NHS Lothian

Internal Audit 2024/25

Risk Management

October 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 0131 659 8568
E hannah.l.mckellar@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's management and directors to ensure there are adequate arrangements in place in relation to risk management, governance, control and value for money.

Report Distribution

Executive Lead:

- Tracey Gillies, Medical Director

For action:

- Jill Gillies, Associate Director of Quality

For Information:

- Caroline Hiscox - Chief Executive
- Craig Marriott – Director of Finance
- Audit and Risk Committee

Executive summary

Background

Corporate risks are uncertainties or potential events that could negatively impact the achievement of an organisation's objectives at a strategic level. These risks can arise from various sources and affect different aspects of the organisation's operations. Corporate risks can range from operational and compliance risks to financial and technological risks.

NHS Lothian has a Risk Management Policy which highlights that the Corporate Management Team is responsible for directing the application of the policy through operational management structures, while the Audit and Risk Committee is responsible for assurance on the overall system of risk management and overseeing all risks on the corporate risk register. Each corporate risk is assigned to a named Executive Lead who is responsible for overseeing the management and mitigation of that risk. Each risk is assigned to a relevant committee or committees of the Board for assurance, in line with the committee's' terms of reference.

The purpose of the internal audit is to provide assurance on the internal controls relating to the management and mitigation of corporate risks. This will be achieved by selecting a sample of three corporate risks, each reported through different oversight committees. The audit will assess the design and application of controls for assessing, mitigating, and monitoring these risks to ensure that any impact on NHS Lothian's objectives is minimised.

Objectives

The objective of this review is to provide an independent assessment of the design and operational effectiveness of NHS Lothian's corporate risk management arrangements. Our review focussed on the following potential risk areas:

- Inadequate policies and documentation may lead to ineffective risk management practices and regulatory non-compliance.
- Poor risk assessment processes could result in the failure to identify significant risks or improper resource allocation.
- Insufficient documentation of gaps and mitigations can lead to incomplete risk management efforts, preventing the Board from obtaining a comprehensive understanding of the risk landscape.
- Ineffective mitigation controls may lead to insufficient risk reduction, exposing the organisation to unacceptable levels of risk.
- Ineffective risk management may result if risk handlers and owners do not collaborate and work together effectively.
- Inadequate monitoring and reporting processes at committee level can result in a lack of appropriate risk management oversight.

Executive summary

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 with a focus on the Corporate Risk Register and have concluded that the processes have provided a MODERATE LEVEL OF ASSURANCE. This was confirmed through testing in specific areas of the organisation and through discussions with various individuals across the organisation.

We have provided 'Moderate Assurance' based on our findings, indicating that the controls upon which the organisation relies are suitably designed and, in most cases, effectively applied. However, a moderate amount of residual risk remains. We have reported by exception against the areas where we consider that Management and the Audit and Risk Committee should focus their attention.

Our internal audit of NHS Lothian’s risk management processes identified that NHS Lothian made revisions to the Risk Management Policy and its associated Risk Management Operational Procedure in April 2023. However, there are opportunities to further enhance the governance arrangements in place to ensure the roles and responsibilities of sub-Committees and risk handlers are clearly defined and communicated.

Additionally, there are opportunities to strengthen the Assurance Report and Risk Mitigation Plan template to ensure consistent reporting, expanding the risk descriptions to ensure these are fully defined and setting out how each risk aligns to the relevant underlying corporate strategic objectives.

In a previous internal audit during the 2023/24 financial year, it was noted that there was opportunities to enhance the Datix reports as these are inadequate for managing risks effectively and reports do not include all the expected information, and this is still valid. We recognise that discussions are ongoing around Datix and if this will be replaced moving forward.

Three key weaknesses were identified, resulting in medium risk recommendations. This noted that the Datix reports, Assurance reports and Risk Migration plan templates are inadequate for managing risks effectively as the reports do not include all key information and could be strengthened. Additionally, there was no evidence that the completion of actions to date has resulted in any change to the risk level or score. There is a risk to the Board that despite spending time and resources on actions to date, the Board face continued exposure and unresolved vulnerabilities to the risk area. We note that further actions are ongoing which should reduce the risk level or score.

