Local / Shadow IT

Final Internal Audit Report

2025/26

Cardiff & Vale University Health Board

Reasonable Assurance

Contents

Review Reference	CVU-2526-06
Fieldwork	March 2026 - April 2026
Executive Sign Off	David Thomas
Audit Committee	Sept 2026
Executive Lead	David Thomas, Director of Digital & Health Intelligence
Audit Team	Ian Virgil, 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

To review the processes and guidance in place within the Health Board's Digital team for ensuring appropriate professional oversight of locally managed IT systems to ensure they comply with best practice.

Overview

We have concluded **reasonable** assurance on this area. There is guidance in place, provided by Digital & Health Intelligence (D&HI or 'Digital') over how digital items and Information Governance should be managed, although we note that much is out of date. There is a Committee with formal responsibility for Digital which demonstrates oversight, particularly over D&HI controlled aspects. There are good relations between Procurement and D&HI which facilitates the identification of new items and there are very good technical controls in place to protect the Health Board. We note that there is no full record of digital items across the Health Board and as such no full evaluation of the risk that this presents.

The matters requiring management attention include:

- Although there is a range of guidance in place for the management of digital items, information governance and security, much of this is out of date and requires reviewing and updating. We also note that there is currently a lack of a succinct summary of requirements for managing digital systems and contracts available to relevant staff.
- As noted in our previous report on Cyber Security there is a feed into the wider organisation from the Digital and Infrastructure Committee (DIC), however there is no representation from Clinical Boards and the Chief Operating Officer does not attend, as such there is limited visibility and accountability over how devolved digital items are managed and overseen.
- We noted a number of suppliers without a cyber essentials certification, including the supplier of the Dental system which has been recently upgraded. The specification for this did not include a Cyber Essentials (CE+) requirement and our discussion with Procurement noted that the inclusion of this is reliant on Digital input and not a standard requirement within specifications for applications.
- There is no complete, accurate record of what digital systems and suppliers are in use across the whole organisation and no assessment of criticality, no completion of CAF assessments outside of D&HI and no assessment of the risk that suppliers present.
- There is a wide range of software in use, with some breaching Health Board Policy and Welsh Government requirements. Despite management of these being devolved, these risks are not being recorded within departmental risk registers and so the true risk to the Health Board is unquantified.

Full details of matters arising are detailed within the Findings & Agreed Action Plan. The following opportunities for enhancement have been identified that do not impact the overall opinion and are highlighted for management information:

- D&HI should consider using the reporting functionality from the firewalls to identify medical devices that present a risk to the Health Board.
- D&HI should consider using the SCCM reporting function to populate their records and focus on high risk areas.

Scope & Assurance Summary

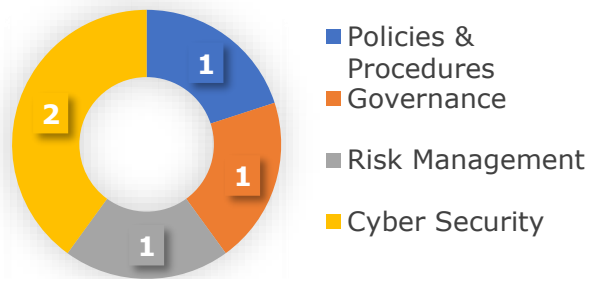
	Objectives (The objectives and associated assurance ratings are not necessarily given equal weighting when formulating the overall audit opinion.)	Related Findings	Assurance
1	IT systems and digital tools procured or managed outside the central IT function are required to comply with relevant digital policies, procedures and guidance and are included within the overall digital governance and oversight arrangements.	1, 2	**Reasonable**
2	Procurement and contract management processes prevent unauthorised or duplicate IT systems from being acquired and supported outside of digital services oversight.	3	**Reasonable**
3	Controls are in place to prevent users from downloading and installing software without explicit approval.	-	**Substantial**
4	Processes are in place to identify shadow IT and ensure risks are managed appropriately (cyber-security, compliance).	4, 5	**Limited**

Management Actions

3 High Priority

2 Medium Priority

Themes



Risk Types

Quality or Safety Issues

Legal & Regulatory Non-Compliance

Choose an item.

