CLACKMANNANSHIRE AND STIRLING INTEGRATION JOINT BOARD

Risk Management Strategy

Date of First Issue	31/03/2016
Approved On	
Approved By	Clackmannanshire and Stirling Integration Joint Board
Review Date (by)	30/06/2025
Version	5.0
Author / Contact	Vicky Webb, Corporate Risk Manager, NHS Forth Valley Ewan Murray, Chief Finance Officer

Approved at August 2024 IJB

Contents

1. Introduction

Risk Management is an integral part to a good system of internal control, supporting and developing day-to-day management of services. This Strategy sets out the principles and approaches to risk management which are to be followed in Clackmannanshire & Stirling Integrated Joint Board (CSIJB). The primary aim of this is to achieve a consistent and effective implementation of risk management, ensuring provision of safe and effective care for patients and clients.

1.1. What is a Risk?

A risk can be defined as 'the effect of uncertainty on objectives' (ISO31000). It is any uncertain event which can have an impact upon the achievement of an organisation's objectives. A risk can have either positive or negative connotations which is frequently described as threats or opportunities. Therefore, risks can either stop achievement of objectives or can create opportunities to better meet objectives.

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. However, we should consider whether identified issues impact on the risks currently identified, or indeed create new risks.

It is important that decision makers are "risk aware" rather than "risk averse," meaning that risk is not a bad thing and does not need to be avoided – it will be almost impossible for a public sector organisation to be completely risk averse. Therefore, risk should be considered, deliberated and, incorporated into decision making processes to allow for efficient and effective risk taking.

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 overall 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 and helping avert high profile failures.
- Empowering all staff to make sound judgements and decisions concerning the management of risk and risk taking – fostering the "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.
- Supporting public confidence in the Integration Joint Board.

Effective risk management will be achieved by:

- Clearly defining roles, responsibilities, and governance arrangements.
- Incorporating risk management in all Senior Management, Integration Joint Board and Assurance Committee reports and when taking decisions.
- Maintaining risk registers that are linked to the IJB's Strategic Plans or delivery of delegated services.
- 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.
- Establishing communication channels which support sharing of risk information through all areas of the IJB.
- Monitoring and reviewing risk management arrangements on a regular basis.
- Seeking assurance that controls relied on to mitigate risks are effective.
- Developing a positive risk culture through the principles of Leadership, Involvement, Learning, Accountability and Communication, and by ensuring that all relevant partner Risk Management Strategies are consistent with their organisation's values.

1.4 Risk Classification

There are many types of risks that will be discussed and considered when implementing a Risk Strategy. Below is a list of some of these types of risks that will be faced and incorporated into the overall risk strategy.

Strategic Risks

Strategic Risks represent the potential for the IJB to achieve (opportunity) or fail to meet (threat) its desired outcomes and objectives as set out within their Strategic Plans. Typically these risks will be long term and require strategic leadership in the development of activities and application of controls to manage the risk.

Risk identification for the Strategic Risk Register is facilitated through annual horizon scanning involving the Board and the SLT, alongside the review of the IJB Strategic Plan, and review of the risk section of board papers to assess whether amendment or addition to the Strategic Risk Register is required.

Risks are not automatically escalated/de-escalated from lower-level risk registers to the Strategic Risk Register. If a risk increases in severity to the extent that it requires strategic leadership/management and Board oversight, then the risk should be re-framed to reflect that and added as a new Strategic Risk. If an existing Strategic Risk decreases in severity and no longer requires strategic leadership/management or Board oversight, then consideration should be given to closing the risk, and creating relevant operational risks. For example, the UK's exit from the European Union created Strategic Risk. As mitigation plans progressed and the UK formally left the EU, the risk no longer needed the strategic oversight, but there were pockets of residual Operational Risks, for example in relation to impacts on supply chains.

Operational Risks

Operational Risks represent the potential for impact within or arising from the operational services delivered by the Health and Social Care Partnership (HSCP), as commissioned through the Strategic Commissioning Plan and Directions by the IJB.   These risks will be managed within the respective risk management frameworks of the Local Authority and the Health Board, through integrated management teams, with relevant risk specialists working together to ensure consistent practice, and that the respective Risk Management strategies are aligned.

Clinical Risks

Clinical Risks represent the risk of harm or negative consequences to a patient or service user, or capability of causing an adverse event. It is the degree to which a foreseeable harm (risk) can be managed by an individual practitioner and requires that person to have an open duty of care for an individual. It is closely aligned to safe staffing, levels of competence and compliance with professional standards of practice.

