6.1.3 WAO Follow-up Information Backup, Disaster Recovery and Business Continuity, and Data Quality Update

Presenter: Karen Miles/Anthony Tracey

SBAR WAO Follow-up Information Backup, Disaster Recovery and Business Continuity, and Data Quality Update ARAC October 2019

For Information: Follow-up Information Backup, Disaster Recovery and Business Continuity, and Data Quality Update March 2018

Bwrdd Iechyd Prifysgol Hywel Dda University Health Board

PWYLLGOR ARCHWILIO A SICRWYDD RISG
AUDIT AND RISK ASSURANCE COMMITTEE

DYDDIAD Y CYFARFOD: DATE OF MEETING:	22 October 2019
TEITL YR ADRODDIAD: TITLE OF REPORT:	WAO Follow-up Information Backup, Disaster Recovery and Business Continuity, and Data Quality Update
CYFARWYDDWR ARWEINIOL: LEAD DIRECTOR:	Karen Miles, Director of Planning, Performance, Informatics and Commissioning
SWYDDOG ADRODD: REPORTING OFFICER:	Anthony Tracey, Assistant Director of Informatics

Pwrpas yr Adroddiad (dewiswch fel yn addas) **Purpose of the Report** (select as appropriate)
Er Sicrwydd/For Assurance

ADRODDIAD SCAA
SBAR REPORT

Sefyllfa / Situation

The purpose of this paper is to provide an update to the Audit & Risk Assurance Committee (ARAC) on progress in implementing the Wales Audit Office (WAO) follow-up review of Information Backup, Disaster Recovery and Business Continuity, and Data Quality.

Cefndir / Background

As part of the Audit Plan for 2017, the Auditor General included local work to provide an updated position on recommendations from the WAO IT reports undertaken between 2012 and 2015. The above named report was the result of the findings.

The overall conclusion was that historically, the Health Board has addressed recommendations slowly, but over the last 12 months, it has implemented the majority of recommendations, and work was underway to complete the remainder.

Asesiad / Assessment

The report combined a number of audit reports and noted the status of the previous recommendations as below:

Audit Report	Complete	In Progress	Overdue	Superseded	Total Recommendations
Wales Audit Office Report	16	9	0	1	26
Total	16	9	0	1	26

The WAO found that the Health Board had fully implemented 16 of the recommendations and made progress against a further 9, with 1 recommendation being superseded. However the report did note that there are still improvements to be made in disaster recovery and business continuity. WAO observed that the Health Board would benefit from a "whole system" test which

would demonstrate the ability to react to a catastrophic failure of Health Board ICT infrastructure and systems.

During the updated field work a further 2 new recommendations were identified around improvements within the backup arrangements, bringing the recommendations to 11 outstanding.

Therefore, the following is the position as at September 2019, based on those recommendations classed as "in progress" and the 2 new recommendations:

Audit Report	Complete	In Progress	Overdue	Total Recommendations
Wales Audit Office Report - 1175A2019-20	9	1	1	11
Total	9	1	1	11

Full details on the remaining overdue recommendation is included within Appendix 1, plus closure of those that were originally overdue.

The remaining overdue recommendation is linked to the need to undertake a "whole system" demonstration of system recovery and failover as a result of a catastrophic fail or successful cyber-attack. To date, the ICT Team have not been able to undertake a full test without greatly affecting the critical live services in operation within the Health Board. A failure would mean the loss of a connection to the network and systems for such areas as critical care, A&E, radiology, pathology, Welsh Clinical Portal and Welsh Patient Administration System (WPAS). In retrospect, the recommendation should have been challenged and clarified with the auditor, as a full test is not feasible without affecting services. Nevertheless, it is acknowledged that if the Health Board did suffer a catastrophic failure then services would be affected. To understand the all Wales position, the ICT Team have contacted other Health Boards and the NHS Wales Informatics Service (NWIS) to ascertain whether they undertake a "whole system" test, and organisations have responded stating that they undertake partial testing, but no "whole system" tests are undertaken, due to the complexities and the unavailability of a full test environment which mirrors the production infrastructure.

Therefore, the proposal, until such time that a mirrored environment is available, is that a number of smaller tests (i.e. recovery of a random set of 10 critical and 10 standard servers) is undertaken monthly to test the backup recovery facility, and also specific system tests (e.g. WPAS) have been undertaken. The lessons learned from these will be utilised to change the backup plan if necessary. As noted within the diagram (Appendix 2) the Health Board operates a very complex infrastructure with 643 servers. The diagram illustrates the backup strategy for the Health Board, where 493 servers are backed up every 4 hours, critical servers, (which include systems such as CarePartner, Ophthalmology, Cellma, Dental, Diabeta3, WPAS, Child Health) are backed up every 2 hours, all of which are replicated between the Primary and Secondary Data Centres. With regards to the physical servers, these are backed up daily to the backup storage which is then replicated between data centres.

The ICT Team have also had discussions with our current backup supplier (Asigra) to ascertain whether they are able to "mirror" or take a snapshot of our infrastructure into a test environment to allow a full test to be undertaken. However, this functionality is not currently available. The Health Board's backup contract is due for renewal (March 2021), with the ICT Team undertaking the retendering in early 2020/21, and it will be requested that this functionality is included within the new contract.

