North Hampshire
Clinical Commissioning Group

NHS North Hampshire Clinical Commissioning Group

Risk Management Policy

(COR/021/V1.0)

Subject and version number of document:	Risk Management Policy
Serial Number:	COR/021/V1.0
Operative date:	June 2014
Author:	R Clarke, Head of Business Development, North Hampshire CCG
Links to other Policies:	Integrated Governing Body Assurance (GBAF) and Risk Management Framework Information Risk Management Policy
Review date:	This document will be reviewed every two years.
For action by:	This policy applies to all directly and indirectly employed staff and other persons working within the CCG.
Policy statement:	The purpose of this policy is to act as a simple support document to NHCCG Integrated Governing Body Assurance (GBAF) and Risk Management Framework to enable staff to undertake effective risk management.
Responsibility for dissemination to new staff:	The Business Development function of the CCG will disseminate this policy in the first instance and then be published on the CCG's website at: http://www.northhampshireccg.com/info.aspx?p=5
Training Implications:	Staff will receive training on this policy on induction and through the course of mandatory training.
Further details and additional copies available from:	All CCG policies ratified by the Governing Body will be published at: http://www.northhampshireccg.com/info.aspx?p=5
Equality Analysis Completed?	No
Consultation Process	Senior Management Committee System Reform Team
Approved by (date):	Senior Management Committee (12/6/14)
Ratified by (date):	Governing Body (24/6/14)

Intranet and Website Upload:

Intranet	Electronic Document Library Location:	N/A
Website	Location in FOI Publication Scheme	http://www.northhampshireccg.com/info.aspx?p=5&pr=X00237
Keywords:	Risk, Management, Policy	

Amendments Summary:

Amend No	Issued	Page(s)	Subject	Action Date
1				
2				
3				
4				
5				

Review Log:

Include details of when the document was last reviewed:

Version Number	Review Date	Name of Reviewer	Ratification Process	Notes

Contents

1. Introduction

NHS North Hampshire Clinical Commissioning Group (NH CCG) is responsible for commissioning Health services for a population of 216,000 people and an annual budget of c. £218m. In doing so, the CCG acknowledges that we make decisions that can have a significant impact on the health and wellbeing of our local population. It is inevitable that many decisions we make are made with an element of uncertainty about the future and each decision has an inherent risk associated with it. In order to estimate the level of risk and the impact should this risk manifest itself, the CCG needs to be able record and understand the profile of risks that face it.

This policy aims to set out the CCGs approach to risk and the procedures that support the recording and assessment of risk. This policy should be read in conjunction with the **NHCCG Integrated Governing Body Assurance (GBAF) and Risk Management Framework** which gives a more comprehensive insight into the way that the CCG identifies the totality of the risk profile facing the organisation in order to successfully deliver on its strategic objectives.

The policy will always aim to foster a proactive, honest, open and just environment where all types of risks can be identified and managed in a positive and timely way. Senior management will ensure that all staff are provided with education, training and support, appropriate to their role, to enable them to meet their responsibilities under the Risk Management Policy.

1.1 Status

This policy is a corporate policy.

1.2 Purpose and Scope

The purpose of this policy is to act as a simple support document to NHCCG Integrated Governing Body Assurance (GBAF) and Risk Management Framework to enable staff to undertake effective:

- identification and recording of risks
- analysis, scoring and evaluation of risks
- management of risks
- escalation of risks through the assurance framework (GBAF)
- monitoring and review of risks

This policy applies to all employees and contractors of the CCG and indeed to those stakeholders who deem that the organisation should be aware of certain risks. Managers at every level have an objective to ensure that risk management is a fundamental part of the approach to integrated governance. All staff at every level of the organisation are required to recognise that risk management is their personal responsibility. The Risk Management Policy therefore sets out the CCG's commitment to supporting the implementation of the assurance framework by clearly communicating the Governing Body's current risk appetite to its managers and the level of authority they have to manage risk before taking action and/or escalating to more senior management.