Project Risks

Project Risks represent the risks to the delivery of a project to time, budget, and specification. These will be managed by the appropriate working group or Project Board and/or Transformation Board which oversees all projects and programmes of work.

1.5 Partnership Risk Management Arrangements

In order to ensure strong risk management partnership arrangements, it will be necessary to agree how some 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 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 HSCPs Senior Leadership Team for approval for inclusion on the Strategic Risk Register.

2. Risk Architecture

This section details the arrangements for communication, governance, reporting, roles and responsibilities regarding risk management, forming 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 the activities of the Integration Joint Board.

Risks, once identified, will be captured on risk registers (which may be managed using a Risk Management Information System such as Pentana). Each service team/specialty will hold a risk register, with risks owned by Heads of Service/Service Senior Management Teams. This forms the bottom layer of the risk register hierarchy.

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, to the groups/committees who require the information for direction of action and/or assurance purposes. The following questions should be asked when deciding whether to escalate a risk:

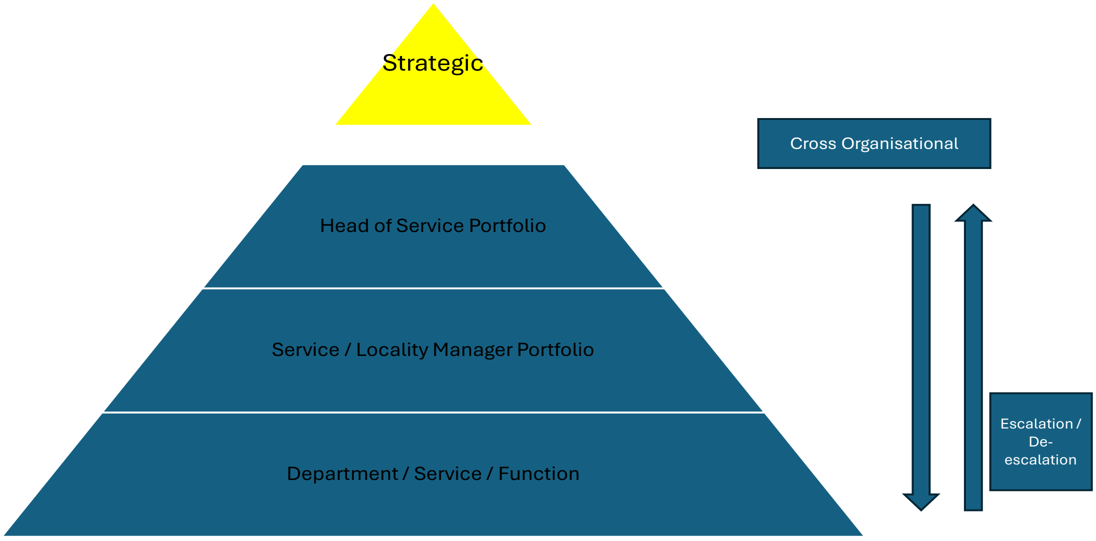
- Does the risk present a significant threat to the achievement of Government objectives and/or standards?
- Is the risk score assessed to be intolerable or beyond the IJB's risk appetite?
- Does the risk have a widespread impact beyond a local area, e.g. does it affect multiple Service Teams, or does it have dependencies on multiple Service Teams/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. 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.

When a risk is escalated, the ownership of the risk will also escalate to the relevant member of the HSCP Senior Leadership Team.

The process is summarised in the Diagram 1 below:

