Cyber Security

Draft Internal Audit Report

2025/26

Cardiff and Vale University Health Board

Limited Assurance

Contents

Review Reference	CVU-2425-04
Fieldwork	May - July 2025
Executive Sign Off	August 2025
Audit Committee	September 2025
Executive Lead	David Thomas, Director of Digital & Health Intelligence
Audit Team	Ian Virgill, Head of Internal Audit
	Martyn Lewis, IT Audit Manager

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

Executive Summary

Purpose

Review how the Health Board is working to improve its cyber security position and the processes in place for monitoring compliance and providing assurance that the risks are appropriately stated in line with the risk appetite.

Overview

We have concluded limited assurance on this area. While cyber risks are formally recognised at the corporate level, key weaknesses in governance, communication, and risk management limit the organisation's ability to manage cyber security effectively. Despite having devolved IT responsibilities across the organisation, there are limited formal communication channels between the cyber team and the asset owners of an estimated 300 critical systems.

Progress in areas such as Security Incident and Event Monitoring (SIEM) implementation, vulnerability scanning and a new secure web gateway is helping to improve cyber security visibility across the organisation. This is particularly important given the scale of the organisation, which employs around 17,000 people and spends approximately £1.4 billion each year. However, the Cyber Security Team currently faces capacity challenges, with two vacancies limiting their ability to complete wider objectives. As a result, their focus remains on business-as-usual operations and maintaining the continuity of critical services.

The significant matters requiring management attention include:

- The cyber security risk register lacks important information and is not regularly updated with actions being taken.
- There is inconsistent cyber security risk awareness across the organisation.
- Although there is devolved responsibility for IM&T within Clinical Boards, there is limited feed in from Clinical Boards into the digital and cyber governance structures. We also note a lack of complete Information Asset Register resulting in a single point of failure in the cyber team.
- The Cyber Improvement does not cover the cyber needs of the whole organisation.

The following opportunities for enhancement have been identified that do not impact the overall opinion and are highlighted for management information:

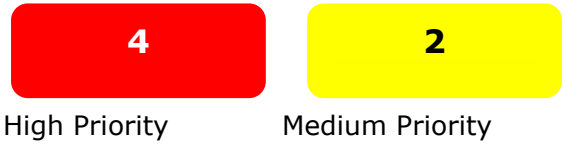
- The Terms of Reference (ToR) for both the Cyber Security Sub-group and the Technical and Cyber Group should be reviewed and refreshed as they both currently say they report into the Cyber Security Sub-group.
- Whilst there is a key finding regarding the cyber risk register included, closed risks with a high residual risk score should be reviewed and reopened on the risk register if appropriate.

Full details of matters arising are detailed within the Findings & Agreed Action Plan.

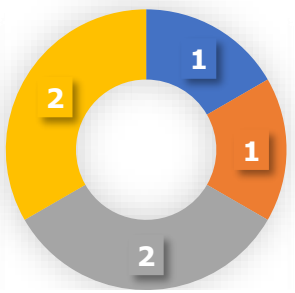
Scope & Assurance Summary

Objectives (The objectives and associated assurance ratings are not necessarily given equal weighting when formulating the overall audit opinion.)		Related Findings	Assurance
1	The risks associated with cyber security are appropriately stated, recorded, understood and managed within the organisations risk appetite.	1, 2, 3	**Limited**
2	An appropriate governance process for cyber security across the organisation is in place which enables monitoring, reporting and effective management.	4, 5	**Limited**
3	Identified actions to improve cyber security are progressed appropriately.	6	**Reasonable**

Management Actions



Themes



Risk Types

Quality or Safety Issues

Legal & Regulatory Non-Compliance

Cyber security questionnaire summary of responses

As part of our fieldwork, we distributed a questionnaire to Board members, Clinical Board Management Teams and a sample of directors. It was sent to 43 staff members in total, and we received a total of 16 responses.

