions such as Risk Management, who will assist the first line in developing an approach to fulfilling their assurance responsibilities. Internal Audit forms the third line, (providing independent assurance, and checking that the risk management process and framework are effective and efficient).

The levels of assurance and associated system and control descriptors are shown below:

Overall Risk Assurance Assessment		
Level of Assurance	**System Adequacy**	**Controls**
Substantial Assurance	A sound system of governance, risk management and control, with internal controls operating effectively and being consistently applied to support the achievement of objectives.	Controls are applied continuously or with only minor lapses
Reasonable Assurance	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement identified which may put at risk the achievement of objectives.	Controls are applied frequently but with evidence of non-compliance
Limited Assurance	Significant gaps, weaknesses or non-compliance identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives.	Controls are applied but with some significant lapses
No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives.	Significant breakdown in the application of controls

Assurance should be provided to the relevant committees for their consideration on an ongoing basis. Any papers submitted as a source of assurance for the committee should explicitly reference the related strategic risk and should provide a conclusion as to whether performance indicates that controls are operating effectively and as intended. At the start of the year, assurance mapping principles will be used to determine the assurance requirements, and this will be set out in the committee assurance workplan. Assurance provision over the course of the financial year will be tracked and managed utilising the Pentana system.

Risks on the strategic risk register are subject to a rolling programme of 'deep dives' managed by the relevant assurance committee. Deep dive reviews are facilitated by the Risk Owner and Corporate Risk Manager and provide expert, objective assessment of the following key areas:

- Comparison of current risk score and target risk score
- Requirements to achieve the target risk score – success criteria for managing the risk
- Assessing the importance and effectiveness of implemented controls
- Assessing the proportionality of further controls required – i.e. will they help to achieve target score?
- Reviewing the assurance activity aligned to the risk controls in order to establish an overall assurance statement for the risk

Refer to Appendix C for guidance on risk controls assurance.

4.8. Communicate and Consult

Communication at all levels is important to allow for informed decision making, and provision of assurance that our risk profile is effectively managed – this is achieved through risk reporting.

Risk Reporting

A quarterly risk management report is presented to the Health Board which reports on our strategic risks. In addition, Assurance Committees are provided with a regular risk management report on strategic and organisational risks assigned to their area of scrutiny.

The Executive Leadership Team acts as the Risk Management Steering Group and provides recommendations to the Board on the status of strategic level risks. Directorates and Departments are expected to carry out regular review, monitoring and reporting on their risk registers (supported by the risk management function) to ensure that risks are identified and escalated to the appropriate level at an early stage.

The risk management reporting in place includes a range of risk management KPIs and trend analysis that enhances oversight and assurance for the Health Board. An annual report on risk management is also produced for the Health Board.

The Health and Social Care Integration Schemes for both Falkirk Integration Joint Board (IJB) and Clackmannanshire and Stirling IJB, detail the requirements and responsibilities regarding Risk Management for the IJBs and constituent parties. The IJBs will establish a Risk Management Strategy including a risk monitoring framework. Risks to delegated services which are identified will require to be communicated across partner organisations with clear responsibilities, ownership and timescales, and with mechanisms to ensure that assurance can be provided to the relevant Boards. Risk specialists from all parties will work together to ensure that Risk Management strategies are aligned to facilitate effective escalation of risks and provision of assurance.

APPENDIX A: GLOSSARY

Assurance. Stakeholder confidence in our service gained from evidence showing that risk is well managed, achieved by risk owners and leads confirming that significant risks are being adequately managed, that critical controls have been identified, implemented and are effective.

Contingency. An action or arrangement that can be implemented to minimise impact and ensure continuity of service when things go wrong.

Current Risk Score: The risk score identified taking into account any controls that are currently in place to manage the risk.

Governance. The system by which organisations are directed and controlled to achieve objectives and meet the necessary standards of accountability, probity and openness in all areas of governance.

Internal Control. Corporate governance arrangements designed to manage the risk of failure to meet objectives.

Issue: Something that has happened and is currently affecting the organisation in some way and needs to be actively dealt with and resolved.

Likelihood. Used as a general description of probability or frequency which can be expressed quantitatively or qualitatively.

Risk: An uncertain event, or set of events, which, should it occur, will have an effect on the organisation's ability to achieve its objectives.