Diagram 1 - Risk Register Hierarchy

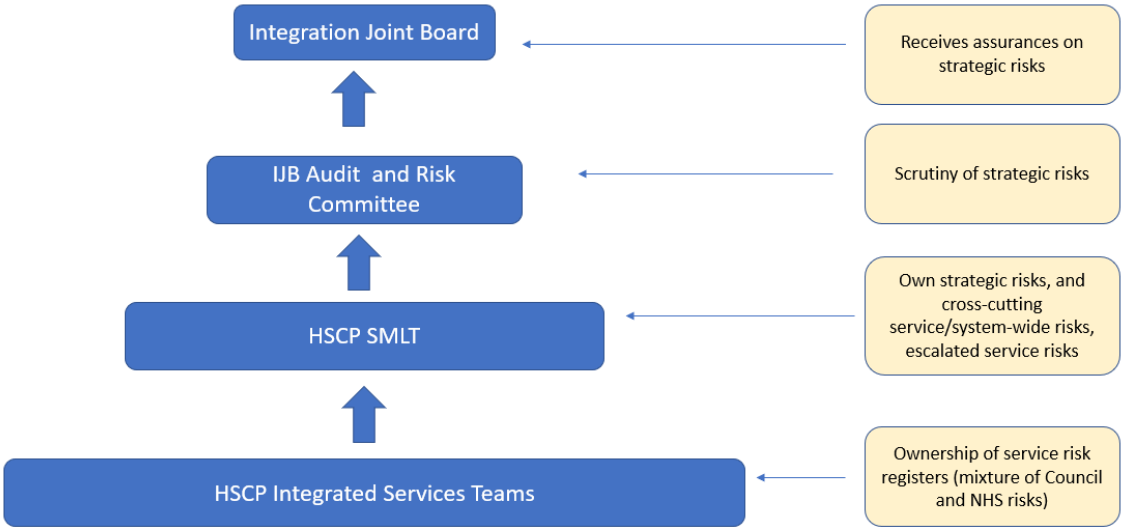

Strategic
Head of Service Portfolio
Service / Locality Manager Portfolio
Department / Service / Function
Cross Organisational
Escalation / De-escalation

2.1. Governance & Reporting

The Clackmannanshire & Stirling IJB is corporately responsible for the Risk Management Strategy and for ensuring that significant risks are adequately controlled. To support the Board in the implementation of the Strategy, the Audit & Risk Committee have a key role in scrutinising the Strategic Risks and monitoring the implementation of the Risk Architecture.

Diagram 2 illustrates CSIJB's risk management governance structure.

Diagram 2: Risk Management Governance Structure


Integration Joint Board
IJB Audit and Risk Committee
HSCP SMLT
HSCP Integrated Services Teams
Receives assurances on strategic risks
Scrutiny of strategic risks
Own strategic risks, and cross-cutting service/system-wide risks, escalated service risks
Ownership of service risk registers (mixture of Council and NHS risks)

2.2. Roles & Responsibilities

Risk Management Roles and Responsibilities
Integration Joint Boards and/or delegated Committee
Members of the Integration Joint Board, including as members of the appropriate delegated Committee are responsible for: • Oversight of the IJBs risk management arrangements including seeking assurance that these are effective. • Receipt, review and scrutiny of reports on Strategic Risks and any key Operational Risks that require to be brought to the IJBs attention. • Ensuring that all IJB Board and Committee papers adequately explain associated risks and overtly refer to the IJB Risk Register where relevant. • Ensuring that the Chief Officer implements and monitors mitigating actions and reports progress. • Approval of IJB's Risk Appetite.
Chief Officer
The Chief Officer has overall responsibility for: • Ensuring the IJB has a risk management and assurance framework in place. • Ensuring that suitable and effective arrangements are in place to manage the risks relating to the functions within the scope of the IJB. • Keeping the Chief Executives of the IJB partner bodies (Council and Health) informed of any significant existing or emerging risks that could seriously impact the IJB's ability to deliver the outcomes of their Strategic Plans, and vice versa; and • Production of a Risk Management Annual Report.
Chief Finance Officer
On behalf of the Chief Officer, the Chief Finance Officer will be responsible for: • Ensuring risks are identified and mitigating actions identified for the consideration of the IJB and delegated Committees as appropriate. • Supporting, including deputising as appropriate, for the Chief Officer in discharging the responsibilities set out above.
IJB Audit & Risk Committee
The Audit & Risk Committee's purpose (with regard to Risk Management) is to: • Ensure existence of and compliance with an appropriate Risk Management strategy. • Reviewing risk management arrangements. • Receiving regular risk management updates and reports, including an annual report which confirms that the risk management arrangements were adequate and effective throughout the year.

- Scrutiny of the Strategic Risk Register
- Provision of advice on Strategic Risks to the IJBs including Risk Appetite and Tolerance

HSCP Senior Leadership and Management Team

Members of the Senior Leadership & Management Team are responsible (either collectively, or by nominating a specific member of the team) for:

- Supporting the Chief Officer in fulfilling their risk management responsibilities
- Arranging professional risk management support, guidance, and training from partner bodies.
- Ownership of Strategic Risks.
- Receipt and review of regular risk reports and assurances on strategic, shared key Operational Risks and escalating any matters of concern to the IJB; and
- Ensuring that the processes outlined in this strategy are actively promoted across their teams and within their areas of responsibility.

Risk Owners

Risk Owners are those accountable for ensuring the effective management of a risk, and providing assurance that key controls are operating effectively. For Strategic Risks and escalated Operational Risks, this will be the relevant member of the HSCP SLT.

