Information Governance			
Management of Risk Policy			
Policy No.		Contact	Brian Orpin
Version	3.0	Email	Brian.orpin@nhs.net
Issue Date	28/11/2014	Telephone	0131 314 5360
Review Date	28/11/2016	Status	Approved
IA Date	09/08/2013		

Change Control

Date	Version	Change	Owner
28/11/2014	3.0	Approved by Board	Board

Introduction

1. This document has been developed in line with the Management of Risk (M_o_R®) 2007 framework produced by the Office of Government Commerce (OGC). The NHS Scotland standard for risk management, Australia/New Zealand Risk Management Standards 4360: 2004 (Australia/New Zealand equivalent to British Standards Institute), has been incorporated. The M_o_R framework provides better provision for an overall Risk Management System (RMS) while allowing for the inclusion of other standards to manage the risks themselves.

2. Risk management is defined as 'the culture, processes and structures that are directed towards realising potential opportunities whilst managing adverse effects'. (AS/NZ 4360:2004)

3. NHS Health Scotland understands that it is important to recognise and deal effectively with the many risks that surround it. It is the policy of NHS Health Scotland that its Board Members, officers and staff must adopt a proactive approach to risk management by complying with the risk management policy and processes.

4. Whilst it is acknowledged that risk cannot be eliminated, NHS Health Scotland is committed to its intelligent management so that the organisation continually:

   a) meets its statutory obligations and acts within the law

b) safeguards the public at large, its Board Members, staff, partners and all those to whom it has a duty of care

c) protects its property whether that be buildings, equipment, vehicles or other assets and resources

d) preserves and enhances service delivery, fostering continuous improvement

e) maintains effective control of public funds

f) maintains and promotes its reputation

g) promotes increasing healthy life expectancy and reducing health inequalities

h) produces work that is timely, useful and of consistently high quality.

5. To be most effective, risk management must become part of an organisation's culture. It should be embedded into the organisation's philosophy, practices and business processes rather than be viewed or practised as a separate activity. When this is achieved, everyone in the organisation becomes involved in the management of risk. Furthermore, as an integral component of the Statement on Internal Control, it is a mandatory requirement that NHS Boards have systems and processes in place to manage risk.

References

6. The following documents are referenced;

a) Office of Government Commerce (OGC) Management of Risk (M_o_R®) 2007.

b) Australia/New Zealand Risk Management Standards 4360: 2004.

c) Thinking about risk, managing your risk appetite; A practitioner's guide, HM Treasury, November 2006.

Document Purpose

7. The purpose of this document is to define how NHS Health Scotland will approach the management of risks associated with its activities.

Framework

8. This document is the top level risk management policy document for NHS Health Scotland. Other Risk Management Policies may be developed to manage specific areas such as Health & Safety, or specific projects as required.

9. A Risk Management Protocol document will define the processes to be followed to manage risk.

10. A Risk Management Strategy document may be produced to describe specific risk management activities for a particular organisational activity.

11. A Corporate Risk Register will be maintained and published annually. A Master Risk Register, linked to the Corporate Risk Register will be maintained.

Benefits of Risk Management

12. Risk management offers NHS Health Scotland the prospect of both tangible and intangible benefits in the form of more considered service plans and projects, better operational and financial management and less exposure to financial loss, service disruption and bad publicity. It is NHS Health Scotland's intention that the positive application of risk management concepts will serve to reduce the "fear of the unknown" and so help to generate greater innovation through an improved understanding of risk and the willingness to seek more adventurous solutions.

13. Organisations that manage risk effectively and efficiently are more likely to achieve their objectives and do so at lower overall cost.

Principles and Objectives

14. Risk management is the systematic identification, assessment and reduction of risks to stakeholders, staff and the organisation.

15. Risk management proactively reduces identified risk to an acceptable level by creating a culture founded on assessment and prevention rather than reaction and remedy. It plays a vital role in supporting and informing decision-making in providing a safe and secure environment for stakeholders, staff and visitors.

16. NHS Health Scotland will systematically identify, analyse, evaluate, control and monitor those risks that potentially endanger or have a detrimental effect upon its stakeholders, property, reputation and financial stability. It holds its Board Members, officers and staff accountable for the performance of these tasks.

