

IT Backup & Recovery Arrangements Final Internal Audit Report December 2021

Hywel Dda University Health Board

NWSSP Audit and Assurance

Contents

Executive Summary	3
1. Introduction.....	4
2. Detailed Audit Findings.....	5
Appendix B: Assurance opinion and action plan risk rating	9

Review reference:	HDUHB-2122-19
Report status:	Final
Fieldwork commencement:	17 November 2021
Fieldwork completion:	26 November 2021
Draft report issued:	29 November 2021
Debrief meeting:	29 November 2021
Management response received:	Not applicable
Final report issued:	01 December 2021
Auditors:	Sian Harries
Executive sign-off:	Huw Thomas (Director of Finance)
Distribution:	Anthony Tracey (Digital Director), Paul Solloway (Deputy Digital Director)
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 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.

Executive Summary

Purpose


The purpose of the review is to provide assurance to the Audit Committee that a process is in place for ensuring that adequate plans exist, which are followed for the routine backup of systems or critical data and for the recovery of these items after an interruption of processing.

Overview

We identified multiple areas of best practice and no issues for reporting in our review:

- Comprehensive strategy in place underpinned by SOPs.
- Newly acquired backup solution (Rubrik) simplifies and unifies backup, data protection and instant recovery onsite, in the cloud and at the Data Centres.
- Data is immutable, logically air gapped and safeguarded from unauthorised access so it cannot be modified, encrypted, or deleted.
- Real-time monitoring of backup activities, system health and capacity.
- Immediate notification of failed backup activities for swift resolution.
- Regular testing of backups undertaken.

Report Classification

		Trend
	Substantial Few matters require attention and are compliance or advisory in nature.	N/A
	Low impact on residual risk exposure.	First Review

Assurance summary¹

Assurance objectives	Assurance
1 Backup Strategy	Substantial
2 Policy and Procedures	Substantial
3 Access Controls	Substantial
4 Monitoring	Substantial
5 Critical Systems and Information	Substantial
6 Retention	Substantial
7 Testing	Substantial

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

1. Introduction

- 1.1 Our review of the local IT Backup and Recovery arrangements was completed in line with the Hywel Dda University Health Board Internal Audit Plan for 2021/22. The relevant lead Executive Director for this review is the Director of Finance.
- 1.2 System and information backups are an important component of the Health Board's Business Continuity, Disaster Recovery (DR) and IT Resiliency plans and capabilities. System backups involve making point-in-time copies of all data on a given system. Suitable backup solutions can restore anything from a single file to an entire system, to a recent, 'known good' state.
- 1.3 The Health Board's ability to successfully backup and restore data in the event of a disruption is critical to its ability to function. Backups are crucial in situations such as:
 - A database accidentally or otherwise deleted, and it needs to be restored to resume normal business activities.
 - One or more servers fail due to a software update problem and must be restored to the operational state in effect prior to the start of the update.
 - One or more servers, systems or data is impacted by ransomware or other malware.
 - A user accidentally deletes a file from a shared drive.
 - A disaster renders the primary data centre unusable, and production must be resumed in an alternative location.
- 1.4 To address identified challenges within the Health Board's previous backup environment (Asigra), such as slow backup and recovery times, and susceptibility to ransomware attacks, the Health Board undertook a comprehensive assessment of multiple backup solutions as a replacement. In September 2020, the Health Board purchased Rubrik, which not only addressed the identified issues but also the prospective requirements for cloud migration.
- 1.5 The potential risks considered in this review were as follows:
 - loss of key processing or services;
 - loss of Health Board data;
 - adverse impact on the Health Board, and inability to provide an appropriate service in the event of disruptive events; and
 - reputational damage.

2. Detailed Audit Findings

Objective 1: Backup Strategy – an overarching strategy and plan for backups in place that sets out the requirements and responsibilities.

