

DRAFT

Code of Corporate Governance

**SECTION E:
Integrated Risk Management Approach**

April 2011

Contents

1	Introduction
2	Purpose
3	Approach to risk management
4	Risk Register
4.1	How to identify a risk
4.2	How to assess a risk
	4.2.1 How to Establish likelihood
	4.2.2 How to assess impact
	4.2.3 Risk rating
4.3	How to respond to a risk
	4.3.1 Corrective action/mitigation
4.4	Review
	4.4.1 Escalation and reporting
5.	Roles and responsibilities
	5.1 Staff
	5.2 Operational Management (Risk Managers)
	5.3 Executive Directors/Senior Managers (Risk Owners)
	5.4 Governance Committees
	5.5 Audit Committee
	5.6 Healthcare Improvement Scotland Board
	5.7 Controls Assurance Manager
6.	Risk challenge
7.	Performance Management
8.	Internal controls assurance
9.	Learning and Development

Appendix 1: Organisational structure
Appendix 2: Risk assessment: impact/consequences definition
Appendix 3: Risk Registers data sets
Appendix 4: Risk Register template

Table 1: Risk category
Table 2: Likelihood definitions
Table 3: Impact descriptions
Table 4: Risk rating
Table 5: Risk challenge

1 Introduction

Risk can be defined as ‘...the chance of something happening that impacts on the organisation’s ability to achieve its objectives’. An organisation needs to proactively manage risk to an acceptable level by embedding processes focussed on assessment and prevention, rather than reaction and remedy. Risk management plays a vital role supporting and informing decision making in providing a safe and secure environment.

Implementation of a comprehensive, effective risk management approach throughout the organisation is a means of improving business activity. The processes described in this document can be used both to reduce negative impacts for the organisation and identify opportunities for improving outcomes.

The management of risk involves everyone to ensure the process is embedded into the organisation’s everyday activity

2 Purpose

It is necessary to have a robust and consistent approach to the management of risk throughout the organisation that is aligned and prioritised to support the achievement of our strategic objectives. This approach should then provide assurance to the Board members and the Accountable Officer of the effectiveness of our risk control measures.

Many of the organisation’s existing practices and processes already include elements of risk management. The integrated approach consolidates these elements in order to:

- provide a consistent approach to risk management
- demonstrate how risk management is integrated into our strategic planning, operational and day to day activities
- ensure that risk management is embedded in the decisions we make
- clarify roles and responsibilities in the risk management process
- continuously improve our risk management approach and the quality of risk information we hold
- provide a framework which will give assurance to the Board and stakeholders of our ability to deliver our strategic objectives.

3 Approach to risk management

Risk management proactively reduces identified risks to an acceptable level by creating robust systems for assessment and prevention, rather than reaction and remedy. It plays a vital part in informing decision making and supporting a culture of quality improvement within an organisation. A risk management system is based on a systematic process of:

- identification
- assessment
- response
- review

4 Risk register

The risk register is a tool which will be used to record and manage the organisation's risks. The full detail of the key information, electronically recorded, on the register is provided below and in **Appendix 3 and 4**. Additional guidance on completion is provided in the **online User Guide**.

The risk register has been designed to allow risks to be recorded consistently across the organisation and directs users to the key information required to record and manage risk.

4.1 How to identify a risk

In order to manage risk, the organisation needs to know what risks it faces, and how to evaluate them. Identifying risks is the first step in building the organisation's risk profile. Maintaining a record is critical to effective risk management. The identification of risk can be separated into two distinct phases.

- initial risk identification
- ongoing risk identification, for example, to identify new risks which did not previously arise or changes in existing risks.

All organisation risks link to the strategic objectives. A statement of a risk should encompass both the possible cause and the impact to the strategic objectives.

All members of staff have a role to play in identifying risks. Risks can be identified from a number of sources including:

- planning and performance management
- review of significant changes in our service
- internal and external audit
- changes to guidance / guidelines
- legal or regulatory reviews
- horizon scanning
- incident processes
- Health and Safety at Work
- business cases and project plans
- training needs analysis
- recruitment / retention / absenteeism data

Identifying risks will promote a continuous flow of information. The key areas for risk have been categorised under the 9 headings below. The categorisation of risk will provide a focus to support the effective management of risk within the governance structure (**see Appendix 1**).