The aim of the questionnaire was to assess the organisation's awareness, understanding, and appetite for cyber security risks.

Below is a summary of the responses to the questions for which we can provide a qualitative analysis.

What is the best description of your current role?	Number of responses
Board Member	3
Clinical Board Director	3
Executive	5
Independent Member	1
Operational Manager	4
Total	**16**

Cyber security updates

Do you regularly receive updates on cyber security risks and incidents during board meetings?
Do you regularly receive updates on cyber security risks and incidents during any other committee meetings?
Do you receive cyber security updates at any other meetings?

- **3/3** Board Members answered 'Yes' to at least one of the questions above.
- **5/5** Executives answered 'Yes' to at least one of the questions above.
- **1/1** Independent Members answered 'Yes' to at least one of the questions above.
- **0/3** Clinical Board Directors answered 'Yes' to at least one of the questions above.
- **1/4** Operational Managers answered 'Yes' to at least one of the questions above.

Cybersecurity risks and actions to mitigate the risks

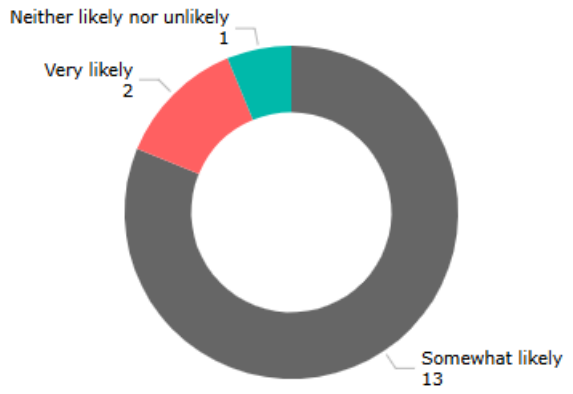
Have you seen cyber security risks on a risk register?
Are you aware of any actions being taken to reduce the current cyber security risk to its target level, or a cyber improvement plan?

- **3/3** Board Members answered 'Yes' to at least one of the questions above.
- **5/5** Executives answered 'Yes' to at least one of the questions above.
- **1/1** Independent Members answered 'Yes' to at least one of the questions above.
- **0/3** Clinical Board Directors answered 'Yes' to at least one of the questions above.
- **1/4** Operational Managers answered 'Yes' to at least one of the questions above.

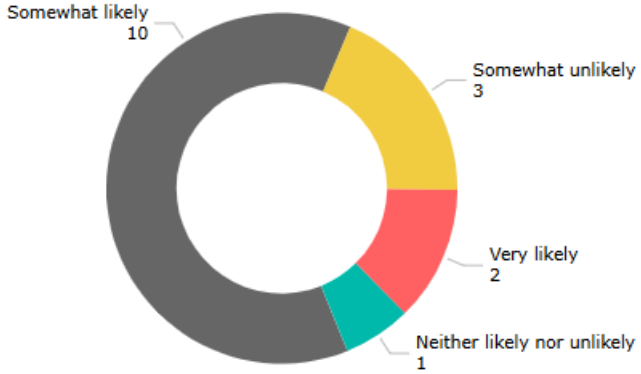
What do you think are the most significant cyber weaknesses for the organisation?

75% of responses to this question highlighted people/ individuals or emails/phishing as the most significant cyber weakness for the organisation.

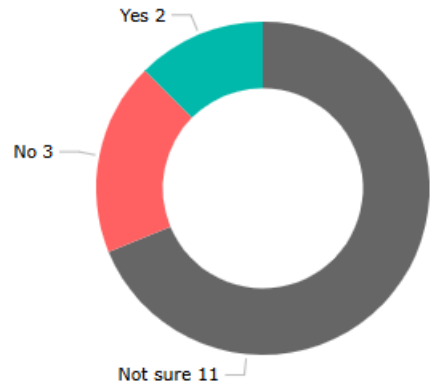
How likely do you think it is that the organisation will suffer a moderate cyber security incident?



