Internal Audit

Risk Management

February 2019

Internal Audit Assurance Assessment:

Objective One	Objective Two	Objective Three	Objective Four	Objective Five
Significant Assurance	Significant Assurance	Moderate Assurance	Limited Assurance	Limited Assurance

Timetable

Date closing meeting held: 12 February 2019

Date draft report issued: 12 February 2019

Date management comments received: 14 February 2019

Date Final report issued: 14 February 2019

Date presented to Audit and Risk Committee: 25 February 2019

Contents

1. Introduction

1.1 NHS Lothian has a well established Corporate Risk Register. Recently work has been undertaken to consider the corporate risks reflected in the risk register and whether the risks included are the strategic risks that would impact on NHS Lothian failing to achieve its strategic objectives alongside how risks are articulated, reported, monitored and actions taken.

1.2 At the Audit and Risk Committee meeting in August 2018 the updated risk management framework was approved and a new approach to the strategic risk register discussed including the update of the register into a new improved format. The future register will link risks to corporate objectives and set out a risk description, linked key risks, associated strategic plans, controls and key measures.

1.3 The revised format is designed to focus on what the plans are to address the risks and how plans need to be flexed and changed in a changing risk environment.

Scope

1.4 Recognising the ongoing work in respect of the corporate risk register we performed a review of risk by focusing on three corporate risks. The risks sampled were chosen because they represent clear challenges to the effective provision of healthcare. We explored with the assigned risk handler questions including:

- How they understand and articulate the risk
- What assurance do they get the risk is being controlled and managed
- How do they devise suitable plans to mitigate the risk and how do they ensure they are action focused and flexible.

1.5 In addition, we supported the work of the Associate Director for Quality Improvement & Safety and together worked with the risk handler to map the controls and actions in place considering how the risk will be mitigated. This mapping work will support the better articulation of controls within the register and support management in identifying gaps within the control environment.

1.6 The specific risks which were covered by this audit were:

- Risk 3726 – Timely Discharge of Inpatients
- Risk 3829 – GP Workforce Sustainability
- Risk 3828 – Nursing Workforce – Safe Staffing Levels.

Acknowledgements

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

2. Executive Summary

Summary of Findings

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

No.	Control Objectives	Assurance Level	Number of findings			
			Critical	High	Medium	Low
1	Risk owners are unaware of their role in respect of risk management and are unaware of the controls or plans in place to mitigate risks.	Significant Assurance	-	-	-	-
2	Plans to mitigate risks are not considered “live” or suitably flexible to deliver the plans in place.	Significant Assurance	-	-	-	-
3	Plans to mitigate risks are static and therefore not altered to reflect the changing risk conditions and are not reassessed.	Moderate Assurance	-	-	2	-
4	The controls in place to mitigate risk are either: not controls; are not clearly articulated and understood or are not designed to mitigate the risks required.	Limited Assurance	-	1	-	-
5	Where the risks are shared risks and / or require the support of others to mitigate the risks the plans are not shared, joined up and could lead to gaps in the management of the risk.	Limited Assurance	-	1	-	-
TOTAL			**-**	**2**	**2**	**-**

Conclusion

2.2 The risk owners for the three risks sampled for this review were all aware of their responsibilities with regard to managing the risks, and risk management plans are changed as required to reflect changes to circumstances. However, Datix is not being updated with sufficient frequency, risk handlers may need additional risk management training to support their work, risk controls are not always stated as SMART objectives or have associated KPIs, and there is no regular confirmation that the risk registers of the HSCPs are being reviewed by risk handlers.

2.3 One of the risks sampled as part of this review was GP Workforce Sustainability (risk 3829). In addition to the analysis performed during this review, an in-depth audit of the management of this risk is currently being performed by Internal Audit.

Main Findings

2.4 The risk owners for the three risks sampled for this review were all aware of their responsibilities with regard to managing the risks, and also with regard to providing updates to the electronic system Datix and to relevant groups and committees. The plans in place to manage the risks are being updated on Datix, with plans changing as required to reflect changes to circumstances and reported through the pertinent governance committees.