17. NHS Health Scotland's key objectives in relation to risk management are:

    a) To manage risk in partnership with staff, stakeholders, the public and other organisations, thus reducing risks to the achievement of NHS Health Scotland's business objectives.

b) To identify and understand the key risks affecting NHS Health Scotland in risk registers, clearly identifying uncontrolled and tolerated risks.

c) To identify the acceptable Risk Appetite for defined risk topics and to manage the risk within those levels.

d) To escalate risks to an appropriate level and adopt both a top down and a bottom up approach (through appropriate escalation procedures) thus ensuring risks are managed at an appropriate level.

e) To identify, train and support key staff to ensure that risk management is part of the delivery of NHS Health Scotland's services.

f) To establish systems of monitoring and evaluating risk management through the creation of clear accountability arrangements which report to the Board via the Corporate Management Team and the Audit Committee.

g) To ensure all standards and legislation are met, eg Clinical Negligence and Other Risks Indemnity Scheme, health and safety and information governance.

h) To foster the development of an open culture which allows and encourages staff to raise issues and be supported in finding new ways to overcome risks without fear of adverse consequences. This culture does not mean action will not be taken in cases of gross negligence or recklessness.

i) To ensure effective use of information technology to support these objectives.

j) To learn from experience and develop a learning, supportive and open culture.

k) To ensure that effective communication routes exist to inform appropriately of risks and their controls.

l) To ensure that risk is managed in partnership and relevant issues are raised through the Partnership Forum.

Compliance

18. It is acknowledged that mandatory clinical governance requirements do not always apply to special health boards such as NHS Health Scotland who do not deliver direct patient care. None-the-less, the principles of effective governance are recognised as good practice for any organisation and as such act as a useful tool for assessing governance arrangements.

19. All Health Scotland staff (permanent, fixed term, interim or temporary) and secondees must comply with this policy.

Roles and Responsibilities

The Board

20. The Board of NHS Health Scotland is responsible for ensuring that appropriate risk management activities take place. NHS Health Scotland's Chief Executive is the Board's Accountable Officer and has overall responsibility for risk management arrangements.

21. The Board is responsible for ensuring a risk register is published in line with the organisations responsibilities under The Freedom of Information (Scotland) Act.

22. The Board must define a set of risk topics for the organisation and the risk appetite for each of those topics.

23. The Director of Equality People and Performance is the nominated member of the Board responsible for the funding and championing of Risk Management to the Board and the rest of the organisation.

24. The Board is responsible for approving this policy.

Audit Committee

25. The Audit Committee, on behalf of Board, ensures the organisation has a robust risk management process in place. It will review the corporate risk register, seek assurances that the risks are being controlled and report its findings and recommendations to the Board. It will also make recommendations to the Corporate Management Team (CMT) to improve the risk management process and monitor the progress of improvements.

Other Board Standing Committees and Groups

26. Other standing Board committees and groups have a responsibility to examine risks relating to activities within their areas of responsibility to ensure that the risks are being managed appropriately. They may request that a risk is created where they feel there is a gap.

Corporate Management Team

27. The Corporate Management Team must routinely examine the risk registers and ensure that appropriate actions are taken to control risk within the organisation. The CMT will provide assurances to the Audit Committee that risk is being managed and controlled.

28. The CMT is responsible for ensuring that risk is managed within the appetite set by the Board.

Risk Committee

29. The NHS Health Scotland Risk Committee will consist of Risk Champions for all areas of the organisation representing each directorate.

30. It will be chaired by the Information Governance & Risk Manager (IG&RM) on behalf of the Director of Equality People and Performance and its role is to advise the board on risk management and to monitor and review the risk management process.

Risk Manager

31. The IG&RM is nominated as the risk manager

32. The risk manager is to

    a) Advise senior management on risk management

    b) Prepare or support the preparation of risk management policies, the process and advise on techniques to be used and the tools to be acquired or developed.

    c) Develop a maturity model.

    d) Embed risk management by providing seminars, training and workshops.

    e) Advise on when risk management activity should be undertaken, carry out or supervise the risk process and prepare risk strategies.

    f) Provide reports to senior managers.

    g) Advise on risk appetite, escalation, contingencies and risk capacity.

    h) Support completion of statements on Internal control, annual review reports and answer internal and external auditors questions.

    i) Drive implementation of risk management process

    j) Manage the organisations risk registers.