Choose an item.

Findings & Agreed Action Plan

Objective 1: IT systems and digital tools procured or managed outside the central IT function are required to comply with relevant digital policies, procedures and guidance and are included within the overall digital governance and oversight arrangements.	Reasonable

Overview / Summary of Observations

The Health Board website contains a policies section which includes a page specifically for digital related guidance. This holds a range of guidance, some very specific and some more general. Our review of these noted that guidance is in place for Records Management, Information Governance, IT Security, Data Quality, IT Access Control, and Software Licencing.

The guidance in place applies to the whole organisation and contains clear expectations over managing key aspects of digital, together with a stated requirement for D&HI to review all new applications prior to purchase. As such there is an intent of professional oversight and leadership, however a number of the guidance documents are out of date and have not been updated to reflect recent changes in requirements.

There is a committee with a remit that covers Digital, the Digital and Infrastructure Committee (DIC). The terms of reference state it is to provide assurance that "appropriate processes and systems are in place for data, information management and governance to allow the UHB to meet its stated objectives, legislative responsibilities and any relevant requirements and standards".

Our review of DIC business confirmed that it covers core digital aspects including monitoring progress against projects, Information Governance, Cyber Security and digital risks. Attendance at the DIC includes the Chief Executive and Director of Finance and so there is a feed into the wider organisation, however there is no representation from Clinical Boards and the Chief Operating Officer does not attend, as such there is limited visibility and accountability over how devolved digital items are managed and overseen.

We reviewed a sample of locally managed digital systems and our discussions with staff responsible for managing these noted that they had not been provided with clear guidance over requirements which they felt would be useful, although D&HI were uniformly felt to be very helpful when approached. As such, our review noted that although digital systems are, in general, being managed appropriately with appropriate access controls there were weaknesses in the approaches taken to data quality management, logging and general system administration tasks. There were also weaknesses in the management of digital contracts, with this being supplier led in many cases and without provision of performance reports.

We also noted that staff were unaware of the Network and Information Systems (NIS) regulations and the associated cyber assessment framework (CAF) process, despite the systems being, in many cases business critical, and although most systems had been subject to a data protection impact assessment (DPIA), not all had been, in particular the older ones and we also identified suppliers without the WG mandated Cyber Essentials Certification.

Our previous report on Cyber Security, completed in September 2025, noted the governance gap regarding Clinical Board digital operations and we note from our discussions that meetings have been held between Clinical Board directors and D&HI. However, until there is a clear digital oversight and governance mechanism for the whole organisation there will be a risk that digital items do not fully comply with required standards.

Key Findings		Risk & Impact	Agreed Management Action
1	**Guidance** Although there is a range of guidance in place for the management of digital items, information governance and security, much of this is out of date and requires reviewing and updating. We also note that there is currently a lack of a succinct summary of requirements for managing digital systems and contracts available to relevant staff and system owners.	Digital items may not be managed appropriately or protect the UHB appropriately.	**Agreed Action:** D&HI team to review and update guidance to include a quick checklist for system owners / managers and make that available on the internal SharePoint site for all staff to access.
			Expected Evidence of Implementation: Checklist document on CAV UHB SharePoint site. Guidance documentation updated and published.
		High Priority	**Officer:** Head Of Digital Operations/Head of Information Governance and Cyber Security
	Theme: Policies & Procedures	Control Operation	**Target Implementation Date:** Sept 26
2	**Governance** As noted in our previous report on Cyber Security there is a feed into the wider organisation from DIC, however there is no representation from Clinical Boards and the Chief Operating Officer does not attend, as such there is limited visibility and accountability over how devolved digital items are managed and overseen.	There is a risk that digital items do not fully comply with required standards.	**Agreed Action:** D&HI - Continue to work to feed in. Extend invitation for COO or nominated CB lead to sit on the Digital & Infrastructure committee of the board. Establish a Teams channel for owners. Formally communicate that the D&HI team are the professional leads and that guidance must be followed. Seek endorsement from SLT to require the identification of all DDAT systems / owners to join Teams channel.
			Expected Evidence of Implementation: Documented actions from SLT; communication; set up of Teams channel with appropriate membership.
		Medium Priority	**Officer:** Director D&HI
	Theme: Governance	Control Design	**Target Implementation Date:** Nov 26