Table 1: Risk Category

Risk category	Description
Patient Experience	Risks which impact on patient experience and /or clinical outcome.
Objectives / Project	Risks which impact on the ability to meet project/programmes objectives.
Injury (physical and psychological) to patient, visitor or staff	Risks which lead to incidents or adverse events that could cause injury.
Complaints / claims	Risks which could result in serious complaints or claims against the organisation.
Service / Business Interruption	Risks which could impact on the organisation's ability to undertake it's core business
Staffing and competence	Risks which impact on the implementation of staff governance.
Financial (including damage / loss / fraud)	Risks which impact on financial and operational performance.
Inspection / Audit	Risks which could lead to critical reports, enforcement or prosecution.
Adverse Publicity / reputation	Risks which have an impact on the reputation of the organisation.

It is important to give a clear description of the risks that have been identified and the potential impacts on the organisation should they occur. This will allow the risk to be more easily understood and more effectively managed.

Through this identification and categorisation process a **Risk Owner** and **Risk Manager** should be identified. A risk owner, in line with their accountability for managing the risk, should have sufficient authority to ensure that it is effectively managed. The risk owner and manager may be different people. Risk Owners should ensure that the risk is escalated where necessary to the appropriate level of management in line with **Section 4.4.1**.

4.2 How to assess a risk

Risk can be assessed as the combination of the **likelihood** of an event occurring and the **impact** of that event. Establishing how we assess likelihood and impact is key to determining the risk level and subsequent actions to be taken.

4.2.1 How to establish likelihood

The likelihood of an event occurring should be assessed using the table below. Having assessed the likelihood of the event happening you should determine the likelihood score (1 to 5).

Table 2: Likelihood definitions

Score	Description	Chance of occurrence
1	Rare	Very little evidence to assume this event would happen – will only happen in exceptional circumstances
2	Unlikely	Not expected to happen, but definite potential exists – unlikely to occur.
3	Possible	May occur occasionally, has happened before on occasions – reasonable chance of occurring
4	Likely	Strong possibility that this could occur – likely to occur
5	Almost certain	This is expected to occur frequently / in most circumstances – more likely to occur than not

4.2.2 How to assess impact

The impact on the organisation of an event happening should be assessed using the criteria outlined below. Further detail is provided in **Appendix 2**.

Table 3: Impact descriptions

Score	Description	Risk Category		<i>Continued – see Appendix 2</i>
		Patient Experience	Objectives/ Project	
1	Negligible	Reduced quality of patient experience/clinical outcome not directly related to delivery of clinical care	Barely noticeable reduction in scope, quality or schedule.	
2	Minor	Unsatisfactory patient experience/ clinical outcome directly related to care provision – readily resolvable.	Minor reduction in scope, quality or schedule.	
3	Moderate	Unsatisfactory patient experience/ clinical outcome; short term effects – expect recovery <1wk.	Reduction in scope or quality of project; project objectives or schedule.	
4	Major	Unsatisfactory patient experience/ clinical outcome; long term effects – expect recovery >1wk.	Significant project over-run.	
5	Extreme	Unsatisfactory patient experience/ clinical outcome; continued ongoing long term effects	Inability to meet project objectives; reputation of the organisation seriously damaged.	

4.2.3 Risk rating

The risk rating is assessed by multiplying together the **likelihood** and **impact scores**. Risk will then be classified as Red, Amber or Green (High, Medium or Low Risk) based on the Table 4 below. The score achieved determines the response of the organisation in relation to the risk as outlined in the key below.

Table 4: Risk rating

			IMPACT				
			Negligible	Minor	Moderate	Major	Extreme
LIKELIHOOD		Score	1	2	3	4	5
	Almost certain	5	5	10	15	20	25
	Likely	4	4	8	12	16	20
	Possible	3	3	6	9	12	15
	Unlikely	2	2	4	6	8	10
	Rare	1	1	2	3	4	5

Key:

Risk Level	Combined Score	Response
High	15-25	Poses a serious threat. Requires immediate action to reduce / mitigate the risk
Medium	5-12	Poses a threat and should be pro-actively managed to reduce / mitigate the risk
Low	1-4	Poses a low threat and should continue to be monitored

4.3 Response

The response to an identified risk will be based upon what resources the organisation has at its disposal to effectively manage the risk. Some common examples of how we may respond to risk are provide below:

- **tolerate:** for example, unavoidable risk or risk that has been assessed with a low impact and/or likelihood score, or
- **treat:** for risks that their impact and/or likelihood can be managed effectively

When the response to the risk has been agreed the corrective action / mitigation should be included within the appropriate risk register (**See Appendix 4**).

