Appendix 1

# Lancashire Combined Fire Authority

# Internal Audit Service monitoring report: period ended 4 March 2025

## 1 Purpose of this report

1.1 The Internal Audit Plan for 2024/25 was approved by the Audit Committee in March 2024. This report details the progress to date in undertaking the agreed coverage.

## 2 Internal audit work undertaken

2.1 Work carried out during the period 1 April 2024 to 4 March 2025 was in accordance with the agreed audit plan. To date, 63.5 days have been spent this financial year on completing the 2024/25 plan, equating to 91% of the total planned audit activity of 70 days. The table below shows the current status of all audit work.

*Use of this report*

2.2 This report has been prepared solely for the use of the Lancashire Combined Fire Authority. We accept no responsibility to any third party who may receive this report, in whole or in part, for any reliance that they may place on it. In particular, we expect the external auditors to determine for themselves the extent to which they choose to utilise our work.

| Audit review | Audit days | | | Status | Assurance opinion |
|---|---|---|---|---|---|
| | Planned | Actual | Variation | | |
| ***Governance and business effectiveness*** | | | | | |
| Overall governance, risk management and control arrangements | 3 | 2 | 1 | Ongoing | |
| ***Service delivery and support*** | | | | | |
| Cyber security | 15 | 14.5 | 0.5 | Final | 🟡 Moderate March 2025 |
| Implementation of learning from national incidents | 15 | 15 | 0 | Final | 🟢 Substantial November 2024 |
| ***Business processes*** | | | | | |
| Accounts payable | 9 | 8.5 | 0.5 | Draft Report | N/A |

| | | | | | |
|---|---|---|---|---|---|
| Accounts receivable | 9 | 8.5 | 0.5 | Draft Report | N/A |
| General ledger | 6 | 5 | 1 | Draft Report | N/A |
| ***Follow up audit activity*** | | | | | |
| District planning activity | 2 | 1.5 | 0.5 | Final | N/A |
| ***Other components of the audit plan*** | | | | | |
| Management activity | 10 | 7.5 | 2.5 | Ongoing | |
| National Fraud Initiative | 1 | 1 | 0 | | |
| **Total** | **70** | **63.50** | **6.5** | | |

## 3 Extracts from Audit Reports

3.1 Extracts of assurance summaries are shown below

## Cyber Security: Governance

**Overall assurance rating**

●

**Moderate**

*See Appendix A for Rating Definitions*

**Audit findings requiring action**

| Extreme | High | Medium | Low |
|---|---|---|---|
| 0 | 0 | 2 | 2 |

The Fire and Rescue Service received its Cyber Essentials Plus accreditation in August 2024, a government backed certification scheme that helps to keep organisation's data safe from cyber-attacks. The organisation complies with the National Cyber Security Centre's cyber assessment framework, with the outlined principles evident across its policies and procedures. The service has sound controls in place surrounding business continuity and incident response, with thorough plans in place and an active process to stress-test processes through simulated exercises. The ICT service was recognised for its sound technical controls by the National Fire Chiefs Council, winning their Excellence in Cyber award for 2024.

The service is in the process of drafting a cybersecurity plan for 2025-2027 which is due for review and approval from the Senior Information Risk Officer later this year. A recommendation has been raised to help current drafts further comply with the National Cyber Security Centre's framework which the organisation adheres to. The Senior Information Risk Officer receives regular updates on cyber issues through a standing quarterly meeting with the security lead, however updates are not provided to the Executive Board, and information provided to committees are inconsistent in detail.

Policy documents referencing cyber security provide guidance and direction on the organisation's cyber security framework and plans in the event of a cyber-attack, However, we have identified some inconsistent practices which may impact the consistent application of these policies by all staff, including accessibility of policies via the intranet and inconsistent document version controls.

During our audit, the Interim Head of ICT identified a system error which resulted in mandatory 12-monthly training on cyber awareness to be issued on a two-yearly basis. This has since been rectified; however, some 231 staff were outstanding on their training as of the 24 January. Members of the Executive Board are enrolled onto the training module but is not accessible to members of committees, who may otherwise benefit from additional training to support their decision making and scrutiny on cyber security matters.

## Audit assurance levels and residual risks Appendix 1

Note that our assurance may address the adequacy of the control framework's design, the effectiveness of the controls in operation, or both. The wording below addresses all of these options, and we will refer in our reports to the assurance applicable to the scope of the work we have undertaken.

- 🟢 **Substantial assurance**: the framework of control is adequately designed and/ or effectively operated overall.
- 🟡 **Moderate assurance**: the framework of control is adequately designed and/ or effectively operated overall, but some action is required to enhance aspects of it and/ or ensure that it is effectively operated throughout.
- 🔴 **Limited assurance**: there are some significant weaknesses in the design and/ or operation of the framework of control that put the achievement of its objectives at risk.
- ⚫ **No assurance**: there are some fundamental weaknesses in the design and/ or operation of the framework of control that could result in failure to achieve its objectives.

### Classification of residual risks requiring management action

All actions agreed with management are stated in terms of the residual risk they are designed to mitigate.

⬛ **Extreme residual risk**: critical and urgent in that failure to address the risk could lead to one or more of the following: catastrophic loss of the LRFS services, loss of life, significant environmental damage or significant financial loss, with related national press coverage and substantial damage to the LRFS reputation. *Remedial action must be taken immediately.*

🟥 **High residual risk**: critical in that failure to address the issue or progress the work would lead to one or more of the following: failure to achieve organisational objectives, significant disruption to the LRFS business or to users of its services, significant financial loss, inefficient use of resources, failure to comply with law or regulations, or damage to the LRFS reputation. *Remedial action must be taken urgently*.

🟨 **Medium residual risk**: failure to address the issue or progress the work could impact on operational objectives and should be of concern to senior management. *Prompt specific action should be taken*.

🟩 **Low residual risk:** matters that individually have no major impact on achieving the service's objectives, but when combined with others could give cause for concern. *Specific remedial action is desirable.*