

NHS Lothian

Internal Audit 2023/24

Risk Management

April 2024

FINAL REPORT

Emily Mayne

Head of Internal Audit

T 0121 232 5309

E emily.j.mayne@uk.gt.com

Hannah McKellar

Manager, Public Sector Audit

T 0141 233 0886

E hannah.l.mckellar@uk.gt.com

Pippa Jackson

Senior Manager

T 0121 232 3567

E pippa.g.jackson@uk.gt.com

Linda Chadburn

Independent Consultant

T: 0161 953 6915

E: linda.g.chadburn@uk.gt.com

Contents



This report is confidential and is intended for use by the management and directors of NHS Lothian. It forms part of our continuing dialogue with you. It should not be made available, in whole or in part, to any third party without our prior written consent. We do not accept responsibility for any reliance that third parties may place upon this report. Any third party relying on this report does so entirely at its own risk. We accept no liability to any third party for any loss or damage suffered or costs incurred, arising out of or in connection with the use of this report, however such loss or damage is caused.

It is the responsibility solely of NHS Lothian management and directors to ensure there are adequate arrangements in place in relation to risk management, governance, control and value for money.



Section	Page
Executive summary	03
Headline messages	04
Summary of findings	06
Detailed findings & action plan	07
Appendices	16
Appendix 1 Staff involved	17
Appendix 2: Documents reviewed	18
Appendix 3: Our assurance levels	19
Report Distribution	
Executive Lead:	
• Tracey Gillies, Medical Director	
For action:	
• Jill Gillies, Associate Director of Quality	
For Information:	
• Calum Blackburn, Chief Executive	
• Craig Marriott, Director of Finance	
• Corporate Management Team	
• Audit and Risk Committee	

Executive summary



Background

Risk management enhances strategic planning and prioritisation, improves service delivery, assists in achieving objectives and strengthens the ability to be agile to respond to the challenges faced. There will always be a degree of risk in whatever an organisation is trying to achieve. For NHS Lothian, that is the provision of safe and effective healthcare care services in secondary, community and primary care settings.

NHS Lothian's Board has a systematic approach to the management of risk in all of its functions and services. As part of this approach, the Board expects employees to give greater priority to managing and reducing risks associated with the safety of people, the experience of people who receive care, and the delivery of effective care. Our review, as directed by management, focussed on the risk management arrangements in place which integrate with the Health & Social Care Partnerships, specifically focusing on East Lothian and West Lothian Health & Social Care Partnerships.



Objectives

Our review focussed on the following key risks at the interface between NHS Lothian and the Health and Social Care Partnerships:

- Roles and responsibilities for risk management are not consistently defined across operational services and staff are unaware of their responsibilities.
- There is an absence of an accessible risk management training programme and operational services staff are not equipped and capable to deliver their responsibilities in relation to risk management.
- Identification, assessment, treatment and control, reporting and monitoring of risks does not take place consistently and in a timely manner across operational services and as set out in the Risk Management Framework.
- There is no clear and consistent approach to escalate operational risks from an operational service level to divisional level for inclusion on the Risk Register.



Limitations in scope

Please note that our conclusion is limited by scope. It is limited to the risks outlined above. Other risks exist in this process which our review and therefore our conclusion has not considered. Where sample testing has been undertaken, our findings and conclusions are limited to the items selected for testing.

This report does not constitute an assurance engagement as set out under ISAE 3000.



Acknowledgement

We would like to take this opportunity to thank your staff for their co-operation during this internal audit.

Headline messages



Conclusion

Moderate Assurance

We have reviewed the processes and controls around Risk Management at the interface between NHS Lothian and the Health and Social Care Partnerships and have concluded that we can provide a **MODERATE level of assurance**. This was confirmed through testing over specific areas of the organisation, reviewing key documents, observations at meetings and through discussions with management.

Following approval of the audit scope, we initially agreed to focus our work on the risk management processes used within five departments of the organisation; three from Acute Services and two from the Health and Social Care Partnerships (HSCPs). At the onset of our fieldwork, the focus of our work was revised by management to focus on the HSCPs only, with an overall aim of informing the understanding of the processes used by each Partnership and identifying any variances and inconsistencies. The outcomes would be used to influence future NHS Lothian risk management strategy development.

Due to the amount of fieldwork required to meet the overall objective, it was agreed that the field work would be reduced to review two of the four HSCPs, East Lothian and West Lothian, with an option to focus on the processes used at the remaining two HSCPs at a future audit cycle. Additional days were also provided due to the amount of interviews undertaken to inform our findings.