Risk Leads

Risk Leads are responsible for managing a risk on a day-to-day basis. Risk leads are likely to be those with management or supervision duties, and are responsible for:

- Clearly defining and articulating risks, and effectively analysed to identify the causes and impacts of the risk.
- Assessing the risk score for probability and impact using the risk assessment matrix.
- Formulating a management plan with controls which are proportionate to the level of risk and that are effectively applied in practice.
- Recording the details using the relevant risk management system.
- Reviewing the risk on a regular basis, considering any changes in context, and considering the impact of controls on the scoring of the risk; and
- Identifying sources and levels of assurance regarding control effectiveness, to allow risk owners to provide assurance.

Chief Social Work Officer (CSWO)

The Chief Social Work Officer (CSWO)'s responsibilities are set out in the Clinical and Care Governance Framework (Approved March 2024).

The role of the CSWOs is to provide professional advice on the provision of social work services. The principal functions relate to governance, management of risk, protection and the deprivation of liberty.

Other Persons with a Professional and/or Statutory Role/Other Specialists
• Designated Officers responsibilities in relation to provision of assurance and promotion of good governance, including Risk Management activities, should ensure that they discharge their risk management responsibilities in line with their job descriptions, and relevant legislation and Professional Standards. • Relevant specialists from partner bodies should attend meetings as necessary to provide advice, including risk officer, clinical and non-clinical advisors and health and safety advisors
Risk Champion
• The person/role with responsibility within an individual department or business are for maintaining lines of communication with the various risk professionals, administering the risk register and co-ordinating risk activities.
All Persons Working In Services Which are to be Integrated (per Annex 1 Part 2 and Annex 2 Part 2 of the Integration Scheme)
Risk Management should be integrated into daily activities with everyone involved in identifying risks related to their working practices and service areas. Everyone is therefore required to: • Understand the risks related to their roles and activities. • Understand how their actions relate to their own safety, and that of their patients, service users/clients and the wider public. • Understand their accountability for particular risks and how they can manage them. • Feed into the provision of assurance by the Risk Leads. • Understand the importance of reporting incidents and/or near misses to allow lessons to be learned and contribute to ongoing improvement of risk management arrangements; and • Understand that good risk management is a key part of the IJB's culture.

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 or Organisational/System-wide Risk Register

- Clackmannanshire and/or Stirling Councils Strategic Risk Register
- Clackmannanshire and Stirling IJB Strategic Risk Register
- Falkirk IJB Strategic Risk Register

Any such emerging risks will be discussed by the appropriate parties to ensure inclusion on the appropriate 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 which will help assist determining the target score range for Strategic Risks. 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 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 risk 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 (as decisions will be based on the risk appetite of the IJB)
- allows further prioritisation of risk as areas of risk will be prioritised based on the appetite of the IJB.

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 which the IJB will use. 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 IJBs. 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:

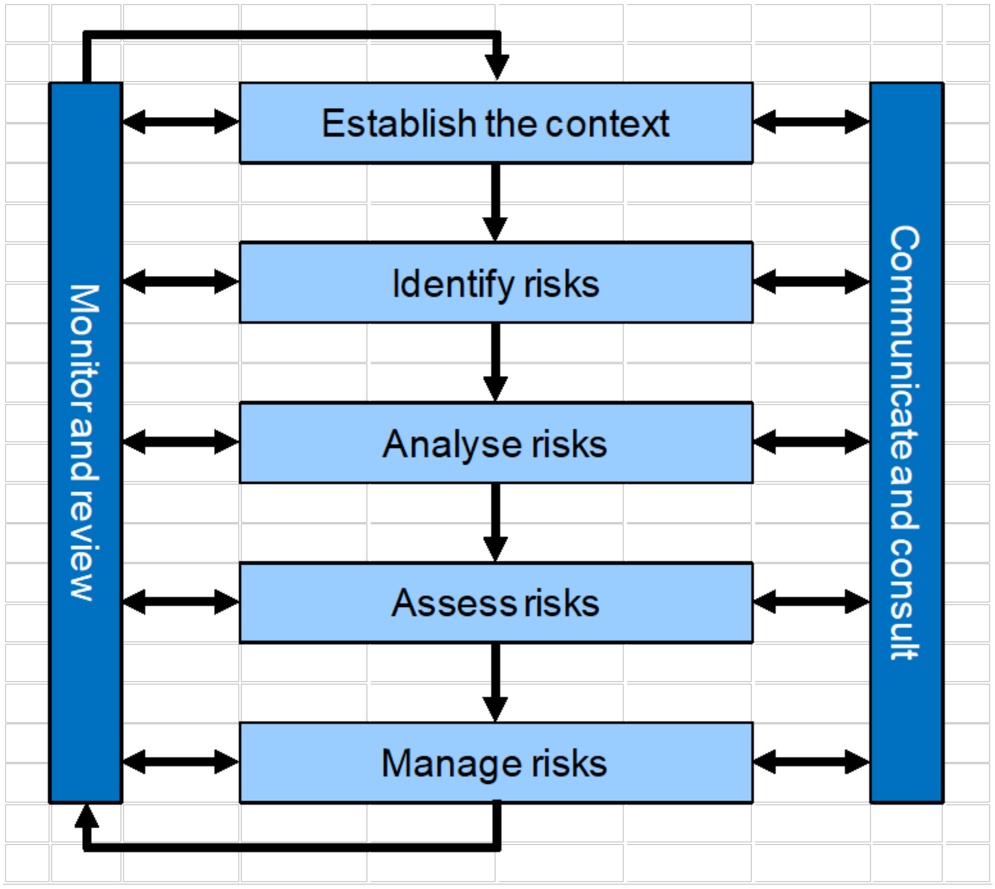
- Acceptance that risk must be more actively taken in the pursuit of transformation or that a high level of risk must be tolerated.