We will review progress made as part of our recommendation tracking during 2024/25.

Headline messages

Conclusion

We have raised eight recommendations including two improvement point. The grading of the recommendations are based on risk and summarised in the table below.

Risks	Assurance rating	Number of recommendations			
		High	Medium	Low	Imp
1. Inadequate policies and documentation may lead to ineffective risk management practices and regulatory non-compliance.	Moderate Assurance	-	2	1	1
2. Poor risk assessment processes could result in the failure to identify significant risks or improper resource allocation.	Significant Assurance	-	-	1	-
3. Insufficient documentation of gaps and mitigations can lead to incomplete risk management efforts, preventing the Board from obtaining a comprehensive understanding of the risk landscape.	Significant Assurance	-	-	-	-
4. Ineffective mitigation controls may lead to insufficient risk reduction, exposing the organisation to unacceptable levels of risk.	Moderate Assurance	-	1	-	-
5. Ineffective risk management may result if risk handlers and owners do not collaborate and work together effectively.	Significant Assurance	-	-	1	-
6. Inadequate monitoring and reporting processes at committee level can result in a lack of appropriate risk management oversight.	Significant Assurance	-	-	1	-

Summary of findings

Examples of where recommended practices are being applied

- The Risk Management Policy and Risk Management Operational procedure are in date and are accessible via the internet. The two documents sit alongside each other giving easy access and providing the relevant information to employees.
- The risk assessment process is described well within the Risk Management Operational Procedure. The procedure includes a well described process to defining a risk and includes a good range of examples. This means that risk handlers and owners can ensure a risk is fully understood at the onset of the risk assessment process, leading to a more meaningful identification of gaps and controls to mitigate a risk.
- Assurance Reports produced for the Governance Committees evidence that a detailed update of the progress made in relation to the actions associated to each 'key factor' is reported.

Areas requiring improvement

- Datix reports do not include all the information expected to be in the report to enable effective risk management. This means that the key people involved in the management of a risk cannot see the full picture and vital information relating to the risk (note, this was raised as a recommendation in the 2023/24 audit).
- The Risk Assurance Report template does not capture the information we would expect to be included in the report. This leads to Governance Committees not being provided with information which may help them make informed decisions.
- Risk Mitigation Plans are used inconsistently and do not detail the controls, gaps in controls and the adequacy of the individual controls already in place. This leads to Committees not being aware of important information.
- A Corporate Risk Register generally contains strategic risks which compromise the delivery of the organisations objectives and any operational risks which cannot be managed at a lower level or have an impact across the system, and this is reflected in the Risk Management Operational Procedure. Unfortunately, there was no evidence that the risks we reviewed were mapped to the relevant corporate objectives.
- Although actions have been completed for each of the three risks we reviewed, no action has had an impact on the level of the risk to date and no risk level or score has reduced. This may be due to key actions not completed and focus should be given to those actions.
- Risk handlers are not sure of their status, and this should be clarified to ensure the right people are involved in the management of risks.
- The Governance Committees terms of reference are not consistent and do not include any reporting into the Committees.

Detailed findings & action plan

1.	Moderate Assurance	Inadequate policies and documentation may lead to ineffective risk management practices and regulatory non-compliance.