Argymhelliad / Recommendation

The Audit & Risk Assurance Committee is asked to note the contents of this report and take assurance regarding progress to date

Amcanion: (rhaid cwblhau) **Objectives: (must be completed)**	
Committee ToR Reference Cyfeirnod Cylch Gorchwyl y Pwyllgor	5.3 In carrying out this work, the Committee will primarily utilise the work of Internal Audit, Clinical Audit, External Audit and other assurance functions, but will not be limited to these audit functions. It will also seek reports and assurances from directors and managers as appropriate, concentrating on the overarching systems of good governance, risk management and internal control, together with indicators of their effectiveness.
Cyfeirnod Cofrestr Risg Datix a Sgôr Cyfredol: Datix Risk Register Reference and Score:	No specific risk are contained within the document, the projects outlined are reflected within the Informatics Risk Register. Risk Reference Codes are as follows: 332- Data Centre Failure at WGH, Risk Score - 16 438 - Server room failure at BGH, Risk Score – 15 412 – Age of Servers, Risk Score - 15
Safon(au) Gofal ac Iechyd: Health and Care Standard(s):	3.4 Information Governance and Communications Technology 5. Timely Care 3.5 Record Keeping
Amcanion Strategol y BIP: UHB Strategic Objectives:	4. Improve the productivity and quality of our services using the principles of prudent health care and the opportunities to innovate and work with partners. 5. Deliver, as a minimum requirement, outcome and delivery framework work targets and specifically eliminate the need for unnecessary travel & waiting times, as well as return the organisation to a sound financial footing over the lifetime of this plan
Amcanion Llesiant BIP: UHB Well-being Objectives: Hyperlink to HDdUHB Well-being Statement	Improve efficiency and quality of services through collaboration with people, communities and partners Develop a sustainable skilled workforce

Gwybodaeth Ychwanegol: **Further Information:**	
Ar sail tystiolaeth: Evidence Base:	Not applicable
Rhestr Termau: Glossary of Terms:	Included within the report

Partïon / Pwyllgorau â ymgynhorwyd ymlaen llaw y Pwyllgor Archwilio a Sicrwydd Risg: Parties / Committees consulted prior to Audit and Risk Assurance Committee:	Business Planning and Performance Assurance Committee Information Governance Sub-Committee

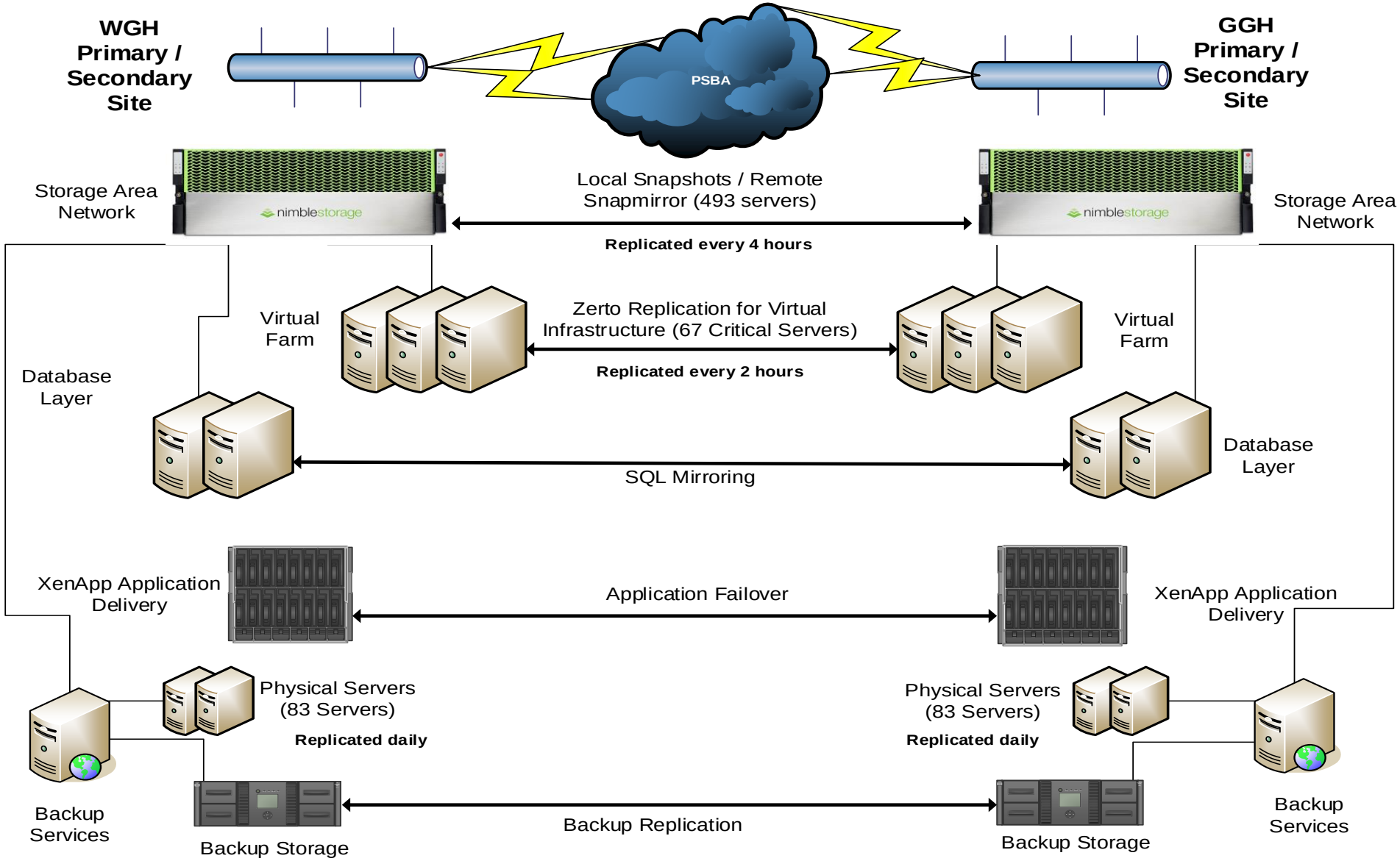
Effaith: (rhaid cwblhau) **Impact: (must be completed)**	
Ariannol / Gwerth am Arian: **Financial / Service:**	Not Applicable
Ansawdd / Gofal Claf: **Quality / Patient Care:**	The lack of a robust disaster recovery and business continuity may affect the provision of services within the Health Board and therefore patient care. Poor quality data could result in misidentification of patients along with service changes without a full accurate picture
Gweithlu: **Workforce:**	Not Applicable
Risg: **Risk:**	The risk of a catastrophic failure is being managed by the ICT Team.
Cyfreithiol: **Legal:**	Not Applicable
Enw Da: **Reputational:**	A catastrophic failure of ICT systems will cause business disruption and reputational issues with the public as services will be affected.
Gyfrinachedd: **Privacy:**	Not Applicable
Cydraddoldeb: **Equality:**	Not Applicable

