Automation / AI

Final Internal Audit Report

2026/27

Cardiff & Vale University Health Board



Reasonable Assurance

Contents

Executive Summary 1
Findings & Agreed Action Plan 3
Appendix A 11

Review Reference	CVU-2627-28
Fieldwork	June - August 2026
Executive Sign Off	23 September 2026
Audit Committee	November 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 how the Health Board is developing and delivering a governance structure around the use of AI and automation.

Overview

We have concluded **reasonable** assurance on this area. The Health Board has a stated intent to increase the use of automation and AI, and there are relevant targeted milestones within the Annual Plan. Whilst there is no 3rd party automation provider, there is increasing use of Power Automate within the organisation. There are a number of AI products in use, and the governance arrangements over AI have been improved recently.

The matters requiring management attention include:

- There is minimal resource within Digital to coordinate and improve the uptake and use of AI and Automation, in particular 365 products, and there is no capacity to develop and mobilise structured plans to increase use, though use is growing amongst the user base as expected with a lo-code solution. As such the Health Board will struggle to gain the benefits of AI and automation and there is an increased risk of developing silos should Clinical Boards move forwards with the power platform without coordination and monitoring.
- There is currently no actively maintained register of AI in use across the Health Board which includes the benefits of use.
- The guidance on the use of AI misses some key aspects that would be expected within a fully complete good practice guide.
- There is currently no guidance in place for the use of automation (Microsoft Power Automate). The use of automation can introduce risks, including both data leakage and siloing of data, as such without formal guidance in place the health board has not set out guidelines for approved use, development standards, data handling, change management and monitoring and ownership.
- The assessment and approval process for AI use does not formally consider and document the accuracy of the model against metrics, understanding of the training of the model or associated benefits.
- The assessment and prioritisation mechanisms for potential automations are, in most cases, informal, undocumented and reliant on professional judgement, with no true assessment of benefits.
- The design of automations is not fully, consistently recorded, neither is the testing, outcomes of that and agreement of operation by the user.
- Automated workflows are, in many cases currently operating under the developers account and not within a dedicated service account.
- There is no coordinated process to ensure that changes to the operating environment are fully assessed for the impact on automated workflows and communicated to relevant staff. This is exacerbated by the lack of design documents for automations and a lack of change control over the automations.

Full details of matters arising are provided within the Findings & Agreed Action Plan. The following opportunity for enhancement has been identified that does not impact the overall opinion and is highlighted for management information:

- The Health Board should consider appointing a Digital Clinical Safety officer and complying with DCB0160.
- Guidance for Power Automate should include the assessment and prioritisation mechanisms for potential automations.

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 use of evolving technology is included within organisation plans, with appropriate resources available to develop their use.	1	**Reasonable**
2	An appropriate governance structure with controls and guidance is in place for the use of AI and automation which protects information, accounts used for AI and RPA and ensures that models are accurate, free from bias and protect information.	2, 3, 4	**Limited**
3	An appropriate process is in place to control the use of AI and the creation of robots and the resource use, with an assessment process to ensure AI use is appropriate, only suitable processes are automated and benefits are defined and realised.	5	**Reasonable**
4	Appropriate processes are in place to fully document development of AI models, the design of automated process and test the final product and monitor the operation of robots to ensure they operate as expected.	6, 7	**Reasonable**
5	An appropriate process is in place to ensure that changes to the environment in which automated processes operate are assessed for the impact, changes to automated processes are recorded and appropriate continuity planning is in place to enable the organisation to operate in the event of the failure of the technology.	8	**Limited**

Management Actions

3 High Priority

5 Medium Priority

Themes



Risk Types

Quality or Safety Issues

Legal & Regulatory Non-Compliance

Public Perception & Reputational Risk

Choose an item.

Findings & Agreed Action Plan

Objective 1: The use of evolving technology is included within organisation plans, with appropriate resources available to develop their use.	Reasonable

Overview / Summary of Observations

Both AI and automation can be delivered from within the Microsoft 365 suite using Copilot (AI) and the power platform (automation) and from other third parties such as Blue Prism (automation) and a variety of AI products.