How likely do you think it is that the organisation will suffer a serious cyber security incident?



Do you think the current level of cyber risk is acceptable for the organisation?



Findings & Agreed Action Plan

Objective 1: The risks associated with cyber security are appropriately stated, recorded, understood and managed within the organisations risk appetite.	**Limited**

Overview / Summary of Observations

The Cyber Security Team oversees cyber security across the organisation, and is responsible for identifying, assessing, and monitoring cyber security risks. The team maintains a cyber security risk register, which at the time of the audit, contained 85 open risks. The register was maintained in an Excel spreadsheet, with plans to migrate it to AMaT at the early stages of implementation.

We note weaknesses with the cyber risk register, with key information missing such as risk owners, target dates and actions undertaken or planned. During our audit, 58% of the 85 open risks on the register had a risk evaluation of 'Tolerate'. However, there was no narrative recorded for why this decision was made and we were informed that these decisions would be made within the Cyber Security Team and would not be escalated or reported to the Digital and Infrastructure Committee (DIC) for consideration.

Our testing confirmed that the closure of risks were appropriate following completed actions, however we noted one risk with a "High" residual risk was closed and not currently reported or noted as 'Tolerate'.

Cyber security risks are appropriately recognised at the corporate level, with a consolidated risk recorded on both the Corporate Risk Register (CRR) and the Corporate Digital Risk Register (CDRR) which is regularly reported to the Digital and Infrastructure Committee (DIC). However, the minutes for DIC do not show active scrutiny or challenge of the risk register, and there are no meeting notes for the Cyber Security Sub-Group which would demonstrate active review. In addition, although a risk appetite framework exists, its practical application is inconsistent and there is no risk appetite score recorded on any of the risk registers referenced.

As part of our audit, we shared a questionnaire with Board members, Clinical Board Management Teams and a sample of directors (43 staff in total were sent the questionnaire, with 16 responses). Whilst Board members and executive leadership reported receiving regular updates on cyber security, Clinical Board Management Teams reported a lack of visibility of cyber risks, incidents, and mitigation plans in their responses. This gap in awareness presents a risk, given the devolved nature of IT responsibility in the organisation, and it may hinder local risk identification and response in the Clinical Boards. Additionally, we observed limited communication and reporting between the Cyber Security Team and Clinical Boards, as well as minimal Clinical Board representation at the Digital and Infrastructure Committee (as highlighted in Key Finding 4) which further highlighted the disconnect in cyber risk awareness between the central Cyber Security Team and Clinical Boards.

As such, we note a structural weakness in terms of the management of cyber risk management. The Cyber Security Team maintains the central cyber risk register, however this only includes risks of which they are aware. Due to the decentralised management of IT systems- approximately 300 critical systems across the organisation -the Cyber Security Team do not have the resource to be able provide full oversight and management of the cyber risks associated with all these systems. Responses to the questionnaire and follow-up discussions identified that Clinical Boards do not currently record cyber security risks on their local risk registers, despite being responsible for managing their own IT systems. As such cyber risks within Clinical Boards may not be appropriately identified, monitored or reported.