Appendix 1 – Overdue Recommendations

Recommendation / Finding	Original Reporting Status	Original Management Response	Lead Director and Officer	Target date for implementation	September 2019 update
Wales Audit Office Report - Disaster Recovery and Business Continuity					
R3 - Finalise the Disaster Recovery Strategy and develop an ICT assurance work plan, which includes a disaster recovery improvement programme. The programme should incorporate ICT disaster recovery training, the data centre project and the backup system project					
Finalise the Disaster Recovery Strategy and develop an ICT assurance work plan, which includes a disaster recovery improvement programme. The programme should incorporate ICT disaster recovery training, the data centre project and the backup system project	Overdue	Additional training is being scheduled for our backup and disaster recovery products during September / October 2018. - complete The Data Centre project at GGH will be completed by the end of October 2018 now the new unit has recently been delivered and commissioning underway. Backup project has been completed.	**Lead Director(s)** Director of Planning, Performance, Informatics and Commissioning **Lead Officer(s)** Assistant Director of Informatics / Head of ICT	No date provided	Complete The Health Board has a documented Disaster Recovery and Business Continuity Strategy, which has been supplied to WAO for information. The strategy is based around technology focused recovery plans, and generic test plans for systems. The diagram in Appendix 2, details at a high level the replication services currently in operations within the Health Board. Appendix 3 provides an extract from the strategy on the backup approach. As part of the disaster recovery programme, 10 servers at the replication storage level (1), and 10 at the replication VM (virtual machine) (2) level are tested monthly, and any lessons learned are developed. The Glangwili data centre has been completed and is now fully operational. Work is now underway to replace the Prince Philip Hospital data centre, which will further improve resilience as there is a direct 10gb link between these sites which will reduce the strain on the network when replication and backups are being taken. The PPH data centre will be commissioned in 2019/20, and be delivered on site by March 2020, and commissioned in 2020/21.
R5 - Develop and document an ICT Disaster Recovery plan for all systems for which the Health Board has disaster recovery responsibility					
Develop and document an ICT Disaster Recovery plan for all	Overdue	Plans will be developed to support the DR test for the end of the calendar year and	**Lead Director(s)** Director of	December 2018	In Progress

Recommendation / Finding	Original Reporting Status	Original Management Response	Lead Director and Officer	Target date for implementation	September 2019 update
systems for which the Health Board has disaster recovery responsibility		these will be communicated to the IAO group for approval.	Planning, Performance, Informatics and Commissioning **Lead Officer(s)** Assistant Director of Informatics / Head of ICT	Revised date March 2020 – this is linked to the Information Asset Owners work. The ICT work has been completed	Generic recovery plans have been developed, which are technology based rather than system specific. For instance, the necessary steps to recovery the virtual server environment are the same for the vast majority of services and systems. This information has been supplied to WAO for consideration. Work is still progressing with the Information Asset Owners (IAO) to ensure that the services have their business continuity processes in place. The Assistant Director of Informatics is continuing to work with the Head of Emergency Planning to ensure that connections are made between the work that associated with major incidents and business continuity and the Information Asset work.
R8 - Design and implement a schedule of regular back-up media and disaster recovery testing to provide assurance that applications and data can be successfully restored in the time required after the loss of a system					
Design and implement a schedule of regular back-up media and disaster recovery testing to provide assurance that applications and data can be successfully restored in the time required after the loss of a system	Overdue	Plans will be developed to support the DR test for the end of the calendar year and this will be scheduled along with backup testing once maintenance windows have been agreed with IAO. This is tied in with the project to adopt formal patching strategies for all services.	**Lead Director(s)** Director of Planning, Performance, Informatics and Commissioning **Lead Officer(s)** Assistant Director of Informatics /	No date provided	A regular schedule of backups is in operation within the Health Board as outlined within the Disaster Recovery and Business Continuity Strategy and the diagram in Appendix 2.

Recommendation / Finding	Original Reporting Status	Original Management Response	Lead Director and Officer	Target date for implementation	September 2019 update
			Head of ICT		However, the recommended “whole system” test has not been completed. The current backup system does not have the functionality to mirror the infrastructure to allow a full test to be completed. Without this functionality the ICT Team would have to make critical services unavailable to the Health Board for 3-4 hours to undertake the full failover. This would mean that the Health Board would be without ICT for 3-4 hours. The ICT Team have been working with key clinical areas to test individual systems within their agreed maintenance window, however a full system test is not able to be undertaken. The Health Board’s current backup solution (Asigra) is out of support in March 2021, so the ICT Team will be undertaking reprocurement of a backup solution during early 2020/21, and as part of this will be requesting the functionality to mirror the production (live) environments into a test facility to demonstrate and provide assurances that the failover will work on a “whole system” approach.


