# Cyber Security

# Final Internal Audit Report

January 2023

Swansea Bay 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 Bae Abertawe
Swansea Bay University Health Board

EXTERNAL • QUALITY • ASSESSMENT

# Contents

| | |
|---|---|
| Review reference: | SBU-2223-021 |
| Report status: | Final |
| Fieldwork commencement: | 11th October 2022 |
| Fieldwork completion: | 14th November 2022 |
| Draft report issued: | 1st December 2022 |
| Debrief meeting: | 9th January 2023 |
| Management response received: | 9th January 2023 |
| Final report issued: | 11th January 2023 |
| Auditors: | Osian Lloyd (Head of Internal Audit),<br>Martyn Lewis (Senior IM&T Audit Manager),<br>John Cundy (IM&T Senior Auditor) |
| Executive sign-off: | Matt John (Director of Digital) |
| Distribution: | Gareth Westlake (Assistant Director of Digital Services)<br>Carl Mustad (Assistant Director of Digital Technology)<br>Gareth Ayres (Head of Cyber, Networks & Telecommunications) |
| 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

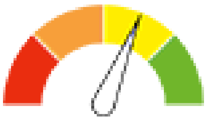
To provide assurance that the organisation is working to improve its cyber security position, and that appropriate reporting is in place that shows the current status.

### Overview

We have issued Reasonable assurance on this area. There is one matter arising which is detailed at appendix A.

- The use of the risk management process to manage the improvement plan results in some loss of clarity over timing of progress and detail of risk.

## Report Classification

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

## Assurance summary[1]

| | Assurance objectives | Assurance |
|---|---|---|
| 1 | Cyber security improvement plan progress | Reasonable |
| 2 | Cyber security reporting | Substantial |
| 3 | Backup security | Reasonable |

## Matters Arising

| | | Assurance Objective | Control Design or Operation | Recommendation Priority |
|---|---|---|---|---|
| 1 | Clear timescales to deliver improvement activities | 1 | Operation | 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.

1.2 A core piece of legislation relating to Cyber Security are the Network and Information Systems (NIS) Regulations of 2018, transposed into UK law in May 2018 from the EU Security of NIS Directive, with the intention to raise levels of cyber security and resilience of key systems across the EU.

1.3 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 both digital 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.

1.4 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.

1.5 Within NHS Wales, the Cyber Resilience Unit (CRU) hosted within 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

1.6 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 the cyber security position.

1.7 The key risk considered during the review was inadequate stewardship in relation to cyber security, which could lead to a failure to comply with NIS Regulations, resulting in a loss of data or services and inappropriate access to information.

# 2. Detailed Audit Findings

2.1 The table below summarises the recommendations raised by priority rating:

| | Recommendation Priority | | | Total |
|---|---|---|---|---|
| | High | Medium | Low | |
| Control Design | 0 | 0 | 0 | 0 |
| Operating Effectiveness | 0 | 1 | 0 | 1 |
| Total | 0 | 1 | 0 | 1 |

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

2.2 Swansea Bay University Health Board (the 'health board') manages the improvements identified from the CAF assessment through its risk management arrangements. The impact of failing to make the necessary improvements can be escalated through this mechanism, including reporting to the Board through the health board risk register, to ensure oversight sight of the requirements and the potential consequences of not taking appropriate action.

2.3 We noted a clear link between the improvement needs identified on the CAF assessment and the risks described on the health board CAF risk register, which as been created for the specific purpose of managing the CAF risks. This approach has been accepted by the CRU.

2.4 The required improvements are grouped under four digital themes: Digital Governance; Digital Identity; Secure Digital Access; Digital Incident Response and Testing, which are the four CAF objective themes. These themes are subdivided into headings which align to the CAF principles. The Digital Team describes the approach current status as '*developing funding and priorities*', and are liaising and planning with DHCW and the CRU to establish actions, timeframes and funding requirements. We consider the current position to be reasonable, given resource constraints and the complexity of the requirements.

2.5 Agreed health board developments are then run as a project and subject to standard project management disciplines and methodologies in place used by the Digital Team, including appropriate consideration of benefits, deliverables, budgets, resources, timescales etc.

2.6 The Digital Team has commented that focus on delivery dates can be unhelpful, as they can create an impression that required security improvements have been completed once a specific activity has been implemented. They wish to promote the concept that security requirements need to be managed on an ongoing basis due to the need to remain vigilant to new potential threats.

2.7 Adopting this approach to manage necessary improvements could mean that there is no defined timeframe for the delivery of improvement activities, a risk review date is not an expected delivery date.

