Internal Audit Progress Report
Audit Committee (25 November 2025)

Pendle Borough Council

Contents

Global Internal Audit Standards (UK public sector)

Our work was completed in accordance with Global Internal Audit Standards (UK public sector).

1 Introduction

This report provides an update to the Accounts & Audit Committee in respect of progress being made with delivery of the 2025/26 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 Global Internal Audit Standards (UK public sector).

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 22 September to 14 November 2025.

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:

- **Payroll** – Substantial assurance
- **IT Critical application review – IDOX system** – Limited assurance
- **Follow up** – see Appendix D

The following reviews are at draft report stage:

- **Governance** – draft report stage

The following reviews are in progress:

- **VAT** – fieldwork concluding
- **Health & Safety** – fieldwork
- **Contract Management** – fieldwork
- **IT Asset Management** – fieldwork
- **Procurement** – fieldwork
- **Nelson Town Deal** - 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 68 recommendations set out in Appendix D, 16 of these are not due for follow up.
- This leaves 52 recommendations of which 29 (56%) have been fully actioned and 23 (44%) recommendations which are in progress.
- There are no critical and 3 high priority recommendations outstanding and past their original implementation date. All three high priority recommendations relate to the Information Governance audit and are in progress with a revised date of 31 December 2025.

See **Appendix D** for further details.

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 are no proposed changes to the audit plan.

MIAA – Assured provider to the NCSC Cyber Resilience Audit Scheme

We are proud to announce that MIAA has been officially recognised as an Assured provider under the National Cyber Security Centre's (NCSC) Cyber Assessment Framework (CAF).

This accreditation marks a major milestone for MIAA and reflects our ongoing commitment to helping organisations strengthen their cyber resilience and safeguard critical systems and services.

This achievement, which is the result of a rigorous assessment process, demonstrates our credentials in auditing against the NCSC's Cyber Assessment Framework and, highlights the exceptional skills and experience of our staff as well as our organisational commitment to the highest cyber security standards. While this recognition is a tremendous achievement for MIAA, its greatest value lies with our clients, who can be confident they are engaging highly skilled individuals and a trusted, high-quality audit provider.

The Cyber Resilience Audit (CRA) scheme provides assurance for organisations delivering independent cyber audits, with a strong focus on the Cyber Assessment Framework (CAF). By becoming an NCSC Assured Provider, MIAA has demonstrated:

- Expertise in auditing against the CAF.
- Independence and integrity in delivering high-quality assessments.
- Dedication to helping organisations manage cyber risks in an ever-changing threat landscape.

This recognition is particularly important for organisations required to have their NHS Data Security and Protection Toolkit submission independently audited, as NHS England strongly recommends using a CRA scheme-assured auditor. With this recognition, clients can be assured that DSPT audits are delivered to the highest standards reflecting both the detail of the Cyber Assessment Framework and the NHS's own DSPT audit guides.

Added Value

Briefings

Our latest briefings/blogs/podcasts are:

- Celebrating 10 Years of the MIAA Internship Programme: Reflections from Our 2024 Interns
- 25/26 MIAA Insight - AI Governance Checklist

Events

- Powerful Allyship: Everyone's Role (21st January 2026): In this masterclass we will share the principles and practices around allyship and showcase the positive impact allyship has on organisational culture and productivity. We will consider the role we all have as allies, alongside practical tools to facilitate leaders to create the conditions for allyship to thrive.

Appendix A: 2025/26 Contract Performance

The Global Internal Audit Standards (UK public sector) state that 'In the UK public sector, a chief audit executive must prepare such an overall conclusion at least annually in support of wider governance reporting, mindful of any specific sector obligations or processes. This overall conclusion must encompass governance, risk management and control.'

