Technical Resilience

Final Internal Audit Report

October 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

Contents

Review reference:	SBUHB-2324-19
Report status:	Final
Fieldwork commencement:	16th June 2023
Fieldwork completion:	29th August 2023
Debrief meeting:	18th September 2023
Draft report issued:	7th September 2023
Management response received:	8th October 2023
Final report issued:	10th October 2023
Auditors:	Osian Lloyd (Head of Internal Audit) Martyn Lewis (Senior IM&T Audit Manager)
Executive sign-off:	Matt John (Director of Digital)
Distribution:	Gareth Westlake (Assistant Director of Digital Services) Carl Mustad (Assistant Director of Digital Technology) Chris Dancer (Head of Infrastructure, Servers & Clients) Gareth Ayres (Head of Cyber, Networks & Communications)
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 Chartered Institute of Public Finance & Accountancy in April 2023.

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 establish and assess the organisation's position to maintain acceptable service levels through, and beyond, severe disruptions to its critical processes and the IT systems which support them.

Overview

We have issued reasonable assurance on this area.

Resilience is designed into the infrastructure provided by Digital Services, and we note recent improvements to the main site. There are weaknesses due to the network provision, however the health board is maximising the resilience available. There are instructions for restoring services in the event of a failure and the backup process is robust. We note that the resilience position is not fully tested however.

The matters requiring management attention include:

- Ensuring fire suppression is in place at key sites.
- Testing the resilience position to ensure it works as anticipated.
- Improving the documentation for disaster recovery.

Other recommendations / advisory points are within the detail of the report.

Report Opinion

Reasonable

Some matters require management attention in control design or compliance.

Low to moderate impact on residual risk exposure until resolved.

Assurance summary[1]

Objectives		Assurance
1	Design and Implementation	Reasonable
2	Resilience Testing	Limited
3	Recovery Plans	Reasonable
4	Backups	Substantial
5	Continual Improvement	Substantial

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

Key Matters Arising

		Objective	Control Design or Operation	Recommendation Priority
1	Fire Suppression	1	Operation	Medium
3	Testing	2	Design	High
4	Disaster Recovery Plans	3	Operation	High

1. Introduction

1.1 The aim of this review is to assess Swansea Bay University Health Board's ('the health board') position to maintain acceptable service levels through, and beyond, severe disruptions to its critical processes and the IT systems which support them.

1.2 In an environment where technology outages impact an organisation's ability to operate and customers require services to be 'always on', near-instantaneous recovery is often required with minimal data loss. The environment is made up of inter-related layers, each with its own risks and resilience requirements:

Infrastructure – the foundation layer consists of components such as power, network connectivity, physical security and environment controls, and data centres providing the hosting environment.

Environment – the infrastructure supports the environment and is the storage and compute functions of the systems (cloud, physical or virtual servers).

Platform – the environment supports the platform which is the operating systems, databases, and the management of storage and compute resources that host the applications.

Applications – the software tools which allow the organisation to perform its business and operational processes.

1.3 The risks considered as part of this audit are:

- Severe disruptions to critical processes and IT systems, resulting in unacceptable service levels and patient harm.
- Loss of key processing or networking services.
- Legal and regulatory breaches.
- Reputational damage and/or financial loss.

2. Detailed Audit Findings

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

	Recommendation Priority			Total
	High	Medium	Low	
Control Design	1	-	-	-
Operating Effectiveness	1	1	1	4
Total	2	1	1	4

2.2 Our detailed audit findings are set out below. All matters arising and the related recommendations and management actions are detailed in Appendix A.

Objective 1: Resilience is designed into the delivery of the technical infrastructure, the design has been enacted appropriately and applications ensure the designed resilience is utilised.

2.3 There are two dedicated teams in place for the provision and management of the core infrastructure for the health board. One team provides the virtual environment, servers, databases and Citrix environment, and the other provides the communications, network, routing and telephony.

