

Hywel Dda University Health Board

Server Virtualisation

Final Internal Audit Report

November 2019

Private and Confidential

NHS Wales Shared Services Partnership

Audit and Assurance Services



Contents	Page
1. Introduction and Background	4
2. Scope and Objectives	4
3. Associated Risks	4
<u>Opinion and key findings</u>	
4. Overall Assurance Opinion	5
5. Assurance Summary	6
6. Summary of Audit Findings	8
<u>Conclusion and Recommendation</u>	
7. Summary of Recommendations	11

Appendix A
Appendix B

Management Action Plan
Assurance Opinion and Action Plan Risk Rating

Review reference:	HDUHB-1920-21
Report status:	Final Internal Audit Report
Fieldwork commencement:	27 th September 2019
Fieldwork completion:	27 th November 2019
Draft report issued:	28 th November 2019
Management response received:	02 nd December 2019
Final report issued:	03 rd December 2019
Auditor/s:	Kevin Seward
Executive sign off:	Karen Miles (Director of Planning, Performance & Commissioning)
Distribution:	Anthony Tracy (Assistant Director of Informatics) Paul Solloway (Head of ICT) John Hackett (Infrastructure Operations Manager)
Committee:	Audit & 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 & Risk Committee.

Audit reports are prepared by the staff of the NHS Wales Shared Services Partnership – Audit & Risk Assurance Services, and addressed to Independent Members or officers including those designated as Accountable Officer. They are prepared for the sole use of the Hywel Dda 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.

1. Introduction and Background

The assignment originates from the 2019/20 internal audit plan for the Health Board. The relevant lead Executive Director for the assignment was the Director of Planning, Performance & Commissioning.

This review of sought to provide the Hywel Dda University Health Board with assurance regarding the arrangements for server virtualisation within its IT estate.

Virtualisation is the concept of using software to simulate a physical server for managing access to a centralised resources or services in a network. This allows many different systems to be run on a single physical server and can lead to increased efficiencies in service provision and enhanced continuity capabilities.

2. Scope and Objectives

The overall objective of this review was to evaluate and determine the adequacy of the key controls in place for the virtualisation infrastructure to ensure that it is appropriately set up, secure and that benefits are maximised. Our review considered the management of the booking and reasonable offer process for patients administered through the main outpatient departments.

The main control objectives reviewed were:

- i. The virtual architecture is appropriately set up to allow for greater efficiency and continuity;
- ii. Access to the hypervisor and virtual machines is appropriately controlled; and
- iii. The Health Board maximises the benefits gained from virtualisation.

The audit involved a review of processes for infrastructure virtualisation and security of this infrastructure. Testing was undertaken on configuration items in order to confirm the presence of controls in accordance with Health Board rules and industry best practice.

3. Associated Risks

The potential risks considered in the review are as follows:

- The Health Board does not maximise the benefits from virtualisation;
- Loss of a higher number of systems due to physical server failure;

- Unauthorised access to information / data; and
- Failure by the Health Board to comply with licence requirements.

OPINION AND KEY FINDINGS


4. Overall Assurance Opinion

We are required to provide an opinion as to the adequacy and effectiveness of the system of internal control under review. The opinion is based on the work performed as set out in the scope and objectives within this report.

An overall assurance rating is provided describing the effectiveness of the system of internal control in place to manage the identified risks associated with the objectives covered in this review.

The overall level of assurance that can be assigned to a review is dependent on the severity of the findings as applied against the specific review objectives and should therefore be considered in that context.

The level of assurance given as to the effectiveness of the system of internal control in place to manage the risks associated with the process of server virtualisation is **Substantial** assurance.

RATING	INDICATOR	DEFINITION
Substantial Assurance		The Board can take substantial assurance that arrangements to secure governance, risk management and internal control, within those areas under review, are suitably designed and applied effectively. Few matters require attention and are compliance or advisory in nature with low impact on residual risk exposure.

Whenever possible virtualisation is the first choice for the Health Board's servers. This choice has many benefits to the organisation, such as increases the utilisation rate of the hardware and increases the organisations resilience.