4.3.1 Corrective action/mitigation

The corrective action/mitigation section of the risk register is where the risk owner records the actions to be taken and the controls to be adopted to manage/treat the risk. The narrative within this section should include:

- the actions to be taken and the risk they address
- the timescale for implementation and

- any resource/budget requirements

This section of the risk register should be regularly updated (in line with reporting requirements) to provide details of progress against the planned actions. The risk owner should clearly state which actions have been taken to arrive at the current assessment and which actions are still to be implemented.

4.4 Review

The management of risk should be continuously reviewed to monitor whether or not the risk profile is changing, to gain assurance that risk management is effective and to identify when further action is necessary to deliver assurance on the effectiveness of control. In addition, the overall risk management process will be part of the annual internal audit planning process to provide assurance that it remains appropriate and effective.

Organisationally, the Audit Committee, with support from the other standing committees of the Board and Executive Team, will review the risk management arrangements and risk registers every 2 months.

At all levels within the organisation the risks of undertaking individual/team business or activities should be considered. Where there is potential for impact upon the strategic objectives this should be communicated and reported through the defined reporting / escalation channels (Appendix 2 and 3).

4.4.1 Escalation and reporting

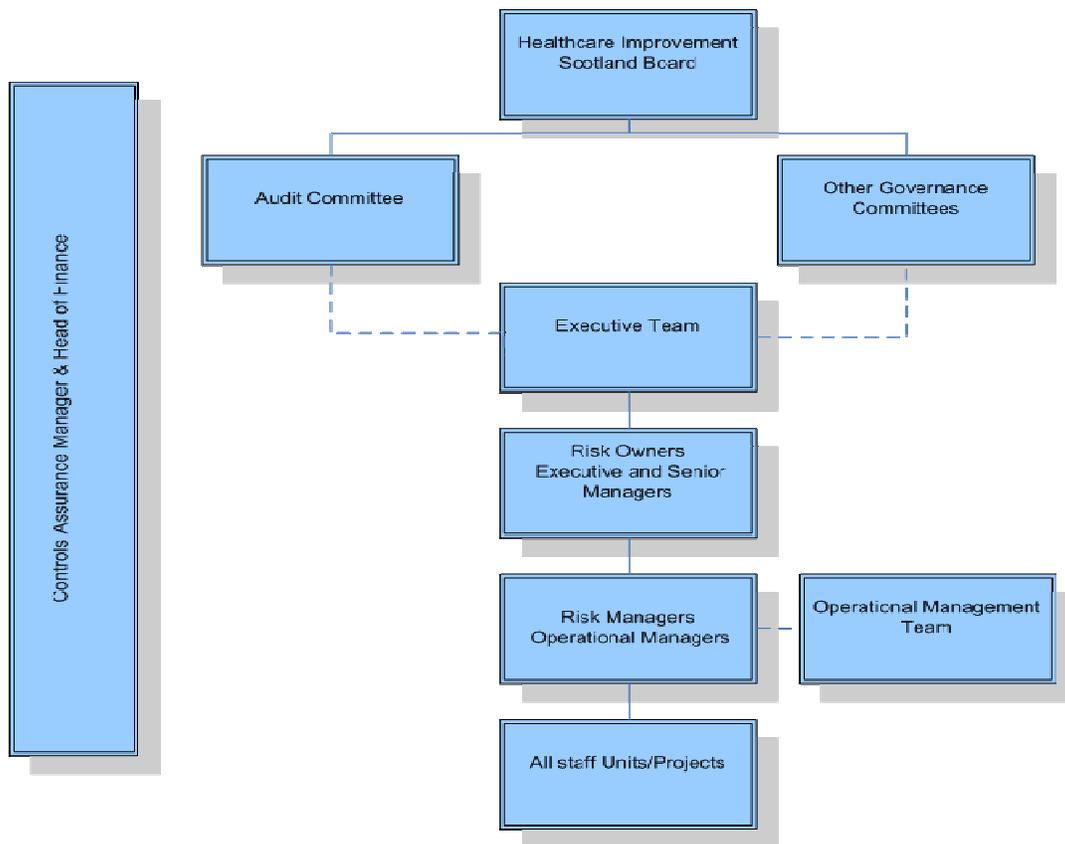
Within the organisation, risk registers should exist for specific projects, programmes and day to day business-as-usual activities. When risks have been identified that could have an impact on fulfilling the strategic objectives of the organisation, for example, medium to high risks, they should be escalated to the appropriate level within the organisation (and to external stakeholders where necessary).

