

NIS Directive (Cyber Security) Final Internal Audit Report September 2022

Public Health Wales NHS Trust



Partneriaeth
Cydwasaethau
Gwasanaethau Archwilio a Sicrwydd
Shared Services
Partnership
Audit and Assurance Services



Iechyd Cyhoeddus
Cymru
Public Health
Wales



Contents

Executive Summary	3
1. Introduction.....	4
2. Detailed Audit Findings.....	4
Appendix A: Management Action Plan	8
Appendix B: Assurance opinion and action plan risk rating	11

Review reference:	PHW-2122-10
Report status:	Final
Fieldwork commencement:	22 February 2022
Fieldwork completion:	7 April 2022
Debrief meeting:	
Draft report issued:	12 April 2022
Management response received:	22 July 2022
Final report issued:	9 August 2022
Auditors:	Martyn Lewis, IT Audit Manager
Executive sign-off:	Huw George, Deputy Chief Executive / Director of Operations
Distribution:	Simon Thomas, IT Operations Lead
Committee:	Audit and Corporate Governance 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 and Assurance Services would like to acknowledge the time and co-operation given by management and staff during the course of this review.

Disclaimer notice - please note

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 and Corporate Governance 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 Public Health Wales NHS Trust 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.

Executive Summary

Purpose

Review arrangements in place for the implementation of the NIS Directive in the Trust, including the Cyber Assessment Framework (CAF), improvement plan and overarching governance.

Overview

We have issued substantial assurance on this area.

An appropriate process was in place to complete the CAF and we note areas of good practice concerning overall cyber security governance.

Matters arising concerned areas for refinement and further development.

- No retention of evidence to support the responses as part of the CAF process.

Report Classification

Substantial



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

Low impact on residual risk exposure.

Assurance summary¹

Assurance objectives	Assurance
1 CAF completion and maintenance of evidence	Reasonable
2 Accurate self-assessed position supported by evidence	Substantial
3 Improvement plan implementation	Substantial
4 Governance	Substantial

¹The objectives and associated assurance ratings are not necessarily given equal weighting when formulating the overall audit opinion.

Key Matters Arising

	Assurance Objective	Control Design or Operation	Recommendation Priority
1	Assessment Evidence	1 Operation	Medium

1. Introduction

- 1.1 Our review of the Network and Information Systems Regulations was completed in line with Public Health Wales NHS Trust's (the 'Trust' or the 'organisation') Internal Audit Plan for 2021/22. The review sought to provide the Trust with assurance that there are effective processes in place to manage the risks associated with the regulations.
- 1.2 Cyber security and resilience is the protection of computer systems and networks from the theft of, or damage to, hardware, software, or electronic data, as well as from the disruption or misdirection of the services provided.
- 1.3 A core piece of legislation relating to cyber security are the Network and Information Systems Regulations of 2018 (NIS Regulations), transposed into UK law in May 2018 from the EU NIS Directive, with the intention to raise levels of cyber security and resilience of key systems across the EU.
- 1.4 At the core of this piece of legislation is the aim to drive improvement in the protection of the network and information systems which are critical for the delivery of digital services and essential services in the UK. These regulations require bodies to have processes in place to protect themselves from attack, detect potential intrusions and react appropriately when intrusions occur.
- 1.5 Although cyber security is not a devolved matter, Welsh Government (WG) is the competent authority for the NIS in the case of essential health services in Wales.
- 1.6 Within NHS Wales, Digital Health and Care Wales (DHCW) takes a leading and coordinating role for the maintenance and improvement of cyber security on behalf of WG, they are responsible for establishing the compliance framework for operators of essential services, which includes defining the scope of the regulations, reporting thresholds, and processes for reporting and dealing with cyber incidents. The individual trusts and health boards which fall within scope must adopt and comply with these arrangements.
- 1.7 The relevant lead Executive Director for the review is the Executive Director Quality, Nursing & AHPs.
- 1.8 The potential risks considered in the review were as follows:
 - poor or non-existent stewardship in relation to cyber security;
 - failure to comply with regulations such e.g. NIS Regulations; and
 - loss of data or services and inappropriate access to information.

