Archwilydd Cyffredinol Cymru
Auditor General for Wales

WALES AUDIT OFFICE
SWYDDFA ARCHWILIO CYMRU

Combined follow-up of Information Management and Technology audits

Cwm Taf University Health Board

Issued: December 2015

Document reference: 592A2015

Status of report

This document has been prepared for the internal use of Cwm Taf University Health Board as part of work performed/to be performed in accordance with statutory functions.

No responsibility is taken by the Auditor General, the staff of the Wales Audit Office or, where applicable, the appointed auditor in relation to any member, director, officer or other employee in their individual capacity, or to any third party.

In the event of receiving a request for information to which this document may be relevant, attention is drawn to the Code of Practice issued under section 45 of the Freedom of Information Act 2000. The section 45 Code sets out the practice in the handling of requests that is expected of public authorities, including consultation with relevant third parties. In relation to this document, the Auditor General for Wales, the Wales Audit Office and, where applicable, the appointed auditor are relevant third parties. Any enquiries regarding disclosure or re-use of this document should be sent to the Wales Audit Office at info.officer@audit.wales.

The person who delivered the work was Gareth Lewis.

Contents

Cwm Taf University Health Board (the Health Board) is strengthening arrangements in the areas we have considered as part of this review however progress against our previous recommendations has been slow.

Summary report

Detailed report

Summary report

Summary

1. The Wales Audit Office has previously undertaken a number of reviews covering aspects of information management and technology (IM&T) at Cwm Taf University Health Board (the Health Board).

2. This follow-up review sought to answer the question: **'Has the Health Board made progress in addressing the key issues and recommendations highlighted in our previous reports and reviews relating to IM&T matters?'**

3. We concluded that the Health Board is strengthening arrangements in the areas we have considered as part of this review but progress against our previous recommendations has been slow.

4. Exhibit 1 summarises the key conclusions from the previous reviews, and the current position.

Exhibit 1: Key conclusions from previous Information and Communications Technology (ICT) reviews, and current position

Review name and date	Key conclusions from previous work	Current position
Information and Communications Technology (ICT) Disaster Recovery and Business Continuity Arrangements (March 2012, 202A2012)	While departments have identified ways in which they would maintain clinical services in the event of ICT failure, ICT business continuity and DR plans are not being adequately documented, tested or scrutinised.	Although most departments have used the Health Board's standard approach to business continuity planning, the available corporate template has not been followed comprehensively; the IT department does not have a DR plan and testing of DR and business continuity plans is limited.
Overview of the arrangements for information backup (November 2013, 616A2013)	Backup arrangements are still under development and there is scope for the Health Board to strengthen them. Only some of the expected backup controls are in place to ensure that backups are complete and capable of being used to restore key IT systems.	Appropriate software, hardware and access controls are used as part of backup delivery but there is no backup policy and not all procedures and backup approaches are adequately documented.
Caldicott – Key findings of 2012 structured assessment (December 2012) and Annual Audit Report 2012 (March 2013, 147A2013)	Overall, Caldicott arrangements appear adequate, but further work is required in some areas.	Caldicott governance arrangements have been strengthened, and training methods improved but some relevant staff are yet to do this training.

Review name and date	Key conclusions from previous work	Current position
Data Quality – Annual Audit Report 2012 (March 2013, 147A2013)	Our 2012 review of data quality did not provide assurance.	There are a number of initiatives to strengthen data quality arrangements, including a data quality audit programme, annual report and the addition of key staff but some of the governance arrangements require improvement.

5. Other findings that were highlighted during the completion of this review include:

- The Health Board does not have an approved ICT strategy. There are some plans to create one with the help of external contractors but, without an agreed ICT strategy, the Health Board has nothing to formally base its ICT policies, governance structure, and infrastructure developmental decisions upon.
- Although there are arrangements in place to track and monitor progress against recent Wales Audit Office audit recommendations, the IM&T related recommendations are not included. It is unclear how the Health Board can be assured that audits are appropriately considered and acted upon to facilitate further improvement.

