NIS Directive (Cyber Security)
Final Internal Audit Report

May 2022

Cwm Taf Morgannwg University Health Board

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

GIG CYMRU NHS WALES
Bwrdd Iechyd Prifysgol Cwm Taf Morgannwg University Health Board

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 14

Review reference:	CTMU-2122-23
Report status:	Final
Fieldwork commencement:	28 February 2022
Fieldwork completion:	25 April 2022
Debrief meeting:	27 April 2022
Draft report issued:	3 May 2022
Management response received:	13 May 2022
Final report issued:	16 May 2022
Auditors:	Murray Gard – Audit Manager Martyn Lewis – IT Audit Manager
Executive sign-off:	Stuart Morris – Director of Digital
Distribution:	Andrew Nelson – Chief Information Officer & SIRO Paul Chilcott – Head of Server Management & Chief Cyber Officer
Committee:	Audit and Risk 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, Finance & Risk 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 Cwm Taf Morgannwg 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-D (Network and Information Systems Directive) in the Health Board, including the Cyber Assessment Framework (CAF), improvement plan and overarching governance.

Overview

We have issued Reasonable assurance on this area. The Health Board has applied rigour and appropriate resource to the self-assessment process. It was in regular contact with the Cyber Resilience Unit (CRU) to ensure transparency, noting the subjective nature to aspects of the CAF.

The matters which require management attention include:

- Partial retention of supporting information maintained, as part of the CAF assessment.
- Improvement actions require refinement with Specific Measurable Agreed Realistic and Timely (SMART) targets.
- The operational risk register does not articulate the cyber security risk associated with the NIS-D.

Report Classification

Reasonable

Some matters require management attention in control design or compliance.

Low to moderate impact on residual risk exposure until resolved.

Assurance summary[1]

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

[1]The 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
2	Assessment evidence	1	Operation	Medium
2	Improvement plan	3	Operation	Medium
3	Reporting and risk	4	Operation	Medium

1. Introduction

1.1 Our review of the Network and Information Systems (NIS) Regulations (the 'Regulations') was completed in line with Cwm Taf Morgannwg University Health Board's (the 'Health Board' or the 'organisation') Internal Audit Plan for 2021/22. The review sought to provide the Health Board 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, their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

1.3 The Regulations are a core piece of legislation relating to cyber security and was brought 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 European Union.

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 them from attack, detect potential intrusions, and react appropriately when intrusions occur.

1.5 Although cyber security is not a devolved matter, the 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 the 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. Individual NHS organisations which fall within scope must adopt and comply with these arrangements.

1.7 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 as the 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 The Health Board engaged with the CRU via workshops and multiple discussion to gain a better understanding of the process prior to completing the CAF.

2.2 The Information and Communication Technology (ICT) department has set up a Cyber Security team within the existing structure. It is acknowledged by the department that there are some gaps within this team, specifically for clinical

devices, and ICT systems. The department commissioned a Target Operating Model review in 2019 and this is incrementally being implemented; this covers some areas of cyber responsibility. Whilst noting the resource constraints, developing the CAF self-assessment involved multiple individuals and experts that contributed to its completion over a two-month period; this included the Chief Information Officer and Head of service management etc.

2.3 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, and as such the assessment responses do not have supporting information to explain how the judgement was derived, or where evidence may be found.

2.4 The national guidance states that 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 particularly if key individuals leave the Health Board. **See Matter Arising 1 at Appendix A.**

Conclusion:

2.6 Significant work was undertaken to prepare and complete the self-assessment. However, evidence and records of discussions have not been retained for future iterations of the CAF. We have provided **reasonable** assurance for this objective.

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

2.7 We note above that evidence was not retained during the self-assessment process so we were unable to fully evaluate the Health Board's self-assessed position. However, we tested a sample of four objectives within the CAF to ensure appropriate scoring, and discussed the position with management. The four objectives related to:

- A1.a Board Direction:
- A1.b Roles and Responsibilities:
- B3.d Mobile Data; and
- C1.b Securing Logs.