Key Findings		Risk & Impact	Agreed Management Action
1	**Cyber security risk register** The Cyber Security Risk Register (or Information Systems Security Risk Register as the document is titled) lacks important information such as: • Dates of when the risk was added to the register or target dates for completion • Named responsible individuals • Actions taken or planned to treat the risk • It is not clear when updates on progress to treat risks were added, and some risks don't have this information at all. • There is no narrative for why a risk will be tolerated and the decision process behind this is not recorded or escalated. • Some risk descriptions do not describe what could happen, why it would happen or what the impact could be. Whilst it is recognised that the plan to migrate the risk register to AMaT has now begun, this will not resolve the issues of missing or incomplete information and work will be required to address the gaps highlighted during the migration.	Risks are not being managed appropriately **High Priority**	**Agreed Action:** All high risks have now been migrated onto AMaT which is a specific risk management platform. There are mandatory fields that require information therefore all entries will be fully completed. Medium and low risks and any new risks, will be recorded on AMaT, which will then form the basis of our cyber improvement plan, which will concentrate on those highest risks. **Expected Evidence of Implementation:** Risk register outputs from AMaT. **Officer:** Head of Information Governance & Cyber Security **Target Implementation Date:** 31st October 2025
	Theme: Risk Management	Control Operation	
2	**Inconsistent cyber security risk awareness across the organisation** Responses to our questionnaire showed that there is a disparity in cyber security awareness and oversight between the Board and Clinical Board Management Teams. Whilst Board members and Executive leadership receive regular updates on cyber security risks and incidents, are aware of mitigation actions and have seen the cyber risk on the Corporate Risk Register - Clinical Board Management Teams do not appear to receive the same level of information. This inconsistency suggests a communication gap that may hinder the Clinical Boards' ability to effectively understand and respond to cyber security threats, and with devolved	Limited visibility at the operational level, despite devolved IT responsibilities, increases the risk of unmanaged threats, inconsistent responses, and reduced organisational resilience.	**Agreed Action:** Engagement with the Clinical Boards management will be implemented via the Strategic Leadership Team (SLT) initially, to raise awareness and provide information on what each CB management team should be sharing in identifying and logging any cyber related risks. This is especially important where shadow IT arrangements exist. We will ensure that Cyber have visibility of CB risks, and vice versa for any other relevant risks.

	responsibility for IT in the organisation this poses a risk. It is recognised that the Cyber Security Team have a dedicated SharePoint page that provides advice and updates, however more targeted updates may be required to the Clinical Boards and wider services.		**Expected Evidence of Implementation:** Presentation to SLT jointly with DD&HI and COO to raise awareness and inform of cyber risk management process.
		High Priority	**Officer:** Director of Digital & Health Intelligence/SIRO **Target Implementation Date:** 31st October 2025
	Theme: Communication & Engagement	Control Operation	
3	**Cyber security risk management across the Clinical Boards** Responses to our questionnaire and follow-up communications highlighted a gap in cyber risk management within the Clinical Boards. Although these teams are responsible for their own IT systems, they are not consistently identifying, assessing or managing their own cyber security risks. While there is a centralised cyber security structure within the organisation that is headed up by the Cyber Security Team; there is devolved IT responsibility. So, while the Cyber Security Team manages the cyber security risk register, this will only include risks that they are directly aware of. However, Clinical Boards do not currently record cyber security risks on their local risk registers, despite being responsible for managing their own IT systems. As such cyber risks within Clinical Boards may not be appropriately identified, monitored or reported.	There is the risk that cyber security risks in the Clinical Boards are not being identified, assessed or monitored due to lack of oversight and awareness and communication.	**Agreed Action:** Engagement with Clinical Boards management teams, initially via the SLT to raise awareness and agree a process for identifying and capturing local cyber or IT security risks in a consistent manner and that that CB service leads fully understand and own these risks. These cyber risks will be monitored centrally via AMaT to ensure that they are managed appropriately and owned by the CBs and the SIRO can take assurance that such risks are fully identified and assessed. Cyber risk ownership policy will need to support CBs help understand roles and responsibilities.
			Expected Evidence of Implementation: Clinical Boards' risk registers contain relevant cyber risks and these are shared with the central Cyber team. Guidance and support to be provided Cyber Security Department.
		High Priority	**Officer:** Director of Digital & Health Intelligence/SIRO (with support from Cyber Department) **Target Implementation Date:** 30th November 2025
	Theme: Risk Management	Control Operation	

Objective 2: An appropriate governance process for cyber security across the organisation is in place which enables monitoring, reporting and effective management.	**Limited**