Recommendations

6. The Health Board should continue to implement any remaining recommendations set out in our previous reports. These are reproduced below alongside new recommendations, which we have made as a result of our follow-up review.

ICT Disaster Recovery and Business Continuity Arrangements (March 2012, 202A2012)

R1 Develop business continuity plans in line with the standard set in the corporate template business continuity plan for the key clinical departments indicated in Exhibit 1 (of the original report, which were Radiology, ITU, Pharmacy, Pathology, A&E, Theatres, ICT) and ensure such plans exist for all other clinical and non-clinical departments.

R2 Develop, approve at senior level and regularly review a business continuity plan for the ICT department, based on a comprehensive risk assessment and the Health Board's template business continuity plan. This should include all risks affecting the department's ability to provide continued support for the Health Board's ICT infrastructure and systems, including staffing levels.

R3 Introduce arrangements to consider cross department and site level business continuity issues.

R4 Test business continuity plans regularly to ensure they operate as intended and adequately support continued clinical service provision within and across departments.

R5 Identify from testing of the business continuity plans and manual procedures the effect on quality, cost and timeliness of clinical service provision of utilising manual processes to inform future continuity planning.

R6 Reinforce business continuity governance arrangements by communication and training for relevant managers, clinicians and other staff and ensure that there is a clear understanding of the difference between business continuity and DR planning.

R7 Establish formal arrangements to review business continuity plans and risk assessments to ensure they are comprehensive, consistent and appropriate for business need.

R8 Improve the current ICT DR plans for each of the systems reviewed, for other key systems and for the ICT infrastructure to ensure they are adequate and meet the following minimum requirements:

- plans should be documented and written in simple language, so they are understandable to all who may need to use them;
- responsibilities for the DR plans should be clearly identified;
- there should be a clear identification of persons responsible for each function within the plan;
- contact information should be clearly identifiable;
- plans should include a step-by-step explanation of the system recovery option;
- the various resources required for recovery should be clearly identified;
- plans should be approved by an appropriate manager; and
- plans should be updated and reviewed regularly with review and version control clearly stated on the front of each plan.

R9 Test all ICT DR plans for the systems and infrastructure regularly to ensure they operate as intended.

R10 Establish and monitor clear performance indicators for the ICT department, systems and infrastructure. Use the results of this performance monitoring to inform DR planning, ICT resource planning and ICT infrastructure and system capital planning.

New 2015 recommendation

R1 Update the business continuity policy and supporting templates to:

- reflect current relevant guidelines and legislation;
- recommend that plans are reviewed and updated regularly to reflect operational changes;
- ensure that arrangements relating to cross department and site level business continuity issues are considered when plans are developed and updated; and
- sufficiently explain the governance structure of business continuity and DR, and how the Health Board specifically acquires assurance that policy requirements are met.

Overview of the arrangements for information backup (November 2013, 616A2013).

New 2015 recommendations

R2 Develop and agree a backup policy to ensure consistent backup procedures, approaches and practices are adopted across the organisation.

R3 Document and make available (to appropriate members of staff) procedures for:

- creating and amending data backups, including information on how to amend the system setting for automated backups; and
- dealing with backup failures or issues.

R4 Ensure that the 'Server Backup and Restore Documentation' referred to in the DR plans exists and meets the needs of the IT systems.

Caldicott – Key findings 2012 structured assessment (December 2012) and Annual Audit Report 2012 (March 2013, 147A2013)

New 2015 recommendations

R5 Ensure that the Caldicott Principles Handout is up to date and accurately refers to the Caldicott Guardian so that there is no misunderstanding amongst staff.

R6 Ensure that appropriate staff undertake relevant Caldicott training and maintain their knowledge by regular refresher training. This should be monitored by and reported to the Information Governance Group (IGG).

