Risk			
Protocol for the Management of Risk			
Instr No		Contact	Brian Orpin
Version	4.0	Email	brian.orpin@nhs.net
Issue Date	27/04/2015	Telephone	0131 314 5360
Review Date	27/04/2016	Status	Issued

Change Control

Date	Version	Change	Owner
28/11/2014	3.0	Approved by Board	Board
14/04/2015	3.1	Modify risk topics	CD
27/04/2015	3.2	Update Job descriptions post AC	BPO
27/04/2015	4.0	Issued	BPO

Introduction

1. This Protocol is designed to detail the process for managing risk in terms of maintaining and up-dating the risk registers.

Document Framework

2. NHS Health Scotland has a Risk Policy in place which is available from the intranet. This document forms the operational instruction for the Management of Risk.

Risk Register Structure

3. NHS Health Scotland has a layered approach to the recording and management of risk. The three levels of risk registers are;

   a) Corporate Risk Register (CRR). This register records risks that might affect the organisation as a whole. It should have a few high level risks identified. This document should be published under our Freedom of Information (Scotland) Act Publication Scheme.

b) Master Risk Register (MRR). This register contains all the risks identified at a directorate level. These are collated to form an overall picture of risk within the organisation.

c) Project/Team Risk Registers. These registers are the registers held at a project or team level and contain significant detail.

Corporate Risk Register

4. The CRR has the following characteristics;

a) It should be available under FOISA.

b) It should list the key risks the organisation has.

c) It is owned by the Corporate Management Team (CMT) with individual directors nominated as the lead for each risk.

d) Each risk must have at least one corresponding entry in the MRR.

e) Risks are added or removed with the agreement of CMT.

f) Risks may be added to the CRR as a result of Horizon Scanning (top down) or by a risk in the MRR being identified as requiring escalation to the CRR (bottom up).

g) The CRR is published on the corporate website and is refreshed at least yearly.

h) It is structured by Risk Topic.

Master Risk Register

5. The MRR has the following characteristics;

a) Each risk in the MRR is allocated to and owned by a Directorate.

b) Each risk must have an identified Risk Owner and Controls Owner.

c) A risk in the MRR can be identified as being related to a risk in the CRR.

d) The structure of the MRR is detailed at Annex A.

e) The MRR will be updated every calendar month following the notes below.

f) The Senior Policy & Risk Officer (SPRO) manages the register and collates all updates into a single register.

g) Directorates will advise if a risk requires to be escalated or removed from the CRR. The responsible Director must then take that proposal to the Directors with a view to the CRR being amended accordingly.

Project/Team Risk Registers

6. There is no set format for team or project risk registers. There is a facility within the Business Planning Tool to record risks against projects but there is currently no mechanism to manage them from there. The risks in these registers will inform the MRR.

Roles and Responsibilities

7. Outline roles and responsibilities are listed in the Management of Risk Policy. Greater detail of these are as follows.

Group/Individual	Responsibilities	Key roles
Board	• Sets Risk Topics and Risk Appetite for the organisation • Ensures Risk Management is embedded in the organisation • Oversees risk management process via reports from Audit Committee • Ensures action is being taken to manage all significant corporate risks	• Chair of Board ensures Board maintains focus on risk management • Chief Executive has overall responsibility for risk management as Accountable Officer • Chair of Audit Committee and Director of Strategy have delegated responsibility to oversee risk management and report to Board
Audit Committee	• On behalf of Board, ensures the organisation has a robust risk management process in place • Approves risk management processes • Scrutinises Corporate Risk Register • Reports findings and recommendations to Board • Makes recommendations to CMT to improve risk management process to manage individual risks	• Chair of Audit Committee ensures risk management is one of the committee's main priorities • Director of Strategy reports to Audit Committee on behalf of CMT • The Auditors facilitate workshops and provide advice and guidance • The Audit Committee will provide assurance to the Board that risks are being managed.
Other Governance Committees	• Ensure that risks that fall under their remit are correctly monitored and managed.	• Provide guidance on the management of risk within their remit.
Corporate Management Team	• Own, review and maintain the Corporate Risk Register, drawing together directorate risk	• Chief Executive ensures risk management is regularly addressed and acted on. • Chief Executive updates the

	registers and escalating risks where necessary • Review all risks exceeding appetite. • Develop and implement action plans to minimise risks • Instructs directors to oversee development, review • Review, update and Publish as appropriate the CRR.	CRR and ensures it is appropriately published. • Directors provide directorate risk registers
Directorates	• Through team heads' meetings, identify and measure all significant directorate risks • Take action to minimise all significant directorate risks • Regularly review and update Master Risk Register • Communicate risks to CMT to be considered as corporate	• Directors ensure that risk register is maintained. • Each Directorate has a risk champion. • Team heads provide team risks and collectively agree directorate risks, ratings and actions. • Provide updates to the SPRO for collation.
Risk Champion	• Provide an update to the SPRO on a monthly basis for their directorate's input to the MRR	• Maintaining the directorate risk register and encouraging the use of risk management. • Link to the SPRO
Teams	• Identify all significant risks at team level • Risk assessment made during planning phase of each project and recorded on Business Planning Tool • Project risks regularly reviewed and managed down where necessary	• Team heads ensure all team risks are identified and appropriately managed • Project leads ensure that significant project risks are managed, seeking advice and support where necessary from line manager
Senior Policy & Risk Officer	• Manage the risk registers to ensure they reflect the current risk position as decided by the risk owners • Report to the Board, Audit Committee and CMT as required	• SPRO maintains risk register and coordinates implementation of relevant agreed actions • Offer advice and assistance as required on Risk

Meeting Papers and Risk

8. All papers produced for business meetings (Board, Committees and CMT) are required to have a risk section. This section should reflect the effect the contents of the paper has on either a Corporate Risk or a risk in the MRR.