2. Definitions

NHS North Hampshire Clinical Commissioning Group defines a risk as:

"A future uncertain event / or events that could influence or have an effect on the achievement of the CCG's objectives and/or obligations"

The following terms are used in this document:

- **Risk Assessment:** is the process for identifying, analysing and evaluating risk
- **Risk Appetite:** the amount of risk an organisation is prepared to be exposed to before it judges action to be necessary
- **Risk Management:** the activity within the risk management process of implementing, monitoring, reporting and reviewing risk management actions against objectives
- **Initial Risk:** the risk before the effect of any risk mitigation, control or treatment activities
- **Current Risk:** the risk after implementing existing controls and actions have been taken to manage it
- **Target Risk:** the risk remaining after the risk response has been applied

Examples of the types of risk that the CCGs might encounter and need to mitigate against include:

- **Corporate risks** – operating within powers, fulfilling responsibilities, ensuring accountability to the public, governance issues
- **Clinical risks** – associated with our commissioning responsibilities and including service standards, competencies, complications, equipment, medicines, staffing, patient information, patient safety
- **Reputational risks** – associated with quality of services, communication with public and staff, patient experience
- **Financial** – associated with achievement of financial targets, commissioning decisions, statutory issues and delivery of the QIPP programme
- **Environmental including health and safety** – ensuring the well-being of staff and visitors whilst using our premises

3. The Risk Management Framework

The process for the management of risk within NHS North Hampshire CCG is summarised in Figure 1 below and is identical to the process contained in AS/NZS 4360, which NHS organisations in England have been working with since the Department of Health issued the 1999 version of the AS/NZS 4360 Standard in 1999.

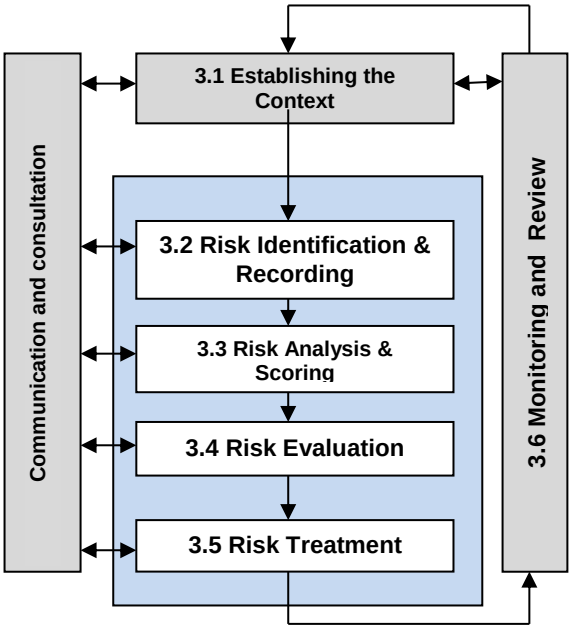

Figure 1: The Risk Management Process

Whenever risks to the achievement of CCGs' strategic objectives have been identified, it is important to record, assess and report the risk using a standardised framework and in a consistent manner using agreed definitions and evaluation criteria. This will allow for comparisons to be made between different risk types and for decisions to be made on the resources needed to mitigate the risk.

3.1 Establishing the Context

In this instance, the context is the entire range of activities conducted within the CCG, including all activities associated with commissioning patient care and treatment. All risks, clinical, strategic, organisational and financial, will need to be assessed rigorously, thus creating a continuum of risk assessments across the length and breadth of the organisation.

3.2 Risk Identification and Recording

3.2.1 Identifying Risks

The first stage in the risk process is to identify what events might prevent or impact in a positive or negative way on the achievement of the organisation's objectives as set out in the CCG's Strategy and Operating Plans.

Any individual within the CCG can help to identify a risk. Indeed, individuals are actively encouraged to go out and proactively identify risks. Risks may be identified

almost anywhere but may include:

- project planning / management – risk workshops/risk prompts
- incident information within the CCG
- risk identification from internal sources e.g external assessors, internal audit, minutes of meetings, word of mouth, informal conversations
- incident/ risk information from external sources e.g impacts of national regulation, from meetings with providers
- Reviews/lessons learned

When identifying risks it is essential to link the risk to an objective or output in order to understand the impact and allow assignment of the risk to an owner. This linkage ensures that the risk management activity is focused on delivery of business objectives; a risk can only be assessed and prioritised in relation to objectives. One way of doing this is to get a team together to brainstorm the possible threats and opportunities that might arise whilst considering each objective that you are trying to achieve in turn. The threats and opportunities are then numbered so that they can be linked to that objective (and any other objectives upon which they might impact regardless of who owns that objective). Risk identification should be considered in two phases:

1. initial identification of risks associated with a new, original activity, project or organisation when producing the business case

2. continuous re-assessment for risks associated with an ongoing activity due to changing circumstances (e.g. new legislation, impact of other risks such as delays, financial or political change)

3.2.2 Recording Risks

It is important to use a common description for each identified risk and it should be clearly identifying how it affects a particular objective or objectives. i.e.