Data Quality – Annual Audit Report 2012 (March 2013, 147A2013)

New 2015 recommendations

R7 Include data quality comparisons against previous years in future annual data quality reports.

R8 Ensure that the information asset owners are named individuals who are aware of their responsibilities, which if allocated by post, should be written into their job descriptions.

R9 Ensure that the Data Quality Policy is reviewed and regularly updated to reflect any changes in operational arrangements. Apply version control arrangements to ensure that there is clarity about the current version. In addition, change the policy's wording to reflect the IGG.

New 2015 recommendations – IM&T

R10 Develop and agree an ICT Strategy.

R11 The Health Board should ensure that ICT recommendations form part of its Wales Audit Office recommendation tracker that is reported to the Audit Committee.

Detailed report

Assessment of progress

7. The tables below list the recommendations from our previous reviews and give our opinion on whether the recommendation has been fully implemented (✓), partially implemented (✓/×) or not implemented (×).

Although most departments have used the Health Board's standard approach to business continuity planning, the available corporate template has not been followed comprehensively; the IT department does not have a DR plan and testing of DR and business continuity plans is limited

Information and Communications Technology (ICT) Disaster Recovery and Business Continuity Arrangements (March 2012, 202A2012)			
Reference	**Implemented?**	**Recommendation**	**Summary of progress made**
Business Continuity			
R1	**✓/×**	Develop business continuity plans in line with the standard set in the corporate template business continuity plan for the key clinical departments indicated in Exhibit 1 (of the original report, which were Radiology, ITU, Pharmacy, Pathology, A&E, Theatres, ICT) and ensure such plans exist for all other clinical and non-clinical departments.	During our previous work, only two departments (of those reviewed) had documented plans in place. Business continuity plans are now in place for the seven departments, but one of them has not used the standard corporate approach. The other plans have followed the approach, but have not all used the available template comprehensively. For example, specific findings are: • The Radiology plan only refers to equipment failure, and does not state who initiated and approved the document, when it was approved and operational from. • The ITU plan only refers to IT system failures, and does not use the corporate template. • The Pharmacy plan has an operational date of June 2015, but no approval date, or version control. Also, it does not refer to IT system failures. • The Pathology plan does not contain a business impact analysis or any action cards.

Information and Communications Technology (ICT) Disaster Recovery and Business Continuity Arrangements (March 2012, 202A2012)

Reference	Implemented?	Recommendation	Summary of progress made
Business Continuity			
			• Although the A&E (medicine) plan appears to follow the corporate template, it is not approved, even though the electronic filename is dated 2012. Also, they do not have specific plans for each site. • The Theatres plan has no approval or operational date. • There is an ICT plan, approved and operational from September 2013, and follows the corporate template, although it does not refer to site access denial. In addition, it does not refer to the Blaenavon Data Centre, a recent addition to the Health Board's ICT infrastructure. The Health Board has a 'BCP template draft' document, and a 'Template for developing a business continuity plan' document (guidance notes), to aid managers in creating their departmental business continuity plans. However, our review of the seven business continuity plans reveals that compliance with the template is mixed. The documents appear to be advisory rather than mandatory.
R2	✓/✗	Develop, approve at senior level and regularly review a business continuity plan for the ICT department, based on a comprehensive risk assessment and the Health Board's template business continuity plan. This should include all risks affecting the department's ability to provide continued support for the Health Board's ICT infrastructure and systems, including staffing levels.	An ICT business continuity plan is in place, approved and operational from September 2013, and follows the corporate template. However, it does not include all risks affecting the department's ability to provide continued support for the Health Board's ICT infrastructure and systems, for example, site access denial. Therefore it is not based upon a comprehensive risk assessment. The plan has not been recently reviewed, and does not incorporate recent changes to the ICT infrastructure eg, the addition of facilities within Blaenavon Data Centre. The document does not specifically state who signed off the document. It was approved by the ICT department, but it is unclear who in particular within the department was part of the approval process, and their level of seniority.

