IT Business Continuity

Final Internal Audit Report

PHW 2020/21

May 2021

NHS Wales Shared Services Partnership

Audit and Assurance Services

RATING	INDICATOR
Reasonable Assurance	

Contents **Page**

Review reference:	PHW2021-11
Report status:	Final Internal Audit Report
Fieldwork commencement:	7 January 2021
Fieldwork completion:	22 March 2021
Draft report issued:	06 April 2021
Management response received:	13 May 2021
Final report issued:	14 May 2021
Auditors:	Paul Dalton, Head of Internal Audit Martyn Lewis, IM&T Audit Manager Kevin Seward, Senior IM&T Auditor
Executive sign off:	Huw George, Deputy Chief Executive and Director of Operations & Finance
Distribution:	Drew Evans, Head of IM&T Daniel Rixon, Emergency Planning and Business Continuity Officer
Committee:	Audit and Corporate Governance Committee

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 Internal Audit Charter and the Annual Plan, approved by the Audit and Corporate Governance 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 Public Health Wales NHS Trust 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

Our review of arrangements of the arrangements in place to ensure appropriate back up, Disaster Recovery (DR) and Business Continuity (BC) arrangements of Information Technology (IT) systems used within Public Health Wales NHS Trust (the 'Trust' or the 'organisation') was completed in line with the 2020/21 Internal Audit Plan.

IT continuity is a subset of Business Continuity Planning (BCP) and encompasses IT disaster recovery planning and wider IT resilience planning. It also incorporates those elements of IT infrastructure and services, which relate to communications such as (voice) telephony and data communications.

It is a systematic process to prevent, predict and manage Information and Communications Technology (ICT) disruption and incidents which have the potential to disrupt ICT services, and should result in a more resilient IT service capability aligned to wider organisational requirements.

Alongside this IT service users should understand that disruptions may still occur and should develop their own continuity plans to maintain operations in the event of a loss of IT service.

The relevant lead for the review is the Deputy Chief Executive and Director of Operations & Finance.

2. Scope and Objectives

The overall objective of this review was to evaluate and determine the adequacy of systems and controls in place in relation to IT continuity. The review is intended to provide assurance to the Trust that IT backup and continuity arrangements are in place and managed appropriately within its departments to ensure that the organisation has sufficient resilience and can maintain services in the event of an IT disruption caused by a major incident.

The key objective areas of the review were as follows:

- ensure appropriate backup, continuity and DR arrangements are in place within Informatics;
- ensure that resources are available to manage an incident, including out of hours, and are targeted to the most critical systems; and
    - ensure departments understand their responsibilities and have continuity arrangements in place to cope with the loss of IT functions and plans are achievable, tested and consider the potential time lag for reinstating IT service provision.

3. Associated Risks

The potential risks considered in this review were as follows:

- the organisation cannot provide an adequate service in the event of a loss of its IT services; and
- loss of Trust data.

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 established controls for IT Business Continuity is **reasonable assurance**.

RATING	INDICATOR	DEFINITION
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.

There are controls in place to manage the IT Business Continuity processes within the Trust. Overall, the controls in place to manage the risks associated with the systems and processes tested within the review are extant and functioning as intended.

We identified one medium priority recommendation concerning testing of the Trust's failover and restore capabilities and appropriately recording successful tests on an auditable central register.

Additionally, we identified three low priority weaknesses which present some opportunities to enhance effectiveness of controls.

The Informatics department has developed comprehensive, up to date backup and recovery procedures for its infrastructure. Responsibilities are understood and the informatics team have been able to put this into practice in the past to perform *ad hoc* recovery actions.

The Trust understands the placement of its Informatics resources, there is a restructure underway to create an operating model which is aligned to Public Health Wales (PHW) operational plan and strategy. With the exception of out of hours cover this is well placed to support the organisation in the management of incidents.

Departments generally understand their requirements for planning for loss of IT, and there is a process, led by the Emergency Planning team to ensure that departments have consistent plans in place for this.

5. Assurance Summary

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

Assurance Summary					
1	Backup, Continuity and DR arrangements			✓	
2	Resources to manage an incident				✓
3	Department Responsibilities				✓

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

Design of Systems/Controls

The findings from the review identified two issues that are classified as weaknesses in the system control/design for IT Business Continuity.