- 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.

The appetite statements for CSIJB can be found in Appendix B – Risk Appetite Statements

4.0 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. 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:

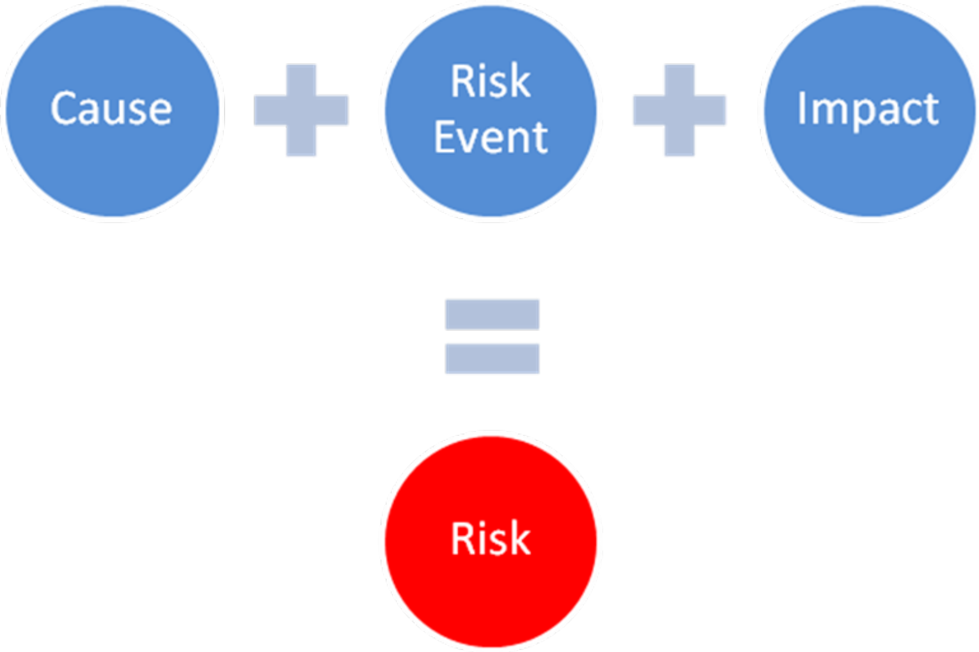
Focused Identification Methods	Other Identification Opportunities
• Risk Identification Workshops • Risk Questionnaires • Review & refresh of existing risk registers • Interviews	• Horizon scanning • Board meetings / working groups / management meetings • Audit & scrutiny reports • Performance data • 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 uncertain 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 external funding and continued uncertainty over our cost base there is a risk that C&S IJB 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 “reasonable 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 and 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 the IJB 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

It has been agreed that staff within the IJB/HSCP will utilise the NHS Forth Valley Risk Assessment Matrix (RAM) to support consistency in the risk assessments.

The RAM 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 RAM is summarised below, and a full copy included at Appendix C.

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 Harm
- Patient Experience
- Transformation/Innovation
- Health and Safety
- Service Delivery / Business interruption
- Workforce
- Financial
- Inspection / Audit
- Public Confidence
- Health Inequalities
- Environmental Sustainability / Climate Change

Where more than one category has the same impact score, select the most appropriate and relevant option for the risk.