The objectives reviewed are set out on page 5 with the assurance rating we have assessed for each one and the number of recommendations raised. We have reported by exception against the areas where we consider that Management and the Audit and Risk Committee should focus their attention. We have raised 8 recommendations as a result of our testing. One of the four objectives has received moderate assurance, which has incurred one medium risk recommendation, as follows:

- To enable those with responsibility to monitor and review risks and risk registers to have all the information required to make an informed decision, reports run from Datix for Partnerships should include 'essential data fields', including the target risk score, as a minimum.

The findings of one risk area of our review were deemed by the Executive Lead to not be within the control of NHS Lothian. We have therefore not provided a level of assurance against this risk area. However we have still reported our findings and have indicated the rating as 'not rated'.

The remaining findings raised within this audit relate to the importance of reflecting risk management responsibilities in relevant job descriptions, providing a centralised link to all Risk Management training resources and introducing a process to monitor that key staff have received an appropriate level of risk management training. Additionally, to formalise a standing agenda item for all relevant meetings where risks should be discussed, and that action plans to address risks attributable to NHS Lothian should be accessible from Datix, and that support is provided to HSCPs to ensure work continues to develop risk registers for those teams and services which do not currently have a risk register or log of NHS Lothian's risks.

We recognise that the Associate Director of Quality has been in post less than one year but shows good vision for the future and is working to develop the risk management framework across all levels of the organisation. It is this consideration which has enabled us to provide a moderate assurance opinion overall. Our recommendations will support the Associate Director of Quality to create a more robust Risk Management Framework.

Headline messages



Conclusion

We have raised 8 recommendations. The grading of these recommendations, based on risk, is summarised in the table below.

Objectives	Assurance rating	Number of recommendations			
		High	Medium	Low	Imp
1. Roles and Responsibilities for Risk Management are not consistently defined across Operational Services and staff are unaware of their responsibilities.	Significant Assurance	-	-	1	-
2. There is an absence of an accessible Risk Management training programme and Operational Services staff are not equipped and capable to deliver their responsibilities in relation to risk management.	Significant Assurance	-	-	1	-
3. Identification, assessment, treatment and control, reporting and monitoring of risks does not take place consistently and in a timely manner across Operational Services and as set out in the Risk Management framework.	Moderate Assurance	-	1	3	2
4. There is no clear and consistent approach to escalate operational risks from an operational service level to divisional level for inclusion on the Risk Register.	Not rated	-	-	-	-

Summary of findings



Examples of where recommended practices are being applied

- NHS Lothian has a Risk Management policy in place which provides a sound foundation to build risk management processes upon.
- The recently appointed Associate Director of Quality has vision and ambition to cascade knowledge and skills across the organisation to deliver a robust, standardised risk management framework.



Areas requiring improvement

- To ensure risk management responsibilities are allocated according to service need and that the required capabilities are aligned to roles, risk management responsibilities should be reflected in key job descriptions.
- To ensure staff are aware of all the risk management training resources and how to access training resources, a centralised link to all Risk Management training resources should be accessible.
- NHS Lothian should be assured staff with responsibility for managing risk registers are sufficiently trained, and a process should be introduced to monitor whether staff have received the training required, including any refresher training.
- Identification of new and emerging risks are not always captured during meetings with General Managers. To ensure this occurs, there should be a formalised standing agenda item on all relevant meeting agendas.
- Reports run from Datix for Partnerships should include 'essential data fields', including the target risk score, as a minimum. This will enable those with responsibility to monitor and review risks and risk registers to have all the information required to make an informed decision.
- Action plans to treat risks attributed to NHS Lothian should be accessible via Datix.
- Not all teams and services have a risk register or log, and work should continue to support Partnerships to develop risk registers on Datix.
- Review of the risk register should be undertaken to address issues or anomalies which should be addressed in a timely manner to ensure the information on Datix is accurate and complete.
- Risk escalation pathways should be visible through the HSCPs and should be reflected in policy and standard operating procedures.