Through the electronic recording system, risk owners will be notified immediately when a new or existing risk has been identified as medium or high. It is the risk owner's responsibility to ensure this risk is managed effectively and that the Executive Team and/or Governance Committees are made aware. The corporate risk register will include risks that are deemed significant enough to have an impact on the organisation as a whole. The corporate risk register will be presented to the Board on a 3 monthly basis.

Reporting structure and Escalation Process

There should be active escalation through the risk management reporting structure shown in the table below.

All staff have a responsibility to identify, record, monitor and review risks. The management of risk should be reported and reviewed, through the structure illustrated below on a regular basis and in line with identified timescales (for an individual risk). Formal risk reports (a collation of risk registers) will be provided to the Board, Governance Committees and Executive Team and will occur at least on a quarterly basis



It is expected that Risk Managers will report to Risk Owners at least on a monthly basis. The Controls Assurance Manager will provide support to produce regular reports. Further information is provided in Section 5 below.

5 Roles and responsibilities

The responsibility for risk management lies with all members of staff, with the Chief Executive, having overall responsibility for ensuring effective risk management in the organisation. The Scottish Executive issued HDL (2002) 11 'Corporate Governance: Statement on Internal Control' – in March 2002 which requires Chief Executives of NHS Bodies as Accountable Officers to sign a Statement on Internal Control (SIC) as part of the annual accounts. The SIC describes the effectiveness of the system of internal control; it is not restricted to internal financial controls and considers all aspects of the organisation's system of internal control including clinical governance, staff governance and risk management.

5.1 Staff

All staff have a responsibility to report events, incidents or accidents and to consider the risks that could impact on their particular area of work. This responsibility, by supporting the approach to risk management outlined in this document and should include:

- identifying, recording, monitoring and reviewing risks associated within their particular area of work

- ensuring actions are taken to manage the risks, including development of contingency plans and
- escalating and reporting risks

5.2 Operational Managers (Risk Managers)

Operational Managers will be assigned responsibility to areas of risk management from Risk Owners within their areas of business. The corresponding risk register should be discussed and shared at the Operational Management Team (OMT) meeting to support knowledge sharing and raise awareness. It is important that there is regular liaison and communication with the Executive Team, particularly where identified risks overlap different areas of work.

5.3 Executive Director / Senior Management (Risk Owners)

Executive Directors / Senior Management of the organisation are responsible for ensuring that risk registers are maintained and reviewed, and that appropriate risk management strategies and practices are adopted within their areas of responsibilities.

Named individuals will be assigned to manage specific areas of risk and become **Risk Owners**. This role will include:

- managing all aspects of the risk(s), including identifying a **Risk Manager**
- determining and/or authorising the actions needed to mitigate risk
- ensuring that risks assigned to them are kept up to date
- regular liaison and communication with operational management team

5.4 Governance Committees

The Governance committees to the Healthcare Improvement Scotland Board should review all associated organisational risks associated with their area of business at least on a 2 monthly basis. The committees are responsible for challenging the relevant risk reports and advise where necessary.

5.5 Audit committee

As well as reviewing and challenging the risks reported to the committee the Audit Committee has responsibility to review the effectiveness of the risk management system within the organisation. The Head of Finance with the Controls assurance manager will provide 2 monthly reports.

Continuous monitoring and review of the effectiveness of the risk management arrangements will be undertaken using a range of methods including:

- internal and external audit reports

- adherence to risk structures and processes
- review of risk registers and levels of risk
- reporting of corporate risk

5.6 Healthcare Improvement Scotland Board

The Board will receive the Corporate Risk Register on a 3 monthly basis for review and assurance.

