

# Internal Audit Progress Report

## Audit Committee (30 September 2024)

Pendle Borough Council

# Contents

## 1 Introduction

## 2 Key Messages for Audit Committee Attention

Appendix A: Contract Performance

Appendix B: Performance Indicators

Appendix C: Key Areas and Actions to be Delivered

Appendix D: Follow up of previous audit recommendations

Appendix E: Assurance Definitions and Risk Classifications

## Public Sector Internal Audit Standards

Our work was completed in accordance with Public Sector Internal Audit Standards and conforms with the International Standards for the Professional Practice of Internal Auditing.

## 1 Introduction

This report provides an update to the Accounts & Audit Committee in respect of progress against the 2024/25 Internal Audit Plan and brings to your attention matters relevant to your responsibilities as members of the Accounts & Audit Committee.

This progress report provides a summary of Internal Audit activity and complies with the requirements of the Public Sector Internal Audit Standards.

Comprehensive reports detailing findings, recommendations and agreed actions are provided to the organisation, and are available to Committee Members on request. In addition, a consolidated follow up position is reported on a periodic basis to the Audit Committee.

This progress report covers the period 23 July 2024 to 19 September 2024.

## 2 Key messages for Accounts & Audit Committee

Since the last meeting of the Accounts & Audit Committee, there has been the focus on the following areas:

### Audit Reviews

The following reviews have been finalised:

- **IT Cyber Resilience** (Substantial Assurance)

Refer to Appendix C for details of Key Areas and Actions to be delivered.

The following reviews are at draft report stage:

- **Colne Muni project briefing note** (report being finalised).
- **Council tax & NNDR**
- **Sickness absence**

The following reviews are currently in progress:

- **Homelessness** (fieldwork complete, report being drafted)
- **Finance deep dives** (fieldwork)
- **Performance reporting & data quality** (fieldwork)

- **Complaints & Learning** (planning)
- **Customer Care** (planning)

### Follow up of previous internal audit recommendations

A summary of the current status of follow-up activity is included in Appendix D, however, we would draw the committee's attention to the following:

Of the 57 recommendations set out in Appendix D, 43 of these have either been fully actioned or are in progress/partially addressed. The remaining 14 recommendations are not yet due for action. There are no critical and 6 high priority recommendations; three of these relate to the Information Governance audit and are in progress; the remaining three recommendations relate to the Staff performance/appraisals and Cyber resilience audits and are not yet due.

### Audit Plan Changes

Audit Committee approval will be requested for any amendments to the original plan and highlighted separately below to facilitate the monitoring process.

- There is one proposed change to the audit plan regarding the timing of our audit of Joint Ventures. Due to the ongoing external review of Joint Ventures, we are proposing to defer this audit from quarter 2 to quarter 4. This has been discussed with the Corporate Leadership team and they are supportive of this. The Accounts & Audit Committee are requested to approve this change to the timing of the audit.

### Public Sector Internal Audit Standards

In January the Institute of Internal Auditors issued revised Global Internal Audit Standards (GIAS).

The Relevant Internal Audit Standard Setters (RIASS) for the UK Public Sector have agreed to use the new GIAS as the basis for internal auditing for the UK Public Sector and have asked the UK Public Sector Internal Auditing Standards Advisory Board (IASAB) to carry out a review of the new standards with a view to identifying and producing any sector specific interpretations or other material needed to make them suitable for UK public sector use.

The implementation date for the new standards in the UK public sector will be 1st April 2025. Until then, the existing Public Sector Internal Audit Standards will continue to apply.

When the IASAB issues material for application in the UK public sector MIAA will review this and amend our processes if required to continue to ensure full compliance with standards.

The latest updates from the IASAB can be accessed via the following link: <https://www.iasab.org/latest-news>

## MIAA Quality of Service Indicators

MIAA operate systems to ISO Quality Standards. Public Sector Internal Audit Standards (PSIAS) require MIAA to 'develop and maintain a quality assurance and improvement programme that covers all aspects of the internal audit activity.' This programme must include internal and external assessments.