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 range assures the overall management of the organisation’s risk profile.

Required risk review timescales are outlined below:

Very High (20-25)	Monthly
High (12-16)	Bi-monthly
Medium (8-10)	Bi-monthly
Low (1-6)	Bi-annually

These are the minimum review timescales – if there are changes in the operating environment which could affect the severity of a risk, it can be reviewed and reported more frequently.

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, and whether the risk requires escalation. Depending on its escalation level, a change to risk score will be reported at the appropriate committee.

Review of the Risk Management Process

In addition to review of the risks themselves by risk leads/owners, the risk management lead from the IJB (currently the Chief Financial Officer) will review the whole system of risk management on behalf of the Chief Officer, supported by partner agency risk leads. This review will consider:

- 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. This activity will align with the production of the Annual Report and review of risk appetite statements and will be subject to approval by the Audit Committee.

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

The IJB Strategic Risk Register is reviewed and updated by the HSCP Senior Leadership Team (SLT) and Audit Committee on a quarterly basis and is presented to the IJB bi-annually.

The Senior Leadership Team acts as the Risk Management Steering Group and provides recommendations to the IJB Audit Committee and the Board on the status of strategic level risks. HSCP Integrated Services Teams and Specialist Groups are expected to carry out regular review, monitoring and reporting on their risk registers (supported by the relevant risk management function) to ensure that risks are identified and escalated to the appropriate level at an early stage.

An annual report on risk management is also produced for the IJB detailing the overview of the risk profile of the organisation, and the overall implementation of the Risk Strategy.

Risks to delegated services which are hosted by one organisation on behalf of both IJBs 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.

4.9 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, the “three lines of defence” model is utilised. Further guidance on controls assurance can be found in Appendix D – Controls Assurance Guidance.

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, 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	Robust framework of key controls ensure objectives are likely to be achieved.	Controls are applied continuously or with only minor lapses.
Reasonable Assurance	Adequate framework of key controls with minor weaknesses present.	Controls are applied frequently but with evidence of non-compliance.
Limited Assurance	Satisfactory framework of key controls but with significant weaknesses evident which are likely to undermine the achievement of objectives.	Controls are applied but with some significant lapses.
No Assurance	High risk of objectives not being achieved due to the absence of key internal controls.	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 ‘Focused Reviews’ considered by the relevant committee. Focused Reviews are facilitated by the Risk Owner/Lead 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 to establish an overall assurance statement for the risk.

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.

5 Training, Learning and Development

A key part of developing a positive risk management culture across the activities under the direction of the IJBs, in support of improving the overall risk maturity, is the delivery of risk management training.

The HSCP Senior Management and Leadership Team will carry out a training needs analysis to identify risk management training and development needs, and source the required training and development opportunities through respective partner bodies.

Risk Management training will be delivered using resources already available to the IJB through partner body risk management functions.

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 are for maintaining lines of communication with the various risk professionals, administering the risk register and co-ordinating 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 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 APPETITE STATEMENTS

Impact Category	Appetite Statement	Tolerance Statement
Patient/Service User Harm	Any injury, illness or loss of life as a result of CSIJB failing to comply with Health and Safety obligations would be unacceptable. Therefore, there is an **AVERSE APPETITE** for risks that may compromise the Health and Safety of patients, staff, visitors and public and others accessing services/venues where the HSCP delivers services. There is no tolerance, but we recognise that on some occasions we will have to accept risks that have been reduced as low as reasonably practicable.	There is no tolerance for this type of risk.
Transformation/Innovation	We will have a **MODERATE APPETITE** accepting that a greater degree of risk is required to maximise innovation and opportunities to improve patient experiences and outcomes, transform services and ensure value for money.	We will operate with an **OPEN TOLERANCE for Transformation/Innovation** to allow the scoping of innovation projects to provide the detail of the case for change. This would be for a defined period while all potential delivery options are considered. Once in the initiation and planning stage for the innovation project to be implemented, the appropriate appetite level would be reconsidered in line with organisational process for initiating a new project.

