

# Internal Audit

## Follow up Audit Committee Summaries

2022/23

## Follow up report Contract monitoring – Homecare Framework Providers

### Follow up report Contract monitoring – Homecare Framework Providers

Original audit assurance rating



**Moderate**

	Extreme	High	Medium	Low
Number of actions			3	2
Implemented			3	1
Superseded				1
Progressing				
Not implemented				

A follow-up audit has been conducted to determine the progress made by Lancashire County Council to implement the actions agreed in the Internal Audit report; Contract Monitoring – Homecare Framework Providers, issued in June 2022. Our original review provided moderate assurance over the adequacy and effectiveness of the contract monitoring arrangements in ensuring commissioned services comply with statutory requirements.

Three medium and two low risk actions were agreed to be implemented by 30 September 2022 and based on the information and evidence provided to us, we are satisfied that adequate progress has been made in implementing the agreed actions. Staff have been reminded to complete the KPI tracker spreadsheet and notes are clearly made to evidence that late submissions are chased. Additionally, staff were reminded of the requirement for providers to complete and send in complaint forms. This is also being raised at the individual provider contract review meetings and it was also referenced during the webinar on Effective Complaints Handling in July 2022. The guidance for dealing with finance queries has been amended and is available to providers on the Care Portal and contains contact details if there is a query. Additionally, staff within Adult Social Care have been reminded to provide timely accurate information to Care Navigation to ensure payments to providers are set up timely and correctly negating errors arising.

## Follow up report: Contract monitoring – Residential Care

### Follow up report: Contract monitoring – Residential Care

Original audit assurance rating



**Moderate**

	Extreme	High	Medium	Low
Number of actions			1	3
Implemented			1	2
Superseded				
Progressing				1
Not implemented				

A follow-up audit has been conducted to determine the progress made by Lancashire County Council to implement the actions agreed in the internal audit report, Contract Monitoring - Residential Care Providers, issued in June 2022. Over original review provided moderate assurance over the adequacy and effectiveness of the contract monitoring arrangements in ensuring commissioned services comply with statutory requirements.

One medium and two low risk actions were agreed to be implemented by 30 December 2022 and based on the information and evidence provided to us, we are satisfied that adequate progress has been made in implementing the agreed actions. A peer review will be considered where providers are not engaging in the RADAR process and in cases where they have been on RADAR for twelve months, the findings of the audit review were shared with the contract management team in a separate meeting and the contract monitoring reporting template is being reviewed to fit with the revised framework.

## Follow up report: Older People Care Services - Safeguarding Alerts

### Follow up report: Older People Care Services - Safeguarding Alerts

Original audit assurance rating



Moderate

	Extreme	High	Medium	Low
Number of actions			3	1
Implemented				
Superseded				
Progressing			3	1
Not implemented				


A follow-up audit has been conducted to determine the progress made by the Older People Care Services with implementing actions agreed in the internal audit report for Safeguarding Alerts, issued in May 2022. Our original review provided moderate assurance over the adequacy and effectiveness of the control framework to support achievement of the Councils objectives in relation to Safeguarding Alerts in Older People Care Services. Three medium priority actions and one low were agreed to be implemented within six months of issuing our final report in May 2022.

Based on the information and evidence provided to us, we are satisfied that the main activity underpinning implementation of all the actions, associated with processes in place for raising, recording and monitoring safeguarding alerts is progressing well. Training and policy documentation has been reviewed, with the training plan completed and issued, and the policy pending final approval prior to issue. Processes for raising, recording and monitoring safeguarding alerts are subject to regular review, with operational and development managers continuing to enhance and develop methods and practices aiming to ensure continuous improvement and best practice is achieved. These include development of data monitoring tools; standardising documents and folder structures; enhanced quality assessments at establishments; and scheduled briefing sessions to managers.

Payment Card Industry Data Security Standard - (PCI DSS)

Payment Card Industry Data Security Standard - (PCI DSS)					
Original audit assurance rating		Extreme	High	Medium	Low
	Number of actions		5	1	
	Implemented				
	Superseded				
	Progressing		2		
	Not implemented		3	1	



**Limited**

Whilst some actions have been taken overall progress towards Payment Card Industry Data Security Standard (PCI DSS) compliance has been limited due to a combination of the draft Policy not being finalised (the initial draft policy was presented to the Information Governance Group in July 2022) due to disagreements with respect to the level of detail contained therein, and delays in the appointment of an external assessor (we were advised due to lack of resources within the IT team to support the activities of an external assessor). This has been exacerbated by the apparent lack of involvement of the oversight process in helping to resolve issues such as those preventing finalisation