Risk Appetite. The level of risk that an organisation is prepared to accept in pursuit of its objectives.

Risk Architecture: All of the Risk Management arrangements within an organisation – sets out lines of communication and reporting, delegation and roles / responsibilities.

Risk Assessment. The scoring of a risk to allow prioritisation. Determining the likelihood and impact of a risk.

Risk Champion: The person / role with responsibility within an individual department or business area for maintaining lines of communication with the Risk Management team, administering the risk register and co-ordinating all risk activities.

Risk Control: Management measures put in place to effectively manage a risk to within an acceptable level. Can be preventative or contingency in nature and will reduce the likelihood or impact of consequence.

Risk Culture: The reflection of the overall attitude of every part of management of an organisation towards risk.

Risk Target Score: An acceptable level of risk based on the category of risk and risk appetite.

Risk Escalation. The process of delegating upward, ultimately to the Board, responsibility for the management of a risk deemed to be impossible or impractical to manage locally.

Risk Lead: The person / role responsible for managing a risk on a day-to-day basis, assessing the risk score and updating the management plan, reviewing the risk on a regular basis.

Risk Management: The integrated approach (culture, processes, structures) to the identification, analysis, control and monitoring of risk.

Risk Management Policy: Statement outlining the objectives of the risk management practices within the organisation.

Risk Management Strategy**:** Sets out the basis for the principles, processes and approaches to risk management to be followed in order to achieve a consistent and effective application of risk management and allow it to be embedded into all core processes.

Risk Matrix: A scoring mechanism used to identify the severity of a risk, using a multiplication of likelihood and impact, across pre-set categories.

Risk Maturity: The level of risk management capability within an organisation.

Risk Owner: The person / role with accountability for ensuring the effective management of a risk

Risk Register: A tool used to capture and monitor risks. Includes all information required about that particular risk and is intended to be used both as a management tool and conduit for risk reporting.

Risk Tolerance. The maximum level of risk the organisation can tolerate regarding each type of risk before the organisation is significantly impacted.

Threat: A negative scenario which could give rise to risks.

Untreated Risk Score: The risk score identified by assessing the risk with no controls, mitigation or contingency plans in place.

APPENDIX B: RISK ASSESSMENT MATRIX

Impact – What could happen if the risk occurred? Assess for each category and use the highest score identified.

The impact scale is from an organisational level perspective. It reflects the key areas that if impacted could prevent the organisation achieving its priorities and objectives. The scale is a guide and cannot cover every type of impact therefore judgement is required.

Category	Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
Patient Experience	Reduced quality patient experience/clinical outcome not directly related to delivery of clinical care	Unsatisfactory patient experience/clinical outcome directly related to care provision – readily resolvable	Unsatisfactory patient experience/ clinical outcome, short term effects – expect recovery less than 1wk Increased level of care/stay less than 7 days	Unsatisfactory patient experience /clinical outcome, long term effects - expect recovery over more than 1week Increased level of care/stay 7 -15 days	Unsatisfactory patient experience/clinical outcome, continued ongoing long term effects
Objectives/ Project	Barely noticeable reduction in scope/quality/schedule	Minor reduction in scope/quality/ schedule	Reduction in scope/quality/project objectives or schedule	Significant project over-run	Inability to meet project/corporate objectives, reputation of the organisation seriously damaged
Health and Safety (Injury /illness (physical and psychological) to patient/visitor/staff)	Adverse event leading to minor injury not requiring first aid No staff absence	Minor injury or illness, first aid treatment required Up to 3 days staff absence	Agency reportable, e.g. Police (violent and aggressive acts) Significant injury requiring medical	Major injuries/long term incapacity /disability (e.g. loss of limb), requiring, medical treatment and/or counselling	Incident leading to death(s) or major permanent incapacity