Workforce	CSIJB will operate with a **CAUTIOUS APPETITE,** to support staff to innovate and improve their workplace, balancing the risk against the reward to be gained from the significant staff knowledge and experience which is available. This will be for a defined period while mitigation plans are implemented. The priority will remain adherence to professional standards, and staff should continue to work within the limits of their competence, exercise "duty of candour" and raise concerns when they come across situations that put patients or public at risk.	There is no tolerance for this type of risk.
Financial	One of CSIJB's strategic aim is high quality and sustainable services. We wish to achieve financial sustainability by spending well and making the most of our resources. Therefore, we have a **CAUTIOUS APPETITE** for Financial risk as budgets are constrained and unplanned / unmanaged budget variance could affect our ability to achieve statutory financial targets, potentially increases reputational risk and places pressure on divisions and departments. Well informed risks can be taken but budget variances are to be minimised and VFM is the primary concern.	We will operate with a **MODERATE TOLERANCE** for a defined period while mitigation plans are implemented. We are prepared to accept the possibility of limited unplanned / unmanaged budget variance. VFM is the primary concern but we are willing to consider other benefits for a limited budget variance.
Compliance	CSIJB has a complex regulatory and legislative framework to operate within. There are many mandatory obligations that need to be met by the IJB. Therefore, the appetite for Compliance risks is **AVERSE**. We are not prepared to take any risk when discussing our regulatory compliance.	CSIJB has a **CAUTIOUS TOLERANCE** for risks impacting on Compliance. We are prepared to take informed risks which could result in recommendations, improvement notices or criticism, provided that the benefit outweighs the negative outcome.
Public Confidence	CSIJB has a **CAUTIOUS APPETITE** for risks impacting on public confidence which flow from informed decision-making, in order that achievement of strategic objectives is not hindered.	We are prepared to operate within a **MODERATE TOLERANCE** range for Public Confidence for a defined period while mitigation plans are being actively developed.

APPENDIX C: RISK ASSESSMENT MATRIX

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

Category	Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
Patient Harm *(through delivery or omission of care, risk results in unintended/unexpected but avoidable physical or psychological harm to a patient)*	Adverse event Negligible effect on patient	Minor episode of harm not requiring intervention	Harm which requires intervention but doesn't trigger organisational Duty of Candour response	Harm, such as sensory, motor, or intellectual impairment which has lasted or is likely to last at least 28 days OR Pain or psychological harm which lasts, or is likely to last, at least 28 days And triggers organisational Duty of Candour	Severe harm such as death or permanent disability, either physical or psychological (e.g., removal of wrong limb/organ or brain damage) And triggers organisational Duty of Candour
Patient Experience *(risk could impact on how a patient, their family or carer feels during the process of receiving care)*	Reduced quality patient experience Locally resolved verbal complaint or observations	Unsatisfactory patient experience directly related to care provision – readily resolvable Justified written complaint peripheral to clinical care	Unsatisfactory patient experience/clinical outcome with potential for short term effects Justified written complaint involving lack of appropriate care Themes emerging – readily or locally resolvable	Unsatisfactory patient experience /clinical outcome with potential for long-term effects Multiple justified complaints Serious problem themes emerging, informed from more than one source	Unsatisfactory patient experience/clinical outcome, continued ongoing long term effects Complex Justified complaints Confirmed serious problem themes from more than one source Involvement of Scottish Public Services Ombudsman
Transformation/Innovation *(risk could impact on ability to successfully adapt and transform)*	Barely noticeable reduction in scope/quality/ schedule Negligible impact on achievement of intended benefits	Minor reduction in scope/quality/ schedule Minor impact on achievement of intended benefits	Reduction in scope/quality/project/programme objectives or schedule Some intended benefits will not be achieved	Significant project/programme over-run Significant proportion of intended benefits will not be achieved	Failure to deliver project/programme Failure to achieve sustainable transformation