2.5 We identified the following areas for improvement during the review:

2.5.1 Periodically the person tasked with handling each risk should record updates on Datix. These updates will be reflected in the documentation provided to senior committees, such as the Audit & Risk Committee. However, for the three corporate risk register risks sampled for this audit, updates were not always provided in a timely manner, and updates were not always sufficiently detailed.

2.5.2 All risks in Datix have a stated risk handler who is charged with managing the risk. As part of their duties the risk handlers must identify how the risk affects the organisation's objectives, what controls will be effective in managing the risk, and how to measure the effectiveness of those controls. However, although the risk handlers sampled for this review are experts in their areas, this audit has highlighted that there are weaknesses in the way that risk register entries are completed and maintained. This may be due to insufficient formal training in risk management.

2.5.3 A review of the three corporate risk register risks sampled by this audit showed that, for all three risks, controls had been stated in Datix, including committee oversight, reporting arrangements, and some performance measures. However, none were stated as SMART objectives, and outcomes measures were not stated for all controls.

2.5.4 It is important for NHS Lothian's risk handlers to be aware of how effectively relevant controls are operating in the HSCPs. However, the quarterly risk register updates made by the risk handlers do not confirm that they have reviewed any relevant risks and controls contained within the risk registers of the HSCPs.

2.5.5 Details of these 2 High findings and 2 Medium findings are set out in the Management Action Plan.

3. Management Action Plan

Finding 1	
Control objective 3: Plans to mitigate risks are static and therefore not altered to reflect the changing risk conditions and are not reassessed. **Associated risk of not achieving the control objective: Updates to Datix are not always sufficiently frequent or detailed.**	**Medium**
Observation and risk NHS Lothian uses the electronic system Datix to record risks affecting the organisation. Periodically the person tasked with handling each risk should record updates on Datix to state the current position. For items on the corporate risk register, staff from the Risk Management team will contact the risk handlers each quarter to request updates. The corporate risk register is reviewed at each meeting of the Audit & Risk Committee and the Board. However, for the three corporate risk register risks sampled for this audit for the period January 2017 to November 2018, quarterly updates were not always provided in a timely manner: • Risk 3726 – Timely Discharge of Inpatients. Only 7 (88%) of the expected 8 updates were provided, with the longest gap between updates being 5 months. • Risk 3828 – Nursing Workforce – Safe Staffing Levels. 8 of the expected 8 updates were provided, but the longest gap between updates was 4 months. • Risk 3829 – GP Workforce Sustainability. Only 6 (75%) of the expected 8 updates were provided, with the longest gap between updates being 6 months. It should be noted that during this period the Director of Primary Care Transformation was in the process of being appointed. If Datix is not updated with sufficient regularity, and updates are not sufficiently detailed, then there will be a reduced confidence that risks are being effectively managed.	
Recommendation Each corporate risk register risk should be updated quarterly in Datix with a detailed narrative, at least including updates to controls and performance against objectives.	
Management Response The team has a reliable process for requesting and receiving risk register quarterly updates which can be altered due to changes in risk owners/handler or requests from governance committees to review a risk. The Audit & Risk Committee asked for the Timely Discharge of Inpatients risk (formerly Delayed Discharge) to be reviewed and the outcome of the review was considered at the June 2017 Committee. This review process resulted in the risk not being updated for one quarter.	

It has however become clear that we do not have a reliable process for ensuring that handlers record assurance levels agreed by governance committees, associated actions and plans. The Management Action 1. Agree a process for recording governance committees' assessment of risks, associated plan, controls and actions. 2. Reaffirm with risk owners and handlers the quarterly review timeline and actions. Escalate to Executive Director for risk management (Medical Director) should updates not be forthcoming.	
Responsibility: Jo Bennett, Associate Director for Quality & Safety	Target date: 31 May 2019