Operation of System/Controls

The findings from the review highlighted two issues that are classified as weaknesses in the operation of the designed system/control for IT Business Continuity.

6. Summary of Audit Findings

In this section, we highlight areas of good practice that we identified during our review. We also summarise the findings made during our audit fieldwork. The detailed findings are reported in the Management Action Plan (Appendix A).

Objective 1: Ensure appropriate backup, continuity and DR arrangements are in place within ICT

We note the following areas of good practice:

- There is resilient architecture in place for IT services and the organisation has implemented a new system to perform backups, these take place nightly and are replicated between two off site and on premises data servers.
- The Informatics department have developed a comprehensive, up to date backup and recovery document which identifies the recovery strategies for all servers. The document lists websites, databases, servers with recovery strategies set in line with the criticality of each.

- Informatics staff have been professionally trained in the use of the software by the supplier, and others could carry out the tasks with the in-house procedural documents which have been produced.
- The informatics department have completed Business Impact Assessments (BIA) and produced a Business Continuity Plan (BCP) setting out achievable continuity and DR arrangements.
- There is a formalised communications process for IT to proactively liaise with departmental leads in the instance of an event.

We note the following findings in relation to this objective:

- While the Informatics department procedures contain steps for checking if backups and replications have been successful and there is a clear process which has been used for ad-hoc restoration of physical machines virtual machines and data there has never been a 100% test of trust DR provision. (Finding 1 – Medium)

Objective 2: Ensure that resources are available to manage an incident, including out of hours, and are targeted to the most critical systems.

We note the following areas of good practice:

- The Trust understands the placement of its Informatics resources, and the Informatics department are undergoing a reorganisation to maximise the distribution of its staff. While the new structure leaves some known gaps in areas such as the technical, desktop and service desk teams, this work gives a blueprint for the future. We understand that once this is complete there will be further work on reviewing funding and resilience of the teams for 2021/22.
- The Informatics department has conducted a skills assessment of its staff in order to assess its resource cover and future training needs.
- Out of hours cover is planned in advance, and the Informatics department maintain an on-call rota which is populated a month in advance, and with the team able to demonstrate they have been able to cover all on-call slots to date.
- To aid the out of hours process the Informatics department have developed an automated triage filter for calls before they are sent to the on-call staff.

We note the following finding in relation to this objective:

- The out of hours cover that has been put in place since the pandemic is being covered on goodwill without any contractual requirement, as a result there is no assurance of its sustainability or fulfilment as the pandemic response continues. (Finding 2 – Low)

Objective 3: Ensure departments understand their responsibilities and have continuity arrangements in place to cope with the loss of IT functions and plans are achievable, tested and consider the potential time lag for reinstating IT service provision.

We note the following areas of good practice:

- There is a suite of corporate business continuity documents, including the Business Continuity Framework, Business Continuity Incident Management Process and Directorate/Divisional business continuity plans.
- For departments the continuity planning process starts with a Business Impact Assessment (BIA) which helps facilitate user buy-in to the BCP concept and process and there are templates in place for continuity planning which should ensure consistent BCP documentation across the organisation.
- There is an Emergency Planning & Business Continuity Leads Group with representatives from across the organisation. Status of emergency planning is reported through the group.
- The organisation has defined objectives for training, exercising, and testing the business continuity plans, stakeholder exercises and training. These are recorded in the organisations emergency planning and business continuity tracking database and performance monitoring at a senior level is evidenced through the Emergency Planning and Business Continuity Progress Report.
- We discussed the individual departmental responsibility for continuity provision with personnel, we confirmed that of BIAs and BC plans are in place to ensure operational continuity in the event of IT failure and system loss. These plans have been discussed within the departments to raise awareness and there have been desktop exercises in the past to test and review the plans.
- We reviewed the documentation provided and confirm the plans have been approved by the senior members of the directorate and the Trust BC department, therefore the plans should be realistic, appropriate and achievable enabling continued operation of critical business processes and/or temporary processing arrangements for scenarios such as the loss of ICT services. Individual nominated officers' responsibilities are stated in the documents and key measures such as Maximum Tolerable Period of Disruption (MTPD), Minimum Tolerable Staffing Level (MTSL) and Recovery Time Objective (RTO) are also included.