Health and Safety *(risk could impact on staff/public, or a patient out with delivery of care)*	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 treatment and/or counselling RIDDOR over 7- day absence due to injury/dangerous occurrences	Major injuries/long term incapacity /disability (e.g., loss of limb), requiring, medical treatment and/or counselling RIDDOR over 7- day absence due to major injury/dangerous occurrences.	Incident leading to death(s) or major permanent incapacity RIDDOR Reportable/FAI
Service Delivery/ Business Interruption *(risk could impact on ability to efficiently and effectively deliver services)*	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/ quality of service provision	Some disruption in service with unacceptable impact on patient care Resources stretched Prolonged pressure on service provision	Sustained loss of service which has serious impact on delivery of patient care Contingency Plans invoked Temporary service closure	Permanent loss of core service/ facility Major Contingency Plans invoked Disruption to facility leading to significant “knock on” effect Inability to function as an organisation
Workforce *(risk could impact on staff wellbeing, staffing levels and competency)*	Negligible impact on staff wellbeing Temporary reduction in staffing levels/skills mix Individual training/competency issues	Minor impact on wellbeing, requires peer support Short-term reduction in staffing levels/skills mix (<6 months) Small number of staff unable to carry out training or maintain competency levels Increased usage of supplementary staff	Moderate impact on staff wellbeing, requires line manager support Medium-term reduction in staffing levels/skills mix (>6 months) Moderate number of staff unable to carry out training or maintain competency levels Reliance on supplementary staff in some areas	Serious impact on staff wellbeing, requires referral to support services Long-term reduction in staffing levels/skills mix (>9 months) Significant number of staff unable to carry out training or maintain competency levels Reliance on supplementary staff in multiple areas	Critical impact on staff wellbeing, co-ordinated response and referral to support services Loss of key/high volumes of staff Critical training and competency issues throughout the organisation Unsustainable reliance on supplementary staff across organisation.
Financial *(risk could impact through unplanned cost/reduced income/loss/non-achievement of intended benefit of investment)*	Some adverse financial impact but not sufficient to affect the ability of the service /department to operate within its annual budget	Adverse financial impact affecting the ability of **one or more** services/ departments to operate within their annual budget	Significant adverse financial impact affecting the ability of **one or more** directorates to operate within their annual budget	Significant adverse financial impact affecting the ability of the organisation to achieve its annual financial control total	Significant aggregated financial impact affecting the long-term financial sustainability of the organisation
Inspection/Audit	Small number of recommendations which	Recommendations made which can be addressed by	Challenging recommendations that can be addressed with appropriate action plan	Mandatory improvement required. Low rating. Critical report.	Threat of prosecution. Very low rating. Severely critical report.

(risk could impact on outcome during/after inspection by internal/external scrutiny bodies)	focus on minor quality improvement issues	low level of management action		High level action plan is necessary	Board level action plan required
Public Confidence *(risk could impact on public/stakeholder trust and confidence, and affect organisation's reputation)*	Some discussion but no impact on public confidence No formal complaints or concerns	Some concerns from individuals, local community groups and media – short-term Some impact on public confidence Minor impact public perception and confidence in the organisation	Ongoing concerns raised by individuals, local media, local communities, and their representatives - long-term Significant effect on public perception of the organisation	Concerns raised by national organisations/scrutiny bodies and short-term national media coverage Public confidence in the organisation undermined Use of services affected	Prolonged national/international concerns and media coverage Issues raised in parliament Legal Action/ /Public Enquiry/FAI/Formal Investigations Critical impact on staff, public and stakeholder confidence in the organisation
Health Inequalities **(***risk could increase health inequalities, particularly those that are healthcare generated)*	Negligible impact on health inequalities such as morbidity/mortality and healthy life expectancy No impact on services	Minor impact on health inequalities such as morbidity/mortality and healthy life expectancy Some services experience increased pressures	Moderate impact on health inequalities such as morbidity/mortality and healthy life expectancy Causes short term increased pressures across the system	Serious exacerbation of health inequalities such as morbidity/mortality and healthy life expectancy Causes long term pressures in system/affects ongoing viability of a service	Critical exacerbation of health inequalities such as morbidity/mortality and healthy life expectancy Affects whole system stability/sustainability
Environmental Sustainability / Climate Change *(risk could impact on environment, ability to comply with legislation/targets or environmentally sustainable care)*	Limited damage to environment, to a minimal area of low significance Negligible impact on ability to comply with climate legislation/targets or ability to reach net zero Negligible impact on ability to provide environmentally sustainable care	Minor effects on biological or physical environment Minor impact on ability to comply with climate legislation/targets or ability to reach net zero Minor impact on ability to provide environmentally sustainable care	Moderate short-term effects but not affecting eco-system Moderate impact on ability to comply with climate legislation/targets or ability to reach net zero Moderate impact on ability to provide environmentally sustainable care	Serious medium term environmental effects Serious impact on ability to comply with climate legislation/targets or ability to reach net zero Serious impact on ability to provide environmentally sustainable care	Very serious long term environmental impairment of eco-system Critical non-compliance with climate legislation/targets or ability to reach net zero Critical impact on ability to provide environmentally sustainable care

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).

LIKELIHOOD	5	Low 5	Medium 10	High 15	Very High 20	Very High 25
	4	Low 4	Medium 8	High 12	High 16	Very High 20
	3	Low 3	Low 6	Medium 9	High 12	High 15
	2	Low 2	Low 4	Low 6	Medium 8	Medium 10
	1	Low 1	Low 2	Low 3	Low 4	Low 5
		1	2	3	4	5
	IMPACT					

APPENDIX D: RISK CONTROLS ASSURANCE GUIDANCE

Risk Controls Assurance Guidance

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)