Monitoring and Review

9. Risks should be updated and or reviewed at the following frequency;

	Directorates	**CMT**	**Audit Committee**	**Board**
Risks Exceeding Appetite	Monthly	Monthly	At least quarterly	Quarterly
CRR	Monthly	Monthly	At least quarterly	Yearly
Complete MRR	All risks should be reviewed within a 90 day period.	MRR – One directorate each month in rotation.	By Exception	By Exception

10. A report on risk will be generated for the Audit Committee at least quarterly.

11. An annual report will be produced for the Board and will form part of the Governance Statement within the Annual Accounts. As part of the annual report

    a) A statement on what improvements have been made to risk management.

    b) A review of this protocol will be carried out and reported on.

    c) A statement of what further developments are planned for the next year including target dates.

Risk Assurance

12. Risk Assurance is the mechanism by which confidence is demonstrated that the risk processes are complete and appropriate and that they are operating effectively. A Risk assurance Framework has been developed (Annex D) although this is still considered draft.

Risk Topics

13. Risk Topics or categories have been defined by the Board. Every risk must be categorised into one of these topic areas so it can be assessed against the Boards appetite for risk within that topic area. The risk topics are defined in Annex B.

Risk Appetite

14. NHS Health Scotland recognises that in order to fulfil the objectives set out in A Fairer Healthier Scotland, it will be necessary to be involved in activities that expose the organisation to a measure of risk.

15. We define our 'risk appetite' as the amount of risk that we are prepared to accept, tolerate or be exposed to at any point in time. Risk appetite is about taking well thought-through risks where the long-term rewards are expected to be greater than any short term losses. Risk appetite needs to be considered at an individual (project) level, at a Directorate level and at an organisational (Corporate) level.

16. The Risk Appetite is defined by the Board and the current level for each risk toipic is defined at Annex B.

17. Risks are scored Gross (before controls are introduced) and nett (showing the net effect of controls in place). The residual (nett) risk scores are then compared to the expressed appetite for risk. The regular reports to the Board and Audit Committee covering the Corporate Risk register will risks exceeding the risk appetite.

18. Where a risk has been controlled such that the net risk score is the same as or lower than the appetite, the risk is deemed to be controlled and no further control measures are necessary (but may still be introduced).

19. It is recognised that the risk appetite at a Local or Project level may be different from that at the Corporate Level as by definition these risks are less critical to the organisation as a whole.

Updating the Master Risk Register

20. All amendments to the risk register should be completed in **BOLD** so that changes and updates can easily be identified.

21. An extract of the MRR will be sent to each directorate to be updated and returned to the SPRO on the last working day of the month.

Master Risk Register - Notes on Completion

22. The following guidelines should be followed when updating the MRR.

    a) **Risk Descriptions**. A risk description should include the event that may happen and the effect and impact it could have. A common error is to make a statement of what might happen but no narrative to explain why this is a risk (impact and effect). Every risk must have an owner.

    b) **Controls**. All risks should have some controls in place. All controls must, by definition, be reviewed whenever the risk register is reviewed. Every control must have an owner.

    c) **Scoring**. When the scoring is amended there must be a narrative to state why the scoring has been changed. Either, a control has been put in place

(reduction), a control is failing (increase) or the perception of the risk has changed.

d) **Action Plan**. This is for actions to be taken and controls to be put in place that will reduce the risk exposure. Once these items are in place they should be moved to the controls section and the risk scored appropriately. All Risks with a score of 10 or above are deemed to be unacceptable and are required to have an Action Plan to reduce the risk.

e) **Closing Risks**. Do not delete a risk. To close a risk, mark it as closed by setting a closed date (last column). There should be a note of why it was closed. Closed risks will be archived out as appropriate.

f) **New Risks**. For any new risks, add them to the bottom of the risk register but do not give it a number. This will be allocated by the IG&RM.

Risk Descriptions

23. To help in forming risk statements such that they accurately describe a risk, all risk descriptions should largely follow this structure;

    a) As a result of [Cause]

    b) There is a risk that [Event that is uncertain]

    c) Which will result in [Effect].

24. The important element is that risk is about uncertainty so clearly identifying what is uncertain is fundamental.

25. The effect is the impact the uncertain event happening will have on the organisation.

Risk Controls and Further Action

26. Risk controls should be considered in how they can reduce the likelihood of the uncertain event happening, or how they can reduce the impact if the uncertain event does happen.

