Recommendations Follow Up Assignment Report 2025/26

North Wales Fire & Rescue Service

June 2025

Contents

MIAA would like to thank all staff for their co-operation and assistance in completing this review.

This report has been prepared as commissioned by the organisation and is for your sole use. If you have any queries regarding this review, please contact the Engagement Manager. To discuss any other issues then please contact the Director.

1 Executive Summary

A key part of the work undertaken by MIAA as your internal auditors involves us making recommendations to improve and strengthen governance, risk management and controls to support the organisation in achieving its objectives. To verify that the benefits of the recommendations are achieved, it is necessary to subsequently follow up on implementation of agreed actions, in order to fully assess:

- Whether implementation has occurred or been superseded by further events; and
- Whether the actions have produced the intended effect.

Follow-up is, therefore, a vital aspect of the internal audit process and it is our policy, in accordance with the Internal Audit plan, to revisit previous assignments.

The table overleaf sets out the areas and recommendations which have been reviewed this time and the level of progress which has been made. Our review confirms that good progress has been made in implementing recommendations.

2 Summary of Findings

The table below sets out the areas and recommendations which have been reviewed this time and the level of progress which has been made.

Audit Report	Total No. of Recs to be followed up	Implemented	Partial				Not Implemented				Superseded/ Not Accepted				Not yet Followed Up				Comments
			C	H	M	L	C	H	M	L	C	H	M	L	C	H	M	L	
2023/24																			
Key Financial Transactional Processing Controls	2	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	All recommendations have now been implemented.
Cyber Organisational Controls Review	6	-	-	1	5	-	-	-	-	-	-	-	-	-	-	-	-	-	6 recommendations have been partially implemented in relation to the following actions: • Incident management and response and threat reporting ***(High)*** • Embedding cyber security, developing a positive cyber security culture and growing cyber expertise ***(Medium)*** • Third party/partner management ***(Medium)*** • Identifying cyber assets ***(Medium)*** • Cyber security regime ***(Medium)***

Audit Report	Total No. of Recs to be followed up	Implemented	Partial				Not Implemented				Superseded/ Not Accepted				Not yet Followed Up				Comments
			C	H	M	L	C	H	M	L	C	H	M	L	C	H	M	L	
																			• Cyber security measures ***(Medium)*** Revised implementation dates – April 2025 These recommendations will be followed up again by our Technology Risk Assurance Team in Q2 2025/26 and an update will be provided at the next Audit Committee in September 2025. Responsible Officer – Head of ICT
2024/25																			
Procurement	3	2	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	1 recommendation has been partially implemented in relation to the following action: • Manual process for contracts ***(Low)*** Revised implementation date – End of Quarter 2 2025/26 Responsible Officer – Procurement and Contracts Manager / Deputy Head of Finance and Procurement

Audit Report	Total No. of Recs to be followed up	Implemented	Partial				Not Implemented				Superseded/ Not Accepted				Not yet Followed Up				Comments
			C	H	M	L	C	H	M	L	C	H	M	L	C	H	M	L	
Key Financial Transactional Processing Controls	6	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	3	3	These recommendations will be followed up as part of the Key Financial Transactional Processing Controls review scheduled in Quarter 3 2025/26.
Training Strategy Implementation Plan	4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	4	-	All implementation due dates have not yet passed (end of Quarter 1 2025/26)
Risk Management	5	-	-	-	-	-	-	-	-	-	-	-	-	-	-	4	-	1	All implementation due dates have not yet passed (September 2025)
TOTAL	26	4	-	1	5	1	-	-	-	-	-	-	-	-	-	4	7	4	

3 Outstanding Critical / High Level Recommendations

Review Title	Recommendation	Responsible Officer (Title)
Cyber Organisational Controls Review	Incident management and response and threat reporting Recommendation – 1. Formalise / implement a plan to update Incident Response Plans and the overarching Business Continuity Plan (BCP) / Cyber Response Plan. 2. Schedule / implement a timetable to test the BCP plans / playbooks and include SLT representation. As part of the testing, review the associated roles and responsibilities, documentation, and assurances around resilience arrangements. Formally capture lessons learnt. 3. Evidence updated documented cyber / IT disaster recovery / incident response plan(s) / schedules to ensure roles and responsibilities for managing a system-wide incident are understood and for ensuring communications are effective. 4. Publish an approved overarching incident response policy across all the providers. Include:- a. a definition of what a cyber incident is. b. key contacts and reporting channels for all localities / third parties / the region / nationally such as NCSC c. service priorities / IAR critical assets agreed by SLT. d. critical assets and a critical system recovery list based upon service priorities. e. escalation routes between SLT / ICT for cyber events and sign off authority/ target groups to make decisions such as the sign off of forensic costs. f. Security notification / advisory incident distribution list. g. alignment with security update processes.	Responsibility for Action – Head of ICT Original Deadline for Action – 1. Mar 24 2. Oct 24 3. July 24 4. July 24 5. ongoing 6. ongoing 7. Oct 24 8. Mar 24 9. Apr 25 10. June 24 11. Apr 25 12. a) June 24 - discussion taken place b) dashboards to be evidenced - date TBC Revised Deadline for Action – end of April 2025 These recommendations will be followed up again by our Technology Risk Assurance Team in Q2 2025/26 and an update will be provided at the next Audit Committee in September 2025.