External assessments must be conducted at least once every five years. Our last external assessment was completed in 2020 and concluded MIAA fully complies with PSIAS (as previously reported to Audit Committee).

We also undertake regular internal assessments to ensure our ongoing compliance with requirements. We have recently completed our annual self-assessment of compliance with PSIAS and can confirm full compliance with PSIAS.



## Added Value





### Events

- [How to Lead in a Hybrid World 16 Oct 2024](#) This Masterclass explores the ways in which organisations can help generate team spirit /culture and support leaders to effectively lead a team with people who aren't in the room.
- [Evidence Based Working \(22 Nov 2024\)](#) How Can a Better Evidence-Based Approach Support Local Government to Meet its Challenges? Rob Brinan, a Professor of Organisational Psychology in the School of Business and Management. will be joining us to explore what we know in relation to how local government responds to situations, and how a more evidence-based approach may improve practice.

## Appendix A: 2024/25 Contract Performance

The Public Sector Internal Audit Standards (PSIAS) state that 'The chief audit executive must deliver an annual internal audit opinion and report that can be used by the organisation to inform its governance statement. Below sets out the overview of delivery for your Head of Internal Audit Opinion for 24/25:

| HOIA Opinion Area                    | TOR Agreed  | Status   | Assurance Level | Audit Committee Reporting |
|--------------------------------------|---|--|-----------------|---------------------------|
| Core/Mandated Assurances             |   |  |                 |                           |
| Performance Reporting & Data Quality |    | Q2 – Fieldwork   |                 |                           |
| Finance Systems Deep Dive            |   | Q4   |                 |                           |
| Revenue & Benefits                   |   | Q4   |                 |                           |
| Risk Based Assurances                |   |  |                 |                           |
| External Governance Review Response  |   | Q3/Q4  |                 |                           |
| Complaints & Learning                |   | Q2 - Planning  |                 |                           |
| Customer Care                        |   | Q2/3 – Planning  |                 |                           |
| Homelessness                         |  | Fieldwork complete, report being drafted.  |                 |                           |
| Joint Ventures                       |   | Proposal to delay review to Q4 (was Q2) due to current external review of JVs (agreed with management) |                 |                           |

| HOIA Opinion Area                             | TOR Agreed  | Status              | Assurance Level | Audit Committee Reporting |
|---|---|---------------------|-----------------|---------------------------|
| Building Control                              |   | Q4                  |                 |                           |
| Sickness Absence                              |  | Draft report issued | Substantial     |                           |
| IT Critical Application: IDOX System          |   | Q3                  |                 |                           |
| 2023/24 reviews not included in 2023/24 HOIAO |   |                     |                 |                           |
| IT Cyber resilience                           |  | Final report issued | Substantial     | September 2024            |
| Finance Deep Dives                            |  | Fieldwork           |                 |                           |
| Revenue and Benefits                          |  | Draft report issued | Substantial     |                           |
| Follow Up                                     |   |                     |                 |                           |
| Qtr 1   | N/A   | Complete            | N/A             | July 2024                 |
| Qtr 2   | N/A   | Complete            | N/A             | September 2024            |
| Qtr 3   | N/A   |                     |                 |                           |
| Qtr 4   | N/A   |                     |                 |                           |

## Appendix B: Performance Indicators

The primary measure of your internal auditor's performance is the outputs deriving from work undertaken. The following provides performance indicator information to support the Committee in assessing the performance of Internal Audit.