Finding 2	
Control objective 3: Plans to mitigate risks are static and therefore not altered to reflect the changing risk conditions and are not reassessed. **Associated risk of not achieving the control objective: Risk handlers are not always provided with sufficient support to manage their risks.**	**Medium**
Observation and risk All risks in Datix have a stated risk handler who is charged with managing the risk. As part of their duties the risk handlers must identify how the risk affects the organisation's objectives, what controls will be effective in managing the risk and how to measure the effectiveness of those controls. However, although the risk handlers sampled for this review are experts in their areas, this audit has highlighted that there are weaknesses in the way that risk register entries are completed and maintained.. This may be due to insufficient formal training in risk management. The Quality & Safety Assurance Lead has met with risk handlers in the past to help them restate within Datix the controls for their risks. If risk handlers do not have formal training in risk management then there is a reduced risk that risk register entries are fully and correctly stated and that risks are effectively managed.	
Recommendation Each risk handler for corporate risk register risks should receive regular training and support to help ensure that risk register entries are fully and correctly stated, and effectively managed.	
Management Response Training has been provided at an operational level and one-to-one support for Corporate Risk handlers as illustrated above. The Management Action All new Corporate Risk handlers will have formal one-to-one training with a member of the risk team. Existing handlers will receive training as part of the introduction to the new template, should it be approved by the Board in April 2019.	
Responsibility: Jo Bennett, Associate Director for Quality & Safety	Target date: 31 December 2019

Finding 3	
Control objective 4: The controls in place to mitigate risk are either: not controls; are not clearly articulated and understood or are not designed to mitigate the risks required. **Associated risk of not achieving the control objective: The controls used to manage risks are not always clearly stated.**	**High**

Observation and risk

Once a risk has been identified, controls to manage the risk should be determined which are comprehensive and clearly stated. A review of the three corporate risk register risks sampled by this audit showed that, for all three risks, controls had been stated in Datix, including committee oversight, reporting arrangements, and some performance measures.

However, our review also noted:

- Risk 3726 – Timely Discharge of Inpatients. 6 controls were stated, but none were stated as SMART objectives. Only two outcome measures were stated, but neither were stated in detail. For example, some controls stated "NHS Lothian's Winter Planning Project Board is now established as the NHSL Unscheduled Care Committee in collaboration with the Integrated Joint Boards" (which does not state what the Board is expected to achieve), and "Integrated Joint Boards will report via the Deputy Chief Executive to Scottish Government on the delivery of key targets which include Delayed Discharges and actions in response to performance" (which does not state what will be achieved by this activity)
- Risk 3828 – Nursing Workforce – Safe Staffing Levels. 12 controls were stated, but none were stated as SMART objectives. Only three outcome measures were stated, but none were stated in detail. For example, some controls stated "Recruitment Group, Safe Staffing and Nursing Workforce Groups to plan requirements" (which does not state when this work will be completed), and "Recruitment meetings to oversee the implementation of the recruitment plan are being held monthly" (which does not state when the work is expected to be completed)
- Risk 3829 – GP Workforce Sustainability. 8 controls were stated, but none were stated as SMART objectives. Only one outcome measure was stated, and it wasn't stated in detail. For example, some controls stated "Regular updates reported to Healthcare Governance Committee" (which does not state what the information will be included in the updates), and "NHS Lothian Board Strategic plan, HSCP primary care transformation plans and reports to Board and Strategic Planning Committee" (which does not state in detail what the committees are expected to achieve and by when).

If the controls used to manage risks are not stated clearly and comprehensively then there is reduced confidence that there is effective oversight of the management of risks.