We were informed that an assessor might be in place by July 2023 to conduct the formal assessment, which could help to drive the implementation of some of the recommendations. However, a new more challenging standard (PCI v4.0) will come into effect on 31 March 2024. Considering the non-compliance with the standard and given the limited time to achieve compliance with the more demanding technical requirements for PCI v4.0, it is unclear whether achieving compliance within prescribed timescales will be possible

Specifically, PCI DSS v4.0 involves actions such as enhanced authentication, including use of Multi-Factor Authentication and minimum password lengths of 12 characters, and extending the scope of the standard to cover mobile, the Internet of Things and cloud computing. In total, v4.0 introduces 63 new requirements, 13 of which must be implemented by 31 March 2024. It is estimated that the remaining 50 new requirements might each involve one to six months of effort, and all are enforceable with effect from March 2025.

Overall, out of the original agreed, five high risk and one medium risk, only two high risk agreed actions are progressing demonstrating a lack of significant progress in dealing with the issues raised. As a result, the council may be in a position of non-compliance if a more proactive approach to meeting the new requirements is not taken at the earliest opportunity.

## Payment Card Industry Data Security Standard - (PCI DSS)

Since the completion of this follow up audit by MIAA's technology auditors the council's Digital Services have provided a further update to the Head of Internal Audit. Digital Services are currently out to tender to award the following scope of work by July 2023

### **Scope of Work**

To reduce the risk of non-compliance and the associated fines and penalties the council seek to achieve compliance against version 4 (March 2022) of the Payment Card Industry Data Security Standard (PCI DSS v4) and are seeking to work with as suitably qualified partner to achieve this as a baseline from which to move forward.

The council anticipates that this work will be undertaken over 4 phases with the supplier directly leading in Phases 1 and 3.

#### 1. Phase 1 – Scope definition/Gap Analysis

In this phase the supplier will follow their standard process for discovery and review against Lancashire County Council's existing architecture and business processes to assist in defining the 'Cardholder Data Environment', the scope boundaries for Payment Card Industry Data Security Standard compliance and identification of any areas in which Lancashire County Council would require corrective measures to address gaps against compliance. This may include opportunities to reduce the scope of the Cardholder Data Environment. This phase will result in a Gap Analysis report.

#### 2. Phase 2 – 'Gap Closure'

In this phase Lancashire County Council will review the findings from Phase 1, develop an agreed Remediation Action Plan and enact the agreed changes to reduce the scope of the Cardholder Data Environment and correct any gaps in compliance identified by the supplier. This phase will conclude when Lancashire County Council believes all identified gaps have been closed. The supplier's assistance may be requested for clarifications and guidance at this stage and these will be subject to variation of contract at the appropriate time.

#### 3. Phase 3 – Successful Compliance Audit and initial submission of ' Attestation of Compliance'.

In this phase the supplier will revisit the changed architecture and business processes to ensure that Lancashire County Council has successfully achieved compliance against Payment Card Industry Data Security Standard version 4.0. The supplier will also work with relevant teams to guide and support the initial 'Attestation of Compliance ' to the Authority's acquiring bank. This phase will result in a final ' Attestation of Compliance ' and completion and submission of relevant Self-Assessment Questionnaire(s) being accepted by the acquiring bank.

#### 4. Phase 4 – Implementation of processes to maintain compliance.

In this phase Lancashire County Council will put in place long term operational procedures to fulfil all regular ongoing compliance tasks required to maintain the Authority's compliance against Payment Card Industry Data Security Standard version 4.0. This phase and the project will close when Lancashire County Council are able to self-sustain compliance.

As the council has not previously undertaken an 'Attestation of Compliance' at Level 3 the Authority is keen to obtain skilled and knowledgeable guidance to identify: -

## Payment Card Industry Data Security Standard - (PCI DSS)

1. Define the current 'Cardholder Data Environment'
2. Gaps in current Business Processes that may adversely impact the council's compliance
3. Gaps in Technical Processes and deployed architectures which may adversely affect the council's compliance
4. Opportunities to reduce the Cardholder Data Environment
5. Guidance on the most appropriate Self-Assessment Questionnaire(s) for the council to complete
6. Any requirements for remaining compliant on an ongoing basis

Whilst it is acknowledged that the council are currently unaware of all the compliance gaps that exist at this time; it is hoped that compliance with PCI DSS v4 could be achieved within 12 months of the Gap Analysis report being generated.