Overview / Summary of Observations

There is a clear governance framework in place, with reporting from the Cyber Security Team to the Digital and Infrastructure Committee and onto the Board. Cyber security governance is centralised under a small, formally structured cyber team of 5 staff (including the Head of Information Governance and Cyber Security), which currently operates with limited capacity due to two vacancies. As a result, the team focuses primarily on business-as-usual and critical service continuity tasks. The team cover cyber security for the whole organisation, which employs around 17,000 people and spends approximately £1.4 billion each year. The Information Governance and Cyber Team's total spend in 2024/25 was 4% of the digital spend for the organisation, and 0.04% of the total organisation spend of £1.4 billion, by month three of 2025/26 the Information Governance and Cyber Team's total spend had decreased to 3% of the digital spend in the same period. Whilst the team cover cyber security for the whole organisation, there is devolved responsibility for IT systems throughout the organisation and with the Senior Information Risk Owner (SIRO) not having managerial responsibility within Clinical Boards, we were informed that the Clinical Boards did not always action requests made by the Cyber Security Team in a timely manner.

We note that there are limited formal communication channels between the cyber team and the asset owners of the approximately 300 critical systems, as such the cyber team cannot be assured that they have oversight of the governance of locally controlled digital systems within the Health Board. This lack of structured engagement is likely to be a contributing factor to low cyber awareness and limited visibility of cyber risks among Clinical Boards and services, which was highlighted in the responses to the questionnaire we shared.

We further note the absence of a complete Information Asset Register (or critical system asset register). This means there is no full visibility of all systems in place, their individual owners and any weaknesses of the systems across the organisation. Consequently, the Cyber Security Team are unable to identify all critical system owners in the organisation and system ownership knowledge is reliant on a single individual, due to their experience and contacts within the organisation, this creates a single point of failure.

Progress in areas such as Security Incident and Event Monitoring (SIEM) implementation, vulnerability scanning and a new secure web gateway is improving cyber security visibility across the organisation, and there is a cyber security intranet page containing guidance, supporting documents, training resources and contact information for the Cyber Security Team. It is also evident from our fieldwork that phishing simulation campaigns are being performed regularly, and cyber training is mandated throughout the organisation (as part of the Information Governance module) - although the completion rate in May 2025 for this training was well below the 85% target, at 70%, being as low as 59% in one Clinical Board and as high as 85% in another.

Cyber security is a standing item at the private session of the DIC, where updates are provided on key areas such as the cyber risk register, cyber improvement plan, cyber security KPIs (that include: updates on legacy systems, end point devices, phishing campaigns and training figures), reported cyber incidents and updates on any completed audits. The chair of the committee also provides regular updates to the Board.

We note however that there is limited representation from Clinical Boards at the DIC. This lack of engagement hinders the flow of information and may reduce the effectiveness of cyber risk oversight across the organisation.

Supporting groups such as the Cyber Security Sub-Group and the Technical and Cyber Group exist, with the sub-group providing assurance to the DIC. The Cyber Security Sub-Group meets monthly and plays a key role in reviewing the cyber risk register and conducting risk assessments for critical systems. However, no formal minutes are taken at these meetings, which limits transparency and weakens governance. This issue was previously raised in a 2022/23 internal audit and remains unresolved.

