

Network and Information Systems (NIS) Directive

Final Internal Audit Report

April 2022

Swansea Bay University Health Board

NWSSP Audit and Assurance



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



Bwrdd Iechyd Prifysgol
Bae Abertawe
Swansea Bay University
Health Board



Contents

Executive Summary.....	3
1. Introduction	4
2. Detailed Audit Findings	5
Appendix A: Management Action Plan	8
Appendix B: Assurance opinion and action plan risk rating	10

Review reference:	SBU-2122-005
Report status:	Final
Fieldwork commencement:	26 January 2022
Fieldwork completion:	11 February 2022
Draft report issued:	01 April 2022
Debrief meeting:	05 April 2022
Management response received:	19 April 2022
Final report issued:	25 April 2022
Auditors:	Simon Cookson, Director of Audit and Assurance, Martyn Lewis, IT Audit Manager, Sian Harries (IM&T Audit Manager)
Executive sign-off:	Matt John (Director of Digital)
Distribution:	Gareth Westlake (Digital Services Business Manager), Gareth Ayres (Cyber Security Manager), Chris Phillips (Deputy Cyber Security Manager)
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 Swansea Bay 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

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

Matters arising concerned areas for refinement and further development:

- No retention of supporting information provided to the Cyber Resilience Unit as part of the CAF process.
- Improvement action plan has not yet been developed.

Report Classification

		Trend
Reasonable	Some matters require management attention in control design or compliance.	N/A
	Low to moderate impact on residual risk exposure until resolved.	First Review

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	Reasonable
4 Governance	Substantial

Matters Arising

		Assurance Objective	Control Design or Operation	Recommendation Priority
1	Supporting information retention	1	Operation	Medium
2	Improvement Action Plan	3	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 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 is the Network and Information Systems Regulations of 2018 (NIS Regulations), transposed into UK law in May 2018 from the EU Security of Networks and Information Systems (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 Regulations 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. It is 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.

- 1.2 The potential risks considered in the review are as follows:

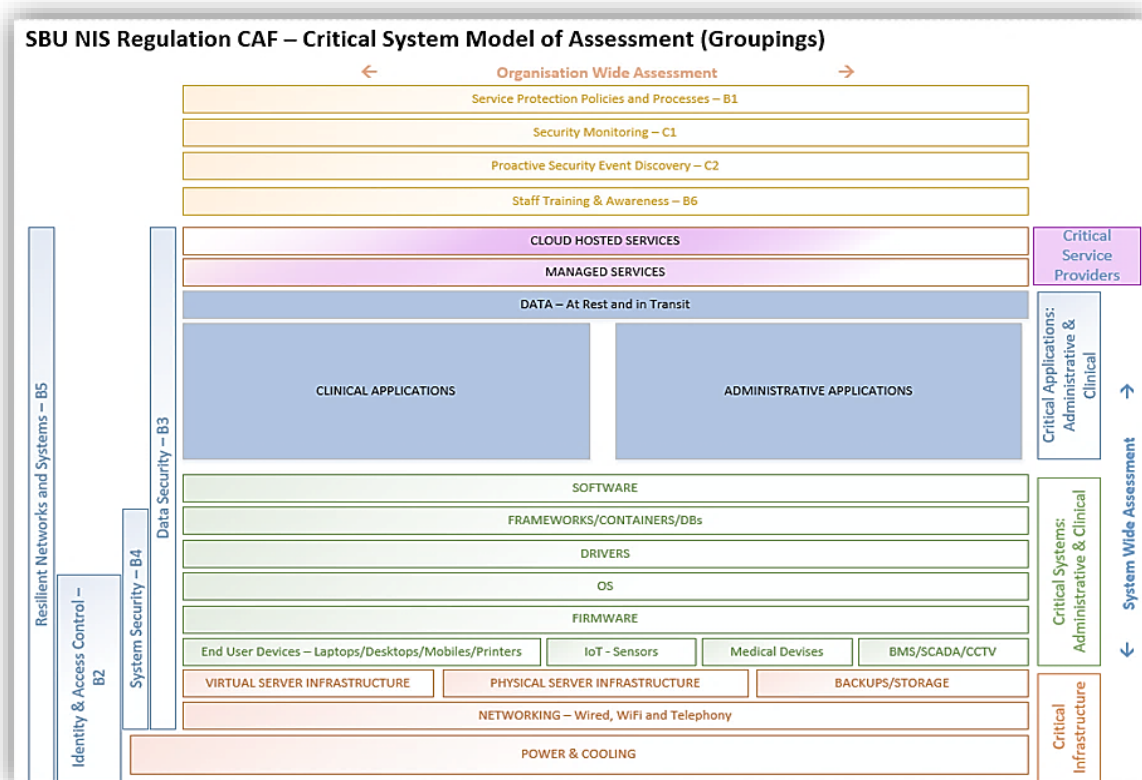
- poor or non-existent stewardship in relation to cyber security;
- failure to comply with regulations; and
- loss of data or services and inappropriate access to information.