Below sets outs the overview of delivery for your Head of Internal Audit Opinion for 25/26:

HOIA Opinion Area	TOR Agreed	Status	Assurance Level	Audit Committee Reporting
Core/Mandated Assurances				
Risk Management		Q3/Q4		
Finance Systems Deep Dive		Q4		
Council tax & NNDR(Revenue & Benefits)		Q4		
Risk Based Assurances				
Payroll	✓	Final report issued	Substantial	25 November 2025
Governance Review	✓	Draft report stage		
VAT Audit	✓	Fieldwork concluding		
Contract Management	✓	Fieldwork		
Health and Safety	✓	Fieldwork		
Nelson Town Deal		Q3 - Planning		
Procurement	✓	Q3 - Fieldwork		

HOIA Opinion Area	TOR Agreed	Status	Assurance Level	Audit Committee Reporting
Licensing		Q4		
IT Critical application review: IT Asset Management	✓	Fieldwork		
Project Management Arrangements (was Carbon Plan)		Q4		
IT critical application review – IDOX system	✓	Final report issued	Limited	25 November 2025
Customer services review	✓	Final report issued	Substantial	30 September 2025
Follow Up				
Qtr 1	N/A	Completed	Not applicable	29 July 2025
Qtr 2	N/A	Completed	Not applicable	30 September 2025
Qtr 3	N/A	Completed	Not applicable	25 November 2025
Qtr 4	N/A	In progress		

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	There is ongoing engagement and communications regarding delivery of key reviews to support the Head of Internal Audit Opinion.
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. MIAA conforms with the Global Internal Audit Standards (UK public sector).

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

Report Title	**Payroll**			
Executive Sponsor	Director of Resources			
Assurance opinion	Substantial			
Objective	To assess the effectiveness of the systems of control operating at the Council to ensure that only employees of the organisation are paid, and only for work that they have performed on behalf of the organisation. **Limitations to scope:** The review did not assess the adequacy of IT controls within the payroll system.			
Recommendations	0 x Critical	0 x High	2 x Medium	1 x Low
Summary	Overall, our review found that there was a good system of internal control, however, our audit has identified a small number of areas for improvement. Liberata is the payroll service provider for Pendle Borough Council, and they manage the payroll of the council. The notifications of new hires, job variations, and terminations had appropriate authorisation, were submitted to payroll in a timely manner, and were accurately processed in the payroll system before the payroll cut-off date. The Council utilises the HR21 online platform for staff and payroll staff to update personal and bank details. New employees are granted access to HR21 upon joining. Bank detail changes trigger automated email notifications to payroll and the employee, ensuring timely awareness and appropriate action. Additionally, dedicated HR and payroll personnel are available to support staff with any queries relating to the update process, thereby reinforcing accuracy and compliance. Amendments to pay were appropriately authorised by designated signatories, accurately processed and uploaded to the payroll system. The following control weaknesses have been identified: • The Council has not established a formal payroll policy. Furthermore, the existing procedural documentation lacks the necessary depth and comprehensiveness to effectively serve as a standardised payroll policy framework. **(Medium priority)**			

	• Access rights are generally aligned with the responsibilities of most roles. However, for managerial and dual-function positions such as the HR and Payroll Manager, Payroll Officer, and HR Officer with payroll responsibilities access configurations are only partially appropriate. **(Medium priority)** • Proper establishment checks on payroll occur only every two months therefore overpayments may go undetected for up to two months, increasing the amount to be recovered and complicating recovery efforts. **(Low priority)**
Key Areas Agreed for Action	• A payroll policy and more detailed procedure notes will be put in place. **(Medium priority, action by 31 March 2026)** • HR Manager will review access rights on a quarter basis this meeting will be documented. It is important to limit access to HR's ability to make changes but if I oversee access rights and review where appropriate. We minimise those with full access to the 3 officers referenced so we don't have a single point of failure and too many people able to make significant changes. **(Medium priority, action by 31 December 2025)** • Establishment checks to be done and documented on a monthly basis between the HR and Payroll Team. **(Low priority, action by 31 October 2025)**
Key Risks Highlighted with No Agreed Action	N/A

Report Title	**IT Critical Application review - IDOX System**			
Executive Sponsor	Director of Resources			
Assurance opinion	Limited			
Objective	The overall objective of this review was to provide an assessment of the effectiveness of the control framework being exercised by management over the IDOX system and data flows and highlight improvements where appropriate. Scope Limitation: The following areas were not considered within the scope of this review: • Information governance, assurance reporting, risk management and legal compliance. • Security arrangements including general interface, database security, network shares, antivirus, and patching.			
Recommendations	0 x Critical	2 x High	1 x Medium	0 x Low
Summary	The review identified that there is a compromised system of internal controls in respect of the IDOX system as weaknesses in the design and/or inconsistent application of controls puts the achievement of the system objectives at risk. Areas for improvement identified included weak password credentials to access the IDOX system, a lack of user management across the system with accounts not being reviewed on a proactive basis to ensure that users still required the correct level of permissions and generic accounts had been created on the system including an administrator account. There were also no monitoring activities carried out to provide assurance regarding the use of the system and to identify any inappropriate access. The review also identified some areas of good practice including backups being stored in a 3-2-1 format (Three copies, two different types of storage and keeping one off site), the backups were also immutable. Third party access to the system had to be agreed prior to accessing the system via an access agreement. Remote access was granted via Cisco VPN with multifactor authentication (MFA) enabled.			