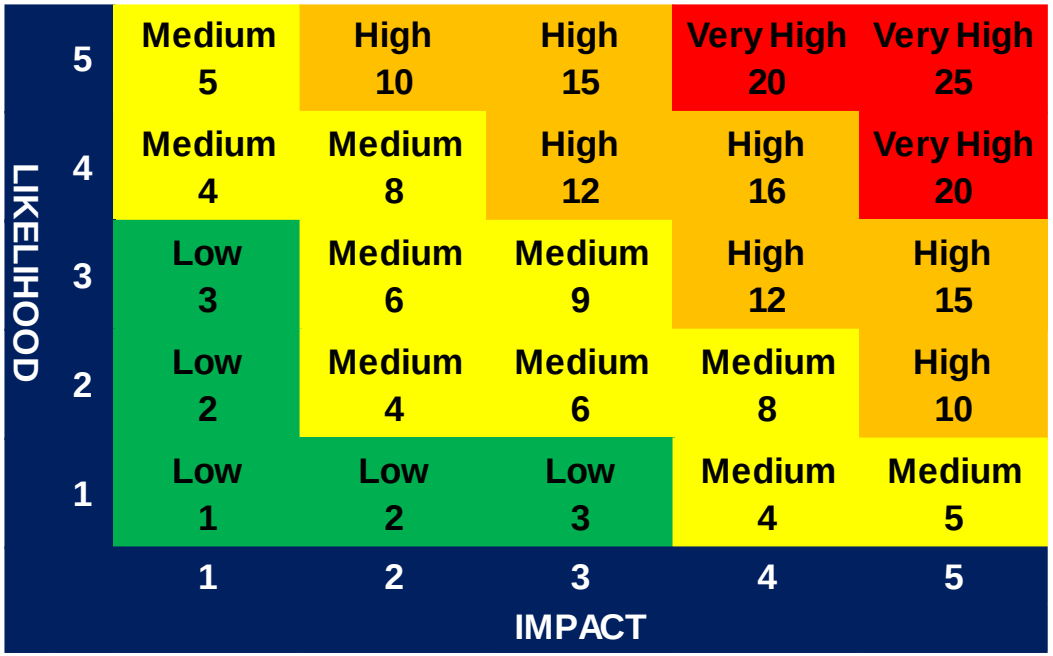
			treatment and/or counselling RIDDOR over 7- day absence due to injury/dangerous occurrences	RIDDOR over 7- day absence due to major injury/dangerous occurrences	
Complaints/Claims	Locally resolved verbal complaint	Justified written complaint peripheral to clinical care	Below excess claim. Justified complaint involving lack of appropriate care	Claim above excess level. Multiple justified complaints	Multiple claims or single major claim Complex Justified complaint
Service/ Business Interruption	Interruption in a service which does not impact on the delivery of patient care or the ability to continue to provide service	Short term disruption to service with minor impact on patient care/service provision	Some disruption in service with unacceptable impact on patient care Temporary loss of ability to provide service Resources stretched Potentially impaired operating capability Pressure on service provision	Sustained loss of service which has serious impact on delivery of patient care resulting in major contingency plans being invoked Potentially impaired operating capability Temp service closure	Permanent loss of core service/ facility Disruption to facility leading to significant "knock on" effect -- Inability to function
Staffing and Competence	Short term low staffing level temporarily reduces service quality (less than 1 day) Short term low staffing level (>1 day), where	Ongoing low staffing level reduces service quality Minor error due to lack of/ ineffective training/	Late delivery of key objective/service /care due to lack of staff Moderate error due to lack of/ ineffective training /	Uncertain delivery of key objective/service/care due to lack of staff Major error due to lack of/ ineffective training /	Non-delivery of key objective/ service/care due to lack of staff. Loss of key staff Critical error due to lack of/ ineffective

	there is no disruption to patient care	implementation of training	implementation of training Ongoing problems with staffing levels	implementation of training	training/ implementation of training
Financial (including Damage/Loss/Theft / Fraud	Negligible organisational/ personal financial loss up to £100k	Minor organisational/ personal financial loss of £100k - £250K	Significant organisational/personal financial loss of £250k - £500k	Major organisational/personal financial loss of £500k - £1m	Severe organisational financial loss of more than £1m
Inspection/ Audit	Small number of recommendations which focus on minor quality improvement issues	Recommendations made which can be addressed by low level of management action	Challenging recommendations that can be addressed with appropriate action plan Improvement Notice	Enforcement/prohibition action Low Rating Critical report	Prosecution Zero rating Severely critical report
Public Confidence	Rumours, no media coverage Little effect on staff morale	Local media coverage – short term Some public embarrassment Minor effect on staff morale/public attitudes	Local media - long-term adverse publicity Significant effect on staff morale/public perception of the organisation Local MSP/SEHD interest	National media adverse publicity less than 3 days Public confidence in the organisation undermined Use of services affected	National/International media/ adverse publicity, more than 3 days MSP/MP/SEHD concern (Questions in Parliament) Court Enforcement/Public Enquiry/FAI

Likelihood – What is the likelihood of the risk occurring? Assess using the criteria below.

Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Almost Certain (5)
It is assessed that the risk is very unlikely to ever happen.	**It is assessed that the risk is not likely to happen.**	**It is assessed that the risk may happen.**	**It is assessed that the risk is likely to happen.**	**It is assessed that the risk is very likely to happen.**
Will only occur in exceptional circumstances	**Unlikely to occur but potential exists**	**Reasonable chance of occurring - has happened before on occasions**	**Likely to occur - strong possibility**	**The event will occur in most circumstances**

Risk Assessment Table – Multiply likelihood score by impact score to determine the risk rating (score).



Review Timescales – When a risk rating has been assigned the criteria below should be used to assess the review timescales.

Very High or High	Requires monthly monitoring and updates.
Medium	Requires quarterly monitoring and updates.
Low	Requires quarterly monitoring and updates.

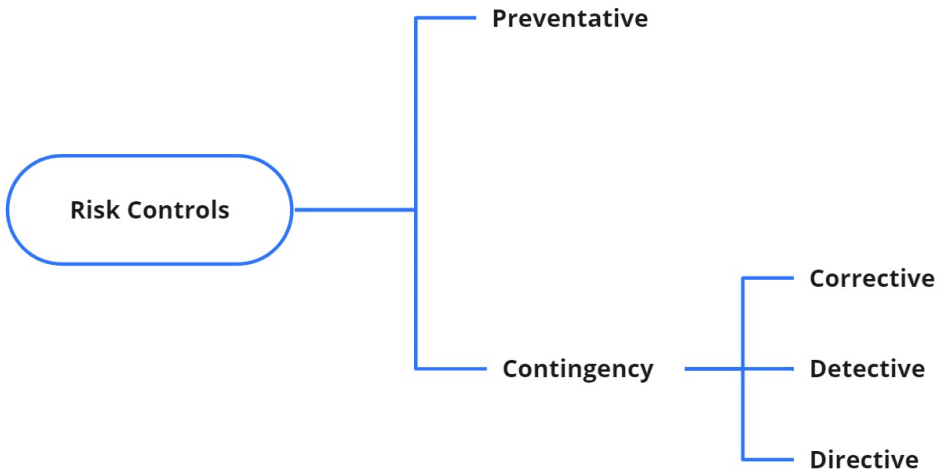
APPENDIX C: RISK CONTROLS ASSURANCE GUIDANCE – NHS Forth Valley

Risk Controls Assurance Guidance – NHS Forth Valley

Overall Risk Assurance Assessment		
Level of Assurance	**System Adequacy**	**Controls**
Substantial Assurance	A sound system of governance, risk management and control, with internal controls operating effectively and being consistently applied to support the achievement of objectives.	Controls are applied continuously or with only minor lapses
Reasonable Assurance	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement identified which may put at risk the achievement of objectives.	Controls are applied frequently but with evidence of non-compliance
Limited Assurance	Significant gaps, weaknesses or non-compliance identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives.	Controls are applied but with some significant lapses
No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives.	Significant breakdown in the application of controls

Control Types		
Type	**Description**	**Examples**
Preventative	Activity to control the underlying risk cause and prevent it happening in the first place	• Removal / substitution of a hazard • Employee vetting / checks • Segregation of duties / authorisation levels to reduce fraud • Restricting access to assets (physical / information) • Password protection • Policies, standards, processes for planning

Contingency (Reactive)	Corrective – limits the scope for loss, reduced undesirable outcomes Directive – direct activity to ensure a particular outcome is achieved Detective – designed to identify occasions when undesirable outcomes have been realised	• Policies, standards, processes to provide direction as to steps required in a certain situation • Budget review / reconciliation process • Performance review – budget-to-actual comparison to identify variance, Key Risk Indicators • Reporting • Inventories • Business Continuity / Disaster Recovery Plans • Whistleblowing / Fraud Detection



Risk Control Effectiveness Assessment	
Effectiveness Score	**Description**
Fully effective: 100% Review and monitor existing controls	Nothing more to be done except review and monitor the existing control. Control is well designed for the risk, and addresses root causes. Management believes it is effective and reliable at all times. Full compliance with statutory requirements, comprehensive procedures in place, no other controls necessary, ongoing monitoring only