Event ➜ Consequence ➜ Impact

A typical phrasing could be:

Failure of…
Lack of… *leads to…* *resulting in…*
Partnership with…
Enhancing of…

If a risk description cannot be easily understood as "if….." "then…." , it is likely to require rewording before making decisions about how that risk should be managed.

Risks can be usually split into operational or strategic type risks but for the purpose of this policy all risks should be categorised as operational by the ORR administrators.

All risks will be recorded in the Operational Risk Register (ORR), and an example is shown in **Appendix A**. The Operational Risk Register is a repository for information on all aspects of risk and is used by NHCCG as a management tool both for the management of risks and for communicating risk information. The Operational Risk Registers need to be maintained by each of the functions/committees listed below on an on-going basis, and should cover all aspects of risk across their area of

responsibility. Each ORR will have a Lead Risk Owner and a named administrator, who will be responsible for maintaining the register and for its review at each meeting.

Risks can be usually split into operational or strategic type risks but for the purpose of this policy all risks should be categorised as operational by the Operational Risk Register (ORR) administrators.

3.2.3 The Use of 'Datix' in the Production of Risk Registers

The CCG has decided that the software system called 'Datix' will be the database to be used by ORR administrators and the CCG Business Development Team to record risks as they emerge and for the production of summary reports including the ORRs.

The procedures for data entry to Datix and the production of ORRs are shown in **Appendix B**.

After the process of risk identification and risk assessment has been completed, those responsible will be expected to add their risks to the following Operational Risk Registers that sit across the organisation. There will be Lead Risk Owners of each of the following groups:

- **Clinical Programmes** including:
  - Planned Care
  - Unscheduled Care
  - Long Term Conditions
  - Mental Health/Learning Disabilities/Continuing Health Care
  - Maternity, New Born and Children
  - Prescribing/Medicines Management

  and the individual ORRs sent to the Head of Business Development for collation into the ORR for the **Clinical Cabinet** for **those risks scoring >12**

- **Clinical Quality Working Group**, **Performance and Assurance Working Group**, **Human Resources, Counter Fraud and CSU South** with the individual ORRs sent to the Senior Management Committee for review.

The ORRs will be reported on a quarterly basis and at time intervals published by the Head of Business Development, but would normally be requested for reporting during the months of:

- June
- September
- December
- March

The following groups:

- **The Senior Management Committee** - will receive the individual ORRs from those groups shown above and act to consolidate the major risks to the CCG into the Corporate Risk Register, and deliver this document as part of the Governing Body Assurance Framework/CRR Report to the Integrated Governance Committee on a quarterly basis

- **The Integrated Governance Committee** – will act to review the contents of the Governing Body Assurance Framework/CRR Report and act to advise the Audit Committee and Governing Body that the management of risk in the CCG

is effective

- **The Audit Committee** – will act to provide assurance to the Governing Body on the effectiveness and adequacy of the processes for managing the principal risks and Integrated Governing Body Assurance and Risk management Framework

- **The Governing Body** – will receive the CRR/GBAF and respond to risk assurance reports from the Integrated Governance Committee and issues raised by the Audit Committee in regards to risk, internal control and assurance

The specific responsibilities of each of the groups above are shown in detail within the CCG Constitution at:

http://www.northhampshireccg.com/page1.aspx?p=2&t=6

or within the NHCCG Integrated Governing Body Assurance (GBAF) and Risk Management Framework available at:

http://www.northhampshireccg.com/info.aspx?p=5

The flow and routing of ORRs through the organisation is shown in Figure 2 below.