Detailed findings & action plan

1.	Significant Assurance	Roles and Responsibilities for Risk Management are not consistently defined across Operational Services and staff are unaware of their responsibilities.	
Finding and implication		Audit recommendation	Management response, including actions
<p><u>Risk management responsibilities are not detailed in key job descriptions.</u></p> <p>We spoke with staff at various levels of the Partnerships including employees of NHS Lothian.</p> <p>From discussions held, it was noted that staff recognised that risk management was part of their responsibilities. However, our review of job descriptions identified that risk management was not included in the responsibilities for the Chief Nurse for West Lothian and the Service Lead for the MSK service in West Lothian, both of whom are employed by NHS Lothian.</p>		<p>Recommendation 1.</p> <p>Risk management responsibilities should be reflected in the relevant job descriptions at the next scheduled review date to ensure responsibilities are allocated according to service need and the required capabilities are aligned to roles.</p>	<p>Actions:</p> <p>As scheduled reviews for key job descriptions are undertaken, risk management responsibilities will be specifically detailed within these.</p> <p>Responsible Officer: Chief Officer West Lothian HSCP</p> <p>Executive Lead: Executive Medical Director</p> <p>Due Date: 31 May 2024</p>

Detailed findings & action plan

2.	Significant Assurance	There is an absence of an accessible Risk Management training programme and Operational Services staff are not equipped and capable to deliver their responsibilities in relation to risk management.	
Finding and implication		Audit recommendation	Management response, including actions
<p><u>Refresher risk management training is not provided.</u></p> <p>As part of induction training requirements, there is accessible Risk Management mandatory training provided to all NHS Lothian staff. Additional training around Risk Management can be accessed by staff on an ad-hoc basis when required or as directed to by their line manager.</p> <p>From conversations held with personnel within the organisation, there was an inconsistent awareness amongst staff regarding the knowledge of additional risk management training available.</p> <p>Furthermore, staff who are responsible for monitoring and reviewing risks noted they had completed risk training numerous years ago and there is no formal requirement to attend, or access, any further refresher training around Risk Management.</p>		<p>Recommendation 2.</p> <p>To ensure staff are aware of all the risk management training resources, how to access them and to be assured staff with the responsibility for managing risk registers are sufficiently trained, NHS Lothian should provide a centralised link to all Risk Management training resources. A process should be introduced to ensure that those staff charged with responsibility for managing, monitoring and reviewing the risk register are required to undertake refresher training in Risk Management and this should be discussed as part of their performance appraisals.</p>	<p>Actions:</p> <ul style="list-style-type: none"> i) Centralised resource on the intranet will be developed to provide links to all risk management training resources. ii) Managers will ensure staff with responsibility for risk management undertake additional training as identified through their appraisal discussions. This will be promoted through the Good Housekeeping Workshops for all Managers. <p>Responsible Officer:</p> <ul style="list-style-type: none"> i) Associate Director of Quality; ii) Associate Director of HR <p>Executive Lead: Executive Medical Director</p> <p>Due Date: 31 May 2024</p>

Detailed findings & action plan

3.1	Moderate Assurance	Identification, assessment, treatment and control, reporting and monitoring of risks does not take place consistently and in a timely manner across Operational Services and as set out in the Risk Management framework.	
Finding and implication		Audit recommendation	Management response, including actions
<p><u>The method to share new and emerging risks should be formalised.</u></p> <p>One of the purposes of NHS Lothian’s Risk Management policy is to provide a consistent and systematic process for the identification of risks. We spoke with staff at various levels of the Partnerships with risk management responsibilities including those employed by NHS Lothian, and senior management indicated that emerging risks can be identified by anyone. These are discussed at both 1 to 1 and team meetings before being shared with the relevant General Manager for discussion at General Management Meetings.</p>		<p>Recommendation 3.</p> <p>To ensure the sharing of emerging risks from teams and services to the Partnerships General Managers, NHS Lothian should ensure there is a formalised standing agenda item associated with risk management on all relevant meeting agendas.</p>	<p>Actions:</p> <p>General Managers in HSCPs should add a standing agenda item associated with risk management to all relevant meeting agendas.</p> <p>Responsible Officer: Heads of Health, HSCPs</p> <p>Executive Lead: Executive Medical Director</p> <p>Due Date: 31 May 2024</p>
<p><u>Reports run from Datix do not provide information required to make an informed decision.</u></p> <p>NHS Lothian’s Central Risk Management Team provided us with reports from Datix providing risks on the Partnership Risk Registers. This highlighted that risk assessments, including scoring, alignment to risk appetite and the risk response was not detailed completely; with only the current score and risk level identifiable as High, Medium or Low as appropriate. A more in-depth review of the live risk registers identified that the ‘consequence’ and ‘likelihood’ data fields and the ‘Target’ data field are not routinely included on the risk register reports produced and shared with the Partnerships.</p> <p>Partnerships request the fields they want within the reports. It is important that those with responsibility to review risks and risk registers have all the information required to make an informed decision. We recommend that reports run from Datix for Partnerships include ‘essential data fields’, including those gathered during risk assessment as a minimum.</p>		<p>Recommendation 4.</p> <p>To enable those with responsibility to monitor and review risks and risk registers have all the information required to make an informed decision, reports run from Datix for Partnerships should include ‘essential data fields’, including the target risk score, as a minimum.</p>	<p>Actions:</p> <p>The Quality Directorate will work with HSCPs to agree ‘essential data fields’ for report run from Datix for Partnerships to enable those with responsibility to monitor and review risks and risk registers have all the information required to make informed decisions.</p> <p>Responsible Officer: Associate Director of Quality and Heads of Health, HSCPs</p> <p>Executive Lead: Executive Medical Director</p> <p>Due Date: 31 May 2024</p>