The 2020 Health Board Digital Strategy notes the need to embrace the use of AI, and the use of technology is included within the Annual Plan and within the Improving Performance Together priorities which notes the intent to roll out AI and automation tools.

The digital portfolio section within the Annual Plan includes greater detail over the intent to increase the governance and use of these technologies, with expected outcomes, quarterly milestone targets and success indicators provided. Associated risks are also noted, along with the fact that Clinical Boards are responsible for the costs of technologies within their areas.

We note that progress has been made against the milestones, with improved governance arrangements and recording of AI in use, with a gradual increase in AI use, in particular to move towards use of ambient voice AI.

Both AI and automation are included within the Microsoft 365 suite and the Health Board hosts a Microsoft 365 SharePoint site with information on these products and links for staff to request access. From reviewing information from the 365 tenancy dashboard, we note that there are 294 premium Copilot licences in use with over 6,000 operations within July and with all Clinical Boards involved. Similarly, we note that there is use of automation being developed across the organisation with over 4,000 flows across 206 departments.

However, there is insufficient resource within Digital to coordinate and improve the uptake and use of these. A champions group is in place which can act as a focal point however there is no structured plan to increase use. Without a plan or resource to ensure value exploitation the Health Board will struggle to gain the benefits of AI and automation.

We also note the risk of developing silos should Clinical Boards move forwards with the power platform without coordination and monitoring.

	Key Findings	Risk & Impact	Agreed Management Action
1	**Resourcing** There is insufficient resource within the UHB to coordinate and improve the uptake and use of AI and Automation, in particular 365 products. A champions group is in place which can act as a focal point however there is no structured plan to increase use. Without a plan or resource to ensure value exploitation the Health Board will struggle to gain the benefits of AI and automation.	The health board may not fully exploit investment in AI and automation.	**Agreed Action:** Resource remains challenging for D&HI to drive this as suggested however we are actively making improvements including: Clinical Design Authority – this is the forum where AI/automation use cases can be brought for guidance and advice by clinicians and enables us as a function to be aware of projects in progress Nurse Informatics hold a database of Power Apps and Automates and their value proposition whilst the M365 team have built an App that displays all 'automate flows' i.e. where a power automate flow/process exists on the CaV estate. These will improve incrementally over time with an emphasis on understanding what value the tool derives and importantly, ow it is supported by the service area

	We also note the risk of developing silos should Clinical Boards move forwards with the power platform without coordination and monitoring.		Co-Pilot and Power Automate 'guardrail' documents are being presented to the Technical Design Authority and will go to the Cyber/IG groups for ratification in September/October 2026 Value exploitation is the responsibility of Clinical Boards as outlined in the AI Governance process circulated to Clinical Boards by the Medical Director https://nhswales365.sharepoint.com/sites/CAV_IT_Security_IG/SitePages/Artificial-Intelligence(1).aspx . The process asks that benefits are brought to the CDA to share knowledge and learning. One such project has come forward so far since we introduced this process (pilot of Heidi AVT AI in Critical Care) In the case of AVT AI (see below) we have secured a PhD student from Cardiff University to look at AVT in use and understand / capture benefits and lessons learned to help ensure benefit realisation • AVT AI is being made available within our current corporate Digital Dictation and Transcription solution for no additional charge. Corporate comms advertising this were sent out 10/09.2026 • There are several AVT AI funded pilots supported by WG in train supported by *Contracts for Innovation Cymru* – for both Dictate IT and for Heidi which the CDA is tracking There is a list of IG approvals for AI/Automation use cases which will be used to contact advocates/users to ascertain status of their use case. Learnings, benefits will be brought to the CDA.
			Expected Evidence of Implementation: • PhD student write up of AVT AI • IG register updated and AI/Automation list maintained by DHI PMO • Attendances at CDA for AI/Automation use cases • Guardrails – CoPilot, Power automate
		High Priority	**Officer:** Director of Digital Transformation **Target Implementation Date:** • October 2026 – CoPilot and MsPa Guardrail documents approved and available/circulated • December 2026 - Our IG team hold a register of AI approved use cases – we will follow these up via the CDA to understand progress and share learnings **Ongoing –** funnel AI/Automation use cases via the CDA
	Theme: Resourcing	Control Operation	