WGH Primary / Secondary Site
PSBA
GGH Primary / Secondary Site
Storage Area Network
Local Snapshots / Remote Snapmirror (493 servers)
Replicated every 4 hours
Storage Area Network
Virtual Farm
Zerto Replication for Virtual Infrastructure (67 Critical Servers)
Replicated every 2 hours
Virtual Farm
Database Layer
SQL Mirroring
Database Layer
XenApp Application Delivery
Application Failover
XenApp Application Delivery
Physical Servers (83 Servers)
Replicated daily
Physical Servers (83 Servers)
Replicated daily
Backup Services
Backup Storage
Backup Replication
Backup Storage
Backup Services

All ICT infrastructures will be backed up using the product selected for backup services across Hywel Dda which is Asigra, Zerto and Nimble snapping and replication technologies. This model will support the site resilience required through the use of dual systems located on each of our two main Data Centre's. Backup systems will be configured to support the "Recovery Time Objective" and the "Recovery Point Objective" set out in our service schedules as below:-

Service Schedule	Recovery Time Objective	Recovery Point Objective
Critical Services	4 Hours	4 Hours
Standard Services	8 Hours	8 Hours

The above will be achieved using the following approach:-

8.1 Critical Services Virtual

- Zerto / 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

8.2 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

8.3 Standard Services Virtual

- Nimble snapshots at 8 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

8.4 Standard Services Physical

- Incremental block level backups at 8 hourly intervals to primary backup disk and then replicated to secondary backup disk on a different site.
- Backup data retained for 1 year

WALES AUDIT OFFICE
SWYDDFA ARCHWILIO CYMRU

Archwilydd Cyffredinol Cymru
Auditor General for Wales

Follow-up Information Backup, Disaster Recovery and Business Continuity, and Data Quality: Update on Progress – **Hywel Dda University Health Board**

Audit year: 2017

Date issued: March 2018

Document reference:

This work was delivered by Melanie Williams and Anne Beegan.

Contents

Historically, the Health Board has addressed recommendations slowly, but over the last 12 months, it has implemented the majority of recommendations, and work is underway to complete the remainder

Summary Report

Introduction

1 The world of technology has developed significantly in the last century and the rate of change is continuing at pace. Two of the more significant outcomes of this is our increased reliance on technology and the exponential increase in the volume of data we now hold and rely on.

2 Health Boards need to ensure they have reliable, secure, and accurate information systems and data on which they can rely to ensure patient safety. Over the last few years and particularly in the last 12 months we have seen increasing cyber-attacks affecting the IT systems of a number of companies and their ability to continue business as usual. This included a cyber-attack in 2017, which affected many organisations worldwide.

3 The 2017 cyber-attack affected a significant number of NHS bodies throughout the UK including here in Wales. In England, the cyber-attack caused a number of NHS bodies to suspend services directly affecting patients. They have acknowledged that their IT disaster recovery and their IT and operational/clinical business continuity did not operate as they anticipated. While this did not result in a loss of any data, there were delays in recovering systems and in continuing normal patient services while these systems were offline. While the impact on the NHS in Wales was not as severe as in England, the NHS in Wales should not be complacent but should learn from the experience of the NHS bodies in England.

4 Since 2012, we have completed Information Technology and Information Governance audits at Hywel Dda University Health Board (the Health Board) which have resulted in numerous recommendations. Previous follow-up reviews have identified that the Health Board has been slow in acting on these recommendations

5 As part of the Audit Plan for 2017, the Auditor General included local work to provide an updated position on recommendations from our IT reports undertaken between 2012 and 2015. We began in September 2017 and asked the following question: **Has the Health Board made sufficient progress in response to the recommendations made in the original reviews?**

6 In undertaking this progress update, we have:

- reviewed a range of documentation, including reports to the Board and its committees;
- reviewed system documentation and viewed live system information including testing some system controls;
- reviewed reports relating to work carried out by Internal Audit and NWIS which have impacted on or superseded our recommendations;
- interviewed a number of Health Board staff to discuss progress, current issues and future challenges.

7 The following section provides a summary of our findings. Appendix 1 provides further details.

Our findings

8 Our overall conclusion is that historically, the Health Board has addressed recommendations slowly, but over the last 12 months, it has implemented the majority of recommendations, and work is underway to complete the remainder.

9 In summary, the status of progress against each of the previous recommendations is set out in Exhibit 1.

Exhibit 1: status of previous recommendations

Total number of recommendations	Implemented	In progress	Overdue	Superseded
26	16	9	-	1

Source: Wales Audit Office

10 We found that the Health Board has implemented 16 recommendations and made progress against nine of the recommendations, with one recommendation having been superseded.

- Information backup arrangements have substantially improved. Information Asset Owners and an Asset Register are now in place. Backup software is now in place, which has strengthened backup arrangements, but the Health Board still needs to develop backup policies for all systems. Currently generic policies exist based on national guidelines for the service type but information asset owners have not yet agreed these policies.
- The Health Board needs to further improve its disaster recovery and business continuity arrangements. Critically, it needs to test the arrangements to ensure they would operate as anticipated in the event of a catastrophic fail or significant successful cyber-attack.
- Data quality arrangements have improved but the Health Board needs to increase the pace of improvement particularly in engaging the information asset owners in the data quality assurance process

Recommendations

11 We have identified two areas in relation to information backup arrangements that merit further recommendations. The Health Board needs to continue to make progress in addressing all outstanding recommendations. New and outstanding recommendations are set out in Exhibit 2.

Exhibit 2: recommendations

Previous recommendations that are still outstanding
Information Backup review
R3 Develop formal backup policies and plans for each system, which are agreed with asset owners and are based on the risk assessment.
Disaster Recovery and Business Continuity
R1 Develop a corporate approach to strengthen and support best practice in Disaster Recovery and Business Continuity (DR/BC), using a risk-based approach to prioritising resources to achieve it.
R3 Finalise the Disaster Recovery Strategy and develop an ICT assurance work plan, which includes a disaster recovery improvement programme. The programme should incorporate ICT disaster recovery training, the data centre project and the backup system project
R4 Ensure in the Health Board's Business Continuity project the following are completed: • business continuity plans are developed for all departments (including ICT); and • define and implement the corporate process for monitoring, auditing and reporting progress for the regular testing of departmental business continuity plans
R5 Develop and document an ICT Disaster Recovery plan for all systems for which the Health Board has disaster recovery responsibility
R8 Design and implement a schedule of regular back-up media and disaster recovery testing to provide assurance that applications and data can be successfully restored in the time required after the loss of a system
Data Quality
R3 Introduce an annual report on data quality to provide organisational-level assurance which covers the arrangements in place to ensure data quality, and the effectiveness of the arrangements.
R5 Review the 'Strategy for Information Assurance within Hywel Dda Health Board' and ensure that it adequately covers all of the elements of a data quality policy, including: • data standards; use of patient information records; security and confidentiality; data and health records accreditation; quality of data used for performance reporting; data sourced from other providers; references to Clinical Coding and Clinical Coding Audit policies.
R8 Review the data quality processes at service level and ensure that good practice and testing mechanisms are shared and used across the whole Health Board. This may include: • routine data cleansing exercises to improve consistency between PAS and Radiology systems; • establishment of weekly clinical coding supervisor sample testing and other good practice departmental checking mechanisms

