Network and Information Systems (NIS) Directive

Final Internal Audit Report

April 2022

Hywel Dda University Health Board

NWSSP Audit and Assurance

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

GIG CYMRU NHS WALES
Bwrdd Iechyd Prifysgol Hywel Dda
University Health Board

EXTERNAL • QUALITY • ASSESSMENT

Contents

Review reference:	HDUHB-2122-18
Report status:	Final
Fieldwork commencement:	17 February 2022
Fieldwork completion:	24 February 2022
Draft report issued:	14 March 2022
Debrief meeting:	23 March 2022
Management response received:	04 April 2022
Final report issued:	04 April 2022
Auditors:	Sian Harries
Executive sign-off:	Huw Thomas (Director of Finance)
Distribution:	Anthony Tracey (Digital Director), Paul Solloway (Deputy Digital Director)
Committee:	Audit 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.

Disclaimer notice - please note

This audit report has been prepared for internal use only. Audit & Assurance Services reports are prepared, in accordance with the Service Strategy and Terms of Reference, approved by the Audit Committee.

Audit reports are prepared by the staff of the NHS Wales Shared Services Partnership – 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 Hywel Dda 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.

Executive Summary

Purpose

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

Overview

Significant work has been undertaken by the Digital Team and Cyber Security Consultant to accurately complete the CAF and to develop a fully costed improvement plan.

Matters arising concerned areas for refinement and further development:

- Insufficient reporting of the NIS Directive to the Board; and
- Outdated Cyber Security Risk documented on Corporate Risk Register.

Report Classification

		Trend
Substantial	Few matters require attention and are compliance or advisory in nature. **Low impact** on residual risk exposure.	N/A First Review

Assurance summary[1]

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

Matters Arising

		Assurance Objective	Control Design or Operation	Recommendation Priority
1	NIS Directive Governance	4	Operation	Medium
2	Cyber Security Risk	4	Design	Medium

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

1. Introduction

1.1 In line with the 2021/22 Internal Audit Plan for Hywel Dda University Health Board (the Health Board) a review of Network and Information Systems Regulations (NISR) arrangements was undertaken.

Cyber Security and Resilience is the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

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.

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.

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.

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.

The relevant Executive Director for the review is the Director of Finance.

1.2 The potential risks considered in the review were as follows:

- poor or non-existent stewardship in relation to cyber security;
- failure to ensure that structures are developed to enable compliance with regulations e.g., NIS Regulations; and
- loss of data or services and inappropriate access to information.

1.3 We note that the purpose of the audit is to provide assurance on the processes within the Health Board for assessing its current position in relation to cyber security and developing an improvement plan that will address the key identified weaknesses. This internal report does not assess the current state of cyber security within the organisation and this function is the responsibility of the Cyber Resilience Unit within DHCW.

2. Detailed Audit Findings

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

2.1 In January 2018, Stratia Consulting undertook an external cyber security assessment within the Health Board. As part of this, a NIS Directive readiness assessment was undertaken, which identified that further work was required to ensure compliance with the NIS Regulations. A summary report and improvement plan were published following the assessment, which the Health Board's Digital Team, together with DHCW, have been successfully working on to enact in preparation for the NISR self-assessment.

2.2 The Health Board commissioned a qualified and independent Cyber Security Consultant from a Professional Services consultancy, to complete the NIS Cyber Assessment Framework (CAF) on their behalf. As part of the NISR process, they conducted a series of interviews with Heads of Services to establish the assets that are critical to the provision of their services. A Critical Asset Register has been developed for each service area and details captured include:

- Information Asset Type (electronic file, application, platform etc.);
- Information Asset Data Type (personal or personal sensitive data, clinical safety, financial data etc.);
- Criticality (high, medium, low);
- Maximum Tolerable Outages (hours, days, weeks); and
- Recovery Point Objectives (the maximum amount of data, as measured by time, that can be lost after a recovery from a disaster, failure, or comparable event before data loss will exceed what is acceptable to the Health Board.)

Further analysis is currently being undertaken to build a complete Critical Asset Register for the Health Board, which includes assessments against each asset to identify the supporting infrastructure including make, model, location, support, and backup arrangements.