| Element  | Reporting Regularity  | Status | Summary   |
|--|-----------------------|--------|---|
| Delivery of the Head of Internal Audit Opinion (Progress against Plan)         | Each Audit Committee  | Green  | We are on track to be able to provide the Council with a Head of Internal Audit Opinion in line with the required timescales.   |
| Issue a Client Satisfaction Questionnaire following completion of every audit. | Each Audit Assignment | Green  | Questionnaire issued with each audit report.  |
| Percentage of recommendations raised which are agreed                          | Each Audit Committee  | Green  | Actions agreed by the Council on all recommendations raised.  |
| Qualified Staff  | Annual                | Green  | MIAA have a highly qualified and diverse workforce which includes 75% qualified staff. The Senior Team delivering the Internal Audit Service to the Council are CCAB/IIA qualified.   |
| Quality  | Annual                | Green  | MIAA operate systems to ISO Quality Standards. The External Quality Assessment, undertaken by CIPFA, provides assurance of MIAA's compliance with the Public Sector Internal Audit Standards. MIAA conforms with the Public Sector Internal Audit Code of Ethics. |



## Appendix C: Key Areas from our Work and Actions to be Delivered

| Report Title (Assurance Level) | IT Cyber Resilience   |          |            |         |
|--------------------------------|---|----------|------------|---------|
| Executive Sponsor              | Director of Resources   |          |            |         |
| Objective                      | <p>The overall objective was to assess the Council's cyber resilience arrangements, in particular review of the following areas:</p> <ul style="list-style-type: none"> <li>• Perimeter protection;</li> <li>• Secure Configuration;</li> <li>• User access control;</li> <li>• Malware protection;</li> <li>• Patch Management;</li> <li>• Data Backups / Data recovery;</li> <li>• Threat and vulnerability management.</li> </ul>  |          |            |         |
| Recommendations                | 0 x Critical  | 1 x High | 1 x Medium | 0 x Low |
| Summary                        | <p>Whilst the review identified several areas of good practice, there were also opportunities to strengthen controls in several key areas including defining recovery objectives, full backup restore testing and user permission reviews for privileged accounts.</p> <p>During the review it was observed that Recovery Point Objectives (RPOs) for critical data and systems had not been formally defined or documented. Without defined RPOs, there is ambiguity regarding the acceptable level of data loss in the event of a disruption. This increases the risk of data loss and could lead to significant financial losses or compliance violations.</p> <p>In addition, full backup restore tests had not been conducted in the production environment for a significant period. Without testing full backup restore procedures in a production environment, there is</p> |          |            |         |

|                             |  |
|-----------------------------|--|
|                             | <p>uncertainty about the organisation's ability to recover data in the event of a disruption or system failure. It was noted that while Liberata have technical procedures in place, there was no overarching council back up policy document. A backup policy would document arrangements agreed with the council in terms of backup arrangements and typically encompass agreed objectives (RPO/RTO), roles and responsibilities, data classification criteria, retention requirements, monitoring key performance indicators, testing and audit for compliance to be effective. <b>(High priority)</b></p> <p>User Access controls were generally effective however there is an opportunity to improve arrangements by defining a process to review user access permissions particularly for users with higher privileges which can be used to make significant harm to systems and data. Without regular access reviews, there is a heightened risk of unauthorised access, misuse of privileges, and potential security breaches. <b>(Medium priority)</b></p>  |
| Key Areas Agreed for Action | <ul style="list-style-type: none"> <li>The Council and Liberata IT Services will work together to ensure that the Council's back-up requirements / arrangements are articulated / captured within the relevant controls documentation and a copy shared with MIAA.</li> </ul> <p>RTOs are regularly reviewed as part of the Council's BC arrangements. However, it is agreed that documentation in respect of RPOs need to be strengthened. This will be captured as part of response (1.) above.</p> <p>Full backup / restore test was planned following the local elections in May 2024; however, the calling of the General Election meant this had to be put on hold. A wider BC/DR test is now currently in the planning stages and is being led by the Council's BC lead, David Walker (Assistant Director – Operational Services). This is expected to take place by the end of October 2024.</p> <p>The IT DR Plan is also being updated to reflect some necessary changes and reflect any necessary information from this recommendation, as appropriate.</p> <p>It is also important to note that the Council is taking part in the Cyber Assessment Framework Pilot. <b>(High priority, action by 30 November 2024)</b></p> |

|   |   |
|---|---|
|   | <ul style="list-style-type: none"> <li>The Council and Liberata IT Services will give this due consideration and amend the User Access Permissions Review Process as deemed appropriate. <b>(Medium priority, action by 30 September 2024)</b></li> </ul> |
| Key Risks Highlighted with No Agreed Action | N/A   |