Detailed findings & action plan

3.2	Moderate Assurance	Identification, assessment, treatment and control, reporting and monitoring of risks does not take place consistently and in a timely manner across Operational Services and as set out in the Risk Management framework.	
Finding and implication	Audit recommendation	Management response, including actions	
<p><u>Action plans are not consistently accessible, reviewed or managed alongside the risk.</u></p> <p>NHS Lothian’s Risk Management policy describes an internal control as ‘a measure put in place to mitigate a risk’.</p> <ul style="list-style-type: none"> • A control can be described as an existing strategy or process already in place; for example, a policy or reporting framework. • A treatment can be described as some additional action needed to help control a risk to an acceptable level. Treatments are generally detailed in an action plan. <p>It is important to have full oversight of the additional actions to ensure the risk can be managed appropriately.</p> <p>Datix has a functionality to capture action plans and to attach an action plan as a stand-alone document. Our review highlighted that these functions are not always used. Both NHS Lothian and Council staff have access to Datix.</p>	<p>Recommendation 5.</p> <p>In relation to risks attributed to NHS Lothian, action plans to treat risks should be accessible via Datix; this could be either through the use of the action planning functionality of Datix or by attaching action plan documents to the system.</p>	<p>Actions:</p> <p>The Quality Directorate will work with HSCPs to ensure the capturing of action plans within Datix or as a stand-alone document.</p> <p>Responsible Officer: Associate Director of Quality and Heads of Health, HSCPs</p> <p>Executive Lead: Executive Medical Director</p> <p>Due Date: 31 May 2024</p>	

Detailed findings & action plan

3.3	Moderate Assurance	Identification, assessment, treatment and control, reporting and monitoring of risks does not take place consistently and in a timely manner across Operational Services and as set out in the Risk Management framework.	
Finding and implication	Audit recommendation	Management response, including actions	
<p><u>There are no standardised timeframes to review a risk.</u></p> <p>Risk management processes generally include a standardised timeframe for the review of risks, and this is usually determined by the current score, level of risk, target score and the risk appetite.</p> <p>Review of NHS Lothian's Risk Management Operational Procedure indicated that risk registers are expected to be reviewed at least every three months.</p> <p>Discussion with the central Risk Management/Datix team found that there are no agreed timeframes for the review of individual risks, and this is currently at each Partnership's discretion.</p>	<p>Recommendation 6.</p> <p>To ensure risks attributed to NHS Lothian are reviewed using a consistent approach, the timeframes for the review of Low, Medium, High, and Very High risks should be agreed and reflected in NHS Lothian's Risk Management Policy/Operational Procedure.</p>	<p>Actions:</p> <p>The Quality Directorate will work with HSCPs to ensure timeframes are agreed for the review of individual risks.</p> <p>Responsible Officer: Associate Director of Quality and Heads of Health, HSCPs</p> <p>Executive Lead: Executive Medical Director</p> <p>Due Date: 31 May 2024</p>	
<p><u>The date to review a risk is not always included on a Datix report.</u></p> <p>Following a review of the Datix report detailing the Partnership's Risk Registers, we confirmed the date a risk was last reviewed is detailed, although the date of the next review was not included on the report.</p> <p>We were informed that the date of the next review is only included on a Datix report to a Partnership when specifically requested; this may result in a risk not being reviewed at regular intervals.</p>	<p>See Recommendation 4 (page 9)</p>	<p>N/A</p>	

Detailed findings & action plan

3.4

Identification, assessment, treatment and control, reporting and monitoring of risks does not take place consistently and in a timely manner across Operational Services and as set out in the Risk Management framework.