2.8 Using our professional judgement, information gleaned from interviews and update reports, we considered the self-assessment to be an accurate reflection of the Health Board's current cyber security position. We note some minor areas where the assessment did not fully reflect the narrative, however the basis of the assessed position was discussed and agreed between the CRU and the Health Board.

Conclusion:

2.9 Whilst we consider the self-assessed position to be accurate, we were unable to verify this through documented evidence. However, our discussions with management 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.

2.10 A formal improvement action plan has been developed following the CAF, although due the timing of our fieldwork we did not look at the implementation. The improvement plan not only highlights gaps in the CAF, but also combines and map's themes with actions arising from other cyber security toolkits, such as the Cyber Essential toolkit. However, further enhancements and refinements are suggested to make the action plan more specific, measurable, agreed, realistic and timely (SMART). **See Matter Arising 2 at Appendix A.**

Conclusion:

2.11 Initial progress has been made to identify gaps in compliance and recommendations to improve the current cyber security position. Welsh Government guidance states that Operators of Essential Services will need to propose appropriate measures for improvement, and it will be for the CRU to determine their sufficiency. Consequently, we have concluded **Reasonable** 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.

2.12 The Health Board has delegated assurance and responsibility for cyber security to the Digital and Data Sub Committee, to allow greater time and depth of the cyber issues to be considered. The Terms of Reference for the committee was reviewed in March 2022 and noted that cyber security would be monitored as part of the committee's duties.

2.13 The Senior Information Risk Officer (SIRO) was not at Board level at the time of fieldwork; although we note that a Director of Digital has since been appointed. We also note that security of critical systems is reported at the Digital and Data Committee at which the SIRO, Caldicott Guardian and other key staff all attend.

2.14 The SIRO has accountability for data protection and information risk, and delegates relevant technical / professional cyber matters to the Cyber Manager.

2.15 The operational and tactical security of critical systems is managed at the Risk Audit Governance and Cyber Security Board (RAGCSSB) and is informed by expert internal guidance. There are sub-groups in place such as the Cyber Group and Operational Risk Group that inform the RAGCSSB.

2.16 In addition, there is a risk relating to cyber security on the organisation risk register, which is monitored and updated on a regular basis at the Digital and Data Committee. However, this does not fully articulate the risk associated with cyber security and does not consider the potential for significant financial penalties for non-compliance. In addition, the operational risk register held by ICT does not fully underpin the corporate level risk. **See Matter Arising 3 at Appendix A**

Conclusion:

2.17 There was regular reporting of cyber security to the Digital and Data committee as part of the risk management framework, and also within other formal reports. The action plan, following the NIS-D self-assessment/ report from the CRU, is still

evolving. While there was little evidence of active monitoring at the time of our fieldwork, there are clear structures in place to allow this to occur. Accordingly, we have provided **reasonable** assurance over this objective.

Appendix A: Management Action Plan

Matter Arising 1: Assessment Evidence (Operation)	**Impact**
Developing and completing the CAF self-assessment process involved multiple individuals and experts within the Health Board, that contributed to its completion over a two-month period, including: • Chief Information Officer, • Head of Service Management, • IT security Manager, and • Cyber Security Officer. We note that the process takes time and interpretation of the questions can be subjective. Through our review, the Health Board were trying to be open and transparent regarding their cyber security position, however, we note that there was no plan in place as to when other critical systems would be mapped against the CAF. We note that the CAF assessment responses did not have supporting information to explain how the judgement was derived, or where evidence may be found. The national guidance states that 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 particularly if key individuals leave the Health Board.	Potential risk of: • poor or non-existent stewardship in relation to cyber security.
Recommendations	**Priority**
1.1 Management should have plans in place to map other critical systems to the CAF. 1.2 Management should ensure that any records of discussions and information pertaining to the CAF are captured for future annual self-assessments.	**Medium**

