Risk Management
Final Internal Audit Report

March 2023

Digital Health and Care Wales

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

GIG CYMRU NHS WALES
Iechyd a Gofal Digidol Cymru
Digital Health and Care Wales

Contents

Review reference:	DHCW-2223-02
Report status:	Final
Fieldwork commencement:	12th January 2023
Fieldwork completion:	19th February 2023
Draft report issued:	23rd February 2023
Debrief meeting:	19th February 2023
Management response received:	N/A
Final report issued:	31st March 2023
Auditors:	Simon Cookson, Director of Audit & Assurance Services Stephen Chaney, Deputy Head of Internal Audit Philip Lewis-Davies, Principal Auditor
Executive sign-off:	Chris Darling, Board Secretary
Distribution:	Julie Ash, Head of Corporate Services Laura Tolley, Corporate Governance Manager Bethan Walters, Risk and Regulation Officer
Committee:	Audit and Assurance Committee

Audit and Assurance Services conform with all Public Sector Internal Audit Standards as validated through the external quality assessment undertaken by the Institute of Internal Auditors

Acknowledgement

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

Executive Summary

Purpose

This internal audit has been undertaken to provide an opinion over the arrangements in place to ensure that risk is being appropriately managed to enable the delivery of DHCW's key objectives. The audit focussed at an operational / service level (e.g. department, directorate and project / programme).

Overview

Significant progress has been made in embedding the Risk Management and Board Assurance Framework Strategy (the 'Strategy') approved by the Board in May 2021.

The Strategy, policy, and associated policies and procedures have been communicated effectively with training provided.

Based upon sample testing of operational risks selected from the Datix risk database maintained by DHCW we found:

- Risk assessment and documentation is compliant with guidance provided.
- The management of recorded risk is compliant with guidance provided. However, it was noted that many application, development and support related risks may potentially require transfer from DHCW to other NHS Wales organisations. This is a recognised issue and work is underway to continue to identify and affect such transfers promptly.
- Monitoring and reporting is compliant with guidance provided.
- Escalation procedures are adhered to with the Corporate Risk Register and Datix risk database consistently presenting information over the management of risks.

We have not raised any matters from this review.

Report Classification

Substantial

Few matters require attention and are compliance or advisory in nature.

Low impact on residual risk exposure.

Assurance summary

	Assurance objectives	Assurance
1	The implementation, and communication of, the Risk Management and Board Assurance Framework Strategy, and associated policies and procedures.	Substantial
2	The effectiveness of how assessment and documentation of operational risk at a service level is delivered.	Substantial
3	The effectiveness of the management of operational risks (e.g. risk score, actions, target dates, responsible owners and impact on strategic objectives)	Reasonable
4	The effectiveness of monitoring and reporting of operational risk information and escalation procedures for risks that cannot be resolved at an operational level	Substantial

1. Introduction

1.1 This internal audit provides an opinion over the arrangements in place to ensure Digital Health and Care Wales (DHCW) risk is being appropriately managed, to enable the delivery of DHCW key objectives. This audit focused at an operational / service level (e.g. department, directorate and project / programme).

1.2 The Chief Executive as Accountable Officer of DHCW has overall accountability and responsibility for ensuring it meets its statutory and legal requirements and adheres to guidance issued by the Welsh Government in respect of governance, which encompasses risk management.

1.3 The Board approved the Risk Management and Board Assurance Framework Strategy at its May 2021 meeting, following endorsement from the Audit and Assurance Committee earlier that month. The document's purpose is to provide guidance to all staff on the management of strategic and operational risks and the Board Assurance Framework within DHCW.

1.4 We completed two internal audits during 2021-22 (Corporate Governance Part One and Part Two) that included commentary and recommendations on strategic risk management matters. These were considered within this review too, where relevant.

1.5 Objectives of the area under review were the:

- implementation, and communication of, the Risk Management and Board Assurance Framework Strategy, and associated policies and procedures;
- effectiveness of how assessment and documentation of operational risk at a service level is delivered;
- effectiveness of the management of operational risks (e.g. risk score, actions, target dates, responsible owners and impact on strategic objectives); and
- effectiveness of monitoring and reporting of operational risk information and escalation procedures for risks that cannot be resolved at an operational level.