	In summary the key issues arising were: • The organisation had a total of twenty generic accounts on the system, including an administrator account with no further information provided on how they were monitored / managed. Password credentials across the system were weak and did not align with NCSC best practice guidance. There was a lack of user management across the system, accounts were not being reviewed on a proactive basis to ensure that access was required, nor were dormant accounts being reviewed and removed, where appropriate. **(High priority)** • There was no evidence of an annual review taking place for the framework arrangement with Liberata, to ensure that the agreement in place is still relevant, contains reference to and confirms compliance with relevant legislation, such as, GDPR/DPA 2018 and reflects current arrangements. There was no evidence of IDOX supplier assurance checks taking place such as a data protection impact assessment (DPIA), certifications check or a Digital Technology Assessment Criteria (DTAC). **(High priority)** • At the time of the review there was currently no formalised process for the reviewing of audit trails and activity across the IDOX system. No evidence of a logging and monitoring standard for the IDOX system. **(Medium priority)**
Key Areas Agreed for Action	• Agree that a review of generic administrator accounts should be undertaken and this number reduced if possible. Where these accounts are being used for a legitimate reason each account should be allocated to a responsible officer. Dispute the findings around passwords. The standards you have referenced are appliable only to web based or publicly accessible systems. As IDOX must be accessed only from inside the Council's network there is no viable external attack vector. This would mean that any attacker would first have to breach the Council substantial security, remain undetected and then attempt to gain access to IDOX. The likelihood of this is very low as Council security meets the standards of Cyber Essential's and we are undertaking a programme of hardware and software upgrades that will improve security further (Firewalls & VPN's). Agree that accounts should be reviewed. **(High priority, action by 31 December 2025)** **MIAA response to Council's management response - *Although the council advises it has robust network controls in place, strong password controls are also required for systems that are not accessible outside of the organisation or are behind firewalls, as they are still***

	at risk from insider threats, credential sharing, malware/compromised endpoints, for example, that would leave a system and its data exposed. • Will consult with Council and Liberata Contract managers on how IDOX SLA can be incorporated into the ongoing contract review process. IAR & ROPA presently under review and being updated. This will capture data processing undertaken in IDOX. Agree DPIA is needed. **(High priority, action by 31 January 2026)** • Before implementation we would first have to understand the capabilities of IDOX to identify and audit "unauthorised activity". All staff are assigned roles and given access according to their needs. Unauthorised activity needs to be considered in that context of people operating outside of their assigned roles or without permission to use Idox. Monitoring also needs to be proportionate to the limited risk. We would need to explore what built in tools there are to monitoring. **(Medium priority, action by 28 February 2026)**
Key Risks Highlighted with No Agreed Action	N/A

Appendix D: Follow up of previous internal 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	
Council Tax and NNDR (2022/23)	3	Substantial	2	1	-	-	-	-	1	-	One recommendation is in progress regarding production of debt write off policy, work on this is concluding and expected to be completed in December 2025.
Mandatory Training (2023/24)	5	Substantial	1	4	-	-	-	-	4	-	Revised dates have been provided again for these recommendations 31 March 2026. (Original dates were June/July 2024, then revised to 30 Nov 24 & 31 January 2025, 30 June/31 July 2025 and 31 October 2025). The outstanding recommendations relate to putting in place a mandatory training policy, developing a training needs assessment, putting in place a process so that mandatory training can be recorded and monitored centrally, and producing compliance reports on mandatory training. All recommendations are in progress and are expected to be completed and evidenced by March 2026. Corporate Leadership Team have confirmed mandatory training requirements which have been communicated to staff. PowerBi Apps are being utilised to create a dashboard, currently in draft form, to host the various learning management sites information to be utilised as a centralised recording method. Compliance is soon to be reported, reminders sent and formally discussed within the performance clinic.
Information Governance (2023/24)	5	Limited	-	5	-	-	-	3	2	-	Recommendations in progress. Revised dates of 31 December 2025 (original implementation date 31 August 2024, then revised to 31 December 2024, 31 May 2025 and 31 August 2025). The high priority recommendations relate to review of Council's IG resources, identifying IG training needs, ensuring there is a Record of Processing Activity including policy, ensuring all information assets are recorded in an Information Asset Register with IAO and IAA identified and ensuring that any contracts with suppliers which have an IG implication or provide support to IT systems that process council data are identified and that the contracts include the relevant IG clauses and a DPIA is undertaken.