2.4 There is no separate design team with responsibility for designing infrastructure, however the department does include a principal solutions architect role, who works with the infrastructure team to ensure that services are fit for purpose, with resilience being a factor for consideration. We also note that Digital Services has recently created a new role of network architect, which will be dedicated to design and enable a focus on this aspect of digital provision.

2.5 We also note that the Informatics Directorate includes a dedicated IT Facilities Manager, with a background in estates and with responsibility for managing the underlying building and site related infrastructure, such as power and cooling.

2.6 Infrastructure is provided in the main across two datacentres, with the main one being within Morriston Hospital. Prior to the Bridgend disaggregation, the secondary site was the Princess of Wales (POW) Hospital, however this is now moving to Neath Port Talbot (NPT) Hospital. We note that each hospital has dedicated rooms for infrastructure items relating to that site.

2.7 The Morriston datacentre has recently been upgraded to improve functionality and resilience. This was undertaken via a formal project, and the specification ensured that the site was well designed and was clear on key items that impact on resilience such as:

- requirement to move overhead water pipes and provide a raised floor;
- requirement to provide two power supplies to provide N+1 redundancy (a form of resilience that ensures system availability in the event of component failure, with components having at least one independent backup component);
- requirement for two communications routes to enable connectivity resilience; and
- requirement for each cabinet to contain two power distribution units.

2.8 We reviewed the resilience in place for the key sites within the health board and note the following.

2.9 There is uninterruptible power supply (UPS) in place for all key areas. This is centralised for Morriston with approximately two hours of supply, and rack based for the other sites with approximately 30 minutes supply. Although, over the whole estate, which includes hub rooms, we were informed that supply for some cabinets is as low as seven minutes, and there is work ongoing to upgrade these. As such, we haven't raised a recommendation on this basis.

2.10 There is cooling at each site, with Morriston having four units providing N+2 redundancy and the others having N+1. We note that an issue was raised in relation

to hub rooms, with not all containing cooling, this has resulted in some overheating in the recent hot weather which resulted in the appropriate actions being taken by Digital staff.

2.11 All areas have fire detection in place, with Morriston having gas suppression within the data centre. Other sites have no suppression, partly due to the areas having dual use for Digital Team staff. **Matter Arising 1**

2.12 There is monitoring in place for water and humidity and, in general, all areas are away from water pipes. We do note that the Morrison PBX (Telecoms) room is under the main catering unit and has had issues with water ingress, this is managed by the provision of overhead drip trays.

2.13 The health board uses Solar Winds and NetBotz software to monitor its infrastructure. These provide alerts and there is a dashboard for site monitoring, which shows the rooms monitored, the environment position and the CCTV.

2.14 Our testing of the design of applications in terms of resilience noted that resilience is designed with the following items included to varying extents:

- Geographic resilience;
- Use of load balancing and multiple servers;
- Virtualisation;
- Clustering;
- Provision of replica server and log-shipping to enable an active replica; and
- Provision of a disaster recovery environment.

2.15 We noted that there is greater resilience built in for those services defined as critical (both clinical and administrative), which confirms that the health board is focussing resources on the most valuable services.

2.16 The provision of the network enables some resilience. There is a virtual local area network (VLAN) between POW and NPT which enables full resilience, although with the Bridgend disaggregation, the health board is moving out of POW. However, the cabling / network provision between Morriston and the other hospitals has no layer 2 network, and so does not enable automatic failover and would require internet protocol (IP) readdressing.