27. Elements that are listed in the Controls column are those things that are already in place. The Further Action column is for things that have been identified that, once in place, will control the risk further.

Escalation Process

Escalation to CRR

28. During the monthly review of the Master Risk Register at directorate level, consideration should be given to the current status of the risks marked as corporate. If a risk currently marked as corporate needs to have that status removed, or if a risk is deemed to be at a level that it should be added to the corporate risk register (either as a new risk or as part of an existing CRR risk), this should be noted in the MRR update and the issue raised by the Director at the next CMT meeting (or directors' meeting if urgent).

29. Any decision at that meeting, and the full textual changes, should be communicated to the IG&RM so the CRR can be updated.

Escalation of Project Risk to MRR

30. Due to a lack of risk tools at project level, project risk is not formally managed but is encouraged to be identified at project level either in the BPT or a project risk log.

31. Directorates are encouraged to discuss risk and identify where there are project risks that should be escalated to the MRR for monitoring and managing.

Annex A

Master Risk Register Data Definition

32. The following is a table of the Data definitions for the Risk Register.

Data Entry	Definition	Mandatory
Risk No.	This is a unique number for a risk. Number must not be reused.	Assigned by Risk Manager
Directorate	The HS Directorate Name	Yes
Team	The HS Team Name	Yes
Risk Topics	Compliance Financial & Planning Operational Reputational	Yes
Date risk recorded	This is the date the Risk was recorded in the risk register	Yes
Risk Description	This description must define what the risk is, its likelihood and its impact.	Yes
Gross Risk Likelihood	This is the likelihood of the event occurring with no controls in place (1-5)	Yes
Gross Risk Impact	This is the impact of the event occurring with no controls in place (1-5)	Yes
Gross Risk Total	Likelihood x Impact (1-25) of event with no controls in place	Yes
Date controls recorded, updated or reviewed	This is the date the risk was last reviewed. This date must be updated if the risk is reviewed whether or not any changes are made to the controls or the scoring or the risk.	Yes
Controls in place	This text box should list the controls that are in place and affecting the Nett Risk scores.	Yes
Nett Risk Likelihood	This is the likelihood of the event occurring with controls in place (1-5)	Yes
Nett Risk Impact	This is the impact of the event occurring with controls in place (1-5)	Yes
Nett Risk Total	Likelihood x Impact (1-25) with controls in place	Yes
Status	This is an assessment of what is happening to the risk and takes one of 3 values; Static, Increasing, Decreasing	Yes
Appetite Exceeded	Based on the Risk Topic and looking up the maximum allowable score a True or False will be calculated	Automatic
Date further action recorded	Date the Action Plan was updated	Yes if Appetite exceeded
Action Plan (further action)	This is the action to be taken to improve the controls put in place to mitigate the level of risk (Likelihood or impact) and when these actions should be complete by.	Yes if appetite exceeded

Data Entry	Definition	Mandatory
Risk Owner	This is the owner of the risk.	Yes
Controls Owner	This is the owner of the controls	Yes
Notes	Any further information	No
Flagged by CMT as "Corporate"	If the risk is considered to be related to a risk in the CRR, a reference to that risk should be included here. This must be agreed by CMT.	No
Date Closed	This is the date a risk is closed. On closure, the risk is moved to a separate sheet.	No

Annex B

Risk Assessment Matrix

		Likelihood				
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
Impact	1. Negligible	1 Very Low	2 Very Low	3 Low	4 Low	5 Medium
	2. Minor	2 Very Low	4 Low	6 Medium	8 Medium	10 Medium
	3. Moderate	3 Low	6 Medium	9 Medium	12 High	15 High
	4. Major	4 Low	8 Medium	12 High	16 High	20 Very High
	5. Extreme	5 Medium	10 Medium	15 High	20 Very High	25 Very High

Risk Appetite Matrix

Net Risk Assessment	Risk Appetite	Risk Appetite Response
20-25 – Very High	Hungry	Eager to be innovative and to choose options offering potentially higher rewards despite greater inherent risk.
12-16 – High	Open	Willing to consider all options and choose the one that is most likely to result in success, while also providing an acceptable level of reward
5 -10 – Medium	Cautious	Preference for safe delivery options that have a low degree of inherent risk and may only have limited potential for reward
3 - 4 – Low	Minimalist	Preference for ultra-safe business delivery options that have a low degree of inherent risk and only have potential for limited reward
1-2 – Very Low	Averse	Avoidance of risk and uncertainty is a key organisational objective

Risk Topics & Appetite

Topic	Description	Appetite
Reputational	Strategic risks; stakeholder perception	Open
Financial & Planning	Scottish Government funding; value for money; Efficacy of spend	Cautious
Compliance / Regulatory	Health and safety; Freedom of Information; Business Continuity Planning; Human Resources; Data Protection	Minimalist
Operational	Projects; innovation; quality; outcomes	Open

Page Intentionally Blank

Annex C

Impact/Consequence Definitions (Source - ISD)

Descriptor	Negligible	Minor	Moderate	Major	Extreme
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.

Annex D

Risk Assurance Framework (Draft)