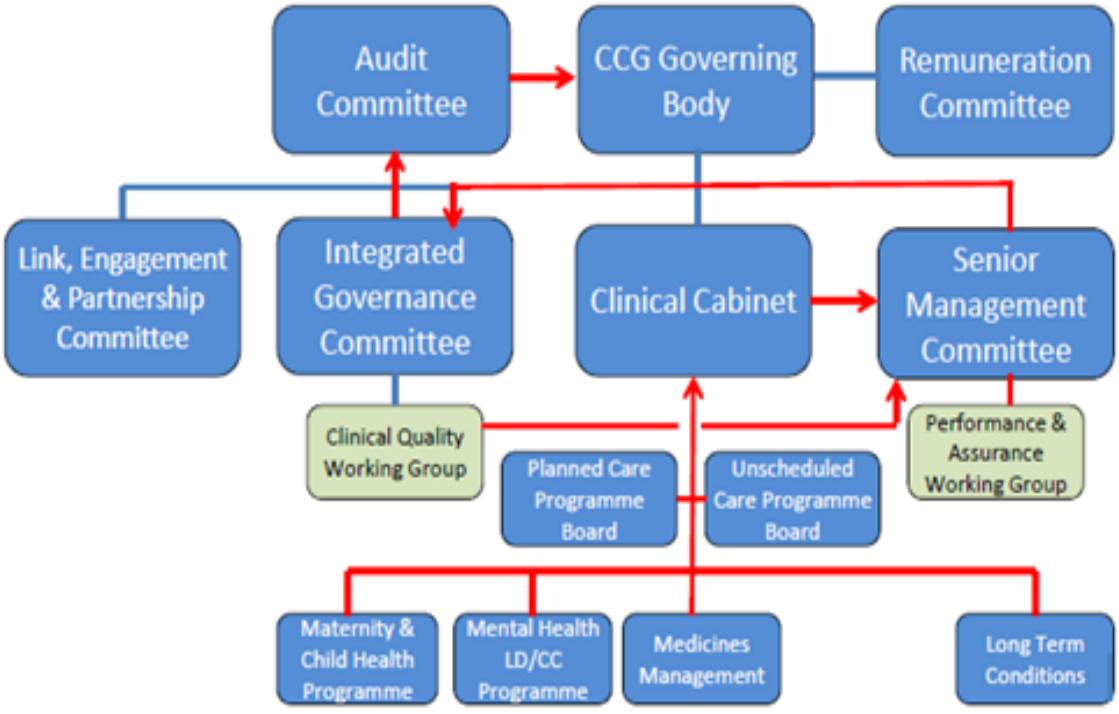

Figure 2: Structure of NHS North Hampshire CCG Committees and flow of the Operational Risk Registers

3.3 Risk Analysis & Scoring

The purpose of scoring risks is quite simply to highlight the most important threats and opportunities so that they can be actively managed within the scarce resources available.

3.3.1 Analysing Risks

Risk analysis involves the systematic use of all available information to determine **how often specified events occur** (the likelihood) and the **magnitude of their consequences** (the impact). In order to grade the risks identified the CCG utilises the risk assessment tool and matrix shown in Figure 3. All risks highlighted to the CCG need to be graded using this risk matrix. If other quantitative methods are used then risk analysis will be inconsistent, and the population of the risk register will be unreliable. Risk identification and risk assessment is a continuous process and should not be considered as a one-off exercise.

3.3.2 Scoring Risks

Having identified a risk event, the likelihood of it occurring should be agreed and quantified. Where possible, the period during which the risk is most likely to arise and terminate should also be noted. The risk impact must also be considered since there is little point in wasting time and effort recording and managing risks that have little consequence and do not affect the achievement of objectives. In deciding the risk impact all possible outcomes should be considered, these could occur in terms of time and/or cost and/or performance. Performance can be subjective, such as damage to reputation, or measurable such as failure to deliver acceptable quality or sufficient capacity.

Multiplying the **Impact** and **Likelihood** scores provides the **total risk score** that can be plotted on the Risk Matrix below and associated with an appropriate level of managerial response.

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

The total risk score = Likelihood score X Impact score

Figure 3: The Risk Scoring Matrix

….where **Likelihood** of occurrence is described and scored as shown in Figure 4 below.

Figure 4: The description and scoring of 'likelihood'

Likelihood	**1**	**2**	**3**	**4**	**5**
Descriptor	Rare	Unlikely	Possible	Likely	Certain
Frequency How often might it/does it happen	This will probably never happen/recur	Do not expect it to happen/recur but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur but it is not a persisting issue	Will undoubtedly happen/recur, possibly frequently

……and **Consequence** is described using the 5 categories:

- **Catastrophic:** the consequence of these risks could seriously impact upon the achievement of the organisation's objectives, its financial stability and its reputation. Examples include loss of life, extended cessation or closure of a service, significant harm to a patient(s), loss of stakeholder confidence, failure to meet national targets and loss of financial stability

- **Major:** these are significant risks that require prompt action. With a concerted effort and a challenging action plan, the risks could be realistically reduced within a realistic timescale.

- **Moderate:** these risks can be realistically reduced within a realistic timescale through reasonably practical measures, such as reviewing working arrangements, purchase of small pieces of new equipment, raising staff/patient awareness etc.

- **Minor:** these risks are deemed to be low level or minor risks which can be managed and monitored within the individual department

- **Negligible:** these risks cause minimal or limited harm or concern

The categories are further described with associated scoring in **Appendix C**.