Programme, project and operational managers

33. Programme, project and operational managers will be responsible for the management of risk within their defined projects or teams, escalating risks that are above the agreed tolerance levels to senior management.

Glossary

34. A Glossary of terms generally used in risk policies and procedures is at Annex C.

Risk Management Process

35. The process that NHS Health Scotland will use to manage risk will be defined in the HS Risk Management Protocol document.

When Risk Management Should be Implemented

36. Risk management should be applied to the following business perspectives and functions;

    a) Strategic Risks

    b) Programme Risks

    c) Operational Risks

    d) Project Risks

    e) Business Continuity

    f) Health & Safety

    g) Financial Risks

    h) Communications

37. Where necessary and on the advice of the Information Governance & Risk Manager, a risk strategy should be produced for a specific organisational activity.

38. A PESTLE analysis may be carried out to ensure that full coverage of all risk areas has been achieved.

Reporting

39. Risk will be reported as laid down in the Risk Protocol document. Reports will be generated on a timely basis to the Audit Committee and the Board.

Budget

40. Risk management will be supported across the organisation with both the provision of personnel to manage risks and support services to enable the management of risk.

    a) A Risk Manager has been identified as part of a substantive post.

    b) Each Directorate will nominate a risk champion who will be a member of the risk committee.

    c) Budget will be allocated to provide training and tools as identified by the risk manager.

Quality Assurance

41. All documents will meet the quality standards of HS.

Review

42. Reviews of this policy will take place on a biennial basis.

Date Policy Approved…….

Agreed by ……

Annex A

Glossary of Terms as defined by the OGC M_o_R Framework

Term	Definition
Accounting Officer (Accountable Officer – NHS Health Scotland)	A public sector role with personal responsibility for the propriety and regularity of the finances for which he or she is answerable; includes responsibility for governance issues, and custodianship of the management of risk and its adoption throughout the organization.
Audit committee	A body of independent directors who are responsible for monitoring the integrity of the financial statement of the company; the effectiveness of the company's internal audit function; the external auditor's independence and objectivity; and the effectiveness of the audit process.
Benefit	The measurable improvement resulting from an outcome perceived as an advantage by one or more stakeholders.
Business Case	The justification for an organizational activity (strategic, programme, project, operational) which typically contains costs, benefits, risks and timescales and against which continuing viability is tested.
Business change manager	The role responsible for benefits management, from identification through to realization, ensuring the implementation and embedding of the new capabilities delivered by the projects. Typically allocated to more than one individual. Alternative title: 'change agent'.
Business continuity management	A holistic management process that identifies potential impacts which threaten an organization and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities. The management of recovery or continuity in the event of a disaster; also the management of the overall process through training, rehearsals and reviews, to ensure the business continuity plan stays current and up to date.
Business continuity plan	A plan for the fast and efficient resumption of essential business operations by directing the recovery actions of specified recovery teams.
Business risk	Failure to achieve business objectives/benefits.
Communications plan	A plan of the communications activities during the organizational activity (strategic, programme, project, or operational) that will be established and maintained. Typically contains when, what, how and with whom information flows.
Contingency plan	A plan to be executed if a particular risk occurs in order to minimize the impact after the event.
Contingency planning	The process of identifying and planning appropriate responses to be taken when a risk actually occurs.