	Control is likely to be of a preventative nature (for example, prevents the risk from occurring) and be systematic or automatic (for example, electronic banking authorisation process)
Mostly Effective: 80-99% Most controls are designed correctly and are in place and effective.	Control is designed correctly and largely in place, effective and regularly reviewed. Some more work to be done to improve operating effectiveness or management has doubts about operational effectiveness and reliability. Control is likely to be of a preventative nature (for example, prevents the risk from occurring) but may not be automated and require manual intervention / review
Partially effective: 50-79% Some controls poorly designed or not effective	While the design of control may be largely correct in that it treats the root of the risk, it is not currently very effective. **or** While it operates effectively, the control does not seem correctly designed in that it does not treat root causes. Reasonable compliance with statutory requirements established, some preventative measures in place, controls can be improved Control is likely to be either reactive (for example, business continuity plan) or of a deterrent nature (for example corporate policy, training) and as such would not be considered as effective as a purely preventative control
Not effective: <50% Significant control gaps due to poor control design or very limited operational effectiveness	Significant control gaps. Either control does not treat root causes or does not operate at all effectively. Virtually no credible control. Management has no confidence that any degree of control is being achieved due to poor control design or very limited operational effectiveness Insufficient control, weak procedures, limited attempt made to implement preventative measures Control is either not in place or not working as intended

Effectiveness of Controls – Questions to Ask:

- Do the controls in place already work – have they prevented the risk materialising or mitigated its effects?
- Are there any gaps in controls?
- Is further information required about the cause and impact of the risk in order to design and implement appropriate controls?
- If several controls are required for mitigation, how are they prioritised?

- Are there any dependencies or critical points of failure in implementing the controls?
- Will planned controls be sufficient to bring the risk to target score?

Risk Control Criticality Assessment	
Control Rating	**Description**
Low Importance	The control is of negligible importance in effectively mitigating the risk. Failure of the control will not result in an increase in the likelihood or impact of the risk.
Moderately Important	The control is of moderate importance in effectively mitigating the risk. Failure of the control will result in an increase in the likelihood or impact of the risk, but the risk score will remain within appetite.
Important	The control is important in effectively mitigating the risk. Failure of the control will result in an increase in the likelihood and impact of the risk beyond risk appetite, but within tolerance. Additional controls will be required to mitigate the risk if this control cannot be executed.
Very Important	The control is very important in effectively mitigating the risk. Failure of the control will result in an increase in the likelihood and impact of the risk beyond risk appetite and tolerance. Significant additional controls will be required to mitigate the risk if this control cannot be executed.
Absolutely Critical	The risk control is an essential component of the mitigation plan for the risk. If the control is not in place and working effectively the risk cannot be successfully mitigated to within risk appetite or tolerance.

1st Line of Defence: The function that owns and manages the risk

Under the first line of assurance, operational management has ownership, responsibility and accountability for directly assessing, controlling and mitigating risks.

2nd Line of Defence: Functions that oversee or specialise in risk management, compliance and governance

The second line of assurance consists of activities covered by several components of internal governance (compliance, risk management, quality, IT and other control departments). This line of defence monitors and facilitates the implementation of effective risk management practices by operational management and assists risk owner in reporting adequate risk related information up and down the organisation.

3rd Line of Defence: Functions that provide independent assurance – e.g. Internal and External Audit

Internal audit forms the organisation's third line of assurance. An independent internal audit function will, through a risk based approach to its work, provide assurance to the organisation's board of directors and senior management. This assurance will cover how effectively the

organisation assesses and manages its risks and will include assurance on the effectiveness of the first and second lines of defence. It encompasses all elements of an institution's risk management framework (from risk identification, risk assessment and response, to communication of risk related information) and all categories of organisational objectives: strategic, ethical, operational, reporting and compliance.

Examples of Assurance Activity

- Training
- Policies and Procedures
- Communication, Consultation and Information
- Executive Management / Assurance Committee Oversight
- Management Review and Reporting (1st Line of Defence)
- Independent Review (2nd Line of Defence) – e.g. internal compliance functions such as Finance, Legal, Risk Management, Procurement, Information Governance, Infection Control, Emergency Planning / Resilience etc etc
- Internal and External Audit (3rd Line of Defence)