Finding and implication	Audit recommendation	Management response, including actions
Committees' responsibilities are not reflected in policy. A review of the Risk Management Policy confirmed it is in date and accessible via NHS Lothians internet pages. The policy defines the responsibilities of the Audit and Risk Committee, the Healthcare Governance Committee and the Staff Governance Committee. No other Committees are referred to in the policy and this should be revised to reflect the responsibilities of other Committees which have oversight of individual risks, for example the Finance and Resource Committee. If roles and responsibilities are not detailed, there is the potential for confusion, inefficiency, and a lack of accountability, which can hinder effective decision-making and oversight within the organisation.	**Recommendation 1. Policy** To ensure there are robust governance arrangements and consistent responsibilities of all Committees which may hold oversight of corporate risks, the policy should be revised to include the responsibilities of ALL Committees with responsibility. This may be a generic statement of responsibly for Committees rather than specifying the names of individual Committees.	**Actions:** Specific references to Healthcare Governance and Staff Governance Committees will be removed. **Responsible Officer:** Associate Director of Quality. **Executive Lead:** Medical Director. **Due Date:** 31 October 2024.
Datix reports are inadequate for managing a risk effectively. Review of an extract from Datix provided by the Corporate Risk Management Team highlighted that not all expected information to enable effective risk management is made available to key persons. Issues identified included the following: • The individual likelihood and consequence ratings for a risk are recorded narratively and a numerical score is not provided as seen in other organisations, for example Extreme = 5, Almost Certain = 5, therefore risk score = 25. • We noted there was no target rating for two of the three risks indicating the risk tolerance following mitigating actions being taken. We were informed that this would be discussed with relevant risk owners at the bi-monthly meeting, due late July /early August 2024. • Gaps within the controls of a risk are not detailed within Datix. • The decision to either treat, tolerate, transfer or terminate is not captured within Datix and we were informed all risks are expected to be treated. We note that this decision is described as part of the process within the Risk Management Operational Procedure. • The corporate objectives to which a risk relates is currently being updated by the Corporate Risk Management Team and will be confirmed with the relevant risk owners. Further discussion highlighted that Datix is only used as a 'dock' of information for Corporate Risks rather than to manage the risks. There are plans to replace Datix in the future and that system may be used in a different capacity at that point.	**Recommendation 2. Datix** To ensure an effective and consistent approach to managing corporate risks, the Risk Management System should capture all relevant information relating to a risk, including the numerical make-up of the risk score, the target rating/score, the gaps in the controls, as well as the current decision to either treat, tolerate, transfer or terminate the risk or the activity associated to the risk. These factors should be considered during the procurement of a Risk Management System in the near future.	**Actions:** Findings acknowledge that reports from Datix are not used to update risks and alternative documentation is used, with the final updates, as ratified by the Board being recorded in Datix. Current documentation including the risk assurance table is currently being reviewed to incorporate all relevant information. Datix fields also being reviewed to enable relevant information to be captured and enhanced report to be provided. **Responsible Officer:** Associate Director of Quality. **Executive Lead:** Medical Director. **Due Date:** 31 December 2024.

Detailed findings & action plan

1.	Moderate Assurance	Inadequate policies and documentation may lead to ineffective risk management practices and regulatory non-compliance.

Finding and implication (ctd.)	Audit recommendation	Management response, including actions
<u>The Assurance Report and Risk Mitigation Plan template could be strengthened.</u> A template document is available which includes an Assurance Report and a Risk Mitigation Plan. Review of the Assurance Report highlights a gap in the information we would expect to be included, and these can be mapped to those gaps we have highlighted within Datix described earlier within this report. Review of the Risk Mitigation Plans of the three risks in our sample highlighted a general inconsistency in the reporting style and format. Discussion with risk handlers confirmed they feel the template works well overall, and the template can be adjusted as required to meet their reporting needs. In addition, our review of the templates also identified the following issues: • Assurance Reports and Risk Mitigation Plans do not detail the controls and gaps in controls in place to manage a risk and interviews with risk handlers highlighted uncertainty to how a Governance Committee is made aware of these. • Assurance Reports do not state the adequacy of individual controls to the Governance Committees. However, the summary section of the reports state the '*overall*' adequacy of controls. • Interview with the Corporate Risk Management Team informed us that gaps are expected to be detailed in the 'key factors' of the risk mitigation plan but our review highlights the 'key factors' are generally the individual areas of focus or workstreams relating to a risk rather than a gap in the controls. • We were unable to determine whether completed actions have become a control within the Assurance reports. • We noted inconsistencies that there were overlaps within the HSDU Assurance report, with progress on actions reported in more than one section. Furthermore, review of Governance Committee meeting minutes indicated that the Healthcare Governance Committee like the format of the 'Access to Treatment Assurance Report' and would like all risks presented to the Committee to be in this format. The Committee suggested it would be helpful to define the highest risk areas and associated measurements for improvement. The Staff Governance Committee highlighted the significant work undertaken and progress achieved against the six workstreams of the Violence and Aggression risk.	**Recommendation 3. Assurance Report & Risk Mitigation Plan template** To promote consistent reporting and ensure the Governance Committees are provided with the full picture of the position of a risk, we recommend that discussions are held regarding a redesign of the template Assurance Report and Risk Mitigation Plan, including the following: • A breakdown of the score (Likelihood/Consequence) • Target score • Risk response (tolerate, treat, transfer or terminate) • Relevant corporate objective to which the risk relates • Gaps in controls and actions • Controls, including the movement of an action to a control. This may be in the form of a dashboard or revisions to the current template.	**Actions:** Current Risk Mitigation template will be reviewed to include recommended information. **Responsible Officer:** Associate Director of Quality. **Executive Lead:** Medical Director **Due Date:** 31 December 2024.