2. Detailed Audit Findings

Objective 1: a process exists for completion of the self-assessment and maintenance of appropriate evidence.

- 2.1 Foundation work on the CAF was undertaken by the Head of IM&T by reviewing the CAF and performing an initial assessment prior to the formal release of the document. This gave the organisation an early indication of where issues lay.

- 2.2 The critical systems were identified via linking with the Trust's programmes. The number of systems assessed as critical was reduced down from 40 identified systems to 23 following discussions between the service owners and IM&T.
- 2.3 The completion of the CAF was on a workshop basis with the Cyber Resilience Unit (CRU). Part A included the Head of IM&T and the Senior Cyber Security Engineer, together with lead Executives. Part D included the Business Continuity lead in addition to the above. Parts B and C, as technical assessments, were completed by the Head of IM&T and the Senior Cyber Security Engineer.
- 2.4 We note that there was involvement of stakeholders in the process. These were the staff deemed as service owners, and the risks and business continuity issues were discussed with them.
- 2.5 There was a review process in place for the CAF assessment. The outcomes were shared with the Deputy Chief Executive / Director of Operations and Finance, and the Executive Director Quality, Nursing & AHPs as Senior Information Risk Owner (SIRO), for approval prior to submission.
- 2.6 Information to support each CAF response was provided through discussions with the CRU where required. The CRU did not specifically request evidence in the form of documentation as part of the assessment. We note that records of the discussions and information provided have not been retained, although there is an awareness of what evidence would be needed and where this is located. As the self-assessment will be repeated annually, the lack of recorded information and clarifications sought from the CRU may hinder the timeliness and efficiency of future iterations. **See Matter Arising 1 at Appendix A.**

Conclusion:

- 2.7 Our review highlighted the significant work undertaken by the team to prepare for, and complete, the self-assessment, although, evidence and records of discussions have not been appropriately retained for future iterations of the CAF. Consequently, we have concluded **reasonable** assurance for this objective.

Objective 2: the self-assessed position is accurate and supported by evidence.

- 2.8 As part of this review, we conducted interviews with the Head of IM&T.
- 2.9 During this review, as we note above, there was no retention of evidence and so we were unable to fully evaluate the Trusts' self-assessed position. However, we tested a sample of four objectives within the CAF to ensure appropriate scoring and discussed the position:
- A2.a Risk Management;
 - B4.b Secure Configuration;
 - B5.b Design for Resilience; and
 - C1.a Monitoring Coverage.
- 2.10 Using our professional judgement, information gleaned from interviews and update reports, we consider the self-assessment to be an accurate reflection of the Trust's current cyber security position.

Conclusion:

- 2.11 Whilst we consider the self-assessed position to be accurate, as noted above, we were unable to verify through evidence. However, discussion confirmed the appropriateness of the self-assessed responses. Consequently, we have provided **substantial** assurance for this objective.

Objective 3: an improvement plan is in place to improve the cyber security position within the organisation and is being implemented appropriately.

- 2.12 Following the initial assessment that was undertaken by the Head of IM&T, actions to address areas of weakness were identified. These actions have fed into a cyber workplan which is based on Cyber Essentials.
- 2.13 Funding has been sought, and work is ongoing with several security improvement projects already in progress. These include work to improve patch compliance, to improve the firewall position and to improve security log retention.
- 2.14 We note that a formal improvement action plan for NIS is not yet in place as the Trust is awaiting the outcome of the CAF from CRU. However, as the CAF assessment was undertaken, actions to resolve areas of weaknesses were defined. These actions have fed into a cyber work plan. The cyber work plan combines actions to resolve gaps identified through the CAF, the Cyber Essentials assessment and ISO assessment.
- 2.15 Our testing of a sample of identified gaps from the CAF assessment confirmed that the associated actions have been included within the cyber work plan or are already work in progress. The items tested were:
- A4 a5 - All network connections and data sharing with third parties is managed effectively and proportionately;
 - B2 a1 - Only authorised and individually authenticated users can physically access and logically connect to your critical systems;
 - B4 d9 - You regularly test to fully understand the vulnerabilities of the critical systems;
 - C1 a2 - Your monitoring data provides enough detail to reliably detect security incidents that could affect the operation of your critical system; and
 - D1 c - Testing and Exercising.