Key Findings		Risk & Impact	Agreed Management Action
4	**Cyber security governance gaps and communication challenges** • There are inadequate communication channels between the Cyber Security Team and asset owners within the Clinical Boards. • Representatives from the Clinical Boards do not consistently attend the Digital and Infrastructure Committee meetings, nor do they contribute to the cyber security updates presented to the committee. • The organisation's Information Asset Register (IAR) is incomplete. As a result, the Cyber Security Team lacks full visibility of systems, risks and their respective asset owners. • There is a single point of failure due to there being no communication channels or an IAR, as knowledge of asset ownership is heavily reliant on the personal experience of the Head of Information Governance and Cyber Security.	Incomplete oversight, as the cyber team cannot verify the cyber security risks of all systems. Single point of failure with only one member of staff knowing how to contact system owners if a cyber event occurs.	**Agreed Action:** Presentation to SLT which includes the management teams from each Clinical Board to make them aware of requirements of asset owners in relation to managing cyber risks specifically. Information Asset Registers to be completed and shared centrally. A process to be agreed for ensuring appropriate communication channels with CBs. Process to be developed and shared to ensure that CBs become conversant with procedures should a cyber event occur. SLT to agree to a specific forum where Cyber and the CBs can raise and discuss cyber risks, and critical systems along with their key contacts can be determined and logged. **Expected Evidence of Implementation:** Clinical Boards' cyber risks identified and shared centrally. Regular communication channels established.
	Theme: Governance	**High Priority** Control Design	**Officer:** Director of Digital & HI (SIRO)/Head of Information Governance & Cyber Security **Target Implementation Date:** April 2026
5	**Lack of minutes for the Cyber Security Sub-group** While risk assessments completed by the Cyber Security Sub-Group record decisions and advice provided, there are no formal minutes or records of the group's meetings. Given the group's role in reviewing the cyber risk register, assessing critical systems and subsequently providing assurance and advice to the SIRO and CCIO to make decisions, as well providing assurance to the Digital and Infrastructure Committee (as outlined in the ToR for the group), the absence of minutes for the meeting limits transparency and weakens governance. Introducing formal minutes or meeting notes would strengthen oversight and ensure a complete audit trail of discussions and decisions.	Without documented evidence of discussions, decisions, and advice provided, there is limited transparency and accountability in the group's oversight of cyber risk management.	**Agreed Action:** Although an Action Log is maintained we will ensure that future meetings are recorded and transcriptions made available so that an accurate record of the meeting is recorded. **Expected Evidence of Implementation:** Meeting minutes.

	(This was a recommendation in the 2022/23 Cyber Security internal audit).	**Medium Priority**	**Officer:** Head of Information Governance & Cyber Security. **Target Implementation Date:** August 2025
	Theme: Governance	Control Operation	

Objective 3: Identified actions to improve cyber security are progressed appropriately.	**Reasonable**

Overview / Summary of Observations

There is a Cyber Improvement Plan in place, and this is being managed by the Cyber Security Team with progress reported to the Digital and Infrastructure Committee. The plan is comprised of the high-priority risks (scoring 12+ and with a risk evaluation of 'Treat') on the cyber risk register, these will include recommendations/findings from the Cyber Resilience Unit (CRU) audits and the original CAF assessment of the Patient Management System (PMS). However, the plan's scope is limited due to the absence of CAF assessments from across other services/critical systems throughout the organisation. Despite reported efforts by the cyber lead to initiate broader assessments within the wider services, it was reported that there was resistance to these requests.

Risk identification and assessments for new systems is ad hoc, relying on requests via a shared inbox. A draft NIS assessment was created by the Cyber Security Team for all new critical systems; however, this remains unimplemented. Engagement with Clinical Boards and critical system owners is limited as previously highlighted and these gaps suggest the plan does not fully reflect the organisation's cyber needs, which is inconsistent with NIS Regulations 2018 and CRU guidance.

It is recognised that the plan includes key risks and actions, and most of these objectives are being progressed with updates reported via the cyber security KPI metrics to each Digital and Infrastructure Committee. However, several limitations were identified; these include unclear timescales or actions past their target date, undefined resource requirements, and inconsistent progress reporting to the Digital and Infrastructure Committee or some objectives. For the objectives that are not included within the KPI metrics, progress was confirmed with the cyber lead, however, resource limitations were outlined as an issue for achieving more. We tested one of the three closed objectives on the plan and confirmed and evidenced that the required actions had been completed.

With the cyber risk register now being migrated to AMaT, and with the Cyber Improvement Plan being derived from the high scoring risks on the register, it is hoped that this will ensure regular updates are provided as well as the population of target dates to ensure there can be enhanced scrutiny and accountability of progress.