Finding and implication	Audit recommendation	Management response, including actions
<p>One of the purposes of a Risk Management policy is to provide a consistent and systematic process for reporting risks.</p> <p>We have already mentioned that reports are produced via a data extract from Datix. We are aware that reports are run according to the requests of the Partnerships (see Recommendation 4).</p> <p>Within the scope of our review, we were directed to determine the main reporting forum for each Partnership.</p> <ul style="list-style-type: none"> • Interviews with staff confirmed that appropriate forums to receive risk reports are determined by the individual Partnership. • We concluded that both Partnerships have numerous forums with risk management responsibilities and acknowledge that risks are reported to the forum according to the risk type. • We noticed that there was no single overarching forum in either Partnership that has oversight of the full HSCP risk register prior to any reporting to the IJB. 	<p>Considered outside the responsibility of NHS Lothian but reported as context.</p>	

Detailed findings & action plan

3.5	Moderate Assurance	Identification, assessment, treatment and control, reporting and monitoring of risks does not take place consistently and in a timely manner across Operational Services and as set out in the Risk Management framework.	
Finding and implication		Audit recommendation	Management response, including actions
<p><u>Not all teams and services have a risk register or log of NHS Lothian's risks.</u></p> <p>NHS Lothian's Risk Management policy states that risk registers are held at all levels of the organisation.</p> <p>We spoke with staff at various levels of the organisation, and they informed us that not all services and teams across both Partnerships have a risk register or a log of their risks. This is not in line with NHS Lothian's policy.</p> <p>We were informed that East Lothian are in the process of developing service level risk registers and one is almost ready to go live.</p>		<p>Recommendation 7.</p> <p>Work should continue to support Partnerships in developing service level risk registers on Datix to ensure all services and teams with the Partnerships maintain a risk register to record NHS Lothian risks.</p>	<p>Actions:</p> <p>The Quality Directorate will work with HSCPs to ensure service level risk registers are developed and maintained through Datix.</p> <p>Responsible Officer: Associate Director of Quality and Heads of Health, HSCPs</p> <p>Executive Lead: Executive Medical Director</p> <p>Due Date: 28 June 2024</p>

Detailed findings & action plan

3.6	Moderate Assurance	Identification, assessment, treatment and control, reporting and monitoring of risks does not take place consistently and in a timely manner across Operational Services and as set out in the Risk Management framework.	
Finding and implication	Audit recommendation	Management response, including actions	
<p><u>There are anomalies within the Partnership's risk registers which need addressing.</u></p> <p>As requested, and as part of the audit scope, we undertook a review of the Partnership's risk registers to identify areas where NHS Lothian could potentially drive improvements.</p> <p>Interviews of NHS Lothian's Risk Management/Datix team confirmed that review of the risk registers are undertaken to identify anomalies recorded on Datix.</p> <p>Review of the Partnership's Risk Registers on Datix identified several issues. We recommend that the Partnerships are supported by the Quality Improvement Service Team (QIST) to address these to ensure information is accurate and complete.</p> <p>Issues identified included:</p> <ul style="list-style-type: none"> • The risk register indicates the 'Adequacy of controls'. Risks stating that the controls were 'Adequate but partially effective' or 'Inadequate' did not always have further treatment / actions planned clearly detailed. • Numerous risks did not state the 'Adequacy of controls'. • The same person is at times identified as the owner and the handler for numerous risks. There is no segregation of duties which makes it difficult to hold individuals to account or cover absences. • Generally limited documentation to evidence actions taken at review, therefore, unclear if there is any progress or if mitigations are having a positive impact (East Lothian). 	<p>Recommendation 8.</p> <p>The Quality Improvement Support Team should instigate conversations with the Partnerships to discuss areas where data and information recorded could be strengthened or made more accurate and complete.</p>	<p>Actions:</p> <p>The Quality Directorate through the work outlined above will discuss with HSCPs areas where data and information currently captured could be strengthened to ensure completeness.</p> <p>Responsible Officer: Associate Director of Quality and Heads of Health, HSCPs</p> <p>Executive Lead: Executive Medical Director</p> <p>Due Date: 28 June 2024</p>	

