Cyber Security
Internal Audit Report

December 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

Review reference:	CTM-2223-20
Report status:	Final
Fieldwork commencement:	26 September 2022
Fieldwork completion:	05 November 2022
Draft report issued:	16 November 2022
Management response received:	01 December 2022
Final report issued:	02 December 2022
Auditors:	Kevin Bridgman, IT Audit Manager Martyn Lewis, IT Audit Manager
Executive sign-off:	Stuart Morris, Director of Digital
Distribution:	Andrew Nelson, Chief Information Officer Andrew Elliot, IT Security Manager
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 and 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

To ensure that the organisation is working to improve its cyber security position, and that appropriate reporting is in place that shows the current status.

Overview

There is a cyber security improvement plan in place, and progress is being made, although we note slippage due to resource constraints. There is a reporting structure which enables progress and risks to be escalated to committee level, and backups are securely stored and tested.

The key matter requiring management attention is that there is a need to give consideration of including security KPIs within committee reporting.

Further matters arising concerning the areas for refinement and further development have also been noted (see Appendix A).

Report Opinion

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

Assurance summary[1]

Objectives		Assurance
1	Improvement Plan Progress	Reasonable
2	Reporting arrangements	Substantial
3	Back-up testing and security	Substantial

Key Matters Arising

		Objective	Control Design or Operation	Recommendation Priority
1	KPI reporting	1	Operation	Medium

1. Introduction

1.1 In line with the 2022/23 Internal Audit Plan for Cwm Taf Morgannwg University Health Board (the 'Health Board' or 'organisation') we have reviewed cyber security.

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 Core pieces 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 Security of Networks & Information Systems (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 legislation is the aim to drive improvement in the protection of 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, Welsh Government (WG) is the 'competent authority' for the NIS regulations 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. DHCW 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. Individual Trusts and Health Boards which fall within scope must adopt and comply with these arrangements.

1.7 Following an assessment against the Cyber Assurance Framework (CAF) in the previous year, all organisations should have an improvement plan in place, and be working to improve their cyber security position.

1.8 Risks identified in our audit brief were:

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

1.9 Our audit was a review of the processes in place for the delivery of the cyber security improvement plan and the reporting structures. We have not assessed the cyber security status of the Health Board as part of this review.

2. Detailed Audit Findings

The table below summarises the recommendations raised by priority rating:

	Recommendation Priority			Total
	High	Medium	Low	
Control Design	-	-	-	-
Operating Effectiveness	-	1	1	2
Total	**-**	**1**	**1**	**2**

Objective 1: Appropriate progress has been made against cyber improvement plans, and the cyber security position within the organisation is improving.

2.1 The organisation has established a Cyber Security Improvement Plan (the plan). The plan uses the NIST framework for cyber security and includes the identified actions from the previous CAF assessment, along with requirements from Cyber Essentials+ (a cyber security certification scheme).

2.2 The plan represents a significant amount of work and contains a large number of actions to be undertaken. The actions within the plan are assigned to named individuals and have targeted dates, along with an indication of priority.

2.3 The cyber improvement plan shows progression against the actions. In particular there has been a focus on user awareness and training.

2.4 We reviewed progress against a random selection of improvement actions, and it was evident progress is being made on several fronts. However, we note that there are areas of slippage, with some actions not on target, although work is ongoing to address these. The slippages against the plan are mainly due to resource considerations.

2.5 The actions undertaken within the plan are resulting in an improved cyber security position within the organisation, for example:

- Reviewing and improving firewall rulesets, although we note that documentation surrounding this process has not yet been fully defined.
- Migrated servers to Trend Micro for anti-malware protection.
- Work is ongoing to identify all systems in order to undertake NIS CAF part B and C assessments.
- There is a detailed Cyber Incident report plan and this describes the process that will be followed in the event of a cyber incident being reported to the Health Board's ICT team and escalated as necessary.

- Work is ongoing to develop a business case to better enable secure management of endpoints (the physical devices that connect to the network).
- Phishing simulation software has been obtained in order to get a base line on staff awareness to cyber security and phishing.

Conclusion:

2.6 The Health Board has a cyber improvement plan in place and good progress is being made, with improvements in the organisation's cyber security position. We note that there has been some slippage due to resource constraints, but work continues on all the identified actions, accordingly we have provided reasonable assurance over this objective.

Objective 2: There is appropriate reporting on cyber security, which presents an accurate picture of the current position.

2.7 There is a structure for managing and reporting on cyber security within the Health Board from ICT to committee.

2.8 Within ICT, the Risk and Audit Governance, Cyber Security Board (RAG-CSB) meet bi-monthly, with regular reporting on cyber security being to this forum. This group reviews progress against the improvement plan and compliance against key cybersecurity items, with some inclusion of KPIs. (patch compliance and server updating) along with key risk indicators.