Detailed findings & action plan

1.	Moderate Assurance	Inadequate policies and documentation may lead to ineffective risk management practices and regulatory non-compliance.

Finding and implication (ctd.)	Audit recommendation	Management response, including actions
<u>Other Risk Management tools are used in isolation.</u> It was noted that some risk handlers use the SCART tool, a critical analysis framework which provides an extra layer of assurance. We note that the tool is not mandated, and the Corporate Risk Management Team is not aware of it. An assessment of the SCART tool may determine whether this framework would further enhance the risk management process and ensure a consistent approach across the organisation.	**Improvement Point 4. SCART Tool** To ensure the risk management process makes use of all available resources, we recommend that the Corporate Risk Management Team undertake an assessment of the SCART tool to determine whether this critical analysis framework would further enhance the risk management process.	No action required but may be of interest to management.

Detailed findings & action plan

2.	Significant Assurance	Poor risk assessment processes could result in the failure to identify significant risks or improper resource allocation.

Finding and implication	Audit recommendation	Management response, including actions
Risk descriptions are not written in accordance with policy. The risk assessment process is outlined within the Risk Management Operational Procedure. Generally, an effective assessment and management of a risk commences with a clearly defined risk description, describing, what event could happen, why the event could occur and what would be the consequence, and this is advocated in the procedure with described guidance on how to define a risk with examples. A review of the risk descriptions of the three risks in our sample, highlighted that not all risks state why the event could occur. Understanding 'why' an event can occur will assist in the identification of the best actions to take to minimise risk, and the importance of considering 'why' is well defined in the Operational Procedure. Additionally, for each risk, it is not clear which corporate objective the risk relates to, and we were unable to confirm alignment of risks to the corporate objectives from interviews with the Corporate Risk Management Team or the Risk Handlers. We would expect that identification of the corporate objective to which a risk relates is identified during the risk assessment phase when a risk is being added to the Corporate Risk Register. We recommend that the risk owners and handlers consider whether risk descriptions are sufficient with the support of the Corporate Risk Management Team at the next planned meeting and ensure each risk is clearly aligned to corporate strategic objectives.	**Recommendation 5. Risk Descriptions** To ensure the continuous assessment and monitoring of corporate risks is effective, we recommend that risk descriptions are reviewed by the risk handlers and owners at least annually, with the support of the corporate Risk Management Team at the scheduled bi-monthly meetings. We recommend that identification of the relevant strategic objectives to which the risk impacts upon is identified during risk assessment and reviewed during these meetings. This should be easily identifiable in all reporting.	**Actions:** All risk descriptions will be reviewed at the next bi-monthly meetings. Associated strategic objective now included risk assurance table and in Datix. **Responsible Officer:** Associate Director of Quality (in conjunction with risk owners). **Executive Lead:** Medical Director. **Due Date:** 31 December 2024.