1.6 The risks considered in the review included:

- lack of awareness of the Risk Management Strategy and Board Assurance Framework Strategy within DHCW;
- key operational risks are not being identified, assessed, and / or recorded;
- operational risks identified are not being effectively managed; and
- operational risks are not being escalated within DHCW.

1.7 The audit has considered the management of operational risks actioned and evidenced during 2022. Sample testing of operational risks was also undertaken based on the Datix risk database information held in January 2023.

2. Detailed Findings

Objective 1: The implementation, and communication of, the Risk Management and Board Assurance Framework Strategy, and associated policies and procedures

2.1 The Risk Management and Board Assurance Framework Strategy, (the 'Strategy') and associated policy and procedures are available to all staff. A risk management page on the intranet / SharePoint has been created by the Corporate Governance Team as a repository of the Strategy, policy, procedures and related templates. The risk management site consists of a number of sections, including:

- Risk Management Group;
- Guidance and Risk Resources;
- Risk Strategies and Policies;
- Risk Training; and
- DHCW Risk Register.

2.2 Support and guidance is available from the Board Secretary via email, but has since been subsumed into the intranet resources, where all risk related information is available. Queries can be logged for the Corporate Governance Team members to address. A specific training log is maintained of all staff who raise queries and training, be it standard or bespoke, provided. Communications with staff are also made via the insider magazine and can cover changes to the risk management system or reinforcement of key messages.

2.3 In addition, to addressing specific queries from staff, communication is provided via training commensurate with the seniority of staff within DHCW. The Corporate Governance Team manages training required and provided. For example, specific training is provided to staff before they can become risk handlers, risk owners or are promoted into a senior position. This ensures that access to the Datix risk database is controlled and users are fully trained.

2.4 All staff can access the risk management page on the intranet via SharePoint and can access training modules. Slide presentations are available currently, but these are scheduled to be developed into video presentations.

2.5 All staff also receive a risk management awareness training element, even if they are not Datix users. The policy is for all staff to be risk aware and to report incidents and risks. There is a general risk awareness training module on the intranet too.

Conclusion:

2.6 We recognise that considerable effort has been invested to communicate with staff and that the development of the risk management page on the intranet and control over training given, has enhanced the effectiveness of risk management within DHCW. We have not raised any matters arising under this objective. Therefore, we have provided **substantial assurance** over this area.

Objective 2: The effectiveness of how assessment and documentation of operational risk at a service level is delivered

2.7 The assessment and documentation of operational risk is detailed in the Strategy and in the Risk Management Policy. The guidance provided is consistent between the Strategy and the Risk Management Policy with regard to the assessment and documentation of operational risk. The guidance provides an appropriate structure detailing the following:

- a standard risk assessment form;
- standard risk scoring (which details domains, consequence, likelihood); and
- a standard risk register format.

2.8 In addition, all risks are recorded on the Datix risk database using an established reporting format. The Datix risk data is reviewed closely by the Corporate Governance Team and drives a consistency of approach to the recording and documenting of individual risks. However, not all risks recorded on Datix are fully managed by DHCW. For example, we noted that DHCW maintains the record of NHS Wales national cyber risks, but is not responsible for the management of such risks.

2.9 The assessment and documentation of DHCW operational risk, based on the risk sample tested, is compliant with guidance. It is driven by the structured Datix risk database input field requirements of risk owners and risk handlers.

2.10 We did note that one of the sample risks selected for testing had the same initial and target risk score. This can occur when a risk is initially recorded on the Datix risk database and further work is required to evaluate the risk and target outcome required. A scan of the whole database was then performed which identified that there are 25 such risks recorded, 16 of which have either been accepted or identified for transfer to other NHS Wales organisations. The final nine are to be reviewed by the Corporate Governance Team alongside the risk owners. In addition, a periodic review of such instances is to be included into the monthly metrics going forward. This has not been raised as a matter arising as the number of instances is low and action has been taken to address the issue.

Conclusion:

2.11 We have not raised any matters arising under this objective. Therefore, we have provided **substantial assurance** over this area.