2.8 This methodology could therefore result in required improvements remaining undelivered, with a de-facto acceptance of a risk that exceeds the risk appetite threshold, especially if they are linked to national plans, are expensive, or involve legacy system replacement. For example, an internal audit in early 2020 on the health board's Theatres Operating Management System (TOMS) raised that its core components were out of date and posed a significant security risk. The management response was to manage the issue through the risk register. Review of the risk register identified that the same security weaknesses remain. **See Matter Arising 1**

2.9 We consider the lack of a defined timeframe for delivery also makes it necessary to expand the detail on the potential impacts of risks 'materialising' and becoming an incident. For example, in relation to the health board's CAF risk register item: '*Major Impact from System Downtimes and Security Breaches*'. Whilst it is appropriate for the health board to focus on critical systems, this should be expanded to include all systems, and the likely 'achievable' recovery time and data recovery points for these should be reviewed, especially in light of lessons learned from recent cyber incidents in the field of digital healthcare.

2.10 These impacts then need to be cascaded to all system user groups, to enable them to liaise with emergency planning teams as necessary, and update resilience and continuity plans accordingly. For example, the Digital Team should recognise the potential impact of unauthorised administrator access on the backup files (see objective 3). **See matter Arising 1**

### Conclusion:

2.11 Since completing the CAF assessment return, the health board has clearly defined and documented a series of objectives that it needs to achieve to improve its cyber security position. Although the improvement activity is at an early stage, and there is a lack of a defined timeframe for all the objectives to be completed, we consider **Reasonable** assurance appropriate for this objective, at this time.

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

2.12 The Digital Team presents a '*Cyber Security Update Report*' to the Information Governance Group (IGG) at its quarterly meetings. The update report is a concise summary of the activities and the management of the identified risks relating to the field for example:

- An update on the usage of Microsoft Security Tools across Wales and the national negotiation of a new Microsoft Contract; and
- The removal of the (Russian) Kaspersky software.

2.13 We note that the reporting is appropriate in tone and detail and is presented at the IGG by the health board's senior information risk owner (SIRO), who is also the Director of Digital Services. These reports are also discussed within the Digital Directorate at the Digital Services Management Group (DSMG).

2.14 As noted under objective 1 above, cyber security threats are managed through the health board's risk management processes. There is a defined risk management hierarchy which monitors risks monthly, or more often as considered necessary, dependent on the level of the risk.

2.15 There is one cyber security risk at corporate level, as well as four at DSMG level, one for each theme, and ten within the Digital Directorate, one for each CAF contributing outcome.

2.16 Operational level risks which contribute to the ten contributing outcome risks are owned and managed by individual teams within the Digital Directorate. They are recorded on SharePoint and are discussed as and when they meet. The Directorate Teams report to the Digital Services Risk Management Group (DSRMG) on a monthly basis.

2.17 The DSRMG can present risks for escalation to the health board risk register, through the health board's established risk management arrangements, as they deem necessary. Digital risks are typically assigned to the Audit Committee currently for oversight, with an overarching cyber security risk escalated to the health board risk register.

2.18 As well as the cyber security reports to the IGG the Digital Teams report regularly against agreed key performance indicators (KPIs), with appropriate actions taken when issues are identified. These are reported using standard data from the security software, and include the Microsoft defender vulnerability exposure scores, comparisons to similar organisations, and data on windows 10 security updates.

2.19 We note that at present there is an absence of reporting on network equipment patching. However, this is currently under review by the newly established Secure Network Group which is determining KPIs for network security. We have not therefore raised a recommendation at this time.

### Conclusion:

2.20 We consider the method and reporting lines for cyber security matters to be appropriate and consider **Substantial** assurance appropriate for this objective.

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

2.21 We noted a recent independent health check report on the '*CommVault*' backup software used by the health board, completed by 'Coolspirit', an infrastructure and security specialist company. It confirmed Commvault was currently well configured, and its operation is consistent with accepted best practice.

2.22 All backups are encrypted in storage, although they are not on immutable storage which means data could be changed or deleted if accessed inappropriately. Encryption won't necessarily stop ransomware from destroying the backups, it is recognised by the Head of Infrastructure that an administrator account being compromised could pose a significant threat.

2.23 Although there is a generic risk on unauthorised access on the CAF risk register, the potential impact on backup files of a privileged account being compromised is significantly greater than of a regular user. **See matter Arising 1**

2.24 The backup routines are monitored daily and weekly and reported through to the weekly ICT management meeting. The processes are governed by standard operating procedure documents, all failures are logged, remediation is completed and the backup is re-run.