5.7 Controls Assurance Manager

The Controls Assurance Manager is responsible for leading on the integrated approach to risk management within the organisation. This includes:

- management and coordination of the processes required to support the approach to risk
- supporting internal controls reviews
- provide support and advice to management and staff
- ensuring training is provided for staff where required
- preparing risk reports for all levels of the organisation

6 Risk challenge

The Governance Committees will review and challenge the relevant Risk Register reports as outlined below. In addition, the Audit Committee will review the effectiveness of the organisational Risk Management arrangements.

Table 5 – Risk Challenge

Committee	Risks reported and reviewed	Content of Risk Register presented	Frequency
Scottish Health Council	Healthcare Improvement Scotland Risk Register SHC Risk Register	As risk reviewed (See Appendix 4)	2 monthly
Finance and performance committee	Healthcare Improvement Scotland Risk Register All red and new amber business risks	As risk reviewed (See Appendix 4)	2 monthly
Evidence, Scrutiny and Improvement Committee	Healthcare Improvement Scotland Risk Register All red and new amber clinical risks	As risk reviewed (See Appendix 4)	2 monthly
Staff Governance Committee	Healthcare Improvement Scotland Risk Register All red and new amber staff risks	As risk reviewed (See Appendix 4)	2 monthly
Audit Committee	Healthcare Improvement Scotland Risk Register All red and new amber reputational risks	As risk reviewed (See Appendix 4) Update paper describing the development and effectiveness of internal control environment for risk management	2 monthly
Board	Healthcare Improvement Scotland Risk Register All Red Any issues which have arisen and whether risk register worked properly All urgent and important risks and issues	Summary	3 monthly or as required

7 Performance Management

The role of risk management is not just to simply detect and address threats to the organisation but also to enhance reputation and improve performance. In order to achieve this we need to have clarity within performance management about the priorities within our core areas of business and an ability to determine how success will be measured. Performance management sets the context in which risks will be evaluated and managed within the organisation. Risk management should therefore be included within the performance reports and be an integral part of planning and performance processes.

8 Internal Controls Assurance

To support the delivery of strategic, business or project objectives, the organisation should understand the key processes and controls which need to be in place to minimise risk, deliver consistently high quality service and comply with relevant regulations, professional standards and internal policies and procedures.

These processes and controls need to be monitored, reviewed and challenged to identify where they are working well and also identify where controls are absent or need to be improved. This is in addition to the work that is undertaken by internal, external and service audit/inspection bodies. The absence of controls or weak controls could result in the organisation being exposed to risks.

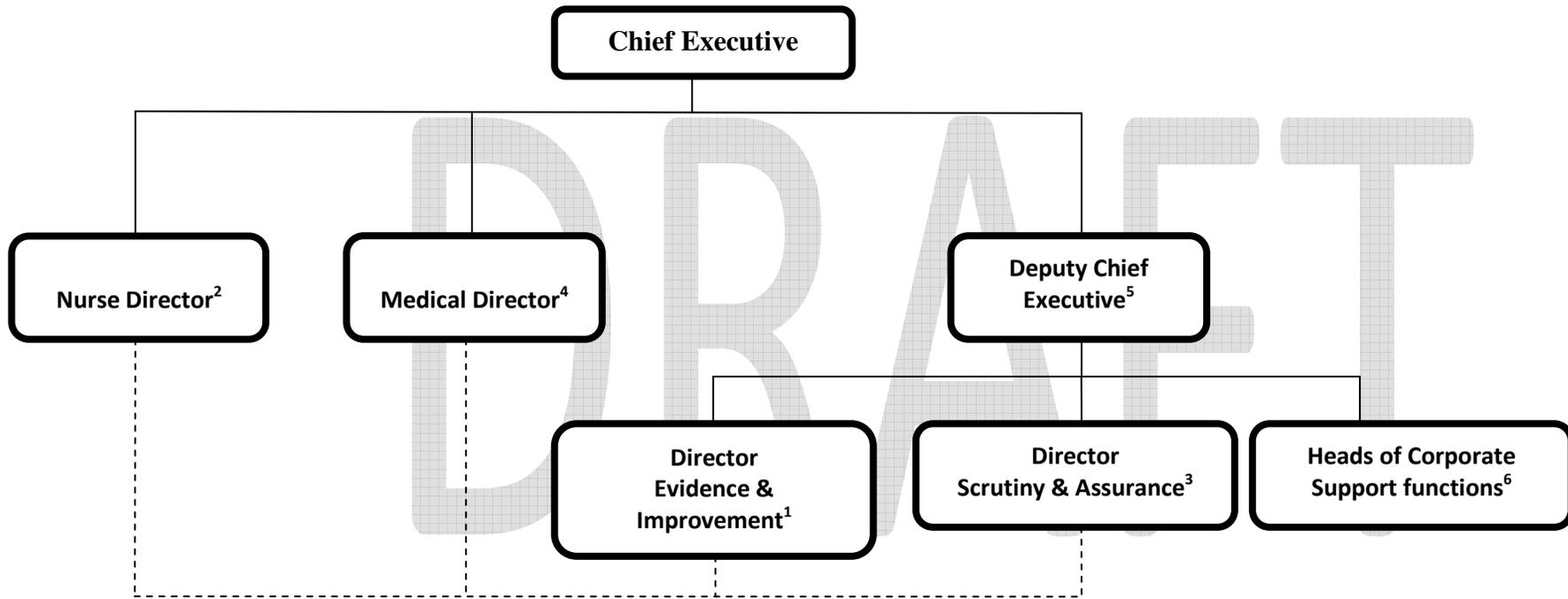
Many processes already exist for assessing controls and identifying risk throughout the organisation. These could for example include the planning mechanism for delivering operational objectives, ensuring regulatory requirements are maintained, internal and external audit reports, Incident reporting, Health and Safety requirements and so on.