AUDIT TITLE (YEAR)	NO OF RECS	ASSURANCE LEVEL	PROGRESS ON IMPLEMENTATION				OUTSTANDING RECOMMENDATIONS				COMMENTS
			✓/S	P	X	Not due/ FUIP	C	H	M	L	
											Work is ongoing to implement these recommendations. MIAA are providing support to the Council in the implementation of these recommendations.
Staff performance/ Appraisals (20234/24)	6	Limited	4	2	-	-	-	-	2	-	The outstanding recommendations relate to a PDR policy, although there is guidance documentation in place and also consideration of competency/values based recruitment processes and standardised role competencies / behaviour framework. There is a revised implementation date of 31/1/26.
Council tax & NNDR (2024/25)	4	Substantial	3	1	-	-	-	-	1	-	The outstanding recommendation relates an enhancement being made to the Citizens Access system. This has been marked as in progress as a new system will be implemented but the full functionality has not yet been tested. The revised implementation date for this recommendation is 31 December 2025.
Colne Municipal Theatre (2024/25)	4	N/A	3	1	-	-	-	-	-	-	The new project/ programme management documentation is being rolled out to the Extended Management Team on 30/9/25 with a view to being used from1/10/25. Recommendations not risk rated.
Complaints & Learning (2024/25)	10	Moderate	2	8	-	-	-	-	6	2	Original implementation date 31 March 2025, revised dates 30 June 2025, now 30 November 2025. Recommendations are in progress. The updated policy was presented to Extended Management Team at the end of June. Working towards November 2025 for completion of outstanding actions.
Finance Deep Dives – AP/AR (2024/25)	8	Moderate	7	-	-	1	-	-	1	-	Remaining recommendation not due until 31 December 2025.
Risk Management (2024/25)	3	Substantial	3	-	-	-	-	-	-	-	All recommendations actioned.
Council tax & NNDR (2024/25)	2	Substantial	1	-	-	1	-	-	1	-	Remaining recommendation not due until 30 November 2025.

AUDIT TITLE (YEAR)	NO OF RECS	ASSURANCE LEVEL	PROGRESS ON IMPLEMENTATION				OUTSTANDING RECOMMENDATIONS				COMMENTS
			✓/S	P	X	Not due/ FUIP	C	H	M	L	
Emergency Planning (2024/25)	4	Substantial	1	-	-	3	-	-	3	-	Follow up not due for remaining recommendations.
Customer Services (2024/25)	3	Substantial	-	1	-	2	-	-	3	-	Follow up not due for two recommendations. The Customer & Digital Strategy has been approved and a comprehensive delivery plan is being developed with the aim to include recommendations from this review.
Disabled Facilities Grant (2024/25)	8	Moderate	1	-	-	7	-	-	6	1	Follow up not due.
Payroll (2025/26)	3	Substantial	1	-	-	2	-	-	2	-	Follow up not due.
Totals	**68**	**-**	**29**	**23**	**-**	**16**	**-**	**3**	**32**	**3**	**Plus one recommendation not risk rated**

Key to recommendations:

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

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: • the efficient and effective use of resources • the safeguarding of assets • the preparation of reliable financial and operational information • compliance with laws and regulations.
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: • has a low impact on the achievement of the key system, function or process objectives; • has exposed the system, function or process to a key risk, however the likelihood of this risk occurring is low.
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

Darrell Davies

Engagement Lead

Tel: 07785 286381

Email: Darrell.davies@miaa.nhs.uk

Louise Cobain

Director Lead

Tel: 07795 564916

Email: Louise.cobain@miaa.nhs.uk