2.25 There is a record of the partial test restores that have been carried out, at least one per month since February 2014. There is a standard operating procedure document covering the process also. These restores are usually carried out when migrating services/servers, and are considered as appropriate as regular tests of the methodology and processes. Our review of the restore records noted that there have been no failed restores, and the process is working appropriately.

### Conclusion:

2.26 We are satisfied with the testing and security of the backup processes. We note that there is still some level of risk relating to the backup files and therefore consider **Reasonable** assurance appropriate for this objective.

# Appendix A: Management Action Plan

| Matter Arising 1: Clear timescales to deliver improvement activities (Operation) | Impact |
|---|---|
| Using risk to manage necessary improvements means that planned timeframes for the delivery of activities may not be clearly defined. This may be especially true where actions include other parties, such as the improving of networks.<br>Risks have an applied score and, once assessed, will remain on the risk register until it is mitigated. This could become de-facto acceptance with potential mitigating improvements being repeatedly delayed, postponed, or reprioritised (refer to paragraph 2.8 on the TOMS system).<br>The different levels of detail on the different risk registers can mean the risk group meeting does not have the full information on a specific system issue. (refer to paragraph 2.23 on privileged access to backup files).<br>Lessons learned from recent cyber incidents suggest that the majority of recovery time objective (RTO) and recovery point objective (RPO) in use are unrealistic and cannot be achieved. This means that all system specific resilience and disaster recovery plans should be reviewed and updated. Any increase in RTO and RPO needs to be fully communicated to all system user groups so they can review and update their resilience and contingency plans as necessary. | Potential risk of:<br>• Necessary improvements never happen, and the actual risk level remains at the maximum level indefinitely. |

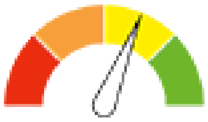
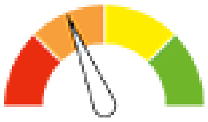
| Recommendations | Priority |
|---|---|
| 1.1 We accept that the risk owners at all levels have the information they need to manage their risks. However, as risks are aggregated though the risk management hierarchy significant amounts of detail are condensed which could result in key information being overlooked. All risk meetings should have enough detail on risks being considered, with a realistic assessment of the potential impacts of an issue arising so that any decisions regarding mitigation / acceptance are always fully informed. Any aggregated risk e.g. 'legacy systems' should be supported with comprehensive details of the systems involved with a full and realistic assessment of the potential impact of any system failure<br>1.2 If the 'preferred' mitigation is likely to be addressed well into the future, for example the risk themes require a national software defined local area network (SD-LAN), it is likely that this solution is several years away and so interim measures may need consideration. If not, then the risk will need to be 'accepted' and recorded as such. For example, the digital infrastructure team should 'accept' the risk of not having their backup files on immutable storage.<br>1.3 The impact of any risk materialisation needs fuller consideration, especially if it is to be accepted. These impacts need to be fully communicated to all user groups, so they can fully update any resilience and continuity plans. This should include realistic assessment of what can be achieved with respect to RTO and RPO. | **Medium** |

| Agreed Management Action | Target Date | Responsible Officer |
|---|---|---|
| 1.1 Implement links between Risks on Datix and Risks on Sharepoint, so the full risk detail is available at all levels of risk management. This should be in both directions. Links between CAF risks and Sharepoint Risks already implemented. | 30/06/2023 | Assistant Director of Digital Operations |
| 1.2 Use Actions and Progress Updates in Risk to review interim mitigations. | 30/06/2023 | |
| 1.3 Risks should be aligned with Services in the Service Catalogue, which should all have RTO and RPOs. These should then be clearly communicated to Service Owners. | 31/12/2023 | |

# 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.<br>**Low impact** on residual risk exposure. |
|  | **Reasonable assurance** | Some matters require management attention in control design or compliance.<br>**Low to moderate impact** on residual risk exposure until resolved. |
|  | **Limited assurance** | More significant matters require management attention.<br>**Moderate impact** on residual risk exposure until resolved. |
| | **No assurance** | Action is required to address the whole control framework in this area.<br>**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.<br>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.<br>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.<br>Some risk to achievement of a system objective. | Within one month* |
| Low | Potential to enhance system design to improve efficiency or effectiveness of controls.<br>Generally issues of good practice for management consideration. | Within three months* |

* Unless a more appropriate timescale is identified/agreed at the assignment.

GIG CYMRU NHS WALES
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]