Objective 3: The effectiveness of the management of operational risks (e.g. risk score, actions, target dates, responsible owners and impact on strategic objectives)

2.12 The management of operational risk is detailed in the Strategy and in the Risk Management Policy. All risks within the Datix risk database are subject to periodic update reviews that vary in frequency based on the risk score. Higher risk score values are reviewed more frequently. Updates focus on the progress made in the delivery of actions to mitigate the risk identified.

2.13 The management of identified operational risk including actions plans, based on the risk sample tested, is compliant with the guidance. It is also driven by the structured Datix risk database input field requirements of risk owners and risk handlers.

2.14 The frequency of risk updates and comments on action plan activity is evidenced in the sample of risks tested where the risk was initially recorded in the last year. However, the Datix risk database does not contain a full history on those risks relating to legacy issues dating back to the NWIS era. For example, one of the samples selected relates to WCCIS and was initially recorded in 2017. The history of this risk is not fully loaded on to the Datix risk database with the monthly reviews evidenced since August 2022.

2.15 We did note that five out of six sample risks selected from the Application, Development and Support (ADS) directorate had update comments that the risk was to be transferred from DHCW to health board(s), with the transfer process via the relevant Service Management Board due to start or in progress. These risks relate mainly to issues identified via the Patient Safety process with risks being assigned to DHCW in the first instance.

2.16 This process ensures that all such risks are captured in one location. However, historically a large number of such risks may not have been transferred promptly to the organisations that are best placed to hold and monitor the risk within NHS Wales. Whilst the volume of such risks within the ADS directorate have reduced in the last year, as risk transfers have been successfully made, continued efforts are required. We have not raised a recommendation, as work is already underway to identify and complete such a transfer promptly. We reviewed the steps being completed and are satisfied that this will reduce the risk going forward.

Conclusion:

2.17 Whilst we have not raised any matters arising under this objective, the volume of risks that may potentially require transfer from DHCW is a recognised issue and work is still underway. Therefore, we have provided **reasonable assurance** over this area, as the risk is still present.

Objective 4: The effectiveness of monitoring and reporting of operational risk information and escalation procedures for risks that cannot be resolved at an operational level

2.18 The monitoring and reporting of risk is detailed in the Strategy and in the Risk Management Policy and includes the escalation processes to be followed.

2.19 As above, the monitoring and reporting of identified operational risk including escalation, based on the risk sample tested, is compliant with the guidance. The Corporate Governance Team reviews entries to the Datix risk database during each month and identifies missing information / review updates required. A monthly directorate review slide presentation is compiled and access for each directorate is provided to their section of the Datix risk database. The Corporate

Governance Team attends each Executive Director's meeting and provides commentary on poor performance identified from their review of the Datix risk database.

2.20 We did note that two of the departments selected in our sample had bespoke reporting and oversight structures that were the responsibility of parties outside of DHCW, notably WCCIS (local authorities) and NHS Wales national cyber security risks (Service Management Boards and Directors of Digital Peer Group). DHCW make available their section of the Datix risk database, but do not provide any other reporting.

2.21 For the sample risks tested, we identified risks that were escalated and matched the Datix risk database record with the movement on the Corporate Risk Register changes reported to the Board during 2022. We also selected a sample of escalated and de-escalated risks as noted on the Corporate Risk Register in 2022 and agreed these movements to the Datix risk database record.

Conclusions:

2.22 We have not raised any matter arisings under this objective. Therefore, we have provided **substantial assurance** over this area.

Appendix A: Assurance opinion and action plan risk rating

Audit Assurance Ratings

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

 **Substantial assurance**	Few matters require attention and are compliance or advisory in nature. **Low impact** on residual risk exposure.
 **Reasonable assurance**	Some matters require management attention in control design or compliance. **Low to moderate impact** on residual risk exposure until resolved.
 **Limited assurance**	More significant matters require management attention. **Moderate impact** on residual risk exposure until resolved.
 **No assurance**	Action is required to address the whole control framework in this area. **High impact** on residual risk exposure until resolved.
 **Assurance not applicable**	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 Recommendations

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

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

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

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

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