Agreed Management Action	Target Date	Responsible Officer
Agreed A process for baselining and ensuring that all critical systems that the UHB actively supports have cyber and data protection improvement plans plus documented backup and disaster recovery programmes has been agreed and initiated. The UHB will be taking a pragmatic approach in that the documentation will incorporate that required to operationally support the systems and provide on-call services. Incident response and business continuity plans already in place in the clinical services will be attached to these documents within a central 'asset register / service catalogue'	Commenced 9th May 2022 Attempting to follow a rolling programme whereby 1 system is updated each week and cyber impact assessments undertaken	SIRO, Head of Server Management & Head of Clinical Systems

Matter Arising 2: Improvement Plan (Operation)	**Impact**
In March the Health Board developed an improvement plan. This was linked to the gaps identified in the CAF submission and the report supplied to the Health Board by the CRU in February 2022. The recommendations have been assessed as either Local or national level, however, the enhancements below would make the action plan more specific, measurable, agreed, realistic and timely. 1. The recommendations did not have target dates for the completion of tasks. 2. The ownership for the recommendations was not defined. 3. No information surrounding costs associated with the implementation of the recommendations was evident. There was also no articulation of how the Health Board would contribute to the recommendations that would be led nationally. .	Potential risk of: • poor or non-existent stewardship in relation to cyber security. • failure to comply with regulations such e.g., NIS Regulations
Recommendations	**Priority**
2.1 Management should ensure that the improvement action plan is further developed to avoid delays in implementation.	**Medium**

Agreed Management Action	Target Date	Responsible Officer
Management response: The final quarter of 2021/22 was used by the UHB to implement numerous improvements to the digital estate which incorporate improving our cyber posture, in line with our existing outline cyber improvement plan and the requirements of NIS-D. A costed schedule of cyber improvements has been provided and is being considered by the board as part of our overarching annual plan. The overarching plan will be a living document and will increasingly have timescales, actions and responsible individuals added. This is considered a key requisite as the plan is dependent upon the wider NHS and also funding from DPIF (WG) which has been heavily reduced over the past 8 weeks due to forecast expenditure being greater than budget in other areas of the department.	High level action plan with dates and owners to be considered for approval by DDB in June 2022	SIRO / Head of Server Management

Matter Arising 3: Reporting and Risk (Operation)	**Impact**
Eight risks are assigned to the Digital and Data subcommittee as the 'assuring committee'. These form part of the corporate risk register, which are reviewed and updated at each meeting. One of these (Datix entry 4664) relates to cyber security *"Ransomware Attack resulting in loss of critical services and possible extortion".* As part of the action plan to mitigate the risk that was discussed at the March 2022 meeting, there is reference to the NIS directive as below. *"CTMUHB is amalgamating the issues arising from the Cyber Essentials plus, the NIS-D assessment and the NCSC board framework in a single plan. Elements of this need to be taken forward at the UHB level, others nationally. - Timeframe: Quarterly updates".* "No change to risk updates or mitigation at this point, however, the Digital team have agreed to break this risk down in to component parts. These risks will eventually replace the current risk. This review is in progress with an update by the 30.04.2022." Once expanded, the above would highlight good practice to ensure the profile, and potential financial penalties associated with non-compliance of the NIS-D, are raised at a strategic level. ICT also has an operational risk register, but we note no risk that underpins the corporate risk, specially referencing the NIS -D.	Potential risk of: • poor or non-existent stewardship in relation to cyber security. • failure to comply with regulations such e.g., NIS Regulations
Recommendations	**Priority**
3.1 Management should ensure that the NIS–D is risk assessed and if appropriate, added to the relevant risk register.	**Medium**

Agreed Management Action	Target Date	Responsible Officer
The risk register is regularly refreshed, especially in light of the ever changing guidance being received form the NCSC as the environment develops relating to the Russian invasion of Ukraine.	May 2022	SIRO & Head of Server Management

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