Information and Communications Technology (ICT) Disaster Recovery and Business Continuity Arrangements (March 2012, 202A2012)

Reference	Implemented?	Recommendation	Summary of progress made
R3	✗	Introduce arrangements to consider cross department and site level business continuity issues.	No progress has been made on introducing arrangements to consider cross departmental and site level business continuity plans. As with our original review in 2012, there is little evidence of consideration for cross departmental business continuity planning, with departments still working in isolation. This is reflected within the business continuity policy and guidance templates.
R4	✗	Test business continuity plans regularly to ensure they operate as intended and adequately support continued clinical service provision within and across departments.	Regular and comprehensive testing of business continuity plans does not occur within the seven departments we reviewed. The Health Board's business continuity policy states that 'business continuity plans are only successful when they have been communicated to staff, tested and rehearsed. It is the responsibility of the manager who 'owns' the plan to ensure that all staff who may use it are trained. Corporate plans will be subjected to regular testing and exercising and staff subsequently trained as required.' Despite this, we found that limited testing occurs, and where it does, it is informal and does not cover the full range of scenarios. For example, the pathology department reported instances of unplanned IT system downtime, resulting in invoking elements of their plan. In reality, this only tests system downtime, and not elements such as site access denial, or major staff shortages. This level of testing is not sufficient to ensure that plans will operate as intended and adequately support continued clinical service provision within and across departments.
R5	✗	Identify from testing of the business continuity plans and manual procedures the effect on quality, cost and timeliness of clinical service provision of utilising manual processes to inform future continuity planning.	No progress has been made on this recommendation. We have seen no evidence during this follow-up to suggest that such potential effects have been recognised. Not carrying out regular comprehensive testing of their business continuity plans further hinders the department's ability to progress this recommendation.

Information and Communications Technology (ICT) Disaster Recovery and Business Continuity Arrangements (March 2012, 202A2012)			
Reference	**Implemented?**	**Recommendation**	**Summary of progress made**
R6	✓/✗	Reinforce business continuity governance arrangements by communication and training for relevant managers, clinicians and other staff and ensure that there is a clear understanding of the difference between business continuity and DR planning.	Although some guidance is available for developing business continuity plans, governance arrangements are not specified and reinforced. There is no clear approach to scrutiny and assurance with regards to business continuity. The business continuity policy refers to managerial responsibilities, but not specifically how the Health Board actually obtains assurance with regards to business continuity. The business continuity policy describes that overall responsibility for business continuity management is with the Chief Executive, who is assisted by director leads. The Corporate Director is the nominated lead director for the co-ordination of business continuity management within the Health Board. Directors are accountable to the Chief Executive for ensuring implementation of the business continuity policy within their Unit. It is from this structure that the policy says the Health Board gains appropriate assurance. There are inconsistencies within the business continuity plans that we reviewed (explained in the next section), this raises questions as to how effective the assurance process is. Because the Health Board still does not have a consistent set of plans, we cannot be sure that it has a sufficient understanding of how adequate business continuity planning at the Health Board actually is. In addition, our review identified that it is not clear who the plan owners are in all instances. Where the distinction between DR and business continuity is important ie, ICT, the staff we interviewed demonstrated an appropriate understanding of the difference.