Recommendation

All corporate risk register risks should be reviewed to confirm that the controls stated are complete, that they are stated as SMART objectives, and that they all have KPIs.
Management Response There are a number of plans, which include objectives, measures and controls, submitted to governance committees for consideration. These however are not reliably recorded on Datix or in NHS Lothian's risk register report. The Management Action 1. Controls will be reviewed as part of the introduction of the new template should it be approved by the April Board (see A&RC risk register paper Feb 19 for recommendation to adopt the new template). This will include explicit measures to assess the impact of plans and strength of controls. If the template is not supported then training and one-to-one support will take place with risk owners and handlers. 2. See management action 1 under findings 1 above

Responsibility:	Target date:
Jo Bennett, Associate Director for Quality & Safety	31 December 2019

Finding 4	
Control objective 5: Where the risks are shared risks and / or require the support of others to mitigate the risks the plans are not shared, joined up and could lead to gaps in the management of the risk. **Associated risk of not achieving the control objective: There is not always effective co-ordination of risk registers.**	**High**

Observation and risk

In order for NHS Lothian to achieve its objectives it is essential to have effective working across all areas, including within the four health & social care partnerships (HSCPs). As such, it is important for NHS Lothian's risk handlers to be aware of how effectively relevant controls are operating in the HSCPs.

However, the quarterly risk register updates made by the risk handlers do not confirm that they have reviewed any relevant risks and controls contained within the risk registers of the HSCPs. An NHS Lothian risk handler for one of the risks sampled for this audit stated that they did not receive copies of relevant risk registers maintained by the HSCPs.

If NHS Lothian's risk handlers are not aware of how well the HSCPs are managing controls relevant to NHS Lothian's corporate risks then there is a reduced confidence that the controls are operating effectively.

Recommendation

Every time risk handlers provide risk register updates they should confirm that they have reviewed all relevant risk registers for the HSCPs to confirm that all relevant controls are operating effectively.

Management Response

There is merit in similar risks at an operational level being considered as part of the corporate risk controls to coordinate plans to mitigate risk, especially those that require a single-system response.

The Management Action

1 Write to all handlers/owners informing them that similar operational risks should be considered as a control mechanism for the corporate risk they are responsible for and record in Datix at a minimum of twice a year.

Responsibility:	Target date:
Jo Bennett, Associate Director for Quality & Safety	30 April 2019

4. Appendix 1 - Definition of Ratings

Findings and management actions ratings

Finding Ratings	Definition
Critical	A fundamental failure or absence in the design or operating effectiveness of controls, which requires immediate attention
High	A key control failure has been identified which could be either due to a failure in the design or operating effectiveness. There are no compensating controls in place, and management should aim to implement controls within a calendar month of the review.
Medium	A control failure has been identified which could be either due to a failure in the design or operating effectiveness. Other controls in place partially mitigate the risk to the organisation, however management should look to implement controls to fully cover the risk identified.
Low	Minor non-compliance has been identified with the operating effectiveness of a control, however the design of the control is effective

Report ratings and overall assurance provided

Report Ratings	Definition	When Internal Audit will award this level
No assurance	The Board cannot take any assurance from the audit findings. There remains a significant amount of residual risk.	The controls are not adequately designed and / or operating effectively and immediate management action is required as there remains a significant amount of residual risk (for instance one Critical finding or a number of High findings)
Limited assurance	The Board can take some assurance from the systems of control in place to achieve the control objective, but there remains a significant amount of residual risk which requires action to be taken.	This may be used when: • There are known material weaknesses in key control areas. • It is known that there will have to be changes that are relevant to the control objective (e.g. due to a change in the law) and the impact has not been assessed and planned for. The controls are deficient in some aspects and require management action (for instance one 'high' finding and a number of other lower rated findings)

Moderate assurance	The Board can take reasonable assurance that controls upon which the organisation relies to achieve the control objective are in the main suitably designed and effectively applied. There remains a moderate amount of residual risk.	In most respects the "purpose" is being achieved. There are some areas where further action is required, and the residual risk is greater than "insignificant". The controls are largely effective and in most respects achieve their purpose with a limited number of findings which require management action (for instance a mix of 'medium' findings and 'low' findings)
Significant assurance	The Board can take reasonable assurance that the system(s) of control achieves or will achieve the control objective. There may be an insignificant amount of residual risk or none at all.	There is little evidence of system failure and the system appears to be robust and sustainable. The controls adequately mitigate the risk, or weaknesses are only minor (for instance a low number of findings which are all rated as 'low' or no findings)