Previous recommendations that are still outstanding
New recommendations
Information backup
R11 Introduce continual monitoring of the Solarwinds software to identify network issues before they become critical.
R12 Implement a daily monitoring rota for the Asigra backup system to identify storage capacity issues before they become critical.

Source: Wales Audit Office

Appendix 1

Progress that the Health Board has made since our previous recommendations made between 2012 and 2015

Exhibit 3: Assessment of progress

Recommendation	Target date for implementation	Status	Summary of progress
Information Backup Review			
Planning for backup arrangements			
R1 Complete the asset register and identification/allocation of asset owners. The register should also identify whether there is a backup plan in place and link to the location of that backup plan. Backup plans should be based on a risk assessment of the individual system, agreed with asset owners and should meet the needs of the users.	March 16	Implemented	In our previous review, we found that while an information asset register existed it was incomplete and difficult to follow. It did not document whether there was a backup plan in place for each of the systems and it did not identify the location of each backup. Weaknesses in the information asset register were also identified in the Disaster Recovery/Business Continuity report of February 2012 and in our IM&T risk assessment in February 2014. Since our review, the Health Board made progress and now has a more comprehensive asset register in place called the service catalogue. This covers all systems and servers, is fully complete for all of the business critical systems (clinical and administration systems) and identifies whether these are national systems or local systems. The catalogue also records whether a backup is in place and details the type of backup and server location. The service catalogue identifies asset owners and there is an Information Asset Owners (IAO) group, which agrees changes to backup schedules and arrangements. The Health Board has an up to date backup monitoring system in place which records and automatically alerts IT staff via system email when

Recommendation		Target date for implementation	Status	Summary of progress
				problems occur with any of the backups. This system records and monitors all backups for servers and systems under the control of IT. (It does not monitor national systems or anything outside the control of IT). IT staff are also able to view the backup system log at any time. In addition to the service catalogue, the information governance team, with support from the IT team and department users, are conducting information asset audits to prepare for the introduction of the General Data Protection Regulations (GDPR) in May 2018. At the time of our audit, not all of the information asset audits had been completed but good progress had been made. These audits will ultimately ensure that the Health Board has a complete understanding of all its information assets. They will also identify any IT systems, which by definition will be information assets, not under the control of IT, should any exist.
R2	Undertake a risk assessment of all IT systems to allow the Health Board to identify a prioritised response to system failure, and senior management to identify whether current IT resources are sufficient to mitigate the risks to the IT infrastructure and network in the event of a catastrophic failure	March 2016	Implemented	Our previous review identified that changes to IT backup schedules were not formally monitored or agreed with asset owners. Our review also identified that no overall risk assessment of all IT systems had been undertaken. The Health Board has still not undertaken a full risk assessment of all its systems due to the lack of resources. However, the Health Board does have an up to date ICT risk register which feeds into the corporate risk register recording the major ICT risks across the Health Board. With Information Asset Owners now in place for all the business critical systems, the IAO group now identifies any significant risks and feeds them into the ICT risk register. This would include identifying the need to increase the backup frequency or type of backup to meet service needs in the event of a catastrophic fail.
R3	Develop formal backup policies and plans for each system, which are agreed with asset owners and are based on the risk assessment put forward in R2 above	March 2016	In progress	Our previous review identified that formal backup policies and plans for each system did not exist and asset owners were not in place. A formal backup policy is now in place and, while not all systems have specific plans in place, generic plans based on the technology type and system use have been developed for all systems and are monitored by backup monitoring software. The Health Board is in the process of developing specific plans for all major business critical systems under

Recommendation		Target date for implementation	Status	Summary of progress
				its control. These are being developed with the Information Asset Owners and IT team.
R4	Agree and formally authorise the backup agreement for the Myrddin national system.	March 2016	Implemented	Our previous review identified that the agreement between the Health Board and NWIS for the backup of the nationally controlled Myrddin system had not been formally agreed or authorised. A formal agreement between the Health Board and NWIS is now in place for the Myrddin national system.
Arrangements to deliver effective backups				
R5	Confirm that critical legacy clinical systems, such as Breast PACS, Cardiology PACS and DAWN Warfarin prescribing system are located within the secure virtual environment. As a minimum all systems should be backed up to a remote site at a time and frequency appropriate to the criticality of the system and its data.	April 2016	Implemented	In our previous review, we found critical legacy systems including Breast PACS, Cardiology PACS and DAWN Warfarin prescribing systems were not located within the secure virtual environment. The status and location of these systems has been reviewed with the following results: • DAWN Warfarin prescribing system has had its infrastructure refreshed and it is now located within the main data centres and is replicated between sites; • Cardiology PACS is located on a separate infrastructure but held within the main data centres; and • Breast PACS is in the process of being migrated to the main Fuji PACS environment but backup arrangements are in place while this is taking place. All systems are backed up and replicated between the main data centres. Backups are monitored.
R6	Develop a procedure to ensure that all changes to backup policies, plans and procedures are fully documented and approved by an appropriate manager.	September 2016	Implemented	Our previous review found that formal change control procedures did not exist to document changes to backup policies, plans and procedures. As referred to above, the IAO group identifies changes to backup plans and procedures. These will then be documented as service management activities in the annual Informatics Operational Plan. Formal backup policy changes will form part of the annual Informatics Operational Plan as necessary or update frequency dictates. Since these procedures are new we have not been able to see these operating but the arrangements are now in place.