Information and Communications Technology (ICT) Disaster Recovery and Business Continuity Arrangements (March 2012, 202A2012)			
Reference	**Implemented?**	**Recommendation**	**Summary of progress made**
R7	✓/✗	Establish formal arrangements to review business continuity plans and risk assessments to ensure they are comprehensive, consistent and appropriate for business need.	Good practice is to review business continuity plans annually. The Health Board's business continuity policy requires that plans and risk assessments are reviewed every three years as a minimum, but this is not put into practice across the Health Board. For example, of the seven plans that we reviewed, the Theatres and Radiology departmental plans have no approval or operational dates. And, although the ICT plan is operational from 2013, it requires updating to take into account the Blaenavon data centre. If plans are not approved or are out of date, they may not meet business needs. In addition, the 'Template for developing a business continuity plan' needs updating (currently its date for review is 'July 2013'), and along with the business continuity policy (approved December 2013), refers to out-dated standards. The documents reference the British Standard 25999 for business continuity management, however, this has since been replaced by the standards ISO22301 (Business continuity management) and ISO 22313 Societal security — Business continuity management systems. The Policy also states that 'a review may be required within the three year cycle as a result of the outcome of a post incident debrief highlighting issues or changes to legislation or guidance'. Although the template states that plans should also be updated within the three years for operational changes, the policy does not. The Civil Contingencies Manager (CCM) role with regards to business continuity planning is in an advisory capacity, notifying departments when their plans are up for review and suggesting amendments if necessary. How plans and risk assessments are managed and maintained is the responsibility of the departments. We were told that Clinical and Corporate Business Meetings are in place across the organisation and are used for all operational matters but they are not mandated to follow any suggestions made by the CCM.

Information and Communications Technology (ICT) Disaster Recovery and Business Continuity Arrangements (March 2012, 202A2012)			
Reference	**Implemented?**	**Recommendation**	**Summary of progress made**
Disaster Recovery (DR)			
R8	✓/✗	Improve the current ICT DR plans for each of the systems reviewed (Telepath, PACS, ICIP (now called ICCA), RADIS, TOMS, PAS A&E, EDS (pharmacy), for other key systems and for the ICT infrastructure to ensure they are adequate and meet the following minimum requirements: • plans should be documented and written in simple language, so they are understandable to all who may need to use them; • responsibilities for the DR plans should be clearly identified; • there should be a clear identification of persons responsible for each function within the plan; • contact information should be clearly identifiable; • plans should include a step-by-step explanation of the system recovery option;	DR plans are in place for Telepath (LIMS), ICCA, RADISII, PACS, TOMS, PAS A&E (Myrddin), and Pharmacy. Of these systems, only two (Telepath and TOMS) are fully supported by the Health Board. The remainder rely on support from external providers. Although DR plans are in place for these systems, they do not all meet the minimum requirements as identified in our recommendation. Our specific findings were: • There is no ICT infrastructure DR plan. • The Theatre and Pathology departments do not have specific step-by-step explanations of the recovery options and procedures. The other system plans do have recovery options, but only to say that it would be the system supplier who is responsible for recovering the system, not how they would do it. This is acceptable; however the Health Board should ensure that it has adequate assurance from the supplier (eg NHW Wales Informatics Service (NWIS)) that it has appropriate recovery procedures in place. • The Health Board's own DR plan document for PACS is blank against the following fields: 'Initiated by', 'Approved by', 'Date approved', 'Version number', and 'Operational date'. There is also a DR procedure which is written by Fujifilm who maintain all backups, and support the system. • The Theatres plan was initiated and approved by the same person. Although ICT staff interviewed know how they would react in the event of a disaster scenario, without documented recovery procedures for each specific system, the Health Board cannot have full assurance that critical systems will be recoverable, as and when needed.