2.17 There is extensive use of virtualisation software in order to provide resilience within each site, with VMWare in use and VSphere high availability being operational. As noted above, the lack of a layer 2 network means that there is no facility to automatically restore to an alternative site should one site fail. We note that VSphere Fault Tolerance (which provides continuous availability for applications) is not in use however, and this could be enabled to provide additional resilience for critical systems. In addition, consideration should be given to using Vcenter Site Recovery Manager to automate disaster recovery. **Matter Arising 2**

2.18 Clustering is in use, however all the physical devices are in the same chassis, as such there is a risk that losing the Morriston room will result in a loss of all services as they are within a single fault domain (a collection of functionality, services or components with a shared single point of failure). In the event of a loss of Morriston, we were informed that there is sufficient capacity to run all services from NPT,

although there may be a performance impact. As noted previously, limitations with the functionality of the network does not allow for automatic failover and so a manual process would need to be invoked, the procedures for which are discussed under Objective 3. We note that overcoming the network limitations would require significant funding, and as such we have not raised a recommendation here.

2.19 There is no formal policy or procedure statement that sets out the requirement for applications to be designed from a resilience perspective, however from our discussions we noted that staff were aware of a need to ensure resilience.

2.20 As part of the development or implementation of new services an assessment is made of the criticality of the service in conjunction with service users. The new service is then categorised accordingly, and the design and implementation processed in order to meet the agreed recovery time objective (RTO) / recovery point objective (RPO) in accordance with service categorisation.

2.21 Discussions regarding the services provided and the related resilience are held at formal meetings, in particular the Digital Project Review Group (DPRG) where services are defined and agreed, and the Digital Services Management Group. These discussions enable clarity over the resilience provided with service users.

Conclusion:

2.22 Digital Services provide the core services to the health board. These are provided using a resilient design, within the limits of the network functionality which prevents automatic failover. The core infrastructure is protected and services are implemented with resilience being considered. Improvements have been made recently, with a new data centre room and the provision of a post to maintain and monitor the physical environment, although we note that not every site has fire suppression in place. The health board uses virtualisation to enable resilience and rapid recovery of services. Accordingly, we have provided **reasonable** assurance over this objective.

Objective 2: Resilience is subject to testing at both infrastructure and application level to ensure that processes are operating as anticipated.

2.23 There is no structured process for testing the resilience of the infrastructure in order to ensure it functions as anticipated.

2.24 There is testing of some of the components as part of normal operations, with restores of virtual machines being an example. We also note that there is testing of generators, and the UPS has a self-test functionality which will trigger an alert if there is less than five minutes power provision within the battery. We also note that as part of the move into the new room in Morriston, there was a period of running from UPS which enabled a test of capacity.

2.25 There is some testing of application failover, as normal operation, and as part of provision of upgrades. We note that the Signal system (provides live patient information) had a failover test as part of the upgrade to version 3, and Chemocare (prescribing system) was failover tested as a test of principle.

2.26 However, there is no structured process for testing the resilience of the infrastructure or applications in order to ensure it functions as anticipated, and there has been no full testing of the resilience of the digital provision as a whole which would ensure that all services could be brought back, or re-provisioned from an alternative site within the timeframes defined in the service catalogue. **Matter Arising 3**

Conclusion:

2.27 Although there is some testing of the components of resilience within the health board, there has been no full test, and there is no structured programme for testing that the processes as designed work fully. Accordingly, we have provided **limited** assurance over this objective.

Objective 3: An effective and tested recovery plan which meets the business requirements should be in place.

2.28 There is a Digital Services Business Continuity Plan (BCP). This is an overarching document that sets out how Digital Services will maintain operations in the event of disruptions, including from loss of power, loss of staff, pandemic.

2.29 The BCP includes an order for restoration of services, however this is 3 years old and we note that this is currently being reviewed.

2.30 The BCP includes planning for loss of server rooms, although we note that there is limited detail for this, with an instruction to "*…use other rooms to relocate DR equipment*". We also note that as failover is not automatic, there is a need to readdress the network, however this is not clear within the BCP.

2.31 As such there is no formal Disaster Recovery (DR) plan that sets out exactly what will be done in the event of a major failure of service. **Matter Arising 4**

2.32 The health board has a good service catalogue in place, which contains key information about all systems, such as the hosting model, purpose of the system, number of users and geographical use. There is ability to drill down into each service for additional information including server information, database information and key documentation such as installation guides. We also note links to restore instructions for the backups.