Detailed findings & action plan

4.	Moderate Assurance	Ineffective mitigation controls may lead to insufficient risk reduction, exposing the organisation to unacceptable levels of risk.

Finding and implication	Audit recommendation	Management response, including actions
<u>There was no evidence that the completion of actions to date have led to a change in the risk level or score.</u> Review of Assurance Reports, Risk Mitigation Plans and interviews with risk handlers highlighted that although actions have been completed for the three risks reviewed, no action has impacted the level of the risk or reduced its score. We acknowledge there are key actions relating to each of the risks which have yet to be completed, and it is considered that the completion of those key actions will reduce the risk score. We therefore recommend that the key actions impacting the risk level are easily identifiable within the Risk Mitigation Plans to encourage discussion with the Governance Committees, and that resources and monitoring of those actions become the focus of the Committees. There is a risk to the Board that despite spending significant time and resources on actions which do not impact on the scoring of the risk level/score, continued exposure and unresolved vulnerabilities still exist.	**Recommendation 6. Key actions** To encourage the direction of resources to mitigate and minimise risks, we recommend: • Risk Mitigation Plans provide focus to the key actions required to reduce risk levels, • Discussion of these key actions should be encouraged at Committee and Board level, including the identification of resources to deliver the most suitable actions. • Future monitoring of those actions should become the focus of reporting to Committees and the Board. • Work should be undertaken to explicitly link key actions of the Risk Management Plan to the actions required to deliver strategic objectives.	**Actions:** Current Risk Mitigation template will be reviewed to ensure identification of key actions to facilitate focussed discussion at Governance Committees. **Responsible Officer:** Associate Director of Quality (in conjunction with risk owners and Committee Chairs). **Executive Lead:** Medical Director **Due Date:** 31 December 2024.

Detailed findings & action plan

5.	Significant Assurance	Ineffective risk management may result if risk handlers and owners do not collaborate and work together effectively.

Finding and implication	Audit recommendation	Management response, including actions
<u>The risk handlers roles and responsibilities should be clearly defined and documented.</u> It was noted that the Corporate Risk Management Team meet with a risk owner on a two-monthly basis, a function developed in response to the recommendations of a previous internal audit. We observed the bi-monthly meeting held between a risk owner and the Corporate Risk Management Team. There was evidence of a detailed report being prepared in advance of the meeting and the risk owner and Corporate Risk Management Team working together with the risk handlers to collate information to report progress against the mitigation actions. The risk owner had a good knowledge base of the risks under their management to ensure discussions focused on progress. Review of the meeting schedule highlighted that risk handlers are not invited to all meetings. The roles and responsibilities of a risk handler is not documented or defined, which can result in a lack of clarity within the organisation and result in difficulties in working together effectively as individuals aren't clear on their role.	**Recommendation 7. Risk handler role** To ensure risks on the Corporate Risk Register can be managed effectively, the risk handler's roles and responsibilities should be clearly documented and defined, including the appropriateness of attending all bi-monthly meetings with the risk owner and Corporate Risk Management Team.	**Actions: Risk handler's roles and responsibilities will be added to documented CRR process.** ***To note: Risk management procedure says: 'The risk handler typically undertakes the detailed work on the particular risk, and reports to the risk owner on that work.'*** ***Also risk handlers do attend bi-monthly meetings for other Exec leads but process slightly different for deputy CE meeting as updates and discussion with handlers takes place prior to the meeting.*** **Responsible Officer:** Associate Director of Quality. **Executive Lead:** Medical Director. **Due Date:** 31 December 2024.

Detailed findings & action plan

6.	Significant Assurance	Inadequate monitoring and reporting processes at committee level can result in a lack of appropriate risk management oversight.

Finding and implication

Risk management responsibilities and reporting requirements are not consistently reflected in the Governance Committees terms of reference.

A review of the terms of reference for the Committees with oversight of each of the risks in our sample confirmed that each Committee holds responsibility for monitoring and reviewing strategic risks and informing updates to risk assurance and mitigation plans.