Objective 2: An appropriate governance structure with controls and guidance is in place for the use of AI and automation which protects information, accounts used for AI and RPA and ensures that models are accurate, free from bias and protect information.	Limited

Overview / Summary of Observations

There is no in house AI development, but there are a number of third party AI products in use across the Health Board. The control over the use of public generative AI such as Chat GPT has been recently improved following an exercise to establish how it was being used. This identified that staff were using it inappropriately and so a warning has been created and restrictions in uploading files applied.

In accordance with the digital plan the governance over the use of AI has been improved with the establishment of a formally defined mechanism for assessing and approving AI use within the organisation. This includes several stages including gaining the relevant Clinical Board approval, completion of data protection impact assessments (DPIA) and cyber assessments and approval by the Clinical Design Authority (CDA).

The digital section within the Annual Plan also noted the aim to create a register of AI tools in use along with the benefits of these. Records have been compiled, both by the Information Governance (IG) team as a response to an Freedom of Information (FoI) request, by the CDA lead for a presentation to the Health Informatics Forum and a Nurse Informatics maintained register, however these do note include the benefits of use.

The Health Board hosts a 365 SharePoint site which includes information, guidance and links to training materials for 365 products including power automate and copilot.

There is no AI policy as the themes are covered by other policies in place. However, guidance has been issued on the use of ambient voice technology (AVT) AI which clearly states the assessment process and provides guidance on acceptable use. We do note that the guidance misses some key aspects, in particular understanding of how the model was trained and noting the potential for hallucinations and the associated need to validate output.

Guidance for the use of Copilot has also been recently developed. Our review of this noted that it gives clear acceptable use and behaviour guidance, required training, notes the potential for hallucinations and references clinical safety requirements. We note that there is confusion over the scope as it states that it covers other generative AI, and also that other generative AI is not in scope.

Taken with the AVT AI guidance the organisation therefore has the basis for a coherent AI policy in place, however we note that some aspects are missing including guidance on how to assess accuracy, validate the model and training data and associated third party vendor assurance requirements, risk model and AI ethics principles.

Although there is use of automation via Power Automate, there is currently no guidance in place for the use of this and our conversations with staff developing automation noted that they rely on guidance sourced from outside the organisation. The use of automation can introduce risks, including both data leakage and siloing of data, as such without formal guidance in place the Health Board has not set out guidelines for approved use, development standards, data handling, change management and monitoring and ownership.

Key Findings		Risk & Impact	Agreed Management Action
2	**AI Register**	The Health Board may not be clear	**Agreed Action:** Please refer to the Management Actions at 1 above.