Recommendation		Target date for implementation	Status	Summary of progress
R7	Implement monitoring procedures for live and backup server hardware and all associated software	April 2016	Implemented but possible further benefits to be gained	Formal procedures for monitoring the live and backup server hardware were not in place during our Backup Review. The Solarwinds system, used in a number of Health Boards, is now being used to monitor network and both live and backup servers. It provides a visual dashboard display and daily reports on system/server health and backup performance. The effectiveness of this system would be further enhanced to enable the IT team to identify issues before they become system/server critical if display monitors showing the live dashboard were available to and monitored by staff on an ongoing basis, perhaps by the help desk team.
R8	Where possible, replace ageing hardware that is due to go out of support to ensure security of the systems and data. This was also recommended in our 2012 Disaster Recovery (DR) and Business Continuity (BC) report	April 2016	Implemented	Both our Backup Review, and our Disaster Recovery and Business Continuity Review recommended that aging hardware that is due to go out of support should be replaced where possible. Most legacy systems in place during our reviews and within the control of the Health Board have now been replaced but with the technology landscape moving forward at pace this is an ongoing challenge for the Health Board. However aging hardware is being replaced as capital funding allows and this is demonstrated by the legacy hardware and software scheduled to be replaced on the 2017/18 ICT Operational Plan as follows: • Network hardware at Glangwili Hospital • E-Mail • VMWARE • Storage systems Although aging hardware and software is still being replaced, we have considered this recommendation implemented as the Health Board is replacing outdated hardware and systems as funding allows. We will continue to monitor this as part of our annual risk assessment to ensure the Health Board is not putting patient safety at risk by not replacing hardware and software that is out of date and no longer supported.

Recommendation	Target date for implementation	Status	Summary of progress
Performance monitoring for backups			
R9 Consider standardising the backup software used as this may prove more efficient and be more easily monitored. As a minimum: • all backup software and hardware should be up to date and monitored regularly; and • backups should tested on a regular basis. Backup testing, where test systems are regularly created from backup media, can be evidenced by recording each test system creation as a Disaster Recovery test.	April 2016	Implemented	Our Backup Review identified that there were a number of different backup software in use. This was largely due to legacy backup systems still being in place for some systems. Monitoring the variety of systems was inefficient as was maintaining the number of backup systems Since our review, the Health Board has purchased the Asigra backup system, which is now used to backup the systems under the control of the Health Board (National systems are subject to national backup arrangements and not within the control of the Health Board). Initially, full implementation of the new backup system was delayed due to storage issues but this was rectified in March 2017 and the final legacy backup system has now been decommissioned. Asigra backup also monitors all backups and provides alerts of any backup fails or issues allowing the IT team to take appropriate remedial action. This system also allows full scheduling of backups to be recorded along with any changes to the scheduling, providing an audit trail for backups.
R10 Ensure that performance of backups, file size, issues encountered, time to resolve issues are recorded and reported formally to senior managers and appropriate committees. Collection of performance information can identify potential data storage issues, hardware:	April 2016	Implemented but further benefits to be gained	In our previous review, we found that the performance of backups was not consistently monitored or reported, and there was a risk that potential hardware, software and data storage issues would not be identified with sufficient time for the Health Board to take remedial action. As detailed above, the new Asigra backup system provides reports and active monitoring of the backups. However, this system is not actively monitored on a daily basis and, while actual faults will be emailed to staff by the system, this may still not provide sufficient time for the Health Board to take action on issues such as storage capacity. To mitigate this, the Health Board should timetable/schedule staff to review the Asigra system reports on a daily basis with a view to identifying arising problems before actual failure occurs.
Disaster Recovery & Business Continuity			

Recommendation		Target date for implementation	Status	Summary of progress
R1	Develop a corporate approach to strengthen and support best practice in Disaster Recovery and Business Continuity (DR/BC), using a risk-based approach to prioritising resources to achieve it	-	In progress	Our previous reviews identified that there was a lack of interaction between users and IT, and that no disaster recovery risk assessments had been completed resulting in a lack of clarity on system recovery times Our original report was issued in 2012 and we reviewed progress in 2015 when no significant progress had been made. Since 2015, the IT team recognised that it was taking time to set up the IAO group and that action was needed in the interim. The IT team have therefore used national recovery point objective (RPO) /recovery time objective (RTO) guidelines based on the service categorisation to set up interim recovery points and times for each system. While this still lacks the interaction with users, it does provide more clarity on DR/BC and represents progress against the recommendation. The plan is that the IAO group will discuss and agree the RPO and RTO for all major business critical systems in the near future. Since the IAO group is still in the early stages of development and have only met a few times at the time of our audit, this is still work in progress and as such, we will review progress against this in future audits.
R2	Review the contracts and agreements with external suppliers of clinical systems to ensure that there is adequate definition of: • responsibilities of the supplier and recipient organisations; • service location, set-up and resilience features; • service availability and contacts; • Key Performance Indicators (KPIs) and reporting these; • back-up arrangements; and • disaster recovery and business continuity arrangements.	-	Implemented depending on undertaking from the Health Board	Our 2015 review of progress against this recommendation identified that contracts for all major business critical IT systems had been reviewed. However, at that time we were unable to confirm that all contracts had been reviewed. The IT team have confirmed that no further progress has been made against this recommendation due to the number of contracts in place and the significant resources it would take to carry out a formal review of all contracts. Contracts will be reviewed as they come due for renewal. We recognise the pressures on the IT teams limited resources, that the contracts associated with the business critical IT systems have been reviewed, and that the majority of these are under formal SLA or managed services. We consider this recommendation implemented providing the Health Board agree that as contracts come to an end and they are renewed or replaced, the new contracts have adequate definition of the points made in the original recommendation as follows: • responsibilities of the supplier and recipient organisations;