Information and Communications Technology (ICT) Disaster Recovery and Business Continuity Arrangements (March 2012, 202A2012)			
Reference	**Implemented?**	**Recommendation**	**Summary of progress made**
R8	✓/✗	• the various resources required for recovery should be clearly identified; • plans should be approved by an appropriate manager; and • plans should be updated and reviewed regularly with review and version control clearly stated on the front of each plan.	In addition to this, there is no overall IT DR plan, which includes a prioritisation of all IT systems to allow for a co-ordinated, and risk-based approach to recovery in the event of a disaster. In a major disaster situation where many systems fail, the Health Board does not have assurance that its systems could be recovered in an appropriate and timely manner. We have not reviewed any support contracts between the Health Board and third-party providers; however the Health Board needs to have assurance that in a disaster scenario, recovery processes for those systems meet business needs.
R9	✗	Test all ICT DR plans for the systems and infrastructure regularly to ensure they operate as intended.	No progress made. Regular, formal and robust testing of all DR plans does not occur. Our review found that DR testing is limited to system restores which are undertaken on a responsive ad-hoc basis, as part of daily activities if a system fails. There is a log of restores, backup logs and failure, but even if all restores and failures are documented, this will not record systems that have not had any issues, and would not therefore have had any previous/regular restores, failures or recovery procedures. If one of these systems were to fail, then the Health Board has no assurance that they will be able to be adequately restored. If the disaster scenario were more serious, ie, the loss of a site/location, then relying on the ability to carry out simple system restores would be inadequate. The Health Board needs to have assurance that systems can be recovered in all eventualities.
R10	✗	Establish and monitor clear performance indicators for the ICT department, systems and infrastructure. Use the results of this performance monitoring to inform DR planning, ICT resource planning and ICT infrastructure and system capital planning.	No progress has been made on this recommendation. Despite identifying a number of indicators in our 2012 report, the Health Board has not adopted any measures to manage and improve the performance of the ICT department.

Appropriate software, hardware and access controls are used as part of backup delivery but there is no backup policy, and not all procedures and backup approaches are adequately documented

Overview of the arrangements for information backup (November 2013, 616A2013) In 2013 we concluded that the Health Board had inadequate or partial arrangements appear to be in place to ensure data backup	
Areas reviewed	**Findings**
Does the Health Board have an effective backup policy in place, alongside a full knowledge of its IT systems and those responsible for them?	**Although the Health Board is in the process of documenting its systems and responsibilities, there is no backup policy in place.** **Catalogue** The Health Board are taking positive steps to document their IT systems and services. There is a draft IT service catalogue which aims to outline the services that the ICT Department provides to the Health Board. The catalogue outlines the ICT services received by the Health Board, with annexes for each departmental system. Each entry aims to describe the ICT service being delivered from a user perspective, when it is available, what is included and how the level of service is measured. It also lists those clinical systems are supported on call, and those which are not. Specifically the document details the following for each system: • Service name • Service description • Service components • Service exclusions • Service availability • Support availability • Service measurements • Service Owner

Overview of the arrangements for information backup (November 2013, 616A2013)

In 2013 we concluded that the Health Board had inadequate or partial arrangements appear to be in place to ensure data backup

Areas reviewed	Findings
Does the Health Board have an effective backup policy in place, alongside a full knowledge of its IT systems and those responsible for them?	• Users • Users' responsibilities • Service Criticality • Service dependencies Currently, the service catalogue only includes on-call clinical systems, with work in progress to include other clinical systems, as well as infrastructure elements in the future. The document is planned to be completed by October 2015 and published on the Health Board's SharePoint. We noted that the Theatre TOMS system is not included in the copy of the service catalogue that we received. **Backup Policy** Although the Health Board has been documenting its clinical systems, and the IT services and availability each system requires, it does not have a documented a backup policy. Without an agreed and documented policy, the Health Board does not have something on which to base consistent backup procedures, approaches and practices across the organisation**.** **Asset Register** A new information asset register is currently under development, with a draft version planned for the completion by the end of November 2015. The Head of Clinical Systems is compiling data collection forms for each of the Health Board's clinical systems. Included in the forms are the information owners for each IT system. However, as described in more detail in the data quality section of this report, these responsibilities are not allocated to individuals for each system.