Term	Definition
Corporate governance	The ongoing activity of maintaining a sound system of internal control by which the directors and officers of an organization ensure that effective management systems, including financial monitoring and control systems, have been put in place to protect assets, earning capacity and the reputation of the organization.
CRAMM	A formalized security risk analysis and management methodology originally developed by CCTA (now part of the Office of Government Commerce) in collaboration with a number of private sector organizations.
Disaster recovery planning	A series of processes that focus upon recovery processes, principally in response to physical disasters. This activity forms part of business continuity planning, not the totality.
Dis-benefit	Outcomes perceived as negative by one or more stakeholders. Dis-benefits are actual consequences of an activity whereas, by definition, a risk has some uncertainty about whether it will materialize.
Enhancement	A risk response for an opportunity. Enhancement of an opportunity refers to both the realization of an opportunity and achieving additional gains over and above the opportunity.
Expected value	This is calculated by multiplying the average impact by the probability percentage.
Exploitation	A risk response for an opportunity. Exploitation refers to changing an activities scope, suppliers or specification in order to achieve a beneficial outcome.
Gateway review	Independent assurance review that occurs at key decision points within the lifecycle of a programme or project.
Horizon scanning	The systematic examination of potential threats, opportunities and likely future developments which are at the margins of current thinking and planning.
Impact	Impact is the result of a particular threat or opportunity actually occurring.
Inherent risk	The exposure arising from a specific risk before any action has been taken to manage it.
Issue	A relevant event that has happened, was not planned, and requires management action. Could be a problem, query, concern, change request or risk that has occurred.
Issue actionee	A role or individual responsible for the management and control of all aspects of individual issues, including the implementation of the measures taken in respect of each issue.
Management of risk framework	Sets the context within which risks are managed, in terms of how they will be identified, assessed and controlled. It must be consistent and comprehensive, with processes that are embedded in management activities throughout the organization.
Maturity level	A well-defined evolutionary plateau towards achieving a mature process (five levels are often cited: initial, repeatable, defined, managed and optimizing).

Term	Definition
OGC Gateway™ Review	A review of a delivery programme or procurement project carried out at a key decision point by a team of experienced people, independent of the project team.
Operational risk	Failure to achieve business/organizational objectives due to human error, system failures and inadequate procedure and controls.
Opportunity	An uncertain event that could have a favourable impact on objectives or benefits.
Outcome	The result of change, normally affecting real-world behaviour and/or circumstances. Outcomes are desired when a change is conceived. Outcomes are achieved as a result of the activities undertaken to effect the change. In a programme, the outcome is the manifestation of part or all of the new state conceived in the blueprint.
Output	The tangible or intangible product resulting from a planned activity.
Probability	This is the evaluated likelihood of a particular threat or opportunity actually happening, including a consideration of the frequency with which this may arise.
Product	An input or output, whether tangible or intangible, that can be described in advance, created and tested. Also known as an output or deliverable.
Programme	A temporary flexible organization structure created to coordinate, direct and oversee the implementation of a set of related projects and activities in order to deliver outcomes and benefits related to the organization's strategic objectives. A programme is likely to have a life that spans several years.
Programme risk	Risk concerned with transforming high-level strategy into new ways of working to deliver benefits to the organization.
Project	A temporary organization that is created for the purpose of delivering one or more business products according to a specified Business Case.
Project risk	Project risks are those concerned with the successful completion of the project. Typically these risks include personal, technical, cost, schedule, resource, operational support, quality and supplier issues.
Proximity (of risk)	The time factor of risk, i.e. the occurrence of risks will be more likely at particular times, and the severity of their impact will vary depending on when they occur.
Quality assurance	Independent check that products will be fit for purpose or meet requirements.
Realization	A risk response for an opportunity. The realization of opportunities ensures that potential improvements to an organizational activity are delivered.
Reduction	A risk response for a threat. Proactive actions are taken to reduce: • the probability of the event occurring by performing some form of control, or • the impact of the threat should it occur.