2.33 The information contained within the service catalogue is sufficient to enable Digital Services staff to restore any service in the event of a failure.

2.34 Our testing of the information available in terms of DR planning noted that the information is generally in place for all systems. However, there were some gaps e.g., instructions for how to move to DR environment, database installation, or back up (BU) method.

2.35 Whilst the key information is in place, the use of this in a disaster scenario relies in the user knowing where the information is and how to use it. We note that DR plans may need to be invoked late at night, by an individual who may not be familiar with the service. Whilst Digital Services operate an on-call rota, and if necessary will declare an incident in order to bring key individuals on site, the current DR planning may lead to delays in service restoration. **Matter Arising 4**

Conclusion:

2.36 Key information about each service is recorded within the service catalogue, together with key instructions for recovery of services. We also note the existence of a BCP for Digital Services. The information is split however and may need pre-existing knowledge in order to utilise. We also note the lack of a structured, detailed plan for more extensive recovery. Accordingly, we have provided **reasonable** assurance over this objective.

Objective 4: Back ups are taken appropriately, are tested and protected from unauthorised access and change to enable resilience.

2.37 We note that backup processes have recently been covered within our 2022/23 Cyber Security internal audit report, which noted a good position with reasonable assurance being assigned.

2.38 There is a Backup Policy in place which sets out the overall aims, defines what is in place to enable backups and what is being backed up. The policy provides information on RTO / RPO and notes that the information is within the service catalogue. The policy provides some information on resilience using clusters and refers to standard operating procedures (SOP) for this and for the differing backup types.

2.39 There is a process for ensuring backups of health board data are taken, this uses the Commvault facility, with backups taken to disk and then to tape, with cross site replication in place. Backups are stored securely and are encrypted, and there is a process of monitoring the backup process and testing backups by restore to confirm their validity.

2.40 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.

2.41 The health board has had an independent health check review of the backup process, undertaken by the Cool Spirit consultancy, which showed a positive picture and confirmed that Commvault was well configured and its operation was consistent with accepted best practice.

2.42 Backups are not held on immutable storage, due to the costs involved in this. However, we note that Digital Services are working to ensure that backups are protected as much as possible within the resources available. Work is underway to further improve the protection of backups, including removing backups from the domain, enacting the lock feature in Commvault and the use of multi-factor authentication and stand-alone accounts for managing backups.

Conclusion:

2.43 There is a formal Backup Policy in place, along with a formal process for taking backups and testing these to ensure validity. The backup regimen in place has been assessed recently and improvements continue to be made. Accordingly, we have provided **substantial** assurance over this objective.

Objective 5: There is a continual process of review and assessment, including post-incident reviews to identify the root causes of disruptions.

2.44 As noted previously, there is a process for monitoring the status of core infrastructure (network, servers, firewalls), with alerts provided once the defined trigger points have been met. Our work confirmed that there are resilience related alerts set up within the dashboard available. These event alerts are reviewed and patterns and repeated alerts are identified, subject to investigation and actions defined to improve resilience.

2.45 We note that there has been some adjustment of alert thresholds in order to obtain more meaningful alert information. We also note that the health board is currently using Cisco Stealthwatch for the network. This sets a baseline for operation after 30 days of monitoring and then provides alerts if there is a statistically meaningful deviation from this.

2.46 Any failures within the infrastructure are dealt with using a service management approach, with incidents recorded and subject to investigation in order to identify the root cause. As part of this process, improvement actions are defined and progressed. We note that previous internal audit work on service management showed that incidents are managed appropriately, and a review of current incidents confirmed that this process is still operational.

Conclusion:

2.47 There is a process for reviewing the operation of the core infrastructure and identifying and rectifying any issues. There is a service management process in place which appropriately deals with incidents to enable improvements to be made. Accordingly, we have provided **substantial** assurance over this objective.