The controls around core business delivery should be reviewed, assessed and improved where appropriate. Internal and external audit play a crucial role in the risk assessment process.

9 Learning and development

Effective risk management depends on all staff having a clear understanding of the subject and the contribution they can make to managing risk. Managers are responsible for ensuring that through Personal Development, of their staff they are enabled to identify learning needs and participate in appropriate risk management related activities.

Appendix 1 – Organisational Structure



Appendix 2 – Risk Assessment – Impact / Consequence Definitions

Descriptor	Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
Patient Experience	Reduced quality of 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 <1wk.	Unsatisfactory patient experience/ clinical outcome; long term effects – expect recovery >1wk.	Unsatisfactory patient experience/ clinical outcome; continued ongoing long term effects
Objectives / Project	Barely noticeable reduction in scope, quality or schedule.	Minor reduction in scope, quality or schedule.	Reduction in scope or quality of project; project objectives or schedule.	Significant project over-run.	Inability to meet project objectives; reputation of the organisation seriously damaged.
Injury (physical and psychological) to patient/visitor/ staff.	Adverse event leading to minor injury not requiring first aid.	Minor injury or illness, first aid treatment required.	Agency reportable, e.g. Police (violent and aggressive acts). Significant injury requiring medical treatment and/or counselling.	Major injuries/long term incapacity or disability (loss of limb) requiring medical treatment and/or counselling.	Incident leading to death or major permanent incapacity.
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.	Some disruption in service with unacceptable impact on patient care. Temporary loss of ability to provide service.	Sustained loss of service which has serious impact on delivery of patient care resulting in major contingency plans being invoked.	Permanent loss of core service or facility. Disruption to facility leading to significant “knock on” effect
Staffing and Competence	Short term low staffing level temporarily reduces service quality (< 1 day). Short term low staffing level (>1 day), where there is no disruption to patient care.	Ongoing low staffing level reduces service quality. Minor error due to ineffective training/implementation of training.	Late delivery of key objective / service due to lack of staff. Moderate error due to ineffective training/implementation of training. Ongoing problems with staffing levels.	Uncertain delivery of key objective/ service due to lack of staff. Major error due to ineffective training/ implementation of training.	Non-delivery of key objective/service due to lack of staff. Loss of key staff. Critical error due to ineffective training/ implementation of training.
Financial (including damage / loss / fraud)	Negligible organisational/ personal financial loss. (£<1k). (NB. Please adjust for context)	Minor organisational/personal financial loss (£1-10k).	Significant organisational/personal financial loss (£10-100k).	Major organisational/personal financial loss (£100k-1m).	Severe organisational/personal financial loss (£>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.	Enforcement action. Low rating. Critical report.	Prosecution. Zero rating. Severely critical report.
Adverse Publicity / Reputation	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 and public perception of the organisation.	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 concern (Questions in Parliament). Court Enforcement. Public Inquiry/ FAI.