3.4 Risk Evaluation and Managerial Response

The organisation's **'Risk Appetite'** ensures that risks are considered in terms of both opportunities and threats and are not confined to the financial consequences of a risk materialising. Risks can also impact on the capability of the CCG, its performance and its reputation. Risk appetite is influenced by the objectives set by the organisation, individual programmes of work and the NHS landscape.

The Risk Appetite and approach to risk will be reviewed annually by the Governing Body and quoted on its website at:

http://www.northhampshireccg.com/info.aspx?p=5

The current appetite quoted is:

"The Governing Body has a moderate but considered appetite for risk which will promote innovation and growth, whilst:

· *We have no appetite for fraud/financial crime risk*

· *We have a zero tolerance for regulatory breaches*

· *We will at all times attempt to avoid negative press coverage*

· *We will not take risks that affect the quality of customer service provided*

· *We are committed to protecting the environment"*

3.4.1 Ownership and Managerial Response

Each risk identified must be allocated to an owner (the Lead Risk Owner) who has the

authority to agree actions that would mitigate the risk even though the practice of mitigation might be delegated to someone else who is empowered accordingly. The value of these actions should be measurable (even if only qualitatively). This inevitably requires the objectives themselves to be written in a measurable way and to have appropriate performance indicators where possible.

The Governing Body acknowledges that risk is a component of change and improvement and therefore does not expect or consider the absence of risk as a necessarily positive position. The organisation will, where necessary, tolerate overall levels of risk that are classified as **high** (high or up to a score of 10 or below using the Risk Scoring Matrix), where action is not cost effective or reasonably practicable.

The organisation will not normally accept levels of risk rated **high or extreme** (amber/red) which are scored between 12 - 25 using the Risk Scoring Matrix. This would 'trigger' the need to enter a specific risk to the Corporate Risk Register and be reported to the Governing Body in the stated way. The organisation will ensure that plans are put into place to lower the level of risk whenever this level of risk has been identified.

The organisation requires that all staff take responsibility for the treatment of identified risks. Identifying and reporting a risk does not end the responsibility of the individual staff member. A major part of risk treatment is control and the control to mitigate the risk may be easily put in place, for example by cleaning up a spillage.

3.4.2 Roles, Responsibilities and Duties

The Accountable Officer is ultimately accountable to NHS England for all risks relating to the operations of the organisation and will lead on determination of the strategic approach to risk, establishing and maintaining the structure for risk management.

The Chief Finance Officer will undertake the role of **Senior Information Risk Officer (SIRO)** and is required to:

- understand how the strategic business goals of the organisation may be impacted by information risks
- act as an advocate for information risk on the executive team and provide adequate briefing on information issues
- own a risk assessment process for information risk to support an annual review statement.
- successfully complete strategic information risk management training
- oversee the development of policy and strategy with regard to information risk within the information governance framework
- communicate to all staff and those with specific roles (including Information Asset Owners/Data Custodians), ensuring that they have appropriate training and resources for delivery of, their role in the information risk related polices

A number of other risk areas, including Safeguarding Children and Safeguarding Adults, will have a specified lead, who for NH CCG will ultimately be the Accountable Officer via the work of the **Chief Nurse.**

In addition to the **Lead Risk Owners** and **ORR administrators**, whose duties have

been described above, **Senior Managers** will provide leadership for the risk management agenda and ensure that responsibilities to identify, record, analyse, control and communicate risk issues are undertaken according to the authorities and lines of delegation described in Figure 5 below.

Level	Authority / Ownership	Managerial Response
Low risk 1-3	Individuals and Team Managers	Managed through normal local control measures. Acceptable level of risk. Individuals should manage low risks by maintaining routine procedures and taking proportionate action to implement any additional new control measures to reduce risk where possible. Individuals must escalate higher levels of risk.
Moderate risk 4-6	Managers	Review control measures through formal risk assessment, record on the relevant Risk Register. Managers must ensure that an action plan is identified to reduce risk or remove the risk. Managers must escalate higher levels of risk.
High risk 8-12	Senior Manager	Above a normal tolerable level of risk. Action required to be taken, recorded on the relevant Risk Register. Scores of 12 and above will be entered to the **Corporate Risk Register** by the Head of Business Development. Senior Managers must prepare an action plan for high risks. Appropriate management assurance must evidence and control the risk assessment, and oversee the action plan to reduce the risk. The risk may be a low score as it is in its early stages. Senior Managers must consider developing implications of the risk and report to the Integrated Governance Committee if appropriate.
Extreme risk 15-25	Relevant Committee and Integrated Governance Committee	Intolerable level of risk. **Immediate action** must be taken and the risk will be escalated to the Corporate Risk Register. Management action is required to ensure immediate risk treatment, in line with the context of the risk. An action plan must be overseen by a Lead Risk Owner who will give updates and be monitored by the Integrated Governance Committee. Consider the **'Fast Track'** for extreme and urgent incidents.