2.3 In addition, the Cyber Security Consultant held interviews with Executives, General Managers, Business Leads and DHCW Cyber Specialists and reviewed all relevant documentation including:

Board Minutes
Risk Registers
Information Governance & Security Policies
Data Protection Impact Assessments
Information Asset Registers
Business Continuity Plans
Audit Reports

Training materials
Employment contracts
Supplier contracts
Service Level Agreements
Technical documentation
System Reporting

2.4 Records of interviewed personnel, information captured, and documentation have been maintained throughout the process for future iterations of the CAF assessment.

Conclusion:

2.5 A comprehensive process was undertaken by the Health Board to ensure the self-assessment was completed accurately with appropriate evidence maintained. Consequently, we have concluded **Substantial** assurance for this objective.

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

2.6 As part of this review, we conducted interviews with the Cyber Security Consultant, Digital Director and Deputy Digital Director, and reviewed information reported to the Information Governance Sub-Committee (IGSC).

2.7 Prior to the submission of the CAF to the NHS Wales Cyber Resilience Unit, hosted within DHCW, it was reviewed internally by the Digital Director and Deputy Digital Director and confirmed as accurate. In an IGSC update report dated 3 December 2021 presented to the Sustainable Resources Committee (SRC), it was confirmed that the sub-committee agreed that the assessment represented an accurate position for the Health Board.

2.8 We reviewed a sample of three objectives within the completed CAF to ensure appropriate scoring:

- B3.d Mobile Data;
- B3.e Media/Equipment Sanitisation; and
- B5.c Backups.

The corresponding Health Board statements were an accurate reflection of current position, and we were able to determine the evidence from the information capture record.

Conclusion:

2.9 Our review of the CAF found the self-assessed position to be accurate and supported by appropriate evidence., consequently we have concluded **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.

2.10 Following the submission of the CAF, the Cyber Security Consultant together with the wider Digital Team, immediately embarked on a gap analysis to identify recommendations to reach an 'achieved' status in each of the CAF objectives. The recommendations and CAF results were then used to classify ten high-level Cyber Security risks to the Health Board.

2.11 In December 2021, the IGSC supported the implementation of a Cyber Security Programme, a business-facing work programme resulting from the gap analysis work, which seeks to implement the necessary risk control measures and organisational changes required to comply with the NIS Regulations.

2.12 The comprehensive Cyber Security Programme includes fourteen workstreams, each with identified owners and leads to take forward the associated key project steps in addition to required technologies and/or resources. Required Capital Expenditure and Operating Expenses investment details have also been captured. The Programme will be led by a Programme Manager supported by three full-time Project Managers, and will report to the Cyber Security Programme Board, who will be accountable to the IGSC.

2.13 At the time of this review, the definition of the programme is complete and fully costed and is due to be presented to the IGSC for approval. The Cyber Security Consultant will shortly be presenting an SBAR to the Board, outlining the programme's details.

Conclusion:

2.14 The Cyber Security Programme is detailed and realistic in its approach and we note the significant amount of work and effort undertaken to address and improve the Health Board's 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.

2.15 Our review highlighted continued comprehensive and timely reporting of the NIS Directive to the IGSC by the Digital Team. It became a standing agenda item for meetings and updates have been received regarding progress made with the self-assessment, identified gaps in compliance and recommended improvements. Evidenced by agendas, papers and meeting minutes, the sub-committee continues to monitor progress made against recommendations and will shortly receive the completed Cyber Security Programme for approval.

2.16 We noted detailed updates pertaining the NIS Directive were provided by the IGSC to the Sustainable Resources Committee (SRC) since its establishment in July 2021 and to the former People, Planning and Performance Assurance Committee (PPPAC) from April 2021 to June 2021. Whilst the Statutory Committees were apprised, the NIS Directive was not communicated to the Board via the Statutory Committees Update Reports until January 2022, and we further noted insufficient information contained within. We learned from interviews with the Digital Director, Deputy Digital Director and Cyber Security Consultant that this matter is being addressed and the Board will shortly receive the completed Cyber Security Programme with an accompanying SBAR to fully apprise them of the NIS Regulations and improvement plan. See **Matter Arising 1** in Appendix A.