Term	Definition
Removal	A risk response for a threat. Typically involves changing some aspect of the organizational activity, i.e. changing the scope, procurement route, supplier or sequence of activities.
Residual risk	The risk remaining after the risk response has been applied.
Retention	A risk response for a threat. A conscious and deliberate decision is taken to retain the threat, having discerned that it is more economical to do so than to attempt a risk response action. The threat should continue to be monitored to ensure that it remains tolerable.
Risk	An uncertain event or set of events which, should it occur, will have an effect on the achievement of objectives. A risk is measured by a combination of the probability of a perceived threat or opportunity occurring and the magnitude of its impact on objectives.
Risk actionee	Some actions may not be within the remit of the risk owner to control explicitly; in that situation there should be a nominated owner of the action to address the risk. He or she will need to keep the risk owner apprised of the situation.
Risk appetite	An organization's unique attitude towards risk-taking which in turn dictates the amount of risk that it considers is acceptable.
Risk cause	A description of the source of the risk, i.e. the event or situation that gives rise to the risk.
Risk committee	A body of independent directors who are responsible for reviewing the company's internal control and risk management systems.
Risk effect	A description of the impact that the risk would have on the organizational activity should the risk materialize.
Risk estimation	The estimation of probability and impact of an individual risk, taking into account predetermined standards, target risk levels, interdependencies and other relevant factors.
Risk evaluation	The process of understanding the net effect of the identified threats and opportunities on an activity when aggregated together.
Risk event	A description of the area of uncertainty in terms of the threat or the opportunity.
Risk identification	Determination of what could pose a risk; a process to describe and list sources of risk (threats and opportunities).
Risk log	*See* risk register.
Risk management	The systematic application of principles, approach and processes to the tasks of identifying and assessing risks, and then planning and implementing risk responses.
Risk management policy	A high-level statement showing how risk management will be handled throughout the organization.
Risk management process guide	Describes the series of steps (from Context through to Implement) and their respective associated activities, necessary to implement risk management.

Term	Definition
Risk management strategy	Describes the goals of applying risk management to the activity, a description of the process that will be adopted, the roles and responsibilities, risk thresholds, the timing of risk management interventions, the deliverables, the tools and techniques that will be used and reporting requirements. It may also describe how the process will be coordinated with other management activities.
Risk manager	A role or individual responsible for the implementation of risk management for each activity at each of the organizational levels.
Risk owner	A role or individual responsible for the management and control of all aspects of individual risks, including the implementation of the measures taken in respect of each risk.
Risk perception	The way in which a stakeholder views a risk, based on a set of values or concerns.
Risk potential assessment	A standard set of high-level criteria against which to assess the intrinsic characteristics and degree of difficulty of a proposed project. It is used to assess the criticality of projects and so determine the level of OGC Gateway Review required.
Risk profile	Describes the types of risk that are faced by an organization and its exposure to those risks.
Risk register	A record of identified risks relating to an initiative, including their status and history.
Risk response	Actions that may be taken to bring the situation to a level where the exposure to risk is acceptable to the organization. These responses fall into one of a number of risk response categories.
Risk response category	For threats, the individual risk response category can be reduction, removal, transfer, retention or share of one or more risks. For opportunities, the individual risk response category can be realization, enhancement or exploitation, or share of one or more risks.
Risk tolerance	The threshold levels of risk exposure, which with appropriate approvals, can be exceeded, but which when exceeded, will trigger some form of response (e.g. reporting the situation to senior management for action).
Risk tolerance line	A line drawn on the summary risk profile. Risks that appear above this line cannot be accepted (lived with) without referring them to a higher authority. For a project, the project manager would refer these risks to the senior responsible owner.
Senior responsible owner	The single individual with overall responsibility for ensuring that a project or programme meets its objectives and delivers the projected benefits.
Severity of risk	The degree to which the risk could affect the situation.
Share	A risk response for a threat. Modern procurement methods commonly entail a form of risk-sharing through the application of a pain/gain formula whereby both parties share the gain (within pre-agreed limits) if the cost is less than the cost plan and share the pain (again within pre-agreed limits) if the cost plan is exceeded.
Sponsor	The main driving force behind a programme or project.

Term	Definition
Sponsoring group	The main driving force behind a programme who provide the investment decision and top-level endorsement of the rationale and objectives of the programme.
Stakeholder	Any individual, group or organization that can affect, be affected by, or perceive itself to be affected by, an initiative (programme, project, activity, risk).
Statement on internal control	A narrative statement by the board of directors of a company disclosing that there is an ongoing process for the identification and management of significant risks faced by the company.
Strategic risk	Risk concerned with where the organization wants to go, how it plans to get there, and how it can ensure survival.
Summary risk profile	A simple mechanism to increase visibility of risks. It is a graphical representation of information normally found on an existing risk register.
Threat	An uncertain event which could have a negative impact on objectives or benefits.
Transfer	A risk response for a threat, whereby a third party takes on responsibility for an aspect of the threat.

Source: OGC Glossary v06, Mar 2008