Figure 5: Management delegation and authority (managerial response) vs risk level

3.5 Risk Treatment and Escalation

This is the activity within the risk management process of developing a plan to manage each of the risks identified. This encompasses the compiling and recording of risk treatment actions and placing review arrangements into the risk register.

3.5.1 Risk Treatment

The organisation expects that all reported and registered risks will be considered for risk treatment options. Risk treatment includes implementing controls, removing the risk completely, reducing the risk, transferring the uncertainty of the risk (for example by insurance) or making a decision to tolerate the risk in line with the manager's level of authority. Risk treatment options are further described in Table 6 below.

The CCG believes that the majority of risks will need to have controls implemented to

reduce the likelihood or severity of the risk. The cost-effectiveness of the control needs to be considered to ensure that the risk reduction benefits outweigh the cost of the control.

Existing control mechanisms/activities and the level of confidence in these existing controls must be considered when identifying options for additional control measures.

To decide the most appropriate response a systematic process should be followed starting with the "do nothing" option of tolerating the risk. Depending on the nature of the risk identified, there may be several risk handling responses available and a brief investment appraisal may be required to identify the most cost effective. This will also help to decide the nature and sequence of measures with some being defined as purely fallback or contingency measures. Both the risk owner and any manager(s) tasked with implementing the risk treatment action must have a full understanding of the original source of the risk in order to best select the control or mitigation to be applied.

Response	Description
TOLERATE	The ability to do anything about some risks may be limited, or the cost of taking any action may be unaffordable or disproportionate to the potential benefit gained. Tolerating risk will therefore be dictated by the current levels of risk appetite that exist in the CCG and by the evidence resulting from a cost/benefits analysis of the potential mitigation measures.
TREAT	By far the greater number of risk responses will be addressed in this way. The purpose of treatment is not necessarily to remove the risk altogether but more likely to contain the risk to an acceptable level. That is to reduce its probability and/or impact.
TERMINATE	Some risks will only be treatable, or containable to acceptable levels, by terminating the activity. This option can be particularly important if it becomes clear that the projected cost/benefit relationship is in jeopardy. It should be noted that the option to terminate activities may be limited due to existing restraints such as statutory duties.
TRANSFER	For some risks the best response may be to transfer them. This will normally be achieved by escalating the risk issue to the next management level or relevant functional process owner. Whilst it may be possible to transfer or escalate such risks, it is important to recognise that there is no guarantee that the impact will not fall on those who originate the risks and their outputs, making the transfer that of the risk management and not of this risk in itself. Another way to transfer risk is through insurance.

Figure 6: Risk treatment options

3.5.2 Escalation

Primacy with regard to making the treatment decisions ultimately sits with the relevant committee or group and thence through the Integrated Governance Committee to the Governing Body. The important consideration for all staff of the CCG is that any risk identified should at least be assessed jointly with a Lead Risk Owner or manager. Any decisions with regard to how a particular risk should be dealt with should be recorded in the minutes of the meeting and communicated to the relevant Lead Risk Owner and committee chairperson.

It would be impossible for the CCG to manage risk in isolation, and clear lines of communication are crucial. The crossing of boundaries is inevitable. It is therefore essential that the management, identification, assessment and analysis of risks is shared and communicated. The CCG have to consider all our external as well as internal stakeholders.

3.6 Monitoring and Review

The final stage of the risk management process is the activity of assessing and revising the risk as the risk treatment measures are applied (or as the risk changes). The risk should be managed down to a tolerable level consistent with demonstrating best value relative to the resources applied.

The Risk Owner and the Manager delegated responsibility for implementing the risk treatment action/s meet to review progress of the control/mitigation actions relating to the risk. During this review the ORR administrator should provide the Lead Risk Owner with an update on each action undertaken to date and any problems encountered. From this review the Lead Risk Owner should satisfy a number of questions so that appropriate changes can be made to the plan if necessary:

- are all the tasks, associated with each action, being carried out and if not what are the constraints?
- can the constraints (where appropriate) be removed?
- are the tasks completed so far having the desired effect in reducing the probability or impact?
- if the actions are not having the desired effect, what other risk responses can be used?
- do fallback/contingency actions need to be applied?
- have any secondary risks been identified as a result of the actions carried out so far?

Whilst pre and post action assessments of the risk can be made using the risk significance criteria defined in the assessment process step, a subjective assessment can also be used to highlight how effective and efficient the existing controls are in addressing the risk on a continuing basis.