Key Findings		Risk & Impact	Agreed Management Action
6	**Coverage of the Cyber Improvement Plan** The cyber security improvement plan is based on high-scoring risks (12+) from the cyber risk register and is overseen by the cyber team. While the plan is intended to be implemented organisation-wide, no CAF assessments have been conducted on critical systems—other than the PMS—and there is limited communication, representation, and cyber awareness among critical system owners, services, and Clinical Boards. Additionally, there are known issues with the risk register and the overall approach to cyber risk management, which underpins the plan (see objective 1 and key finding 1). These factors suggest that the plan may be missing key objectives relevant to services and Clinical Boards and therefore may not fully address the organisation's cyber security needs.	The Cyber Improvement Plan does not fully address the organisation's cyber security needs.	**Agreed Action:** Although the basis of the improvement plan should still focus on those highest risks we face, this will be based on the information contained with AMaT and using this platform. Relying upon AMaT will also help factor in those risks that are identified at Clinical Board level. Engagement with all Clinical Boards will be necessary to ensure all cyber risks are captured and that CBs themselves are aware of their obligations (some education and informing will be needed); CBs will be accountable for logging and managing their risks with support from the central Cyber team.
			Expected Evidence of Implementation: AMaT improvement plan extract.
		Medium Priority	**Officer:** Head of Information Governance & Cyber Security **Target Implementation Date:** December 2025
	Theme: Cyber Security	Control Operation	

Appendix A

Assurance Opinion

	**Substantial**	Few matters require attention and are compliance or advisory in nature. **Low impact** on residual risk exposure.
	**Reasonable**	Some matters require management attention in control design or compliance. **Low to moderate impact** on residual risk exposure until resolved.
	**Limited**	More significant matters require management attention. **Moderate impact** on residual risk exposure until resolved.
	**Unsatisfactory**	Action is required to address the whole control framework in this area. **High impact** on residual risk exposure until resolved.
	**Advisory**	Given to reviews and support provided to management which form part of the internal audit plan, to which the assurance definitions are not appropriate. These reviews are still relevant to the evidence base upon which the overall opinion is formed.

Prioritisation of Findings

Priority	Explanation
High	Significant risk to achievement of a system objective OR evidence present of material loss, error, or misstatement. Poor system design OR widespread non-compliance.
Medium	Some risk to achievement of a system objective. Minor weakness in system design OR limited non-compliance.

Disclaimer

This audit report has been prepared for internal use only. Audit and Assurance Services reports are prepared, in accordance with the agreed audit brief, and the Audit Charter as approved by the Audit Committee.

Audit reports are prepared by the staff of the NHS Wales Audit and Assurance Services and addressed to Independent Members or officers including those designated as Accountable Officer. They are prepared for the sole use of the Cardiff and Vale University Health Board, and no responsibility is taken by the Audit and Assurance Services Internal Auditors to any director or officer in their individual capacity, or to any third party.

The report is based on the review work undertaken and is not necessarily a complete statement of all weaknesses that exist or potential improvements. Whilst every care has been taken to ensure that the information provided in this report is as accurate as possible, no complete guarantee or warranty can be given with regard to the advice and information contained.

Our work does not provide absolute assurance that material errors, loss or fraud do not exist. Responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management of the Cardiff and Vale University Health Board. Work performed by internal audit should not be relied upon to identify all strengths and weaknesses in internal controls, or all circumstances of fraud or irregularity. Effective and timely implementation of recommendations is important for the development and maintenance of a reliable internal control system.

Public Sector Internal Audit Standards

Audit work undertaken by NHS Wales Audit and Assurance Services conforms with the International Standards for the Professional Practice of Internal Auditing and associated Public Sector Internal Audit Standards as validated through the external quality assessment undertaken by the Chartered Institute of Public Finance & Accountancy in April 2023.

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

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