Likelihood definitions

Descriptor	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Almost Certain (5)
Likelihood	Can't believe this event would happen – will only happen in exceptional circumstances.	Not expected to happen, but definite potential exists – unlikely to occur.	May occur occasionally, has happened before on occasions – reasonable chance of occurring.	Strong possibility that this could occur – likely to occur.	This is expected to occur frequently / in most circumstances – more likely to occur than not.

Risk Assessment Matrix (Impact/Consequence (table 1) x likelihood (table 2) = RISK GRADE)

		IMPACT				
		Negligible	Minor	Moderate	Major	Extreme
LIKELIHOOD	Score	1	2	3	4	5
	Almost certain	5	10	15	20	25
	Likely	4	8	12	16	20
	Possible	3	6	9	12	15
	Unlikely	2	4	6	8	10
	Rare	1	2	3	4	5

Key:

Risk Level	Combined Score	Response
High	15-25	Poses a serious threat. Requires immediate action to reduce / mitigate the risk
Medium	5-12	Poses a threat and should be pro-actively managed to reduce / mitigate the risk
Low	1-4	Poses a low threat and should continue to be monitored

Appendix 3 –Risk Registers Data Sets

The Risk Register is a tool for capturing important information about a risk or opportunity, and is a **continual process**. New risks will be identified, some will be terminated, control measures will need to be updated in response to changing internal and external events.

ID	Data Field	Description
1	ID	A unique identifier created for each new record
2	Management team	Indicates the Operational Management Team (area of business) that the risk originates from.
3	Date raised	The date that the risk was first identified and registered
4	Risk Owner	The lead person assigned with responsibility to ensure that the risk is adequately controlled and monitored.
5	Risk Manager	The lead person responsible to ensure the corrective actions (mitigation) happen.
5	Description	A statement of the nature of the risk, including how that risk might present itself and impact on the organisation (linked to organisational objective / imperatives).
6	Risk Level (at last review)	Level of risk based on the consequence and the likelihood (see Appendix 2)
7	Risk level (Current)	Level of risk based on the consequence and the likelihood (see Appendix 2)
8	Corrective Action (Mitigation)	A synopsis of the actions and controls necessary to improve the management of the identified risk (e.g. processes, policy, practices etc to minimise negative risk or enhance positive opportunities).
9	Response	<p>One of the following fields should be identified and described in the Corrective Action field above:</p> <p>Tolerate For example, the ability of an effective action against some risks may be limited or the cost of taking such action may be disproportionate to the potential benefits gained.</p> <p>Treat For example, introduce preventative actions to reduce the probability or impact if the risk occurs and maximise the potential for success. A Risk Level Target should be identified if this response is agreed (see below).</p> <p>Transfer Share the exposure, either totally or in part, with a partner or contractor, or through insurance. Any partnership will need to be carefully monitored as it may not be possible to transfer all risks and certain aspects may remain, such as loss of reputation.</p> <p>Terminate / Closed A decision is made not to undertake the activity that is likely to trigger the risk. Where the risks outweigh the possible benefits, terminate the risk by doing things differently and thereby removing the risk.</p>
10	Risk Level (Target)	The expected risk assessment (based on the consequence and the likelihood (see Appendix 2)) after any actions have been instigated.
11	Position of Risk / Register	Identify whether this Risk has/should be escalated (and verified) to be included within the Corporate Risk Register, Operational Business Risk Register or remain on the Unit / project Risk Register.

Appendix 4 – Risk Register Template

MANAGEMENT TEAM (Area of business -if applicable)Planning and Implementation Team

DATE: DD / MM/ YYYY

ID	Date Raised	Risk Description	Risk Owner	Risk Manager	RISK LEVEL*			RESPONSE	
					At last review	Current Risk Level	Target Risk Level	Tolerate or Treat	Corrective Action (Mitigation)
1	1/1/11	There is insufficient capacity available to the programme team to deliver the objectives within the agreed timescales	MJA	PSR	High	Medium	Low	Treat	Delegation of specific actions to existing staff Territorial Board staff have been drawn in to support programme Programme Board will review capacity issues at monthly meetings

*See Risk Assessment Matrix