Conclusion:

- 2.16 Progress has been made to identify gaps in compliance and actions have been identified to improve on the current cyber security position. Whilst the Trust is awaiting feedback from the CRU prior to developing a formal NIS improvement plan, appropriate measures for improvement have been identified and several projects have been initiated to improve the cyber security position. Consequently, we have concluded Substantial assurance for this objective.

Objective 4: there is monitoring and reporting of the progress of the improvement plan and gaps in compliance to an appropriate governance group.

- 2.17 There is regular, six-monthly reporting of cyber security, including NIS to the Audit and Corporate Governance Committee. These reports provide an update on work that is ongoing regarding cyber security. We also note that additional updates are provided where necessary, for example recently regarding the Ukraine situation. Furthermore, the outcomes from the initial CAF assessment were provided to the Committee.
- 2.18 A risk relating to cyber security is included on the Strategic Risk Register and updates on this risk are provided on a regular basis. The detail of the risk explains the cyber risk and provides information on the current status of actions taken to mitigate the risk. We note however, that the risk does not include the potential financial penalties for non-compliance with the NIS Regulations. **See Matter Arising 2 at Appendix A.**

Conclusion:

- 2.19 There is regular reporting of cyber security to the Audit and Corporate Governance Committee, although we note that this could be more frequent. The risk associated with cyber security is included on the Strategic Risk Register, and regular updates are provided. Accordingly, we have provided substantial assurance over this objective.

Appendix A: Management Action Plan

Matter Arising 1: Supporting information retention (Operation)		Impact
Our review highlighted that records of discussions and supporting information provided to the CRU have not been captured and maintained throughout the self-assessment process.		Potential risk of: <ul style="list-style-type: none"> poor or non-existent stewardship in relation to cyber security.
Recommendations		Priority
1.1 Management should ensure that records of discussions and information provided to and from the CRU are captured for future annual self-assessments.		Medium
Agreed Management Action	Target Date	Responsible Officer
1.1 We will ensure that any discussions or decisions around cyber security are documented going forward so we can draw on the evidence as part of our ongoing assessments.	September 2022	IT Operations Lead



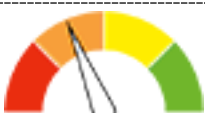


Matter Arising 2: Reporting and Risk (Operation)		Impact
<p>Reporting on cyber security is on a six monthly basis. In addition, the risk relating to cyber security does not fully articulate the risk associated with NIS, in particular the potential financial risk associated with non compliance with the NIS Regulations.</p>	<p>Potential risk of:</p> <ul style="list-style-type: none"> • poor or non-existent stewardship in relation to cyber security; • failure to comply with regulations such e.g., NIS Regulations 	
Recommendations		Priority
<p>2.1 Reporting on cyber security should be to each committee, and include a current state position and an update against the NIS requirements.</p> <p>2.2 The risk description should be reviewed, with inclusion of the potential financial penalties relating to non-compliance with NIS.</p>	<p>Low</p>	
Agreed Management Action	Target Date	Responsible Officer
<p>2.1 We will provide regular six monthly reports to the committee and in between additional updates are provided when necessary. As this was scored as a low risk, we do not feel this warrants more frequent reporting.</p>	<p>December 2022</p>	<p>IT Operations Lead</p>

<p>2.2 We agree to review the strategic risk to include the potential financial penalties relating to non-compliance with NIS. We understand the penalties to be:</p> <ul style="list-style-type: none"> • A category one penalty will not exceed £1,000,000; • A category two penalty will not exceed £8,500,000; • A category three penalty will not exceed £17,000,000. 	<p>September 2022</p>	<p>IT Operations Lead</p>
---	-----------------------	---------------------------

Appendix B: 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](#)