Our review identified numerous issues:

- The terms of reference for the Healthcare Governance Committee do not make direct reference to the management of risks within the 'remit' for the Committee or as a 'core function'.
- The terms of reference for the Corporate Management Team, which has oversight of all risks on the Corporate Risk Register, were recently updated (July 2024) and do not reflect this oversight as a 'purpose' of the group.
- In addition, none of the terms of reference state the reporting requirements into the Committee.

A review of the Workplans of the Committees highlighted inconsistencies in the scheduling of the Risk Assurance Reports.

- The Healthcare Governance Committee workplan indicates that the Corporate Risk Register is a standing agenda item for all meetings and the Access to Treatment Risk Mitigation Plan is scheduled for discussion annually.
- The Staff Governance Committee workplan states updates are to be provided to the Committee at each meeting, and this includes the Violence & Aggression risk.
- The Finance & Resources Committee does not have a formal workplan in place, although we acknowledge update reports are requested by the Committee at least annually, and this includes the HSDU Capacity risk.

Interviews with risk handlers confirmed that there are other forums with responsibilities for the individual elements (key factors) of the risk, for example the Outpatient Delivery Group oversees the actions relating to the Access to Treatment ' Outpatients' element of the Risk Mitigation Plan, and the Cancer diagnostic delivery board oversees the actions relating to the Cancer 31 and 62 days and the Diagnostics elements of the Risk Mitigation Plan. We did not review documentation from these forums as it outside the scope of this review.

Audit recommendation

Recommendation 8.

Governance Committees responsibilities

To ensure the Committees risk management responsibilities are made clear, concise and consistent across the Committees, we recommend the following elements are considered:

- The terms of reference for the Healthcare Governance Committee is revised at the next scheduled review to make direct reference to the management of risks within the remit of the Committee or as a core function.
- All Committees terms of reference detail the reporting arrangement *into* the Committee rather than only *from* the Committee.
- The new terms of reference for the CMT are revised to ensure the group's oversight of all corporate risks is reflected as a 'purpose' of the group.
- The expectations for a risk handler and owner to produce a report to a Governance Committee is consistent for all Committees and reflected in an approved annual workplan.

Management response, including actions

Actions: All Committees Terms of Reference will be revised to include relevant points at next scheduled reviews.

Scheduling of reports will be agreed alongside revision of current risk mitigation templates.

Responsible Officer: Board Secretary.

Executive Lead: Medical Director.

Due Date: February 2025

Appendices

Appendix 1:
Staff involved and documents reviewed

Staff involved

- Tracey Gillies, Medical Director
- Jill Gillies, Associate Director of Quality
- Sue Gibbs, Quality & Safety Assurance Lead
- Alison MacDonald, Executive Nurse Director
- Michelle Carr, Chief Officer, Acute Services
- Fiona Ireland, Nurse Director (Corporate Nursing)
- Morag Campbell, Director of Estates & Facilities
- Robert Aitken, Associate Director of operations, Estates & Facilities
- David Collins, Head of H&S Services
- Alexander Crawford, Business Manager, Estates & Facilities
- Karen Fraser, Head of Risk, Quality & Assurance, Facilities
- Wendy Reid, Head of Performance & Business Unit, Executive Office
- John McHale, Executive Office
- Catherine Kelly, Business Manager, Acute Services

Documents reviewed

- Risk Management Policy, April 2023
- Risk Management Operational Procedure, April 2023
- Extract of Corporate Risk Register (CRR) from DATIX (Sample of three risks)
- Healthcare Governance Committee documentation
- Strategy, Planning & Performance Committee documentation
- Finance & Resources Committee documentation
- Staff Governance Committee documentation
- Corporate Management Team documentation
- Process for managing the CRR
- Risk reporting paper template
- Schedule for CRR meetings with risk owners

Appendix 2: 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	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)
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)
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 respects and require management action (for instance one 'high' finding and a number of other lower rated findings)
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 several HIGH rated recommendations)

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	• 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	• 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.	• 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	• Information for management • Control operating but not necessarily in accordance with best practice

Grant Thornton

grantthornton.co.uk