Appendix A: Management Action Plan

Matter Arising 1: Fire Suppression (Operation)			Impact
Not all sites containing core infrastructure items have fire suppression. We note that this is partly due to those areas which are not within a data centre having dual use. Without fire suppression there is an increased risk of loss of service, in particular during out of hours.			Potential risk of: • Loss of service.
Recommendations			**Priority**
1.1	Consideration should be given to installing fire suppression. Potentially using a system that can be turned off when the room is in use by staff.		**Medium**
Agreed Management Action		**Target Date**	**Responsible Officer**
1.1	Fire suppression is installed in the data centre at Morriston Hospital but not in the data centre at NPT Hospital. This is planned for 2023/24 and capital funding is agreed.	31/03/2024	Assistant Director of Digital Technology.

Matter Arising 2: Use of Virtualisation (Operation)			Impact
There is extensive use of virtualisation software in order to provide resilience, with VMWare in use and VSphere high availability being operational. We note that VSphere Fault Tolerance (which provides continuous availability for applications) is not in use however, and this could be enabled to provide additional resilience for critical systems. In addition, consideration should be given to using Vcenter Site Recovery Manager to automate disaster recovery.			Potential risk of: • Loss of service
Recommendations			**Priority**
2.1	Consideration should be given to expanding the use of VMware tools such as Fault Tolerance and Site Recovery Manager		**Low**
Agreed Management Action		**Target Date**	**Responsible Officer**
2.1	Digital Services will discuss with Dell experts to understand whether this can improve resilience with consideration given on potential limitations due to the current network configuration i.e. lack of layer 2 availability between data centres.	30/11/2023	Assistant Director of Digital Technology.

Matter Arising 3: Resilience Testing (Design)			Impact
There is no structured process for testing the resilience of the infrastructure or applications in order to ensure it functions as anticipated, and there has been no full testing of the resilience of the digital provision as a whole which would ensure that all services could be brought back, or re-provisioned from an alternative site within the timeframes defined in the service catalogue.			Potential risk of: • Loss of service.
Recommendations			**Priority**
3.1	Disaster recovery plans and resilience should be subject to periodic testing. This should be a documented process in order to demonstrate the ability of Digital Services to re-provide services.		**High**
Agreed Management Action		**Target Date**	**Responsible Officer**
3.1	Recovery happens regularly as part of routine work as noted in the audit including testing for Signal, Swansea Bay Clinical Portal and SQL cluster failovers. We will assess the feasibility of implementing periodic testing including resource requirements and impact to services to inform a way forward.	31/01/2024	Assistant Director of Digital Technology

Matter Arising 4: Recovery Plans (Operation)	Impact
The BCP includes planning for loss of server rooms, although we note that there is limited detail for this, with an instruction to "*…use other rooms to relocate DR equipment*". We also note that as failover is not automatic, there is a need to readdress the network, however this is not clear within the BCP. As such there is no formal Disaster Recovery plan that sets out exactly what will be done in the event of a major failure of service We also note that whilst the key information is in place to enable recovery of individual services, the use of this in a disaster scenario relies in the user knowing where the information is and how to use it. We note that DR plans may need to be invoked late at night, by an individual who may not be familiar with the service. Whilst Digital Services operate an on call rota, and if necessary will declare an incident in order to bring key individuals on site, the current DR planning may lead to delays in service restoration.	Potential risk of: • Delays in restoring services.

Recommendations		Priority
4.1	A more structured disaster recovery plan should be defined that builds on the information already available.	**High**

Agreed Management Action		Target Date	Responsible Officer
4.1	Costs to implement an automated failover between Morriston and NPT data centres will be obtained and consideration given based on costs and criticality for local systems including options for cloud hosting.	31/03/2024	Assistant Director of Digital Technology
	The DR plan going forward will change depending on the outcome to the first action above. A more structured plan will then be developed.	30/06/2024	Assistant Director of Digital Technology

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.
	**Unsatisfactory 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