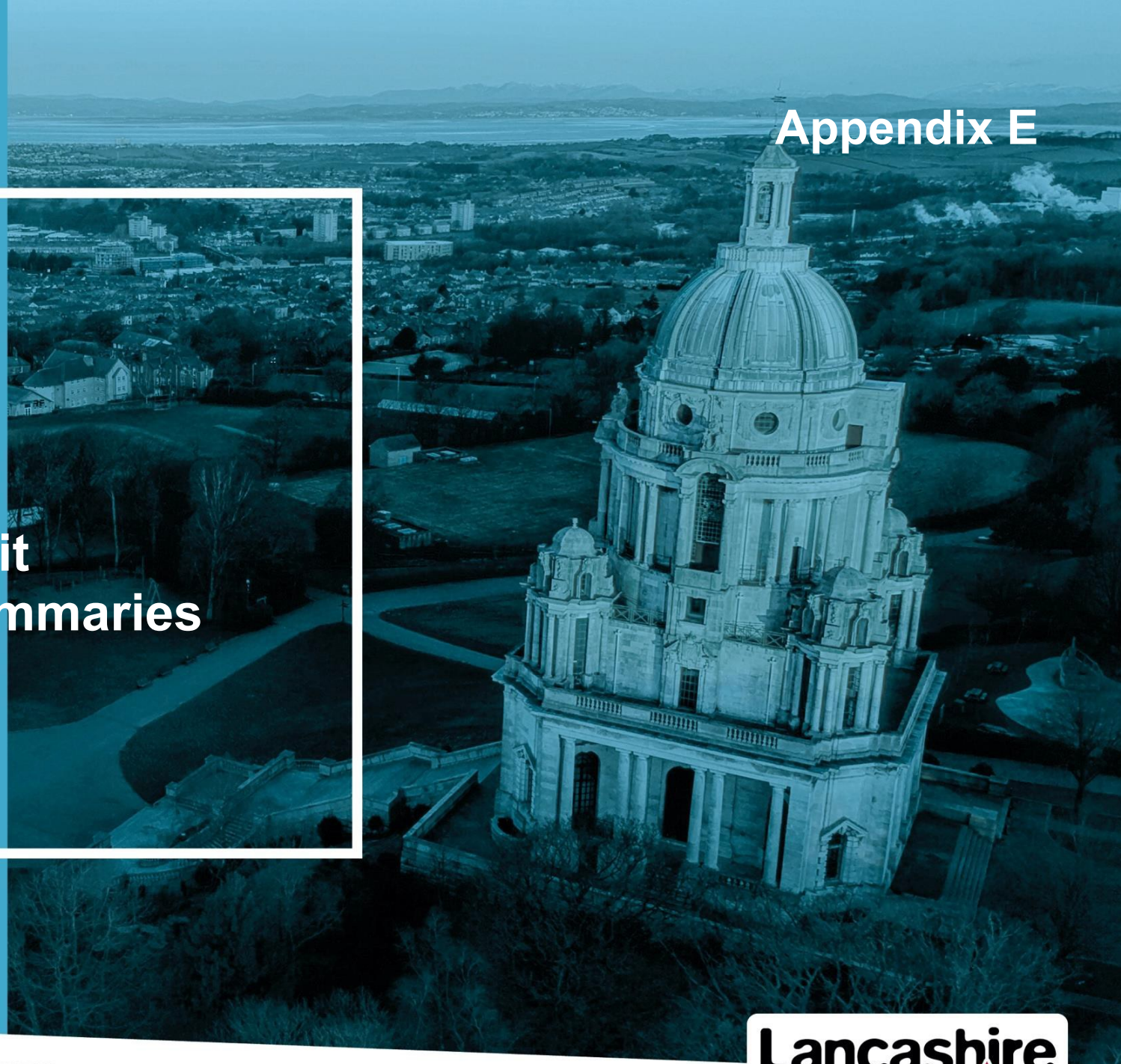
Appendix E

# Internal Audit

# Follow up Audit Committee Summaries



Lancashire County Council

## Occupational Health

**Original audit assurance rating**

**Substantial**

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| Superseded | | | | |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

Our previous review of the Occupational Health Contract, reported in February 2024, resulted in a substantial assurance opinion. We reported that:

- The H&S Team have adequate and appropriate processes, procedures and comprehensive guidance notes in place to effectively manage the contract and also to provide Lancashire County Council (LCC) staff with appropriate information to manage absence situations.
- The H&S Team have regular monitoring meetings with Optima and key stakeholders to address any issues and they evaluate the contract performance through the weekly progress reports received, additionally we found no evidence of any negative customer feedback, thus providing assurance that there are no procedural weaknesses.
- Checks are appropriate by the H&S Team which confirm that the invoices received for the services provided are correct and they monitor any pattern changes within OH services provided.
- A dashboard report is provided to Executive Management Team on a quarterly basis which covers a high-level review of the OH contract performance, and that there were no significant performance issues reported during the year.