- 2.1 A *Disaster Recovery and Backup Strategy* (the 'Strategy') is in place, which outlines the arrangements for providing disaster recovery services for all digital systems and infrastructures provided locally and managed by the Health Board. The Strategy has been appropriately updated to include the newly acquired Rubrik backup solution.
- 2.2 The Strategy covers arrangements in place in detail, including requirements and responsibilities for the following areas:
- **Service Resilience** – this is the ability to provide and maintain the Digital service in the face of faults.
 - **Service Availability** – this is the duplication of critical components of a Digital Service / Data with the intention of increasing reliability.
 - **Site Resilience** – replication of systems across the two Data Centres (primary within Glangwili General Hospital and secondary within Worthybush General Hospital) so that in the event of a site-level incident, critical services can continue to operate by falling over to a redundant site.
 - **Service Backup** – process of making copies of data which can be used to restore data in the event of any data loss.
- 2.3 Service schedules are agreed between system owners and the Informatics department for the expected performance of those services. Each service is defined within the Informatics' service catalogue which are governed by one of the following NHS Wales service categories, which have specific response times, service levels and support arrangements:

<i>Clinical Critical</i>	<i>Clinical Standard</i>
<i>Admin Critical</i>	<i>Admin Standard</i>
<i>Infrastructure Critical</i>	<i>Infrastructure Standard</i>

- 2.4 It was noted during our review that all critical assets have been recently reviewed as part of the Security of Network and Information Systems (NIS) Regulations, which are the legal measures to boost the level of security (both cyber and physical) of network and information systems. In light of the review, the service categories will be refreshed over the next two months.
- 2.5 Service backups are achieved using the incremental forever and synthetic full concepts. Rubrik applies in-line deduplication on the initial full backup and after this, incremental backups are created forever and, once the specified number of incremental backups is reached, Rubrik consolidates the incremental backup into a new 'synthetic' full backup. To detect and mitigate against chain corruptions, Rubrik

runs validation checks on incoming snapshots to verify the integrity of the new data chain is uncorrupted, and then mounts the snapshot to the system to check its filesystem integrity. If corruption is detected in the snapshot chain, the system will notify the administrator and mark the object for a new full backup automatically.

Conclusion:

2.6 A comprehensive strategy is in place, which sets out the arrangements to provide Disaster Recovery services across all Health Board Digital systems and infrastructures. Consequently, we have concluded '**Substantial**' assurance for this objective.

Objective 2: Policy and Procedures – a backup policy is in place setting out the context and responsibilities, and backup procedures and processes are in place.

2.7 Whilst there is no separate Backup Policy, the Strategy contains comprehensive information which outlines the framework and responsibilities for each of the areas noted in paragraph 1.2 and 1.3 above.

2.8 The Strategy is underpinned by service-specific Standard Operating Procedures (SOPs) in the event of a major Digital incident or system failure. We reviewed the Rubrik Backups Process Map, which provides a quick overview of the steps involved, and references the corresponding SOP. The SOPs contain screenshots of the Rubrik system in addition to detailed work instructions.

Conclusion:

2.9 A comprehensive strategy is in place, which is further supported by service-specific SOPs for recovery in the event of a major Digital incident or system failure. Consequently, we have concluded '**Substantial**' assurance for this objective.

Objective 3: Access controls - assess access controls for backup systems and saved backups.

2.10 Backup data managed by Rubrik is stored in an immutable manner and no external or internal operation can modify the data. In the event of a ransomware attack, infected data later ingested by Rubrik cannot infect other existing files or folders.

2.11 Operations on data within Rubrik can only be performed by authenticated users with appropriate credentials. Two-step user verification is enforced on the Rubrik system via a global rule using the Azure Multi-factor authentication (MFA). The initial log-in screen prompts for a username and password, followed by a required time-limited verification code from the user's registered account on the Microsoft Authenticator app.

2.12 We reviewed the Rubrik current accounts and permissions, and we confirm that there are five user accounts with administrative access; three are members of the Health Board's Digital team with appropriate level of seniority, and two are generic (Administrator and HDD-SVC-RUBRIK). The Administrator is a built-in account which forms part of every server and passwords are secured via the Privileged Access Management Solution (Thycotic). HDD-SVC-RUBRIK is a service account to

support automated server backup processes, and passwords are managed via Microsoft's Managed Service Account functionality.