Review Title	Recommendation	Responsible Officer (Title)
	h. formalising the link between learning form incidents and the training needs analysis plan. 5. Review and ensure supplier support arrangements / SLAs provide appropriate coverage in terms of incident management and security assurance reporting. Continue to work with Information Asset Owners (IAOs) to ensure local plans are understood and aligned with the business objectives. 6. Publish and approve as planned an ICT / Digital strategy. 7. Document the logging and monitoring (and data retention) policy and align within the new ICT strategy. For example, to enable prosecution to be enforceable and / or to be able to hold suppliers / staff to account. 8. Formalise and publish a digital plan going forward including for instance, ongoing management / maintenance of solutions, details of planned projects / pilot programmes / enhancements such as further automation / scripting, additional network segmentation / testing, regular review of on call arrangements / supporting toolsets, etc. 9. Schedule / implement CIPR training, as appropriate and review the job description for the Incident Manager. 10. Continue to evidence regular threat reporting being undertaken and reported to an appropriate governance group. 11. Schedule regular penetration testing and evidence progress against associated improvement plans as a result of these tests / scans / reviews. 12. Evidence solution dashboards being calibrated against one another to ensure they align.	

Review Title	Recommendation	Responsible Officer (Title)

Management Response (Remedial Action Agreed) –

1. Plan will be formed in conjunction with the annual departmental strategy (currently in draft). Final version anticipated Feb 2024 (TBC)

2. HoICT to produce playbook in conjunction with infrastructure team with the target of doing a tabletop exercise by the end of Q2 in the year 24/25 in conjunction with ISC. ISC includes SLT representatives from the Control Room, Operations, ICT and a principal officer.

3. An All-Wales Cyber Response Plan is being drawn up by the Local Resilience Forum (lead by North Wales Police). Once this is distributed, NWFRS will adapt to its own technological implementations. It was not possible to establish a publish date at this time although it is expected before the end of the 23/24 year. A draft CRP can be expected mid-way through the following year (2024).

4. As above

5. HoICT to work with supervisory managers in ICT and review as contracts are renewed during the 24/25 year, or during contract reviews for multi-year contracts.

6. See point 1

7. HoICT to work with Infrastructure Manager to produce policy ready for consultation by the end of Q2 of the 24/25 year.

8. HoICT to work with supervisory ICT managers to develop a 1- and 5-year strategy including technological advancements and cyber security testing. Expected end of 23/24 year (March).

9. HoICT to submit financial bid for in the 25/26 financial year with the potential to bring training forward if flexibility in the already agreed 24/25 budget allows

Review Title	Recommendation	Responsible Officer (Title)
	10. Cyber Security Working Group to be formalised at the beginning of the 24/25 year and the Terms of Reference will include this 11. HoICT to submit financial bid for in the 25/26 financial year with the potential to bring training forward if flexibility in the already agreed 24/25 budget allows. Consideration will also be given whether the infrastructure team has sufficient capacity to undertake this work 12. Discussions will need to be held with the Infrastructure Manager regarding this in Q1 24/25, which was not possible at time of writing. Update March 2025 – Parts 6, 8, 10 and 12 have been completed. 1. We were advised that the first iteration of the Cyber Response Action Plan had been created. A draft was expected to be presented to Information Steering Committee (ISC) by the end of 2024/25 period. 2. We were advised that the playbook will be drafted once the Cyber Response Action Plan has been approved, likely to be based on the NCSC exercise in a box. For the ICT objectives for 2025/26, we were advised that there was a plan for a desktop Business Continuity Management (BCM) exercise in the first half of the year, with a possible real-life exercise towards the end of the year. Also, the Head of ICT had joined the new Business Continuity Management group. 3. We were advised that the updated documentation cyber / IT disaster recovery and incident response plans, including schedules that define roles and responsibilities for managing system-wide incident and ensuring affective communication, were to be included as part of the Cyber Response Action Plan. 4. We were advised that the elements of the overarching incident response policy was to be incorporated into the Cyber Response Action Plan.	

Review Title	Recommendation	Responsible Officer (Title)
	5. We were advised that the Service was investigating the cost of the 'Risk Ledger' product by the end of the financial year. Indicative costs (£10-15K) are considered by ICT too much for ICT's use alone but there was potential through conversations with the procurement manager to introduce this to the whole service. Conversations were ongoing and pending a demonstration by Risk Ledger of their capabilities. To evidence - review supplier support arrangements / SLAs provide appropriate coverage in terms of incident management and security assurance reporting. Continue to work with Information Asset Owners (IAOs) to ensure local plans are understood and aligned with the business objectives. 7. We were advised a Logging and Monitoring policy was to be written by the end of the financial year. 9. We were advised that the Head of ICT was to arrange and attend CIPR training in the next 25/26 financial year, finances allowing. 11. Penetration testing for corporate systems was to be arranged for the 2025/26 financial year and sensitive systems such as CAD are scheduled to be tested in 2024/25.	

Appendix A: 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 significantimpact 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.

Appendix B: Report Distribution

Name	Title
Helen MacArthur	Assistant Chief Fire Officer
Audit Committee	

Angharad Ellis
Deputy Regional Assurance Director
Tel: 07469378328
Email: Angharad.Ellis@miaa.nhs.uk

Limitations

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.

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.