	The digital plan also noted the aim to create a register of AI tools in use along with the benefits of these. Records have been compiled, both by the IG team as a response to an FoI request and by the CDA lead for a presentation to the HIF, however neither of these is a register which includes the benefits of use.	over where AI is being used and the benefits from this may not be realised	**Expected Evidence of Implementation:** • IG register updated and AI/Automation list maintained by DHI PMO, informed by Clinical Boards • Attendances at CDA for AI/Automation use cases
		Medium Priority	**Officer:** Director of Digital Transformation **Target Implementation Date:** March 2027
	Theme: Information, Data Quality & Data Accuracy	Control Operation	
3	**AI Guidance** Guidance has been issued on the use of AI, however some key aspects are missing: • The AVT AI guidance does not include understanding of how the model was trained or the potential for hallucinations and the associated need to validate output. • The Copilot guidance does not included information on how to assess accuracy, validate the model and training data and associated third party vendor assurance requirements, risk model and AI ethics principles • The Copilot guidance states that it covers other generative AI, and also that other generative AI is not in scope.	Staff may use AI inappropriately	**Agreed Action:** Guidance documents will be reviewed and revised to take account of the recommendation. Additionally, an AI policy statement will be produced and incorporated into the updated Digital Strategy/Plan document.
			Expected Evidence of Implementation: Guidance documents incorporate the recommendations AI policy statement approved and published and incorporated into the updated Digital Strategy/Plan document
		Medium Priority	**Officer:** Director of Digital Transformation **Target Implementation Date:** February 2027
	Theme: Policies & Procedures	Control Operation	
4	**Automation Guidance** There is currently no guidance in place for the use of automation. The use of automation can introduce risks, including both data leakage and siloing of data, as such without formal guidance in place the Health Board has not set out guidelines for approved use, development standards, data handling, change management and monitoring and ownership.	Staff may use automation inappropriately	**Agreed Action:** Guidance / guardrails will be produced.
			Expected Evidence of Implementation: Guidance / Guardrails
		High Priority	**Officer:** AD Programmes and Head of Digital Services **Target Implementation Date:** February 2027
	Theme: Policies & Procedures	Control Design	

Objective 3: An appropriate process is in place to control the use of AI and the creation of robots and the resource use, with an assessment process to ensure AI use is appropriate, only suitable processes are automated and benefits are defined and realised.	Reasonable

Overview / Summary of Observations

As noted above there is no coordinated development of AI within the Health Board and no central, digital automation work.

There are processes in place to assess AI for appropriateness, with DPIAs required, along with consideration at the CDA. The role of the CDA is to assess and approve the use of clinical information systems once Clinical Board and IG approval have been gained and this is clearly set out within the TOR. The group includes representatives from across the organisation and our review confirmed that AI is a regular topic.

The assessment of the AI use case is not a formal checklist, but our discussion noted that the core questions cover the design, fit with digital strategy, datastore and workflow to ensure a holistic organisational design. However, there is no regular consideration of accuracy using accepted metrics, understanding of the training date for the model within the assessment or associated benefits. There is consideration of these at previous stages but not as part of a formal review and there are limited mechanisms to validate these. We also note the absence of a Digital Clinical Safety officer within the organisation which means that clinical risk is not formally assessed, as required within the DCB0160 (Clinical Safety) framework.

Power Automate is used across the Health Board and our discussions with staff developing automation noted that requests for automation within Clinical Boards are often greater than can be actioned. Within the services there are processes to assess and prioritise requests to ensure that those providing the most value are developed. However, due in part to the absence of guidance, in most cases this process is informal, undocumented and is reliant on professional judgement, with no true assessment of benefits. Given the current, resource constrained position of the Health Board this leads to a risk that resource is not focussed on the areas which provide the most benefit.

	Key Findings	Risk & Impact	Agreed Management Action
5	**AI Assessment** The assessment and approval process for AI use does not formally consider and document the accuracy of the model against metrics, understanding of the training of the model or associated benefits.	AI may be used which is not fully accurate or provide full benefits.	**Agreed Action:** We will include this as part of the Guardrail documentation review. **Expected Evidence of Implementation:** Updated guardrail documents. Overview from CDA and PMO using the register referenced under Management Action 2 above.
		Medium Priority	**Officer:** AD Programmes and Head of Digital Services **Target Implementation Date:** February 2027
	Theme: Information, Data Quality & Data Accuracy	Control Operation	

Objective 4: Appropriate processes are in place to fully document development of AI models, the design of automated process and test the final product and monitor the operation of robots to ensure they operate as expected.	Reasonable

Overview / Summary of Observations

Staff developing automations across the Health Board are often not from a digital or software development background. From our discussions with these staff, we identified that although there is no guidance or training available from the Health Board the staff are trying to apply good practices to the developments.

There is, in general, a level of documentation of the design of the automation and agreement with the requesting user, although we note that this is inconsistent and not always complete. Without documenting the design, including items such as triggers and frequency, data flows, error handling and dependencies there is a risk that automations may fail and fixes may be difficult.