The Health Board's virtual environment is well managed and kept secure with good access controls.

The Health Board's physical hardware on which the virtual environment sits is appropriately secure and protected and the Health Board ensure that it is licence compliant.

Whilst the team itself is small, efforts have been made to share knowledge and upskill additional staff outside the core team. This is enhanced by Standard Operating Procedures (SOPs) for patching and creating virtual machines (VMs) which have been developed to further support the process of virtualisation.

5. Assurance Summary

The summary of assurance given against the individual objectives is described in the table below:

Audit Objective		Assurance Summary*			
					
1	Ensure that proposed benefits in relation to server virtualisation have been identified and the Health Board has not maximised these benefits				✓
2	Ensure controls are in place to avoid the loss of a higher number of systems due to server failure			✓	
3	Prevent unauthorised access to information / data held within the Health Boards virtual infrastructure				✓
4	Take measures to comply with the associated license requirements of a virtualised infrastructure				✓

* The above ratings are not necessarily given equal weighting when generating the audit opinion.

Design of Systems/Controls

The findings from the review have highlighted no issues that are classified as a weakness in the system control/design for server virtualisation.

Operation of System/Controls

The findings from the review have highlighted one issue that is classified as a weakness in the operation of the designed system/control for server virtualisation. This is identified in the Management Action Plan as (O).

6. Summary of Audit Findings

Any key findings are reported in the Management Action Plan at Appendix A.

OBJECTIVE 1: Ensure that proposed benefits in relation to server virtualisation have been identified and the Health Board has not maximised these benefits.

The following area of good practice was noted:

The programme of server virtualisation at the Health Board has brought benefits in terms of greater resilience, reduction in downtime, simplified IT environment and administration, more efficient use of hardware, ease of server provisioning, and environmental and cost implications of less energy use.

No matters arising.

OBJECTIVE 2: Ensure controls are in place to avoid the loss of a higher number of systems due to server failure.

The following areas of good practice were noted:

- the Health Board's systems used to manage its virtual environment are updated and patched to a current, secure standard;
- there is evidence that patching of the virtual environment takes place and this is underpinned and documented in the procedure document for server patching.
- the health board's architecture in relation to the virtual environment is well designed and allows for resources to be shared, thus ensuring resilience;
- there are appropriate physical controls in place to protect the virtual environment;
- the Health Boards virtual estate has sufficient capacity to allow their current processing and the use of resource is monitored and optimised;
- system alarms are operational and monitored, activity logging is turned on and logs retained.
- snapshots are used before configuration changes;

- standardised pre-approved deployment templates are used for virtual machine creation and these are patched;
- the deployment process is documented in a SOP developed by the lead infrastructure engineer; and
- there is a IM&T document which sets out the Disaster Recovery and Business Continuity arrangements in relation to the virtual infrastructure.

We note the following Medium priority finding in relation to this objective:

While Disaster Recovery and Business Continuity documentation sets out the arrangements for backup and recovery of the systems in the Health Boards Virtual environment, testing of backups and whole system recovery has been an issue organisationally.

Historical recommendations made by the Wales Audit Office (WAO) highlighted the need to test recovery from backups and proposed the Health Board should undertake a "whole system" demonstration of system recovery and failover as a result of a catastrophic fail or successful cyber-attack.

As with other Health Boards, the ICT Team at Hywel Dda have not been able to undertake a full test without greatly affecting the critical live services in operation within the Health Board. Therefore, until a technological solution is available to allow whole system testing, the ICT department propose to carry out a number of smaller tests of the backup recovery facility, recovering of a random set of 10 critical and 10 standard servers monthly.

See Finding 01 at Appendix A.

OBJECTIVE 3: Prevent unauthorised access to information / data held within the Health Boards virtual infrastructure.

The following areas of good practice were noted:

- the Health Board exercises satisfactory password control over its virtualisation management systems;
- the Health Board conform to industry best practice with isolated virtual networks for host management, vSphere vMotion, vSphere FT, and so on, improving security and performance;
- an appropriate configured Firewall is in place to protect the virtual environment;

- roles are appropriately controlled within the virtual environment; and
- all management of the virtual environment is done via the management server.