Objective 2: Procurement and contract management processes prevent unauthorised or duplicate IT systems from being acquired and supported outside of digital services oversight.	Reasonable

Overview / Summary of Observations

There is a stated requirement within the Software Licencing Policy, although we note this is out of date, that managers must not directly procure applications without contacting D&HI and gaining approval that the application is acceptable, secure and complies with IG requirements.

Discussion with Procurement indicated that although there is no formal procedure within Procurement, all requests for digital orders, including software are identified and shared with the IT Procurement Officer within the Health Board.

Our discussions with the Head of Information Governance and Cyber Security noted a high degree of confidence that new items that are requested are being appropriately identified and assessed, with Procurement sending staff to D&HI if digital items are requested without a clear approval. However, some items do continue to slip through particularly for older contracts being renewed.

Our testing of a sample of recently purchased digital items confirmed this process, with most having a DPIA and approval, with those without being older items being renewed.

There is a Welsh Government requirement (set out in WHC (2017) 025 Cyber Security & Information Governance) for suppliers of digital systems to be Cyber Essentials (CE+) certified, however we noted a number of suppliers without a cyber essentials certification, including the supplier of the Dental system which has been recently upgraded. The specification for this did not include a CE+ requirement and our discussion with Procurement noted that the inclusion of this is reliant on D&HI input and not a standard requirement within specifications for applications. Given the level of devolved control there is a risk that requirements are defined without full digital input apart from the technical requirements and so this mandated requirement may be omitted.

The historical approach of devolved decision making over digital applications has contributed to the Health Board having a large number of applications in place with duplication and overlap of functionality leading to potentially inefficient management and avoidable expenditure.

The assessment and approval process by D&HI ensures that any application is secure, however it does not consider whether the needs can be met by an application already in place, or the strategic fit of the proposed solution. As noted below (Key Finding 4) there is no complete, accurate record of applications in use and their purpose, as such this assessment cannot be completed. In the event of this record being complete the Health Board should consider taking the opportunity to rationalise and consolidate its digital offerings.

Key Findings		Risk & Impact	Agreed Management Action
3	**Cyber Essentials** We noted a number of suppliers without a cyber essentials certification, including the supplier of the Dental system which has been recently upgraded. The specification for this did not include a CE+ requirement and our discussion with Procurement noted that the inclusion of this is reliant on D&HI input and not a standard requirement within specifications for applications.	Suppliers may be used which do not meet WG requirements	**Agreed Action:** D&HI– notify procurement of Cyber Essentials Plus as a standard requirement in all contracts. If not possible then this needs to be reviewed by the Cyber group with the SIRO to approve any exceptions and include on the Cyber risk register.

			Expected Evidence of Implementation: Procurement pre-requisites to include cyber clause within specifications
		High Priority	**Officer:** Director D&HI/Head of Cyber
	Theme: Cyber Security	Control Operation	**Target Implementation Date:** Sept 26

Objective 3: Controls are in place to prevent users from downloading and installing software without explicit approval	Substantial

Overview / Summary of Observations

There are strong technical controls in place to protect the Health Board and prevent unauthorised software being installed on Health Board devices.

The ability to install software is restricted to specific Active Directory (AD) groups. This is mainly provided to staff within D&HI but due to the devolved nature of IT within the Health Board, some departments have their own staff with install privileges for their machines and dedicated AD groups.