Conclusion:

2.13 The new backup solution uses an architecture that combines an immutable filesystem with a zero-trust design, in which operations can only be performed through authenticated means. Consequently, we have concluded '**Substantial**' assurance for this objective.

Objective 4: Monitoring - ensure there is adequate monitoring of backup jobs and resolution of failed jobs.

2.14 Rubrik has an intuitive user interface, which allows for real-time monitoring of the system's health and capacity, including the status of backup activity tasks (in progress, completed and failed). The live dashboard is monitored daily by the Health Board's administrators, and e-mail notifications are received following activity tasks to allow for swift resolution of any failed activities. E-mail notifications will also be integrated in the Health Board's new Service Desk tool (FreshService) following migration in December 2021.

2.15 A support arrangement is in place between Rubrik and the Health Board; should an issue arise with the health of the system, Rubrik Support will receive notification and they will contact the Health Board's administrators to investigate locally if required.

Conclusion:

2.16 Monitoring is undertaken on a daily basis and the system's intuitive dashboard allows for immediate notification and resolution of failed backup tasks. Consequently, we have concluded '**Substantial**' assurance for this objective.

Objective 5: Critical systems and information - seek validation that business-critical systems and information are included in backups and the arrangements have been appropriately communicated and agreed by stakeholders.

2.17 All Digital infrastructures, business-critical services and information are backed up using the product selected for backup services, namely Rubrik, VMWare and Nimble snapping and replication technologies.

2.18 Various approaches are adopted as below:

Critical Services Virtual

- Nimble snapshots at 2 hourly intervals to disk.
 - Copy of these snapshots replicated to secondary Data Centre immediately
 - Snapshots retained weekly at both Data Centres.
 - Incremental backups created daily which is copied to primary backup disk and then replicated to secondary backup disk on a different site.
 - Backup data retained for 1 year.
-

Critical Services Physical

- Incremental backups created every 4 hours which is copied to primary backup disk and then replicated to secondary backup disk on a different site.
- Backup data retained for 1 year.

2.19 As noted in paragraphs 2.3 and 2.4, backup arrangements are appropriately agreed and communicated to stakeholders.

Conclusion:

2.20 We have concluded '**Substantial**' assurance for this objective.

Objective 6: Retention - ensure the organisation appropriately retains backups, both onsite and at any offsite locations.

2.21 As per the adopted approaches noted under objective 5, critical backups are appropriately retained for one year.

2.22 Snapshots of virtual standard services are exported at 8 hourly cycles to disk, of which copies are replicated to the secondary Data Centre immediately. These snapshots are retained weekly at both Data Centres. Incremental backups are created daily, copied to primary backup disk, and then replicated to a secondary backup disk on a different site. Backup data is retained for one year.

2.23 For physical standard services, incremental backups are exported at 8 hourly cycles to the primary backup disk and then replicated to secondary backup disk on a different site. Backup data is retained for one year.

Conclusion:

2.24 Backup data is appropriately retained by the Health Board. Consequently, we have concluded '**Substantial**' assurance for this objective.

Objective 7: Testing - ensure the organisation periodically test and refresh archived and backup data, maintaining a record of any tests and their outcome.

2.25 In addition to a routine monthly backup testing schedule, individual file restores are undertaken regularly (2-3 times a week) which assures backup validity and integrity.

2.26 Following migration to the new Service Desk tool, scheduled monthly calls will be raised to the Infrastructure team to perform tests.

2.27 In the event of a file restoration failure, a call can be raised to the support partner for Rubrik to ensure a root cause was identified and resolved. In the interim, restorations can be provided from the storage system snapshots taken at 4 hourly intervals and replicated across the primary and secondary Data Centres.






Conclusion:

2.28 Testing is undertaken regularly, and support arrangements are in place to mitigate risk against restoration failures. Consequently, we have concluded '**Substantial**' assurance for this objective.

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](#)