Recommendation		Target date for implementation	Status	Summary of progress
				• service location, set-up and resilience features; • service availability and contacts; • Key Performance Indicators (KPIs) and reporting these; • back-up arrangements; and • disaster recovery and business continuity arrangements.
R3	Finalise the Disaster Recovery Strategy and develop an ICT assurance work plan, which includes a disaster recovery improvement programme. The programme should incorporate ICT disaster recovery training, the data centre project and the backup system project	-	In progress	Our 2015 review identified that while progress had been made against this recommendation and there was a disaster recovery strategy in place, it did not reflect the fact that there were still legacy systems that remained outside the main data centre. Additionally service schedules had still not been agreed with system owners, data owners had not been identified for all systems and a full DR test had not been carried out. Further progress has now been made and the majority of legacy systems now sit within the main data centres. All of the business critical systems are now within this environment and backed up or replicated across the main data sites. Information Asset Owners are identified for all the business critical systems and are in the process of being identified for all systems as part of the GDPR work stream. Despite the progress made, action is still needed to fully comply with this recommendation. The IAO group is still at the early stage of development and therefore have not yet discussed and agreed the disaster recovery points or times for each system – these are currently generic points and times based on national guidelines for the types of services. This needs to be progressed and agreed recovery points and times, with associated resources should be set for each of the Health Boards IT systems/services. Finally, a formal DR test has been planned for the last 2 years but has not yet taken place. This means the Health Board has no definitive confirmation that the DR plans in place will result in the Health Board being able to recover its systems and services in the stated timeframe or indeed recover them at all should a catastrophic fail or significant cyber-attack occur. Feedback from English health organisations significantly affected by the recent cyber-attack identified that in the majority of cases, while they were able to recover their data, they could not do so within

Recommendation		Target date for implementation	Status	Summary of progress
				anticipated timeframes. They also identified that other elements of the disaster recovery plans, such as manual workarounds used while systems were down, did not operate as planned. A full-scale DR test would identify such issues in a controlled environment and allow the Health Board to be better prepared in the event of future cyber-attack or system/network fails.
R4	Ensure in the Health Board's Business Continuity project the following are completed: • business continuity plans are developed for all departments (including ICT); and • define and implement the corporate process for monitoring, auditing and reporting progress for the regular testing of departmental business continuity plans	-	In progress – linked to point 3 above	Business continuity and disaster recovery plans have been developed for all departments but not fully tested – see points against R3 above
R5	Develop and document an ICT Disaster Recovery plan for all systems for which the Health Board has disaster recovery responsibility.	-	In progress	Our previous follow up review in 2015 identified that plans were in place for national systems, Myrddin and the Welsh Clinical Portal but not in place for other systems. Generic ICT DR plans have now been developed for all systems but these have not yet been discussed or agreed with Information Asset Owners (system owners). There are plans to agree formal DR plans for each system with Information Asset Owners once the IAO group is fully established and the GDPR work, which needs to be completed before May 2018, is complete.
R6	Assess the physical and environmental controls at the Glangwili and Withybush data centres and deliver any necessary improvements as part of the data centre project.	-	Superseded by NWIS review	Our 2015 follow up review identified that the access controls at the main data centres were adequate at that time but that the controls at server rooms outside the main data centres were unknown. During 2017, NWIS carried out a formal review of data centres across the Health Board. Actions to address the recommendations from this review have been incorporated into the 2017/18 Information Governance Workplan and are in the process of being completed.

Recommendation	Target date for implementation	Status	Summary of progress
			Assurance will be provided to NWIS on progress against their recommendations and therefore we will consider our recommendation implemented given the NWIS review supersedes our previous review.
R7 Further improve the ICT network infrastructure resilience: • review and update all local area network diagrams to ensure that they reflect the current network configuration; • based on risk assessment, develop a programme of routine replacement of equipment as it becomes obsolete or unreliable; • complete an audit to map the location of all systems' servers and any associated contingency arrangements; and • ensure that adequate backup arrangements are in place for all systems, including storage of backup tapes in an off-site fireproof safe	-	Implemented	Our 2015 follow up review identified that the Health Board had implemented most of the actions required for this recommendation but that adequate backup arrangements were not in place across all systems and the network diagrams covered only the main data centre sites. Our review of backup arrangements covered above addresses the issues of backups not being in place for all systems. Network diagrams are now in place for all sites. An ICT network project is underway to address the current risk associated with the network at the Glangwili site with funding bids planned in future years for the other acute sites.
R8 Design and implement a schedule of regular back-up media and disaster recovery testing to provide assurance that applications and data can be successfully restored in the time required after the loss of a system	-	In progress	Our 2015 follow up review identified that backup testing was in place for some systems but that for other business critical systems such as Mental Health, Data Warehouse, E-rostering etc. there was no evidence of DR testing. A full service catalogue (information asset register) is now in place and we have been informed that testing windows are being developed as part of the further development of the service catalogue. Additionally new backup software now monitors all backups and provides alerts where backup has been unsuccessful or where there were issues. This