4 Future Document Development and Compliance Control

This document and its contents will be reviewed every two years after first review. The most-up-to-date eversion of this document will be published on the CCG's policy webpages at:

http://www.northhampshireccg.com/info.aspx?p=5

Archiving

Reference should be made to the CCG Records Management Policy and the appropriate retention schedule.

Monitoring Compliance

Compliance with the policy will be tested through the work of the Business Development Team in the administration of the risk register reporting process and any remedial actions taken to ensure compliance.

5. Communication, Dissemination and Implementation

The document will be communicated to all staff of the CCG via the CCG newsletter and via the CCG website. The processes and procedures within this policy will be implemented through the quarterly reporting programme and overseen by the Head of Business Development via the facilitation of the reporting process, and by he/she taking any remedial actions and training should the need arise.

6. Approval and Ratification

The policy will be approved by either the Integrated Governance Committee or the Senior Management Committee, as a delegated responsibility from the Governing Body, but ratified by the Governing Body itself.

7. Review and Revision Arrangements

This policy should be reviewed on a two yearly basis. Subject to update in future versions of a risk management strategy, an Annual Risk Management Report will be presented to the Integrated Governance Committee and received by the Governing Body.

8. Training

Staff training with regard to this policy will be included the CCG Induction Programme and individual 1:1 training when the need arises. Risk Management and Information Risk Management training is also part of the Mandatory Training programme.

9. Legislation and Statutory Requirements

This Risk Management policy is developed with reference to Department of Health publications and publications of expert bodies on governance and risk management:

- Data Protection Act 1998
- Principles and framework contained in the legislation including: Health and Safety at Work Act 1974
- Principles contained within the Information Governance toolkit
- Risk Management Matrix for Risk Managers National Patient Safety Agency, (NPSA) (2008) ISO 31000 -2009

Best practice recommendations include:

- NHS Audit Committee Handbook (2011)
- Building the Assurance Framework: A practical Guide for NHS Boards March 2003. Gate log Reference1054
- Integrated Governance Handbook 2006
- Intelligent Commissioning Board (2006 & 2009)
- Making a Difference – Review of Controls Assurance Gateway Ref. No. 4222
- NHS Litigation Authority – CNST Risk Management Standards Governing the NHS: A guide for NHS Boards (2003)

- Taking it on Trust – Audit Commission (2009) Institute of Risk Management
- The Healthy NHS Board: Principles for Good Governance (2010)

Appendix A: An Example Operational Risk Register

Operational Risk Register - Human Resources — March 2014 Review

Group:	Human Resources	Reporting To:	Senior Management Committee
Chair/Accountable Person:	Oliver Anderson	Register Administrator:	Oliver Anderson
Date of Last Review:	24/10/2013		

Programme Area: Human Resources

Programme Code: HR

1 Ref No	2 Relevant Strategic Objectives	Functional Domain	3 Risk Owner	4 Risk Title and Risk Description	5 Original Date entered onto Risk Register	6 Existing Controls	7 Positive Assurance	8 Gaps in Controls, Systems or Assurance	14 Strategy to Manage Risk (Terminate, Tolerate, Transfer or Treat)	9 Initial Risk Score (Impact x Likelihoo	10 Current Risk Score (Impact x	11 Target Risk Score (Impact x Likelihoo	12 Assurance Action Plan and Planned Completion Date
HR/001										3x3=9	6	6	
HR/002										4x2=8	8	4	
HR/003										4x3=12	8	8	
HR/004										4x4=16	4x3=12	6	
HR/005										3x3=9	6	6	
HR/006										2x1=2	2	2	
HR/007										3x1=3	3	3	
HR/008										3x1=4	3	3	
HR/009										4x3=12	12	3	
HR/010										3x3=9	3x3=9	6	

Appendix B: Instructions for the Use of the Datix Database

(in development)