Our original review did not identify any weaknesses in the overall Occupational Health Contract monitoring; however, we did agree one action to strengthen the current process and are pleased to report that the action has been implemented.

## CCTV systems

**Original audit assurance rating**

**Limited**

| | Extreme | High | Medium | Low |
|---|---|---|---|---|
| Number of actions | | 1 | 4 | 1 |
| Implemented | | | 4 | |
| Superseded | | | | |
| Progressing | | 1 | | |
| Not implemented | | | | |

An internal audit of CCTV cameras was undertaken in 2022 and five actions were agreed with management. The audit provided limited assurance over the controls. We have followed up the five agreed actions and confirmed that four have been implemented and the fifth is in the process of being implemented.

An asset register has been compiled and contains information to enable any non-compliance with the CCTV policy to be identified. The information is being reviewed which is why this action has been marked as 'Progressing'. The maintenance of the register is also a continuous ongoing process. Premises managers within Facilities Management have undertaken information governance training. The number and locations of cameras at county hall have been reviewed. A report was produced for the Senior Information Risk Owner detailing how effective surveillance camera systems have been during the year.

## Payment Card Industry Data Security Standard (PCIDSS)

**Original audit assurance rating**

**Limited**

| | Extreme | High | Medium | Low |
|---|---|---|---|---|
| Number of actions | | 5 | 1 | |
| Implemented | | 3 | 1 | |
| Superseded | | | | |
| Progressing | | 1 | | |
| Not implemented | | 1 | | |

The original PCI DSS compliance audit reported in May 2022 included five high and one medium priority management action. A follow up review to report progress against the agreed management actions was undertaken in April 2023 whereby two of the high priority management actions were progressing but four management actions had not been implemented (3 high and 1 medium priority recommendations). As a result of this second follow up review, two high and one medium priority recommendations have now been implemented. One high priority management action is progressing with the remaining two not implemented at this stage. These outstanding management actions relate to gaps in the policies and procedures to ensure the continued compliance with the requirements of PCI DSS standards and the internal assurance mechanisms for reporting continued compliance.

The council have taken some positive steps towards gaining compliance with the PCI DSS standards. In October 2023, the council engaged consultants, Control Case, to undertake a gap analysis between the PCI DSS standards and the council's current arrangements, which resulted in a Gap Analysis report dated November 2023 and an action plan.

The council were commissioning further support from the external consultant to assist with progressing the action plan but waiting on resources to be confirmed. As the gap analysis report did highlight some significant issues beyond the PCI DSS compliance in relation to cyber security, it is essential that the council progress the action plan at pace, to address the control weaknesses identified and to reduce the council's risk exposure.

## Cyber Security: Baseline Technical Controls

**Original audit assurance rating**

**Moderate**

| | Extreme | High | Medium | Low |
|---|---|---|---|---|
| Number of actions | | | 5 | |
| Implemented | | | 3 | |
| Superseded | | | 1 | |
| Progressing | | | 1 | |
| Not implemented | | | | |

The original report, dated March 2021, included 5 recommendations, all rated Medium Risk. The five recommendations included 16 individual agreed management actions, and each one has been followed up resulting in 11 agreed actions confirmed as fully implemented, 2 progressing, 2 superseded and 1 not implemented.

Given the exponential increase in the number of cyber-attacks against UK public sector bodies, some with well-publicised devastating impacts, delays in implementing security features that are designed to improve cyber security is likely to increase the risk profile of the Council.

## Mobile Working and Device Review

**Original audit assurance rating**

**Moderate**

| | Extreme | High | Medium | Low |
|---|---|---|---|---|
| Number of actions | | | 4 | |
| Implemented | | | 2 | |
| Superseded | | | | |
| Progressing | | | 2 | |
| Not implemented | | | | |

The previous report, issued in December 2022, included a Moderate assurance rating and four individual action points in response to the two recommendations, (Recommendation 1 – 3 agreed actions and Recommendation 2 – 1 agreed action) were agreed. The target date for implementing these actions was May 2023.

A governance group has been created (Corporate Cyber Risk and Security Group) and Terms of Reference provided. The service confirmed that risk assessments are “work in progress. Conducting risk assessments on devices prior to connectivity to the council’s network, provides an opportunity to identify security vulnerabilities and to mitigate these.

The Council utilise Microsoft Intune as the council’s mobile device management (MDM) solution. A report was provided to demonstrate that the following devices had been enrolled with Intune as follows Android (c2550) and iPhones, iPads etc (c800) at the time of the follow up.