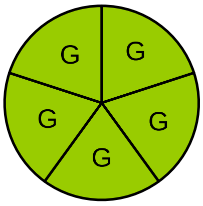
Internal Audit

NHS
Lothian

Risk Management

December 2016

Report Assessment



This report has been prepared solely for internal use as part of NHS Lothian’s internal audit service. No part of this report should be made available, quoted or copied to any external party without Internal Audit’s prior consent.

Contents

Introduction

While risk identification and management remains the responsibility of service managers, specific support is provided by the central Quality Improvement & Support Team. Across the service, risks are recorded electronically on the risk management information system Datix, which facilitates the monitoring and reporting of risks across NHS Lothian.

Datix is populated by local managers based on information from a variety of sources, including adverse event reports, complaints, and litigation. The Quality Improvement & Support Team reviews risk regularly, and produces quarterly reports, for example for service managers, Health & Social Care Partnership managers, and directors.

The Quality Improvement & Support Team can provide risk workshops and provide managers with specialist advice. While risks remain the responsibility of service managers, the Quality Improvement & Support Team aims to provide quality assurances over risk identification, recording and mitigating actions.

This review assessed NHS Lothian's risk management framework against best practice including review of completion of the action plan arising from the 2015/16 self-assessment, and consideration of how risk management is used to inform decision-making within NHS Lothian.

Scope

In accordance with the 2016/17 Internal Audit plan we will perform a review to evaluate the adequacy and effectiveness of the key internal controls that support risk management.

Our review draws on our Organisational Risk Maturity Matrix (Appendix 2), along with NHS Lothian's self-evaluation.

Acknowledgements

We would like to thank all staff consulted during this review for their assistance and cooperation.

Executive Summary

Conclusion

There are appropriate controls in place to for risk management within the organisation, which include a risk management policy and procedure, training which can be provided to both committees and individual staff members, the electronic system Datix which allows for the input and management of risks, and the provision of risk registers to the organisation's governance committees. However, one minor control issue was noted which if addressed would further strengthen arrangements.

Summary of Findings

The table below summarises our assessment of the adequacy and effectiveness of the controls in place to meet each of the objectives agreed for this audit. Definitions of the ratings applied to each action are set out in Appendix 1.

No.	Control Objective	Control objective assessment	Number of actions by action rating			
			Critical	Significant	Important	Minor
1	A risk management framework is in place which promotes effective risk management, including guidance on training, risk recording, and risk reporting.	Green				
2	Good practices in risk management are shared and applied across the organisation.	Green				
3	Risks are recorded and dealt with consistently across the organisation.	Green				
4	There is effective reporting of risks to NHS Lothian committees and the Board.	Green				
5	The actions arising from the 2015/16 self-assessment as set out in the action plan have been completed.	Green				1

Control Objective Ratings

Action Ratings	Definition
Red	Fundamental absence or failure of controls requiring immediate attention

	(60 points and above)
Amber	Control objective not achieved - controls in place are inadequate or ineffective (21 – 59 points)
Green	Control objective achieved – no major weaknesses in controls but may be scope for improvement (20 points or less)

Main findings

We noted a number of areas of good practice during the review.

Both a *Risk Management Policy* and a *Risk Register Operational Procedure* are in place, which provide guidance on the organisation’s risk management framework and how to implement effective risk management practices.

Training has been provided where requested to key committee groups on how to effectively manage risks, and can be provided on request to staff members either in person or over the phone. In addition, training is provided to staff on how to use Datix.

Datix allows all members of staff to log risks, with the risks then being included in the risk registers for all relevant areas. By having a standard form for inputting risks, there is an increased likelihood that risks are recorded and dealt with consistently across the organisation.

Risk registers are provided to the organisation’s governance committees, with the registers allowing committee members to understand the key risks affecting the organisation, and how they’re being managed. Committees manage individual risks where they have the necessary authority and expertise to deal with them. Each meeting of the Board receives a report showing the key risks facing the organisation, enabling it to determine if the risks are being effectively managed.

We identified no significant issues for improvement during the review, though one minor point has been raised which is set out in the Management Action Plan.

Management Action Plan

Control objective 1: A risk management framework is in place which promotes effective risk management, including guidance on training, risk recording, and risk reporting.

We identified no significant issues in relation to this control objective.

Both a *Risk Management Policy* and a *Risk Register Operational Procedure* are in place, which provide guidance on the organisation's risk management framework and how to implement effective risk management practices. These documents include guidance on training, risk recording, and risk reporting.

Control objective 2: Good practices in risk management are shared and applied across the organisation.

We identified no significant issues in relation to this control objective.

Training has provided by the Quality Improvement & Support Team where requested to key committee groups within the past 12 months, including the Acute Services, St. John's Hospital, and Unscheduled Care.

In addition, training can be provided on request by the Quality Improvement & Support Team either by meeting with staff members, or over the phone.

The Risk Management Steering Group has responsibility for monitoring the organisation's risk management arrangements, including the promotion of best practice.