Overview of the arrangements for information backup (November 2013, 616A2013)
In 2013 we concluded that the Health Board had inadequate or partial arrangements appear to be in place to ensure data backup

Areas reviewed	Findings
Are there effective arrangements in place to deliver information backups?	**The Health Board does not have documented backup procedures for all of its key/critical IT systems; therefore the arrangements in place to deliver information backups may not be as effective as they should be.** The Health Board uses appropriate software to deliver backups for the clinical systems under its remit. The software notifies the ICT server team about required tape changes, weekly summaries of backup performance, and any failures (including explanations). Currently, staff pick up issues on an ad hoc basis, which means that there is a risk that issues may be overlooked due to people thinking they are being dealt with by somebody else. In order to address this issue the Server Manager is currently documenting a staff rota to undertake daily checks to ensure that any issues are acted upon appropriately. There are no documented procedures on what to do if backups fail.ie, how to re-configure them/re-take them successfully. With regards to procedures for taking backups, the Health Board places reliance upon the fact that the system is already configured to take backups, and the only documented procedures are the taking of backups off site and tape rotation. The Health Board should ensure that they have the ability to amend automated backup procedures should they need to, particularly in instances where regular ICT staff are unavailable. These procedures should be adequately documented. Controls are in place to allow staff/suppliers to access backups as required (including the appropriate set up of backup system administration rights). This also minimises the risk of accidental deletion or changes. As part of this review, we also looked at the specific backup arrangements for two systems, the Theatre system which is a locally hosted and managed system, and the PACS system, which is a national system, but hosted at the Health Board. **Theatre system:** The Theatre TOMS system's database sits on a cluster of three SQL servers in an active-passive setup. This is backed up daily to the Prince Charles site's main storage area network (SAN). The SAN is linked to backup servers in a different room and fire zone. Whole SAN backups are run by a virtual server initially to disk, and then to tape. The Theatre system DR plan states 'See Server Backup and Restore Documentation', under its backup/recovery details. We have not had sight of this documentation so cannot confirm that any specific documented procedures for the TOMS backup arrangements exist.

Overview of the arrangements for information backup (November 2013, 616A2013)	
Areas reviewed	**Findings**
Are there effective arrangements in place to deliver information backups?	**The PACS system:** The use of the FUJIFILM PACS by the Health Board is part of an NHS Wales National contract with FUJIFILM, managed at a national level, although the system is configured locally. The main PACS database runs on a server in the Prince Charles server room. Both the Prince Charles and Royal Glamorgan hospital sites have a set of Digital Imaging and Communications in Medicine (DICOM) servers and two VEEAM servers are on each site, which are replicated to each other. The VEEAM servers replicate both of the DICOM servers. In addition the main database updates a local DR server which stores the previous two weeks of data, which the Health Board can access while the system is being recovered in a DR situation. This set up provides an appropriate level of resilience. Backup procedures follow an all-Wales backup policy specific to the system, which we have not had access to, and therefore cannot confirm that the appropriate backup/system continuity documentation and procedures exist. The Health Board should ensure that they are content that the level of backup/server documentation available to them is satisfactory. After the RADIS migration and merger (of the two systems currently in place), which was due September 2015, the Health Board plan to replicate the PACS servers to the Blaenavon data centre, for additional resilience.
Is there effective performance monitoring of the completion of information backups?	**Performance monitoring of backup completion is adequate, and is IT system reliant, rather than using manual checks.** The completeness and accuracy of backups for the Theatre TOMS system is reliant upon the IT system doing its job and assurance on this is taken from the Commvault software job controller. Manual checks, ie, of completeness are not undertaken. For FUJIFILM PACS, the Health Board rely on the fact that it is a managed service, and that the supplier appropriately monitors the performance of the servers and their replication. The Health Board should ensure that the supplier does indeed carry out these regular checks.