There are restrictions on the websites that staff can access which prevents access to sites deemed as high risk and which contain software. We also note that there are controls in place to prevent staff from accessing ChatGPT and other generative AI sites which protect the Health Board from data leakage.

The Health Board has invested time and resource to create a highly secure network which protects the wider Health Board from any potential local issues. The network is highly segmented, separating traffic into separate functional areas with defined Virtual Local Area Network (VLANS) and with a number of firewalls in place.

The network uses MAC (device) level authentication and items flagged as higher risk are separated into a VLAN within the Demilitarised Zone (DMZ) to provide greater security. Devices representing significant risks are further restricted using Access Control Lists (ACLs) to restrict their access to very specific connections.

Objective 4: Processes are in place to identify shadow IT and ensure risks are managed appropriately (cyber-security, compliance).	Limited

Overview / Summary of Observations

D&HI hold a record of systems in place, along with the Information Asset Register (IAR) and a knowledge system within the help desk, however as noted in our previous report on Cyber Security, due to Clinical Boards not providing information the records are incomplete and there is no assessment of criticality. Linked to this there has been no completion of CAF assessments for locally managed systems and no assessment of the risk that these present to the Health Board.

In terms of medical devices, these are added to the network on a case-by-case basis and as noted there are good technical protections in place, however there is no reporting that would highlight devices that present a risk due to issues such as out of date operating systems or firmware.

D&HI are recording risks relating to local management of IT within its risk register such as legacy software, poor patching and device management and the lack of recording of all assets. This feeds into committee reporting with the DIC including a regular update on the D&HI risk register, and this does include some that include actions related to local systems, although the risks are not specifically and fully highlighted in terms of the cyber risk, data quality risk and inefficiencies.

The current IG Policy refers to the use of the Snow asset management tool in order to identify and monitor all software, although Snow has been replaced by Microsoft System Centre Configuration Manager (SCCM) there is the facility to identify all applications in place across the Health Board. However, this is not being used effectively and a review of the report noted a number that are not included within Digitals records and which breach the stated Health Board polices, contain vulnerabilities, or which do not comply with WG requirements regarding CE+ certification.

The risks associated with these applications are not being recorded within departmental risk registers, despite the management and control of these being devolved, as such there is a level of risk associated with locally managed / shadow IT which is not being record and managed.

	Key Findings	Risk & Impact	Agreed Management Action
4	**Record of Systems** There is no complete, accurate record of what digital systems and suppliers are in use across the whole organisation and no assessment of criticality, no completion of CAF assessments outside of D&HI and no assessment of the risk that suppliers present.	The Health Board cannot effectively manage digital and cyber risks.	**Agreed Action:** DH&I - Formulate a mail to senior managers requiring staff to complete the form with information on all their digital applications. Update the central Info Assets Register based on the information received Issue formal communication from Dir D&HI asking for details on digital application with a clear statement that managers must comply with the request. **Expected Evidence of Implementation:** Updated and complete record of systems across the UHB

		Medium Priority	**Officer:** Director D&HI **Target Implementation Date:** October 26
	Theme: Cyber Security	Control Operation	
5	**Risk Recording** There is a wide range of software in use, with some breaching HB Policy and WG requirements. Despite management of these being devolved, these risks are not being recorded within departmental risk registers and so the true risk to the Health Board is unquantified.	The Health Board cannot effectively manage digital and cyber risks.	**Agreed Action:** Cyber team to issue guidance on the NIS/CAF/WG requirements relating to systems and software in use. All CBs and corporate services to assess their systems and include on Risk Register where appropriate. Linked to above, where the information identifies non compliance, these should be collated into a report for the Cyber group to review. Notification to be provided to departments manging these systems to include on their risk registers.
			Expected Evidence of Implementation: Risks fully documented; risks register entries complete
		High Priority	**Officer:** Director of D&HI **Target Implementation Date:** October 26
	Theme: Risk Management	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 & 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 & 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]