Risk Management

Internal Audit Report

2025/26

NHS Wales Performance and Improvement

Reasonable Assurance

Contents

Review Reference	NHP-2526-01
Fieldwork	December 2025 – January 2026
Executive Sign Off	5 February 2026
Audit Committee	March 2026
Executive Lead	Sophie Fuller, Assistant Director of Corporate Governance and Business Support
Audit Team	Paul Dalton, Head of Internal Audit
	Emma Samways, Deputy Head of Internal Audit

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

Executive Summary

Purpose

The overall objective of the audit was to review the development, implementation and application of NHSP&I's risk management process.

Overview

The hosting agreement between Welsh Government and Public Health Wales NHS Trust (the Trust) sets out specific responsibilities for NHS Wales Performance & Improvement (NHSP&I) in respect to risk management. The Responsible Officer is responsible for the management of risk within NHSP&I which follows the Trust's risk management framework guidance and monitors and maintains a risk register for NHSP&I on its Datix system. Any potential risks which could impact on the business and safety of the Trust should be escalated to the Trust Chief Executive and the executive with responsibility for risk and should feature in any assurance reports to relevant Board committees of the host organisation.

We found that NHSP&I has made good progress in implementing effective risk management procedures at a corporate and directorate level with regular review of risks and that it will start reporting against its Strategic Risk Register from Q1 of 2026/27. Risk appetite statements are shortly to be approved, and there has been significant work undertaken on starting to identify controls and assurances relating to the strategic risks. The approach is consistent with that set by the Trust.

We have concluded reasonable assurance on this area The matters requiring management attention are:

- Action plans for both strategic and corporate risks need to be documented and reported such that there is assurance that risks are being effectively mitigated.
- Directorate risk registers need to be updated to provide clarity between existing controls/mitigations and planned actions and to ensure that current or residual risk scores are calculated only on those controls or mitigations that are already in place.

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

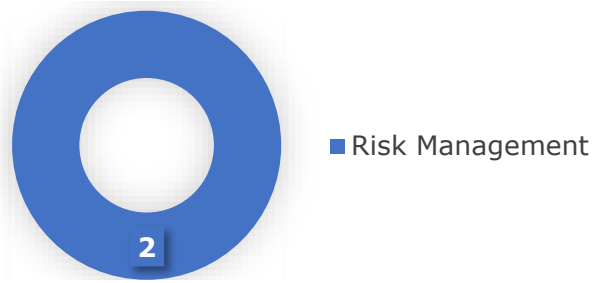
Scope & Assurance Summary

Objectives (The objectives and associated assurance ratings are not necessarily given equal weighting when formulating the overall audit opinion.)		Related Findings	Assurance
1	Risk management and assurance arrangements are defined within an up-to-date policy, framework and associated procedures, aligned to NHSP&I's objectives and strategic direction.	-	**Substantial**
2	Identification of risks aligns to NHSP&I's strategic objectives, and there has been consideration of risk appetite.	-	**Reasonable**
3	Strategic and corporate risks are regularly reviewed at a senior level, and processes are in place to support and evidence changes in risk scores.	-	**Reasonable**
4	Where gaps in control and assurance are identified, action plans that are regularly monitored are in place setting out the work required to close those gaps.	1	**Limited**
5	Directorates have risk management procedures in place that ensure a consistent approach and facilitate timely escalation of key risks where appropriate.	2	**Reasonable**
6	Any significant risks are reported to Welsh Government and/or the Trust in accordance with the Hosting Agreement.	-	**Substantial**

Management Actions

0	2
High Priority	Medium Priority

Themes



Risk Types

Financial Loss

Legal & Regulatory Non-Compliance

Choose an item.

Choose an item.

Findings & Agreed Action Plan

Objective 1: Risk management and assurance arrangements are defined within an up-to-date policy, framework and associated procedures, aligned to NHSP&I's objectives and strategic direction.	**Substantial**

Overview / Summary of Observations

There is a golden thread running from the Trust's risk management policy and procedure through the NHSP&I risk management process document and ending with local operational procedures in at least some of the directorates. All documentation is consistent in its approach and is up to date, with appropriate approvals in place. There is also a clear link to the strategic objectives and direction of NHSP&I, and the responsibilities contained within the Hosting Agreement for NHSP&I are explicitly referenced in the documentation.

Objective 2: Identification of risks aligns to NHSP&I's strategic objectives, and there has been consideration of risk appetite	**Reasonable**

Overview / Summary of Observations

Strategic risks have been identified for each of the four strategic objectives and actions associated with each have been identified, although formal reporting will not commence until Q1 of the new financial year. A suggested risk appetite has been applied to each risk, but the formal risk appetite statement is to be approved jointly by the senior leadership team and Welsh Government following a meeting at the end of January. As the risk appetite statement is still to be formally approved, we have assessed the audit objective as 'reasonable', although we are not raising a formal finding as the required action is shortly to be completed.

Objective 3: Strategic and corporate risks are regularly reviewed at a senior level, and processes are in place to support and evidence changes in risk scores.	**Reasonable**

Overview / Summary of Observations

The development of the strategic risk register is on-going with a plan to commence formal reporting during the first quarter of 2026/27. This will be reported quarterly to the operational leadership forum and bi-annually to both the senior leadership team and the joint meeting with Welsh Government. The corporate risk register is already taken monthly to both these latter meetings and that will continue going forward. The corporate risk covering report provides detail on any removed or new risks, and any changes to risk detail or scores. As the strategic risk register is yet to be reported we have again assessed the audit objective as reasonable but have not raised a formal finding due to the imminent completion of the required action.