- 1.3 We note that the purpose of the audit is to provide assurance on the processes within Swansea Bay University Health Board ('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 report does not assess the current state of cyber security within the organisation, this function is the responsibility of the Cyber Resilience Unit (CRU) 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 July 2020, the Audit Committee and Board received a Cyber Security Update Report to inform members of the NIS Regulations and pending Cyber Assessment Framework (CAF) the following year. The reports set out the preparatory work being undertaken in order to achieve compliance with the NIS Regulations. They outlined the technical and governance arrangements put in place in addition to further planned controls such as recruitment, national tools, and system updates. In July 2021, the Audit Committee was informed of the formal commencement of the NIS Regulations assessment and the forthcoming Board development session to present the National Cyber Security Centre (NCSC) Board Toolkit to encourage engagement.
- 2.2 The health board's Cyber Security Team undertook the completion of the CAF. Initial steps involved a 30-day engagement exercise with the CRU and scoping the key contacts within the health board, including critical system owners and leads of specialist areas. Once identified, the Cyber Security Team gave presentations to over thirty service areas, to introduce the NIS Regulations and the expected requirements.
- 2.3 Following the presentations, a '*Critical Scoping Capture Questionnaire*', reflecting the national requirements, was disseminated to each lead to identify critical clinical and administrative services. An assessment of those services was undertaken, including functions and sub-functions, in order to categorise related and connected systems. These were then modelled into groups, aligned with the NIS CAF objectives as below:



- 2.4 We were informed by the Cyber Security Manager and Deputy Cyber Security Manager that information to support each CAF objective was provided through discussions with the CRU via Microsoft Teams calls. The CRU did not specifically request evidence in the form of documentation as part of the assessment. However, we noted that records of the discussions and information provided have not been retained. Furthermore, we noted that several question marks appear throughout the final CAF, where further clarification was sought from the CRU prior to deciding whether an objective was achieved or not. However, the CAF was not subsequently updated accordingly. 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:

- 2.5 Our review highlighted the significant work undertaken by the Cyber Security Team to prepare for and complete the self-assessment. However, 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.

- 2.6 As part of this review, we conducted interviews with the Cyber Security Manager and Deputy Cyber Security Manager. Prior to the submission of the CAF to the CRU, it was reviewed internally by the Digital Operations Team, Cyber Security Team and Assistant Director of Digital Technology.
- 2.7 During this review, as noted above, there was no retention of evidence and so we were unable to appropriately evaluate the health board's self-assessed position. However, we tested a sample of three objectives within the CAF to ensure appropriate scoring and discussed the position and the evidence that was originally provided:
- B3.a.7 Data Security
 - B2.a.5 Identity and Access Control
 - B1.a.6 Function Protection Policies and Processes

Using our professional judgement, information gleaned from interviews and update reports, we consider the self-assessment to be an accurate reflection of the health board's current cyber security position.

Conclusion:

- 2.8 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 concluded **Substantial** assurance for this objective.

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

- 2.9 Whilst we were informed that a formal improvement action plan is not yet in place due to the health board receiving advice from the CRU to await the outcome of the

CAF, the Cyber Security Team has made progress by identifying improvement objectives. Whilst no urgent remedial work was identified when undertaking the self-assessment, the Cyber Security Team have moved forward the areas highlighted where improvements could be made. For example, raising awareness of cyber security within the health board through phishing campaigns. **See Matter Arising 2 at Appendix A.**

- 2.10A private session was held with the Board in October 2021. Members received a presentation from the Assistant Director of Digital Technology, Cyber Security Manager and a representative from the National Cyber Security Centre on the NIS Regulations and wider cyber security matters. Details of the assessment against the NIS CAF were presented with identified high-level remedial actions.

Conclusion:

- 2.11Initial progress has been made to identify gaps in compliance and recommendations to improve current cyber security position. Whilst the Cyber Security Team are awaiting feedback from the CRU prior to developing a full improvement plan, Welsh Government guidance states that Operators of Essential Services will need to propose appropriate measures for improvement, and it will be for the CRU and Welsh Ministers to determine their sufficiency. Consequently, we have concluded **Reasonable** assurance for this objective.

Objective 4: there is a mechanism in place to provide assurance to the Board that appropriate action is being taken in relation to cyber security.

- 2.12Our review highlighted the continued comprehensive and timely reporting of cyber security, including the NIS Regulations, to appropriate groups, committees, and the Board.
- 2.13We reviewed a sample of papers from the Digital Services Management Group, Information Governance Group and Audit Committee and can confirm Cyber Security Reports are received regularly. The reports provide the health board's current cyber security position and that of NHS Wales, and details of improvement work being undertaken.
- 2.14A high-level cyber security risk was captured on the Health Board Risk Register in July 2019 and has been appropriately updated to include the NIS Regulations. The Board was kept apprised of the NIS Regulations, including via the update report from the Cyber Security Team in July 2020 noted under objective 1 above. The report comprehensively covers the cyber security risks facing the health board and NHS Wales as a whole, and provides an update on the controls, resources and systems put in place to not only comply with the NIS Regulations, but to also improve the effectiveness of cyber security services in general.

Conclusion:

- 2.15Our review highlighted an appropriate governance structure in place to assure the Board of the work undertaken as part of the NIS Directive and wider cyber security matters. Consequently, we have concluded **Substantial** assurance for 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. Several instances of question marks were noted within the final CAF where clarification was sought from the CRU, however, the CAF was not then updated accordingly.		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 Agreed. This will be discussed at the next CRU assessment (tbc). Audit notes are normally recorded by the auditor and a suitable mechanism will be agreed with the CRU for example if via Teams then these will be recorded.	31/12/2022	Gareth Ayres Cyber Security Manager

Matter Arising 2: Improvement Plan (Design)		Impact
<p>Whilst we were informed that a formal improvement action plan is not yet in place due to the health board receiving advice from the CRU to await the outcome of the CAF, Welsh Government guidance states that Operators of Essential Services will need to propose appropriate measures for improvement. We noted that improvement objectives have been identified following the completion of the self-assessment, however, an improvement action plan has not yet been developed.</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.
Recommendations		Priority
<p>2.1 Management should ensure that an improvement action plan is developed promptly in order to avoid delays in implementation.</p>		Medium
Agreed Management Action	Target Date	Responsible Officer
2.1 Agreed. This is being worked on.	31/05/2022	Gareth Ayres Cyber Security Manager

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](#)