Recommendation		Target date for implementation	Status	Summary of progress
				shows that progress has been made but that full testing of backups is not yet in place.
Data Quality				
R1	Review the contribution of all data quality supporting groups and their reporting mechanisms, and ensure that there is a complete escalation process to advise the Board of key issues and risks	-	Implemented	Our 2015 follow up identified that operational meetings were taking place for the systems under the control of IT. The Health Board now have Information Asset Owners in place for all business critical systems and are in the process of identifying Information Asset Owners for the remaining systems. The IAO group meets regularly and covers data quality as part of their remit. The group is monitored by the Information Governance Sub Committee and any issues or risks are escalated to the Executive team or Board via this sub committee
R2	Initiate the Data Quality Steering Group: Agree and authorise the Terms of Reference; assign business-wide departmental data quality champions and ensure this group is included within the reporting mechanism for supporting groups	-	Implemented	As per R1 above, the data quality steering group has been replaced by the IAO group, which has data quality as part of its remit. The Information Asset Owners are the data quality champions for their departments.
R3	Introduce an annual report on data quality to provide organisational-level assurance which covers the arrangements in place to ensure data quality, and the effectiveness of the arrangements	-	In progress	Our 2015 follow up review identified that a data quality report was in place for the Myrddin system but did not include other systems. This has not been further progressed to date but an initial report, which will include additional information, was planned for October 2017 with further development for the 2017/18 annual report. Given the slow progress against this recommendation, we will review the 2017/18 annual report and the data quality information contained within that report. The Health Board needs to increase the pace of its progress on data quality reporting
R4	Clarify data quality roles and responsibilities across the Health Board and ensure,	-	Implemented	Our 2015 follow up identified this as implemented as this is now part of the all Wales job description which includes a specific section on data quality and is used by the NHS Wales wide.

Recommendation	Target date for implementation	Status	Summary of progress
for all staff with responsibility for the accuracy of data, that: • responsibilities are defined within standardised job descriptions; and • these are communicated and understood.			
R5 Review the 'Strategy for Information Assurance within Hywel Dda Health Board' and ensure that it adequately covers all of the elements of a data quality policy, including: • data standards; • use of patient information records; • security and confidentiality; • data and health records accreditation; • quality of data used for performance reporting; • data sourced from other providers; and • references to Clinical Coding and Clinical Coding Audit policies.	-	In progress	Although the Health Board action plan of 2015 identified that a revised strategy had been developed, which was going through the information governance process, we were not provided with a copy of the draft strategy at that time. The Information Assurance Strategy is now being reviewed as part of the GDPR programme which includes a wider review of all information governance documents, such as policies, procedures and WASPI's, to ensure they are GDPR compliant. The plan was not finalised or approved at the time of our audit. We will follow up this recommendation as part of our 2018 IT risk assessment.
R6 Ensure that the migration to a single Myrddin system project includes a: • process mapping exercise to standardise procedures; and • a training and awareness programme for all data input staff	-	Implemented	Our 2015 follow up identified that all, but Mental Health and Sexual Health services had been migrated into a single Myrddin system. The Health Board have made the decision, because of the sensitive nature of the data, to retain a separate Myrddin system for Sexual Health and we accept this decision. Mental Health was initially scheduled to be migrated into the main Myrddin system in April 2015. However, the Health Board and NWIS

Recommendation		Target date for implementation	Status	Summary of progress
				identified, while working through the logistics of the migration with NWIS, that this would be difficult. The Health Board are now waiting for this to be progressed by NWIS and it is therefore largely outside their control. Given this is within the remit of NWIS rather than the Health Board; we have considered this action implemented from the Health Boards perspective.
R7	Ensure that sufficient staffing resources are allocated to all clinical coding teams, and review the structure and educational requirements to maintain equality across the counties.	-	Implemented	Our 2015 review identified that action on this recommendation was complete. Since that review, further guidance has been provided by NWIS regarding the required number of coders and the Health Board has identified that it is complying with this, more up to date, guidance. Our 2018 planned all-Wales follow-up of clinical coding will review coding arrangements in more detail.
R8	Review the data quality processes at service level and ensure that good practice and testing mechanisms are shared and used across the whole Health Board. This may include: • routine data cleansing exercises to improve consistency between PAS and Radiology systems; • establishment of weekly clinical coding supervisor sample testing and other good practice departmental checking mechanisms	-	In progress	Our 2015 follow up identified that progress had been made, but that the progress did not fully address the audit recommendation particularly in relation to the reporting of the accuracy of clinical coding. The Health Board now has Information Asset Owners in place and as part of the IAO group; standardised approaches to data quality in respect of GP updates, patient deaths, duplicate records, etc. are being developed. This has not yet happened. Clinical coding audit process has been developed and implemented, but difficulties have been encountered in conducting the audits due to significant work pressures and changes to national targets. While we recognise that progress has been made in this area we consider that the recommendation has still not been fully met. We acknowledge that not all the barriers to this are within the Health Boards control such as the changes to national targets. We will continue to monitor progress against this recommendation, in particular the input and impact of the IAO group to this process.

Appendix 2

The Health Board's management response to new recommendations relating to information backup

Exhibit 4: management response

Ref	Recommendation	Intended outcome/benefit	High priority (yes/no)	Accepted (yes/no)	Management response	Completion date	Responsible officer
R11	Introduce continual monitoring of the Solarwinds software to identify network issues before they become critical.	To identify emerging system and network issues before they become critical	Yes	Yes	The Health Board is in the process of introducing enhanced monitoring tools within Solarwinds to ensure that alerts can be sent to the Head of ICT and the Infrastructure Manager to ensure that network issues are monitored within and out of hours	June 2018	Assistant Director of Informatics Head of ICT
R12	Implement a daily monitoring rota for the Asigra backup system to identify storage capacity issues before they become critical.	To identify backup storage, which is nearing capacity before the storage capacity, is exhausted and the situation becomes critical.	Yes	Yes	The newly implemented storage infrastructure has an improved monitoring and an embedded analytical tool, which allows ease of monitoring.	June 2018	Assistant Director of Informatics Head of ICT

Wales Audit Office
24 Cathedral Road
Cardiff CF11 9LJ

Tel: 029 2032 0500
Fax: 029 2032 0600
Textphone : 029 2032 0660

E-mail: info@audit.wales
Website: www.audit.wales

Swyddfa Archwilio Cymru
24 Heol y Gadeirlan
Caerdydd CF11 9LJ

Ffôn: 029 2032 0500
Ffacs: 029 2032 0600
Ffôn testun: 029 2032 0660

E-bost: post@archwilio.cymru
Gwefan: www.archwilio.cymru