Objective 4: Where gaps in control and assurance are identified, action plans that are regularly monitored are in place setting out the work required to close those gaps.	**Limited**

Overview / Summary of Observations

As previously stated, the strategic risk register is still under development but is intended to be fully operational from the start of the 2026/27 financial year. Work is still ongoing in terms of controls and assurances, but a number of actions have already been identified for each of the four strategic objectives. Most of these actions have a responsible lead and a date (by quarter) for completion.

Our review of corporate risk reporting identified evidence of regular updates of risks but did not identify any specific action plans with designated responsible officers and dates for completion.

Key Findings		Risk & Impact	Agreed Management Action
1	**Action Plans** Although the corporate risk register shows frequent evidence of updating of risks, none of the risks reviewed in the report taken to the meeting with Welsh Government in December evidenced an action plan.	Risks may not be effectively mitigated, and risk owners are not effectively held to account.	All risks that require further mitigation will have clear action plans with designated responsible officers and dates for completion. Information on progress with completion of the required actions will feature in routine reporting to ensure that the responsible officer can be held to account for their completion. **Expected Evidence of Implementation:** Reporting of documented Action Plans for Strategic and Corporate Risks.
		Medium Priority	**Officer:** Chief of Staff **Target Implementation Date:** 30 April 2026
	Theme: Risk Management	Control Operation	

Objective 5: Directorates have risk management procedures in place that ensure a consistent approach and facilitate timely escalation of key risks where appropriate	**Reasonable**

Overview / Summary of Observations

Currently the directorate risk registers are shared with the business meeting of the senior leadership team on a quarterly basis. From Q1 of 2026/27 the corporate team additionally aim to meet with individual directorates to review risk registers on a quarterly basis.

Escalation of directorate risks to the corporate level can either be processed through the Assistant Director and Director network, or alternatively this can be actioned via Datix. For both routes, we understand that the corporate team will review the suggested escalation and meet with directorate management to discuss it. If it seems appropriate to escalate the risk, the corporate team will provide some detail on the risk for the senior leadership team to formally consider acceptance of the risk onto the corporate risk register. The guidance from the corporate team to directorates in considering risks for escalation is not to focus too heavily on the risk score but to instead consider whether the risk is within their gift to manage with existing resource and/or the potential impact on the whole organisation if the risk were to crystallise.

We reviewed three directorates (Performance & Assurance, Planned Care, and Value Transformation) as part of our audit. Documented guidance, and the directorate risk register for each, were reviewed and interviews held with key staff in each directorate. The three directorates each had their own local risk procedure, but it was clear in each document that these were subservient to, and consistent with, the NHSP&I risk management process which itself sits underneath the Trust risk management policy. Generally, we note a proactive and regular review of risk, particularly in directorates with projects and programmes where they are very used to regular reporting on risks. Populating risks onto Datix at directorate level is a relatively recent development and inevitably we saw some gaps in information. Although risks below Tier 3 (directorate risks) are not yet populated on Datix, the information recorded is consistent with that which would be required. One specific area in need of potential improvement is ensuring that existing controls and mitigations are listed separately from further actions or mitigations and that the current or residual score is based only on those actions/mitigations that are already in place.

	Key Findings	Risk & Impact	Agreed Management Action
2	**Directorate Risk Registers** Directorates have only recently populated their risk registers onto Datix and understandably the information is not always fully complete. In particular, the documentation of action plans with clarity on what is going to be done and by who and when and ensuring that this information is kept distinct from existing controls. There is also a need to ensure that the current or residual risk score is based only on those controls that are already in place.	Directorate risks may not be effectively and appropriately mitigated.	Management will ensure that Directorate Risk Registers are complete with clarity on action plans and a clear distinction between required actions and existing controls. Directorate staff will be reminded also that the current or residual risk score should only be based on existing controls and mitigations. **Expected Evidence of Implementation:** Evidence of inclusion of above in Directorate Risk Registers.
		Medium Priority	**Officer:** Chief of Staff **Target Implementation Date:** 30 June 2026
	Theme: Risk Management	Control Operation	

Objective 6: Any significant risks are reported to Welsh Government and/or the Trust in accordance with the Hosting Agreement.	**Substantial**

Overview / Summary of Observations

The hosting agreement stipulates that NHSP&I is required to report to the Trust audit committee to provide assurance on the risk management arrangements in place and that:

'Any potential risks which could impact on the business and safety of the Host Organisation will be escalated to the Chief Executive and the Executive with responsibility for risk in the Host Organisation and should feature in any assurance reports to relevant Board Committees of the Host Organisation.'

Our review of all Trust audit committee papers for the current financial year confirmed that assurance is provided through a formal and consistently worded NHSP&I assurance report that is taken to the committee four times a year. This also includes reference to, and detail on, one risk that is considered as having a potential impact on the business and safety of the host organisation. NHSP&I also complete and sign an annual compliance statement which specifically includes the requirement to manage key risks appropriately.

In respect of Welsh Government, the hosting agreement states that:

'The Responsible Officer will ensure that the Chief Executive of NHS Wales is appraised of any high risks and the arrangements for providing assurance regarding their management.'

Welsh Government are kept apprised of the risk management arrangements through the monthly meetings between Government executives and the full NHSP&I senior leadership team.

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 NHS Wales Performance and Improvement, 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 NHS Wales Performance and Improvement. 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]