No matters arising.

OBJECTIVE 4: Take measures to comply with the associated license requirements of a virtualised infrastructure.

The following areas of good practice were noted:

- there has been a local review to assess the Microsoft licencing compliance position; and
- as part of the process for considering virtualisation of systems, the departments / vendors are consulted to ensure that their system will be licence compliant in a virtual environment.

No matters arising.

7. Summary of Recommendations

Any audit findings and recommendations are detailed in Appendix A together with the management action plan and implementation timetable if appropriate.

A summary of these recommendation by priority is outlined below.

Priority	H	M	L	Total
Number of recommendations	0	1	0	0

<p>Finding 1 – Recovery and Testing of Backups (O)</p>	<p>Risk</p>
<p>While Disaster Recovery and Business Continuity documentation sets out the arrangements for backup and recovery of the systems in the Health Boards Virtual environment, testing of backups and whole system recovery has been an issue organisationally.</p> <p>Historical recommendations made by the Wales Audit Office (WAO) highlighted the need to test recovery from backups and proposed the Health Board should undertake a “whole system” demonstration of system recovery and failover as a result of a catastrophic fail or successful cyber-attack.</p> <p>As with other Health Boards, the ICT Team at Hywel Dda have not been able to undertake a full test without greatly affecting the critical live services in operation within the Health Board. Therefore, until a technological solution is available to allow whole system testing, the ICT department propose to carry out a number of smaller tests of the backup recovery facility, recovering of a random set of 10 critical and 10 standard servers monthly.</p>	<p>Loss of a higher number of systems due to physical server failure.</p>
<p>Recommendation 1</p>	<p>Priority level</p>
<p>Testing programme above should commence and in order to provide a meaningful audit trail a schedule should be created which identifies which systems will be tested; the schedule should contain a target date for the test and subsequently be completed with the date the test was carried out, the person responsible and the outcome of the test.</p>	<p>Medium</p>

Management Response	Responsible Officer/ Deadline
<p>Agree. A testing schedule has been developed and is currently operational, which incorporates the elements of the recommendation above.</p>	<p>Assistant Director of Informatics, Head of ICT and the Infrastructure Manager</p> <p>Complete</p> <p>The continued testing is ongoing</p>

Appendix B - Assurance opinion and action plan risk rating

2019/20 Audit Assurance Ratings



Substantial Assurance - The Board can take **substantial assurance** that arrangements to secure governance, risk management and internal control, within those areas under review, are suitably designed and applied effectively. Few matters require attention and are compliance or advisory in nature with **low impact on residual risk** exposure.



Reasonable Assurance - The Board can take **reasonable assurance** that arrangements to secure governance, risk management and internal control, within those areas under review, are suitably designed and applied effectively. Some matters require management attention in control design or compliance with **low to moderate impact on residual risk** exposure until resolved.



Limited Assurance - The Board can take **limited assurance** that arrangements to secure governance, risk management and internal control, within those areas under review, are suitably designed and applied effectively. More significant matters require management attention with **moderate impact on residual risk** exposure until resolved.



No Assurance - The Board has **no assurance** arrangements in place to secure governance, risk management and internal control, within those areas under review, which are suitably designed and applied effectively. Action is required to address the whole control framework in this area with **high impact on residual risk** exposure until resolved.

Prioritisation of Recommendations

In order to assist management in using our reports, we categorise our recommendations according to their level of priority as follows.

Priority Level	Explanation	Management action
High	Poor key control design OR widespread non-compliance with key controls. PLUS Significant risk to achievement of a system objective OR evidence present of material loss, error or misstatement.	Immediate*
Medium	Minor weakness in control design OR limited non-compliance with established controls. PLUS Some risk to achievement of a system objective.	Within One Month*
Low	Potential to enhance system design to improve efficiency or effectiveness of controls. These are generally issues of good practice for management consideration.	Within Three Months*

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



Office details: St Brides
St David's Park
Carmarthen
Carmarthenshire
SA31 3HB

Contact details: 01267 239780