2.17 Whilst we established that a risk relating to Cyber Security is included on the Corporate Risk Register, *Risk 451 – Cyber Security Breach* was drafted following the WannaCry cyber-attack in May 2017 and does not refer to the NIS Regulations. In an update report to IGSC in October 2021, risk 451 was recognised as being focussed on the impact of outdated patching of desktops/laptops and server infrastructure rather than a more general risk around Cyber Security which incorporates compliance with the NIS Regulations. At the time of this review, work has been completed to reframe the risk as part of the Cyber Security Programme. See **Matter Arising 2** in Appendix A.

Conclusion:

2.18 The IGSC has continued to have a clear focus on the NIS Directive, self-assessment, and improvement plan and has appropriately reported to the Statutory Committees, however, the absence of communications to the Board on a legislative matter requires attention, particularly due to the potential to receive Revenue / Budget fines for non-compliance. Noting the work undertaken to date by the Digital Team and Cyber Security Consultant as noted above, we have concluded **Reasonable** assurance for this objective.

Appendix A: Management Action Plan

Matter Arising 1: NIS Directive Governance (Operation)	**Impact**
Our review highlighted a lack of communication with the Board on the NIS Directive legislation and the potential to receive fines for non-compliance. We note that the Digital Team and Cyber Security Consultant have undertaken significant work to develop a fully costed Cyber Security Programme and the Board will shortly be receiving full information on the current position of the Health Board and required steps towards its improvement.	Potential risk of: • poor or non-existent stewardship in relation to cyber security; and • failure to ensure that structures are developed to enable compliance with regulations e.g., NIS

Recommendations	**Priority**
1.1 Management should report the NIS Directive to the Board in a private session due to the risk of sharing cyber security details in the public domain, and ensure that members are presented with information including, but not limited to: • NIS Directive and Health Board requirements as an Operator of Essential Services (OES); • Repercussions of non-compliance including potential fines; • Current compliance position of the Health Board; and • Cyber Security Programme.	**Medium**
1.2 Management should ensure that the Board is apprised of wider Cyber Security matters and incidents in a timely manner through appropriate Statutory Committees.	**Medium**

Agreed Management Action	**Target Date**	**Responsible Officer**
1.1 As part of the NIS Directive compliance, an 18-month programme is in development. One of key elements is the requirement for each Board Member to be aware of Cyber Security issues, and as such a suitable Board Seminar session is under discussion with the Board Secretary.	August 2022	Board Secretary / Director of Finance / Digital Director

1.2 Under the auspices of the Information Governance Sub-Committee (IGSC) a specific group has been formed to drive through the Cyber Work Programme. Reports from this Group will be considered by IGSC, and updates presented to the Executive Team, and via the standing agenda item on the Sustainability Resources Committee (SRC). Where applicable information will be passed onto the Board via the committee update or by exception. Please note that specific details of cyber threat issues will be considered as part of the in-committee section of the Sustainability Resources Committee and Board due to their sensitive nature.	Complete	Director of Finance / Digital Director

Matter Arising 2: Cyber Security Risk (Design)	**Impact**
Whilst we established that a risk relating to Cyber Security is included on the Corporate Risk Register, *Risk 451 – Cyber Security Breach* was drafted following the WannaCry cyber-attack in May 2017 and does not refer to the NIS Regulations.	Potential risk of: • poor or non-existent stewardship in relation to cyber security; and • failure to ensure that structures are developed to enable compliance with regulations e.g., NIS Regulations.

Recommendations	**Priority**
2.1 Management should ensure that the current Cyber Security Risk (Risk 451) included within the Corporate Risk Register is reframed to reflect the high-level risks identified from the self-assessment process.	**Medium**

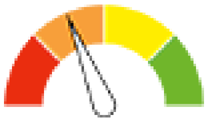
Agreed Management Action	**Target Date**	**Responsible Officer**

2.1	A new Risk has been added to the Corporate Risk Register (1352)	Complete	Digital Director

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.

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

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