Detailed findings & action plan

4.	Not rated	There is no clear and consistent approach to escalate operational risks from an operational service level to divisional level for inclusion on the Risk Register.	
Finding and implication		Audit recommendation	Management response, including actions
<p>The Risk Management policy describes risk escalation as the process for communicating a risk up, down or across the organisation to ensure that it is managed effectively.</p> <p>We understand that the escalation pathway is determined by each individual Partnership and as a result, will vary across each.</p> <p>Interviews with staff at various levels of the Partnerships confirmed that there are numerous escalation pathways through each Partnership.</p> <p>Review of meeting documentation confirmed that the East Lothian HSCP operational risk register was presented to the Audit and Risk Committee and consideration was made as to whether any risks should subsequently be included on the IJB risk register. We noted that the risk register was presented at this forum on an ad-hoc basis.</p> <p>Review of meeting documentation did not provide clear evidence of discussion of West Lothian's risk register.</p>		<p>Considered outside the responsibility of NHS Lothian but reported as context.</p>	

Appendices

Appendix 1: Staff involved



Staff involved

- Jill Gillies – Associate Director of Quality
- Robert Pritchard
- Julia Johnson - Lead Health and Safety Advisor
- David Collins – Head of Health & Safety
- Lorraine Inglis- Risk Management Information System facilitator (Datix)

West Lothian Health Care Partnership

- Yvonne Lawton - Head of Service
- Linda Yule – Chief Nurse
- Mike Reid - General Manager, Mental Health, Addictions and Podiatry
- Neil Ferguson – General Manager
- Laura Miller - Clinical Team Lead - District Nursing
- Orla Crummey – Lead Physiotherapist MSK
- John Mclean – Community Mental Health and Addictions Service Manager

East Lothian Health Care Partnership

- David Hood, Head of Operations,
- Suzanne O’Kane, Project Support Manager
- Sarah Gossner – Chief Nurse and Head of Quality
- Gillian Neil, - General Manager, Acute and Ongoing Care
- Lesley Berry – General Manager Rehabilitation Services
- Steve Elliott – Clinical Nurse Manager Day Services.



Appendix 2:

Documents reviewed



Documents reviewed

- Risk Management Policy, Apr 2023
- Risk Management Operational Procedure, Apr 2023

East Lothian Health Care Partnership & West Lothian Health Care Partnership

- Risk Registers
- Health & Safety Committee documentation
- Integration Joint Board documentation
- General Managers meeting documentation
- Selection of job descriptions

East Lothian Health Care Partnership

- Audit & Risk Committee documentation
- EL Council Risk Management Strategy

West Lothian Health Care Partnership

- Health & Care Governance Group documentation
- Audit Risk and Governance Committee documentation
- MSK team documents
- Quarterly Compliance meeting documentation
- Senior Management team documentation
- Risk Management Operational Procedure



Appendix 3:

Our assurance levels

The table below shows the levels of assurance we provide and guidelines for how these are arrived at. We always exercise professional judgement in determining assignment assurance levels, reflective of the circumstances of each individual assignment.

Rating	Description
Significant Assurance	<p>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.</p> <p>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)</p>
Moderate Assurance	<p>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.</p> <p>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".</p> <p>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)</p>
Limited Assurance	<p>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.</p> <p>This may be used when:</p> <ul style="list-style-type: none"> • 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. <p>The controls are deficient in some aspects and require management action (for instance one 'high' finding and a number of other lower rated findings)</p>
No assurance	<p>The Board cannot take any assurance from the audit findings. There remains a significant amount of residual risk.</p> <p>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 a number of HIGH rated recommendations)</p>

Appendix 3:

Our recommendation ratings

The table below describes how we grade our audit recommendations based on risks:

Rating	Description	Possible features
High	Findings that are fundamental to the management of risk in the business area, representing a weakness in the design or application of activities or control that requires the immediate attention of management	<ul style="list-style-type: none"> • Key activity or control not designed or operating effectively • Potential for fraud identified • Non-compliance with key procedures/standards • Non-compliance with regulation
Medium	Findings that are important to the management of risk in the business area, representing a moderate weakness in the design or application of activities or control that requires the immediate attention of management	<ul style="list-style-type: none"> • Important activity or control not designed or operating effectively • Impact is contained within the department and compensating controls would detect errors • Possibility for fraud exists • Control failures identified but not in key controls • Non-compliance with procedures/standards (but not resulting in key control failure)
Low	Findings that identify non-compliance with established procedures, or which identify changes that could improve the efficiency and/or effectiveness of the activity or control but which are not vital to the management of risk in the business area.	<ul style="list-style-type: none"> • Minor control design or operational weakness • Minor non-compliance with procedures/standards
Improvement	Items requiring no action but which may be of interest to management or which represent best practice advice	<ul style="list-style-type: none"> • Information for management • Control operating but not necessarily in accordance with best practice