We note the following findings in relation to this objective:

- While revised business continuity planning templates require staff to list dependencies such as internal, external suppliers and stakeholders the documents would be improved if a note was added to ensure the business continuity lead completing the documentation

liaise with these groups to ensure expectations are understood and achievable. (Finding 3 – Low)

- Department Business Continuity Plans for the organisation while approved, were dated 2019 with an annual review requirement. Because of the pandemic response the organisation has not reviewed these within the target review date. (Finding 4 – Low)

7. Summary of Recommendations

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

A summary of these recommendations by priority is outlined below.

Priority	H	M	L	Total
Number of recommendations	**0**	**1**	**3**	**4**

Finding 1: Backup Recovery Testing (Control Design)	Risk
While the Informatics department procedures contain steps for checking if backups and replications have been successful and there is a clear process which has been used for *ad hoc* restoration of physical machines virtual machines and data, there has never been an exercise which tests 100% of Trust Disaster Recovery capabilities. Testing failover and restore has generally been *ad hoc* as part of planned maintenance (e.g. upgrades). Although the Informatics team are confident in the resilience of their structure, and their ability to recover any part of their system within Recovery Time Objective (RTO) and Recovery Point Objective (RPO) parameters, they cannot confirm that every service, on every server has been tested.	The organisation cannot provide an adequate service in the event of a loss of its IT services; and Loss of Trust data.
Recommendation	**Priority level**
In line with best practice, Informatics should consider a full failover test in order to confirm that all services can be effectively maintained in the event of a site loss. If this is not possible because of the criticality of services during pandemic conditions, then it should plan a schedule of discrete tests to provide the same coverage. When resilience is effectively tested, e.g. a Service failover is done as part of routine system maintenance, this should be appropriately recorded as test on a central register.	**Medium**

Management Response	Responsible Officer/ Deadline
Management note the finding. Today we do regular backup and restore tests to ensure our backup solutions are tested. We will look to propose a schedule of BCP tests for our Essential services and work with the SROs for each service to agree appropriate dates and time slots. These will be spread over the course of the year and any weaknesses or failures will be recorded against Datix. A schedule will be published by June-2021.	Head of IM&T and Emergency Planning and Business Continuity Officer June-2021

Finding 2: On-call cover (Control Design)	Risk
As a result of pandemic related work, IT equipment and services have been required across the Trust for extended periods of operation, their failure could severely impact pandemic response. The temporary weekend out of hours support for Microbiology, Tarian system, Call centre and Health Protection data extract that has been put in place since the pandemic is being covered on goodwill without any contractual requirement. As a result, it is not clear how sustainable this approach is as the pandemic response continues.	The organisation cannot provide an adequate service in the event of a loss of its IT services.
Recommendation	**Priority level**
If the situation continues, more sustainable and reliable formal arrangements are required, or the organisation must accept the risk formally.	**Low**
Management Response	**Responsible Officer/ Deadline**
Management note the finding. On call services are to be reduced as service provision moves toward more substantive working patterns Mon-Friday as part of the organisation recovery. The IT service will be adjusted to support the relevant services.	Head of IM&T July 2021

Finding 3: BC planning templates (Operating effectiveness)	Risk
While revised Business Continuity Planning templates require staff to list dependencies such as Internal, External Suppliers and stakeholders the documents would be improved if a note was added to ensure the business continuity lead completing the documentation liaise with these groups to ensure expectations are understood and achievable.	The organisation cannot provide an adequate service in the event of a loss of its IT services.
Recommendation	**Priority level**
Notes reminding departments to liaise with stakeholder groups should be added to the organisations BC planning templates.	**Low**
Management Response	**Responsible Officer/ Deadline**
Management note the finding. The Business continuity team will update the templates.	Head of IM&T July 2021

Finding 4: Business Continuity plan reviews (Operating effectiveness)	Risk
Department Business Continuity plans for the organisation while approved were dated 2019 with an annual review requirement. Because of the pandemic response the organisation has not reviewed these within the target review date.	The organisation cannot provide an adequate service in the event of a loss of its IT services.
Recommendation	**Priority level**
As business returns to normality the Trusts departments should review their continuity documentation, taking the opportunity to include learning lessons on continuity and recovery identified during the Covid response.	**Low**
Management Response	**Responsible Officer/ Deadline**
Management note the finding and will update the documentation with lessons learned as part of the pandemic.	Head of IM&T August 2021

Appendix B - Assurance opinion and action plan risk rating

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 can take **no 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 **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.