Control objective 3: Risks are recorded and dealt with consistently across the organisation.

We identified no significant issues in relation to this control objective.

Datix allows all members of staff to log risks. The risk is categorised by both its likelihood and potential impact, and staff must provide information about the risk including the areas of the organisation it affects. The risk is then included in the risk registers for all relevant areas. By having a standard form for inputting risks, there is an increased likelihood that risks are recorded and dealt with consistently across the organisation.

In addition, by providing risk registers to committees there is the opportunity for committee members to review risks and their ratings to ensure that they have been correctly stated.

Control objective 4: There is effective reporting of risks to NHS Lothian committees and the Board.

We identified no significant issues in relation to this control objective.

Risk registers containing High and Very High risks are provided to the organisation’s governance committees, including the Board and the Audit & Risk Committee. These registers allow committee members to understand the key risks affecting the organisation, and also provide them with information on how they are being managed. In addition, through the provision of minutes, the Board receives assurance that sub-committees are dealing with their risks effectively.

In addition, an annual report on risk management is provided to the Audit & Risk Committee which sets out the work being performed in the organisation to effectively manage risks.

Control objective 5: The actions arising from the 2015/16 self-assessment as set out in the action plan have been completed.

5.1: NHS Lothian was not tested against all elements of the Audit Scotland Risk Management Toolkit	**Minor**

Observation and Risk:

Audit Scotland produced a *Best Value toolkit: Risk management* in July 2010 with the aim of helping public sector organisations determine if they have effective risk management frameworks in place. The analysis covers key risk management objectives: is risk management actively supported and promoted by senior staff; is there a systematic approach to help ensure that all key risks are identified, prioritised and matched with appropriate responses; are risks and the action taken to mitigate them regularly monitored; and does risk management contribute toward the achievement of corporate objectives.

NHS Lothian voluntarily used the Toolkit to perform an analysis of its risk management arrangements in 2015, with the results of the analysis being provided to the Audit & Risk Committee in June 2015. A further report was provided to the Audit & Risk Committee in June 2016 to outline progress that had been made in further strengthening processes.

However, the analysis performed by NHS Lothian did not include all elements of the Toolkit. Specifically, element 1.4 ("Is risk management used to help identify opportunities as well as risks?") was not covered. The Quality Improvement & Support Team stated that they did not know why this measure was not included in the analysis, though suspected that it must have been an administrative error.

There is a risk that NHS Lothian's risk management arrangements are not as robust as they could be.

Recommendation:

The Quality Improvement & Support Team should perform an analysis of NHS Lothian's risk management arrangements against objective 1.4 of Audit Scotland's *Best Value toolkit: Risk management* (July 2010), with the results then being provided to the Audit & Risk Committee.

Management Response:

It is not felt to be of added value to conduct an analysis of arrangements against 1.4 'Is risk management used to help identify opportunities as well as risk?' as this is already an integral part of the risk management process. Embedded in the ongoing review of risks, the analysis is used routinely to inform improvements and to look at opportunities to do things differently. For example, risk around sustainability of GP services was used as an opportunity to hold a summit and look at development opportunities for doctors and other staff, for HAI risk, an opportunity to change prescribing practice was identified.

Responsibility: Jo Bennett, Associate Director for Quality Improvement & Safety	**Target date:** N/A

Appendix 1 - Definition of Ratings

Management Action Ratings

Action Ratings	Definition
Critical	The issue has a material effect upon the wider organisation – 60 points
Significant	The issue is material for the subject under review – 20 points
Important	The issue is relevant for the subject under review – 10 points
Minor	This issue is a housekeeping point for the subject under review – 5 points

Control Objective Ratings

Action Ratings	Definition
Red	Fundamental absence or failure of controls requiring immediate attention (60 points and above)
Amber	Control objective not achieved - controls in place are inadequate or ineffective (21 – 59 points)
Green	Control objective achieved – no major weaknesses in controls but may be scope for improvement (20 points or less)

Appendix 2 – Risk Maturity Matrix

Risk Maturity Questionnaire	Risk Naïve	Risk Aware	Risk Defined	Risk Managed	Risk Enabled
Key characteristics	No formal approach developed for risk management	Scattered silo based approach to risk management	Strategy and policies in place and communicated. Risk appetite defined	Enterprise wide approach to risk management developed and communicated	Risk management and internal control fully embedded in the operations
Category/Question	**Explanation of risk maturity level**				
Leadership					
How are the organisation's objectives identified and defined? Who are they communicated to?	No formal objectives set. No guidance on risk management offered	Objectives defined, but a process cannot be evidenced. Only senior staff have knowledge of objectives. Risk management encouraged but no guidance given	Objectives defined and agreed by the Board. Some staff aware of objectives. Some risk management guidance offered by senior management	Objectives defined following a review of the organisation. Staff are aware of the objectives. Senior management have developed and communicated risk management guidance to key people	Rigorous objective setting and risk management process occurs periodically. The output is fully embedded in the organisation and communicated to all staff
How has the risk appetite of the organisation been defined? How does this operate in practice? What is the organisational culture in terms of risk management?	No risk appetite in place. Risk management practices are reliant upon individual integrity.	No formal risk appetite in place but a cultural philosophy is in place. Risk management championed by a senior member of the organisation.	Risk appetite defined in risk methodology, but management apply common sense approach to the application. Board discuss risks as per management's views.	Risk appetite defined in terms of the risk scoring methodology and applied in practice to identify risks in need of further management. Board empower managers with risk management processes but retain oversight.	Risks outside of the risk appetite escalated to the right level of the organisation and decision making process is evidenced through debate. Board champion risk management and drive change through this.