Appendix C: Consequence Score (severity levels) and Examples of Descriptors

	Consequence score (severity levels) and examples of descriptors				
	1	**2**	**3**	**4**	**5**
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Impact on the safety of patients, staff or public (physical/psychological harm)	Minimal injury requiring no/minimal intervention or treatment. No time off work	Minor injury or illness, requiring minor intervention Requiring time off work for >3 days Increase in length of hospital stay by 1-3 days	Moderate injury requiring professional intervention Requiring time off work for 4-14 days Increase in length of hospital stay by 4-15 days RIDDOR/agency reportable incident An event which impacts on a small number of patients	Major injury leading to long-term incapacity/disability Requiring time off work for >14 days Increase in length of hospital stay by >15 days Mismanagement of patient care with long-term effects	Incident leading to death Multiple permanent injuries or irreversible health effects An event which impacts on a large number of patients
	1	**2**	**3**	**4**	**5**
	Negligible	**Minor**	**Moderate**	**Major**	**Catastrophic**
Quality/complaints/audit	Peripheral element of treatment or service suboptimal Informal complaint/inquiry	Overall treatment or service suboptimal Formal complaint (stage 1) Local resolution Single failure to meet internal standards Minor implications for patient safety if unresolved Reduced performance rating if unresolved	Treatment or service has significantly reduced effectiveness Formal complaint (stage 2) complaint Local resolution (with potential to go to independent review) Repeated failure to meet internal standards Major patient safety implications if findings are not acted on Inefficient use of resources and lost opportunity to improve health.	Non-compliance with national standards with significant risk to patients if unresolved Multiple complaints/ independent review Low performance rating Critical report	Totally unacceptable level or quality of treatment/service Gross failure of patient safety if findings not acted on Inquest/ombudsman inquiry Gross failure to meet national standards
	1	**2**	**3**	**4**	**5**
	Negligible	**Minor**	**Moderate**	**Major**	**Catastrophic**
Human resources/ organisational development/ staffing/ competence	Short-term low staffing level that temporarily reduces service quality (< 1 day)	Low staffing level that reduces the service quality	Late delivery of key objective/ service due to lack of staff Unsafe staffing level or competence (>1 day) Low staff morale Poor staff attendance for mandatory/key training	Uncertain delivery of key objective/service due to lack of staff Unsafe staffing level or competence (>5 days) Loss of key staff Very low staff morale No staff attending mandatory/ key training	Non-delivery of key objective/service due to lack of staff Ongoing unsafe staffing levels or competence Loss of several key staff No staff attending mandatory training /key training on an ongoing basis

	1	**2**	**3**	**4**	**5**
	Negligible	**Minor**	**Moderate**	**Major**	**Catastrophic**
Statutory duty/ inspections	No or minimal impact or breech of guidance/ statutory duty	Breech of statutory legislation Reduced performance rating if unresolved	Single breech in statutory duty Challenging external recommendations/ improvement notice	Enforcement action Multiple breeches in statutory duty Improvement notices Low performance rating Critical report	Multiple breeches in statutory duty Prosecution Complete systems change required Zero performance rating Severely critical report
	1	**2**	**3**	**4**	**5**
	Negligible	**Minor**	**Moderate**	**Major**	**Catastrophic**
Adverse publicity/ reputation	Rumours Potential for public concern	Local media coverage – short-term reduction in public confidence Elements of public expectation not being met	Local media coverage – long-term reduction in public confidence	National media coverage with <3 days service well below reasonable public expectation	National media coverage with >3 days service well below reasonable public expectation. MP concerned (questions in the House) Total loss of public confidence
	1	**2**	**3**	**4**	**5**
	Negligible	**Minor**	**Moderate**	**Major**	**Catastrophic**
Business objectives/ projects	Insignificant cost increase/ schedule slippage Key targets: performing	<5 per cent over project budget Schedule slippage Key targets: performing but trends indicate worsening situation	5–10 per cent over project budget Schedule slippage Key targets: performance under review	Non-compliance with national 10–25 per cent over project budget Schedule slippage Key objectives not met Key targets: performance failing	Incident leading >25 per cent over project budget Schedule slippage Key objectives not met Key targets: performance failing - impact on patients
	1	**2**	**3**	**4**	**5**
	Negligible	**Minor**	**Moderate**	**Major**	**Catastrophic**
Finance including claims	Small loss Risk of claim remote Costs less than £10,000	Loss of 0.1–0.25 per cent of budget Cost(s) between £10,000 and £300,000	Loss of 0.25–0.5 per cent of budget Cost(s) between £300,000 and £1 million	Uncertain delivery of key objective/Loss of 0.5–1.0 per cent of budget Cost(s) £1 - £2 million	Non-delivery of key objective/ Loss of >1 per cent of budget Cost(s) £2m+ Failure to meet specification/ slippage Loss of contract / payment by results
Service/business interruption	Loss/interruption of >1 hour	Loss/interruption of >8 hours	Loss/interruption of >1 day	Loss/interruption of >1 week	Permanent loss of service or facility
Environmental impact	Minimal or no impact on the environment	Minor impact on environment	Moderate impact on environment	Major impact on environment	Catastrophic impact on environment