## Appendix D: Follow up of previous audit recommendations

| AUDIT TITLE (YEAR)               | NO OF RECS | ASSURANCE LEVEL | PROGRESS ON IMPLEMENTATION |   |   |               | OUTSTANDING RECOMMENDATIONS |   |   |   | COMMENTS   |
|----------------------------------|------------|-----------------|----------------------------|---|---|---------------|-----------------------------|---|---|---|--|
|                                  |            |                 | ✓/S                        | P | X | Not due/ FUIP | C                           | H | M | L |  |
| Joint Ventures (2021/22)         | 5          | Substantial     | 3                          | 2 | - | -             | -                           | - | 2 | - | The two outstanding recommendations relate to ensuring there are terms of reference in place for any JV working groups and defining the performance information the Council requires from the JV as well as formalising role of executive officers involved in JV and handling of conflicts of interest. These recommendations will be followed up as part of the Joint Venture audit to take place in Q4. |
| Key Financial Controls (2021/22) | 7          | Moderate        | 7                          | - | - | -             | -                           | - | - | - | All recommendations actioned.  |
| Council Tax and NNDR (2022/23)   | 3          | Substantial     | 2                          | 1 | - | -             | -                           | - | 1 | - | One recommendation is in progress in regard to production of debt write off policy with a revised implementation date of 31/10/24.   |
| Housing Benefits (2022/23)       | 4          | Substantial     | 4                          | - | - | -             | -                           | - | - | - | All recommendations actioned.  |
| Key Financial Systems (2022/23)  | 2          | Substantial     | 1                          | 1 | - | -             | -                           | - | - | 1 | One low priority recommendation in progress regarding request that Liberata review the documents in relation to system backup and recovery to ensure they accurately reflect current process. Review dates should be included on the documents to ensure that these are appropriately reviewed.  |
| Mandatory Training (2023/24)     | 5          | Substantial     | -                          | - | - | 5             | -                           | - | 5 | - | Recommendations not due for follow up – revised dates have been provided for these recommendations 30/11/24 – 31/1/25.   |
| Housing Inspections (2023/24)    | 6          | Moderate        | 5                          | 1 | - | -             | -                           | - | 1 | - | The outstanding recommendation relates to the update of the Enforcement Policy which is due by 31/7/24 and is in progress.   |

| AUDIT TITLE (YEAR)                         | NO OF RECS | ASSURANCE LEVEL | PROGRESS ON IMPLEMENTATION |           |          |               | OUTSTANDING RECOMMENDATIONS |          |           |          | COMMENTS  |
|--|------------|-----------------|----------------------------|-----------|----------|---------------|-----------------------------|----------|-----------|----------|---|
|  |            |                 | ✓/S                        | P         | X        | Not due/ FUIP | C                           | H        | M         | L        |   |
| Budget setting & monitoring (2023/24)      | 8          | Substantial     | 5                          | 2         | -        | 1             | -                           | -        | 1         | 2        | Remaining recommendations are in progress or not due.   |
| Third Party Suppliers – Liberata (2023/24) | 4          | Substantial     | 2                          | 2         | -        | -             | -                           | -        | 2         | -        | Outstanding recommendations are in progress with revised implementation dates of 30/9/24 & 30/11/24. The two outstanding recommendations relate to development of Customer Contact Strategy & Digital Strategy as well as the agreement of a performance management framework and KPIs with Liberata. |
| Information Governance (2023/24)           | 5          | Limited         | -                          | 5         | -        | -             | -                           | 3        | 2         | -        | Recommendations in progress. Revised dates of 31 December 2024 proposed.  |
| Staff Appraisals (2023/24)                 | 6          | Limited         | -                          | -         | -        | 6             | -                           | 2        | 4         | -        | Recommendations not due for follow up.  |
| IT Cyber Resilience (2023/24)              | 2          | Substantial     | -                          | -         | -        | 2             | -                           | 1        | 1         | -        | Recommendations not due for follow up.  |
| <b>Totals</b>                              | <b>57</b>  | <b>-</b>        | <b>29</b>                  | <b>14</b> | <b>-</b> | <b>14</b>     | <b>-</b>                    | <b>6</b> | <b>19</b> | <b>3</b> |   |