Risk strategy and policies

How has the strategy of the organisation in terms of risk management been identified and created?	No strategy for risk management in place	No formal strategy in place but a cultural philosophy is present (ie single person's approach communicated)	Documented strategy links to objectives but not developed in consultation with others	Strategy developed through analysis of existing arrangements and Board approved	Detailed strategy developed via consultation from across the organisation. Live document
How is the risk management strategy and/or policy applied in practice?	No strategy or policy in place or not applied	Strategy and/or policy verbally communicated but application not monitored	Application of documented strategy and/or policy by management	Strategy implemented by departmental instruction to other staff members	Staff engaged in strategy development and implementation. Everyone 'owns' the strategy

People

How has the organisation ensured that its people are aware of risk management tools and techniques?	No training provided	Limited training provided	Training has been provided on understanding risks	Training has been provided on risk management strategies and ownership	Training is ongoing, with regular updates across the organisation and new methodologies being applied where relevant.
Who is responsible for risk management within the organisation?	One individual	Senior management	Individuals from across the organisation and management	Groups within each function in combination with management	All staff

Processes

What process has been followed to identify and record risks?	Reactive responses to risks as they occur, no formal logging	Individual identification and logging of risks in own area	Key risks identified, logged and communicated in a consistent manner	Defined process followed to identify and log risks, all parts of organisation involved. Opportunities also part of process	Fundamental part of all activities, including projects. Risks identified, logged and ranked as matter of course, opportunities regularly being identified
What scoring system is used to assess risks? How is this applied in practice?	No scoring system	Some scoring occurs but not consistently applied across the organisation	Standard scoring process applied to corporate risks, but not across the organisation	Defined process for scoring risks that is consistently applied	Process is used to drive change - scoring is challenged and live
How have responses to the risks been identified (eg controls in the risk register), selected and implemented?	No responses to risks identified	Responses not documented but applied in a reactive manner	Responses documented and assessed for adequacy. Management rely upon other to implement actions	Responses selected based upon the need to the organisation. Assurance obtained that responses operating effectively.	Responses identified and implemented as the risk is identified. Assurance built into the controls. Staff identify and implement responses timely
What methods/controls are in place to review risks and monitor the operation of key controls?	None or management rely upon nothing bad happening	Risk logging is isolated and poorly reviewed. Some controls operate without any monitoring, whilst others are tested periodically.	Key risks are logged but rarely reviewed. Controls are monitored on a periodic basis, either through testing or reviews by audit	Risks are logged and regularly reviewed. Controls monitored regularly and assurance sought	Risks logged, ranked and live. Owners champion mitigation and controls. Controls monitored in line with importance. Assurance provided as a matter of course

Risk Handling

How are risks reviewed by the organisation/audit unit? How often does this take place?	No formal review of risks	Some risks are reviewed, but infrequently	Risks are reviewed on a periodic basis by risk owners. Limited documentation	Risks are reviewed in consultation with others to meet the needs of the organisation and documentation exists	Risks are live, continuously reviewed and communicated across the organisation,
What evidence is there that risk management is effectively operating within the organisation? How is it evidenced in decision making?	Reliance placed on no risks crystallising	Management review risk management activities periodically, generally not in conjunction with relevant decision-making	Management required to report on risk management activity periodically and review new decisions in its light	Risk management integrated into decision making, assurance sought from one source and actions addressed	Risk management drives decision making, assurance actively sought from a variety of sources and improvement continuous

Outcomes

How is risk management built into performance management processes?	Risk management exists in isolation	Performance reviews do not consider risk management unless major issue has arisen	Periodic reviews of performance include assessment of negative risk management performance	Periodic reviews of performance include assessment of positive and negative risk management performance	Continuous assessment of risk management performance, both positive and negative. Risks drive performance assessment
How well has the organisation achieved its desired outcomes? How much of this is attributed to effective risk management?	No outcomes achieved	Unknown risks materialised preventing outcomes being achieved or outcomes achieved due to luck rather than judgement	Some outcomes achieved, but some surprises present	Risk management believed to play a part in achieving all outcomes but cannot be evidenced as such	Risk management clearly demonstrates how outcomes have been achieved and is a primary reason