2.9 Cyber security issues are reported to the Digital & Data Committee, which includes updates on the progress against the improvement plan, along with other key items such as critical incident reports and lessons learned.

2.10 However, the security indicators noted above are not reported to the Digital & Data Committee. Reporting this information would enable members to gain a view of the current status of cyber security. (**Matter Arising 1)**

2.11 The risks associated with cyber security are considered and included on the organisational risk register, which is reviewed and discussed at the Digital & Data Committee.

Conclusion:

2.12 There is a clearly defined governance structure and reporting route through the organisation, and up to committee level. Accordingly we have provided substantial assurance over this objective.

Objective 3: Processes are in place to test back-ups and protect them.

2.13 The backup solution employed at the Health Board is supplied by Commvault and uses an immutable storage architecture. This means that back-up files cannot be overwritten, modified, or encrypted so they are read only. We note that the backup system has the ransomware protection setting 'enabled' in order to further protect the Health Board.

2.14 The backup processes make use of the virtualisation functionality and are clearly defined and well monitored. The backup process follows a rotation scheme for

backup media, in which there are three backup cycles, (daily, weekly and monthly). There are alerts raised as notifications when any issue is detected.

2.15 There is a limitation on the local retention of the data due to the physical constraints of available space. This has resulted in the Prince Charles Hospital (PCH) site only have a 14-day retention policy, while the Royal Glamorgan Hospital (RGH) site backs up less data and so has a longer retention period of 28 days.

2.16 The backup hardware is held in separate rooms from the main server hardware and are in a different fire zone and have uninterruptible power supplies (UPS) in place.

2.17 All backups are encrypted and backup tapes are removed from local sites and stored at off-site locations. For PCH they are moved to Keir Hardie Health Park, and for RGH they are moved to the Williamstown Hub.

2.1 Some data is backed up using the deduplication accelerate streaming hash (DASH). DASH copy uses network bandwidth efficiently and minimises the use of storage resources. DASH copy provides a fast method of copying data by transferring only the changed data to a secondary copy and enables faster recovery of data. Only selected data sets are backed up in this way and we note that it is the local IT server team who decide what is backed up via the DASH system. Documentation is available explaining the DASH process and what is backed up. There are plans to expand the use of DASH functionality. (**Matter arising 2)**

2.2 Backup logs are available for the process and there has been regular restore testing of the backups on random data sets. This has included both DASH and tape format with all restore tests logged. We note that Commvault also provides a disaster recovery plan which is documented and readily available to IT staff.

Conclusion:

2.3 The backup solution is well structured, well documented, operating effectively and automatically monitored. The backup files are designed to be protected from cyber threats and secure, with tapes secured off site and readily available when required for restore. There is random restore testing of backup data and outcomes are logged. Accordingly, we have provided substantial assurance over this objective.

Appendix A: Management Action Plan

Matter Arising 1: **KPI reporting** (Operation)			**Impact**
Although there is use of indicators within ICT, there is no reporting of cyber security KPIs to the Digital & Data Committee.			Potential risk of poor or non-existent stewardship in relation to cyber security.
Recommendations			**Priority**
1.	Reporting to Digital & Data Committee should be improved by inclusion of key KPIs that show the status of cyber security within the organisation.		**Medium**
Agreed Management Action		**Target Date**	**Responsible Officer**
1.1a	At the present time we consider that the level of reporting to DDC is appropriate focussing on the numerous clinical incidents and progress in mitigating and managing risk against the NIST / CRU improvement plan. We do accept that we need to improve our level of reporting in to RAGCSSB from an operational perspective as well as more tactical perspective (e.g. we would report on proportion on servers patched, switches EOL, etc into RAGCSSB, and this would inform the more strategic report into DDB & DDC.	KPI proposal drafted and considered by RAGCSSB in January 2022	Chief Information Officer

Matter Arising 2: Data selected for DASH (Operation)			**Impact**
The IT Server team has defined the data to be backed up using the DASH functionality. As this enables rapid recovery, without engaging with user departments there is a risk that the wrong data may be prioritised.			Potential risk of IT priorities being different from clinical and other department priorities.
Recommendations			**Priority**
2.1	As part of the expansion of the use of DASH, there should be engagement with user departments in order to ensure that the most valuable data be included.		**Low**
Agreed Management Action		**Target Date**	**Responsible Officer**
2.1	We agree with the need to provide proportionate protection and business continuity based on the criticality data or service. The extension of DASH will be considered and prioritised as part of the wider process for taking the forward the wider cyber improvement programme within the resources available.	Proposal for improving DASH to be prepared and to have been considered as part of the quarterly review of the cyber improvement plan progress – RAGCSSB January	Head of Cyber Security

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