Key to recommendations:

✓/S      Implemented or Superseded  
P      Partially implemented/recommendation in progress  
X      Recommendation not implemented  
ND/FUIP      Not due for follow up

C      Critical priority recommendation  
H      High priority recommendation  
M      Medium priority recommendation  
L      Low priority recommendation

## Appendix E: Assurance Definitions and Risk Classifications

| Level of Assurance | Description   |
|--------------------|---|
| High               | There is a strong system of internal control which has been effectively designed to meet the system objectives, and that controls are consistently applied in all areas reviewed.                               |
| Substantial        | There is a good system of internal control designed to meet the system objectives, and that controls are generally being applied consistently.  |
| Moderate           | There is an adequate system of internal control, however, in some areas weaknesses in design and/or inconsistent application of controls puts the achievement of some aspects of the system objectives at risk. |
| Limited            | There is a compromised system of internal control as weaknesses in the design and/or inconsistent application of controls puts the achievement of the system objectives at risk.                                |
| No                 | There is an inadequate system of internal control as weaknesses in control, and/or consistent non-compliance with controls could/has resulted in failure to achieve the system objectives.                      |

| Risk Rating | Assessment Rationale   |
|-------------|--|
| Critical    | Control weakness that could have a significant impact upon, not only the system, function or process objectives but also the achievement of the organisation's objectives in relation to: <ul style="list-style-type: none"> <li>the efficient and effective use of resources</li> <li>the safeguarding of assets</li> <li>the preparation of reliable financial and operational information</li> <li>compliance with laws and regulations.</li> </ul> |
| High        | Control weakness that has or is likely to have a significant impact upon the achievement of key system, function or process objectives. This weakness, whilst high impact for the system, function or process does not have a significant impact on the achievement of the overall organisation objectives.  |
| Medium      | Control weakness that: <ul style="list-style-type: none"> <li>has a low impact on the achievement of the key system, function or process objectives;</li> <li>has exposed the system, function or process to a key risk, however the likelihood of this risk occurring is low.</li> </ul>  |
| Low         | Control weakness that does not impact upon the achievement of key system, function or process objectives; however implementation of the recommendation would improve overall control.  |

## Limitations

The matters raised in this report are only those which came to our attention during our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required. Whilst every care has been taken to ensure that the information in this report is as accurate as possible, based on the information provided and documentation reviewed, no complete guarantee or warranty can be given with regards to the advice and information contained herein. Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

Responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management and work performed by internal audit should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify all circumstances of fraud or irregularity. Effective and timely implementation of our recommendations by management is important for the maintenance of a reliable internal control system.

Reports prepared by MIAA are prepared for your sole use and no responsibility is taken by MIAA or the auditors to any director or officer in their individual capacity. No responsibility to any third party is accepted as the report has not been prepared for, and is not intended for, any other purpose and a person who is not a party to the agreement for the provision of Internal Audit and shall not have any rights under the Contracts (Rights of Third Parties) Act 1999.

Lisa Warner

Engagement Manager

Tel: 07825 454 581

Email: [Lisa.Warner@miaa.nhs.uk](mailto:Lisa.Warner@miaa.nhs.uk)

Darrell Davies

Engagement Lead

Tel: 07785 286381

Email: [Darrell.davies@miaa.nhs.uk](mailto:Darrell.davies@miaa.nhs.uk)

Louise Cobain

Director Lead

Tel: 07795 564916

Email: [Louise.cobain@miaa.nhs.uk](mailto:Louise.cobain@miaa.nhs.uk)