Follow-up: Cyber Security
Final Internal Audit Report

April 2024

Cardiff & Vale University Health Board

GIG CYMRU NHS WALES
Partneriaeth Cydwasanaethau
Gwasanaethau Archwilio a Sicrwydd
Shared Services Partnership
Audit and Assurance Services

GIG CYMRU NHS WALES
Bwrdd Iechyd Prifysgol Caerdydd a'r Fro
Cardiff and Vale University Health Board

Contents

Executive Summary 3
1. Introduction 4
2. Findings 4
Appendix A: Management Action Plan 5
Appendix B: Assurance opinion and action plan risk rating 8
Appendix C: Assurance opinion and action plan risk rating 16

Review reference:	CVUHB-2324-15
Report status:	Final
Fieldwork commencement:	08 March 2024
Fieldwork completion:	13 March 2024
Draft report issued:	14 March 2024
Debrief meeting:	Not required
Management response received:	04 April 2024
Final report issued:	05 April 2024
Auditors:	Martyn Lewis (Senior IM&T Audit Manager) Sian Harries (IM&T Audit Manager)
Executive sign-off:	David Thomas (Director of Digital & Health Intelligence)
Distribution:	James Webb (Head of Information Governance & Cyber Security)
Committee:	Audit and Assurance Committee

Audit and Assurance Services conform with all Public Sector Internal Audit Standards as validated through the external quality assessment undertaken by the Chartered Institute of Public Finance & Accountancy in April 2023.

Acknowledgement

NHS Wales Audit and Assurance Services would like to acknowledge the time and co-operation given by management and staff during the course of this review.

Executive Summary

Purpose

The overall objective of this audit is to provide the Health Board with assurance regarding the implementation of the agreed management actions from the Cyber Security (2223-24) review that was reported as part of our 2021/22 work programme.

Overview of findings

Good progress has been made to address the recommendations contained within the original report.

A Cyber Security Improvement plan was developed and implemented in November 2023 and presented to the Digital Health and Intelligence Committee in February 2024.

Terms of Reference for the CAV Cyber Security Meeting and Cyber Security Sub-Group have been implemented and action logs and meeting minutes have been maintained.

We note that two recommendations remain in progress.

- Whilst the Cyber Security Improvement Plan has been developed, it lacks assigned officers and a timetable for implementation.
- Our review of Cyber reports to the Digital Health and Intelligence Committee noted that KPI's have not yet been developed.

Follow-up Report Classification

		Trend
Reasonable 	**Follow up:** Most high priority recommendations implemented and progress on the medium priority recommendations.	2022/23

Progress Summary

	Previous Matters Arising	Previous Priority Rating	Direction of Travel	Current Priority Rating
1	Lack of Cyber Security Improvement Plan	High		Low
2	Cyber security monitoring	High		Closed
3	Cyber Security Improvement reporting	Medium		Closed
4	Performance Measures / KPI's	Medium		Medium
5	Data back-ups and restores	High		Closed

1. Introduction

1.1 The follow-up review of Cyber Security was completed in line with the 2023/24 Internal Audit Plan for Cardiff and Vale UHB (the 'health board'). The opinion provided through this review is a key component, which will inform the Head of Internal Audit's Annual Opinion.

1.2 This was a follow-up review of the original report that was issued in March 2023 (2223-24), which identified five issues and resulted in an overall assurance rating of 'Limited Assurance'.

1.3 The relevant lead director for the review is the Director of Digital and Health Intelligence.

1.4 The potential risks considered in the original review were as follows:

- Poor or non-existent stewardship in relation to cyber security;
- Failure to comply with regulations e.g., NIS Regulations; and
- Loss of data or services and inappropriate access to information.

1.5 The scope of this follow-up review does not aim to provide assurance against the full review scope and objective of the original review. The 'follow-up review opinion' provides an assurance level against the implementation of the agreed action plan only.

2. Findings

2.1 The table below provides an overview of progress in implementing the previous internal audit recommendations:

Original Priority Rating	Number of Recommendations	Implemented / Obsolete (Closed - No Further Action Required)	Action Ongoing (Further Action Required)	Not implemented (Further Action Required)
High	3	2	1	0
Medium	2	1	0	1
Low	0	0	0	0
Total	**5**	**3**	**1**	**1**

2.2 Full details of recommendations requiring further action are provided in the **Management Action Plan** in **Appendix A**.

Appendix A: Management Action Plan

Previous Matter Arising 1: Cyber Security Improvement Plan (Design)		
Original Recommendation		Original Priority
1.1 The team should prioritise and focus on the development of a Cyber Security Improvement Plan as required by the NIS Regulations. 1.2 A realistic timetable should be drawn up for the development and implementation of a Cyber Security Improvement Plan.		**High**
Management Response	Target Date	Responsible Officer
Accepted. The Cyber Security Improvement Plan remains a priority on our workplan.	May 2023	Head of Information Governance & Cyber Security
Current findings		**Residual Risk**
1.1 A Cyber Security Improvement Plan was developed in November 2023, which details recommendations for improvement, their risk priority and current status. We note that 9% of actions are complete, 22% are ongoing and 69% not started and appropriate updates have been recorded against those that have been progressed. Recommendations' start and end dates, and accountable officers have not been recorded within the plan. Whilst we note the above, we acknowledge that there has been continued delay in the recruitment of a Cyber Security Manager, to whom this program of work was to be assigned. **Conclusion:** Action ongoing.		• Failure to comply with regulations e.g., NIS Regulations. • Loss of data or services and inappropriate access to information.
New Recommendations		**Priority**
1.1 A realistic timetable should be developed, and accountable officer(s) assigned to progress the Cyber Security Improvement Plan.		**Low**
Management Response	**Target Date**	**Responsible Officer**