As part of the design process, we note that there is consideration of the need for alerts and these are built in where appropriate for some departments, however this was not the case for all areas.

Automations are tested to ensure that they operate as anticipated and for some departments separate environments are established to enable this, this testing is by developers and by users, however the testing, outcomes and agreement are not documented.

The automated workflows are currently operating under the developers account and not within a dedicated service account, this leads to a continuity risk of the automation failing should the developer leave the organisation and means that maintenance of the automation cannot be shared.

	Key Findings	Risk & Impact	Agreed Management Action
6	**Automation Documentation** The design of automations is not fully, consistently recorded, neither is the testing, outcomes of that and agreement of operation by the user.	Automations may fail and restoration may be delayed	**Agreed Action:** This is not surprising given the nature of lo-code tools which by their design are meant to engage people as autonomous users able to design solutions for themselves. The AI governance model states this is the responsibility of clinical boards, supported by the CDA. As referenced in Management Action 1 processes will improve incrementally over time as there is no resource additionality **Expected Evidence of Implementation:** As Management Action 5 above Updated guardrail documents Overview from CDA and PMO using the register referenced under Management Action 2 above

		Medium Priority	**Officer:** AD Programmes and Head of Digital Services **Target Implementation Date:** February 2027
	Theme: Information, Data Quality & Data Accuracy	Control Operation	
7	**Automation Ownership** Automated workflows are currently operating under the developers account and not within a dedicated service account.	Automations may fail in the event that the owner leaves the organisation	**Agreed Action:** We are sighted on this issue and have taken steps to improve things. All workflows are developed in the 'Developers' account.... i.e. the developers (licences member of staff) 'personal productivity area'. Issues in the past have arisen when a developer leaves as the workflows stop as the account is suspended. This 'awareness' issue is addressed in the guardrail documents, so whilst it is still an ongoing issue, it less common than it was
			Expected Evidence of Implementation: Approved Guardrails documents
		Medium Priority	**Officer:** AD Programmes and Head of Digital Services **Target Implementation Date:** February 2027
	Theme: Information, Data Quality & Data Accuracy	Control Operation	

Objective 5: An appropriate process is in place to ensure that changes to the environment in which automated processes operate are assessed for the impact, changes to automated processes are recorded and appropriate continuity planning is in place to enable the organisation to operate in the event of the failure of the technology.	Limited

Overview / Summary of Observations

As noted, there is no central coordination for the use of automation within the health board, with clinical boards developing their own automated processes. As such there is no coordinated process to ensure that changes to the operating environment are fully assessed for the impact on automated workflows and communicated to relevant staff. As automation is rolled out it is becoming integral to the operation of departments, and failure of automated process will have an increasingly adverse effect.

Again, as noted the documentation of automation design and dependencies is incomplete, which impacts on the understanding of how a potential change may impact an automation.

There is variation in the protection of various aspects of the operating environment. For some services templates are protected using formal document control systems and automation code by version control. Other areas do not utilise these controls however, leaving the automations at increased risk of failure. We also note that general user awareness of the need to inform automation leads of any changes is not complete which has led to failures in processes.

	Key Findings	Risk & Impact	Agreed Management Action
8	**Change Control** There is no coordinated process to ensure that changes to the operating environment are fully assessed for the impact on automated workflows and communicated to relevant staff. This is exacerbated by the lack of design documents for automations and a lack of change control over the automations.	Automated processes which are integral to departmental operation may fail.	**Agreed Action:** As referenced given the nature of lo-code tools enabling autonomous users to design solutions for themselves, responsibility falls to the person doing the development and thus the clinical boards. The Management Actions above we believe will help and we will continue to improve the guidance available however, as observed there is no central resource to co-ordinate and manage this.
			Expected Evidence of Implementation: Incremental improvements in guidance and guardrails including what can be learned from others.
		High Priority	**Officer:** Director D&HI **Target Implementation Date:** February 2027
	Theme: Information, Data Quality & Data Accuracy	Control Design	

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 & 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