1.1	We do recognise progress has been slower than we would like. It is widely reported over many years empirically that recruiting to cyber roles is highly competitive with the public sector often struggling for capable resources as pay points are lower, hence we have spent 12 months running numerous unsuccessful recruitment campaigns including the use of agency to no avail. Our most recent campaign however was successful after we increased the pay scale for an appointee to Band 8a (from Band 7). The Cyber Security Lead is due to commence in post on the 14th May 2024. The improvement plan was largely written in the context of the critical system assessed in 2022 (PMS). PMS is currently migrating to a new environment and once migrated, currently scheduled for April 2024, a number of recommendations will be addressed. This, in addition to the Cyber Security Lead position being filled, will allow us to make some good headway into this action plan.	Q1 2024/2025	Head of Information Governance & Cyber Security

Previous Matter Arising 4: Performance Measures / KPI's (Design)		
Original Recommendation		Original Priority
4.1 Cyber security performance measures and key performance indicators should be developed and reported to the Digital Health and Intelligence Committee on a regular basis.		**Medium**
Management Response	Target Date	Responsible Officer
Accepted. The next committee paper will ensure cyber security KPIs are included.	June 2023	Head of Information Governance & Cyber Security
Current findings		**Residual Risk**

We reviewed Cyber reports to the Digital Health and Intelligence Committee dated August 2023, October 2023, and February 2024. We positively noted that key performance indicators encompassing the number of legacy operating systems and mandatory training compliance are regularly reported. In February 2024, the committee was presented with figures pertaining to quarantined and blocked inbound emails due to identified viruses and contained high antivirus/malware threats. We identified that server patching compliance is not regularly reported, which is a key cyber metric. Whilst cyber security figures are reported, they do not indicate compliance and performance unless captured and reported upon regularly, in order to develop into measurable metrics. **Conclusion:** Action ongoing.		• Failure to comply with regulations e.g., NIS Regulations. • Inaccurate or incomplete reporting of the current cyber security position to the Health Board.
New Recommendations		**Priority**
4.1	Key cyber security figures relating to server patching and perimeter controls should be consistently recorded, upon which performance measures and indicators can be developed and regularly reported to the Digital Health and Intelligence Committee.	**Medium**

Management Response		**Target Date**	**Responsible Officer**
4.1	There have been numerous attempts made to reflect key performance indicators into the Cyber Security Digital Health and Intelligence Committee report. Standard performance indicators are difficult to measure and whilst we have consistently reported legacy Operating System figures, this doesn't truly represent our cyber security position. This will improve as we complete Performance Measures and Metrics. The February 2024 committee paper did report on a number of cyber metrics but this was more for awareness than a representation of performance. We can ensure we continue to report on legacy server OS and include metrics/indicators for other measures for future committees.	May 2024	Head of Information Governance & Cyber Security

Appendix B: Assurance opinion and action plan risk rating

Audit Assurance Ratings

We define the following levels of assurance that governance, risk management and internal control within the area under review are suitable designed and applied effectively:

	**Substantial assurance**	Few matters require attention and are compliance or advisory in nature. **Low impact** on residual risk exposure. **Follow up:** All recommendations implemented and operating as expected
	**Reasonable assurance**	Some matters require management attention in control design or compliance. **Low to moderate impact** on residual risk exposure until resolved. **Follow up:** All high priority recommendations implemented and progress on the medium and low priority recommendations.
	**Limited assurance**	More significant matters require management attention. **Moderate impact** on residual risk exposure until resolved. **Follow up:** No high priority recommendations implemented but progress on most of the medium and low priority recommendations.
	**Unsatisfactory assurance**	Action is required to address the whole control framework in this area. **High impact** on residual risk exposure until resolved. **Follow up:** No action taken to implement recommendations

Prioritisation of Recommendations

We categorise our recommendations according to their level of priority as follows:

Priority level	Explanation	Management action
High	Poor system design OR widespread non-compliance. Significant risk to achievement of a system objective OR evidence present of material loss, error or misstatement.	Immediate*
Medium	Minor weakness in system design OR limited non-compliance. Some risk to achievement of a system objective.	Within one month*
Low	Potential to enhance system design to improve efficiency or effectiveness of controls. Generally issues of good practice for management consideration.	Within three months*

* Unless a more appropriate timescale is identified/agreed at the assignment.

NHS Wales Shared Services Partnership
4-5 Charnwood Court
Heol Billingsley
Parc Nantgarw
Cardiff
CF15 7QZ

Website: Audit & Assurance Services - NHS Wales Shared Services Partnership