Caldicott governance arrangements have been strengthened, and training methods improved but some relevant staff are yet to do this training

Caldicott – Key findings 2012 structured assessment (December 2012) and Annual Audit Report 2012 (March 2013, 147A2013)	
Areas reviewed	**Findings**
In 2012 we considered the Health Board's arrangements to ensure that the NHS body complied with the information confidentiality requirements as set out in the Caldicott manual, and found that: Management arrangements exist and the Caldicott Guardian provides leadership, but: • there was a gap between corporate and operational teams (the Health Board took immediate steps to address this gap, following restructure); • arrangements to deliver the training programme and monitor progress against the Caldicott principles are inconsistent across sites; and • oversight and assurance require strengthening by monitoring progress, and ensuring operational linkages are working. Policies/procedures are in place and the Health Board is aware of the need to improve the consistency of: • staff training, particularly job specific and update training; and • informing patients on the use and access to their information (PCH).	**Corporate and operational teams** The Health Board has addressed the previously identified gap between the corporate and operational teams. Representatives from the health records committee ie, the Directorate Manager for Medical records and outpatients (or a nominee) now attend the IGG. **Oversight and assurance** The Caldicott principles in practice (C-PiP) self-assessment provide Information Governance and Caldicott Leads with a tool to highlight areas where improvements are required, and a benchmark for evaluating progress. Since 2012, the Health Board's self-assessment scores have been: March 2012 – 78 per cent May 2013 – 87 per cent January 2014 – 63 per cent (re-reviewed following an internal audit report recommendation) September 2014 – 84.26 per cent The 2015 C-PiP self-assessment has not been carried out at the time of writing, and it is due to be carried out and reported to the IGG by December 2015, with the results to be published on the Health Board's website. The delay in the self-assessment is due to considerations by the Information Governance Advisory Board to review the current C-PiP process, and the potential to adopt the toolkit used by NHS England. It has been decided that the Health Board should carry out its assessments as planned, until further notice. The Health Board's C-PiP assessments are carried out by the information governance team and presented to the IGG. The Corporate Risk Committee also request C-PiP assurance from the IGG. Information Governance KPIs are reported to the IGG on a quarterly basis, which includes indicators on freedom of information access (FOIA) requests, subject access requests, training compliance and incidents. The IGG also receives updates on any information governance incidents reported within the organisation since the previous IGG meeting. There are guidelines in place to determine whether an information security breach should be considered for reporting to the ICO.

Caldicott – Key findings 2012 structured assessment (December 2012) and Annual Audit Report 2012 (March 2013, 147A2013)	
Areas reviewed	**Findings**
The Health Board understands its Information Confidentiality responsibilities and high risk patient and staff information has been identified but it must ensure other information subject to Caldicott principles is included.	The final decision is usually made by Executive Directors or the IGG, unless exceptional circumstances apply. The two members of staff who support the Caldicott Guardian carry out risk assessments on access requests for personally identifiable information, prior to the Caldicott Guardian signing the requests off. There is no formal documented procedure used to assess the risk, and staff interviewed noted that it would be difficult to create a 'one size fits all' approach. However, adopting more formal arrangements to allow for a uniform approach to risk assessments is being considered, where possible. A data protection policy approved by the corporate risk committee and IGG was approved in November 2013. A Data Protection audit was carried out in January 2014 by the Information Commissioners Office. Further to this, the Health Board were issued with a limited assurance rating in respect of the systems in place. As a result, the Corporate Team were provided with an action plan to progress and update over a given time period. The Health Board is still in the process of implementing the required actions, but once completed, many of the actions will further improve the Health Board's Caldicott arrangements. The Health Board are in the process of piloting a data protection auditing software tool on behalf of NWIS which will identify levels of inappropriate data access on specific Health Board information systems. By the end of 2015, NWIS will link the system to Electronic Staff Record (ESR) system, Myrddin (PAS), and the Welsh Clinical Portal (which will also capture other systems). The contract will be managed centrally by NWIS, however local potential data breaches will be monitored and escalated as appropriate by the Information Governance Team. **Training consistency** Information Governance is part of the Core Skills Training Framework. In addition to the training that was already in place during our 2012 review, there is now an e-learning package for Information Governance training, which specifically refers to Data Protection, Caldicott, Freedom of Information and Personally Identifiable Information (PII). The NHS Wales e-learning package forms part of the training available, and is compulsory for all Health Board staff and new starters, across all sites. Currently the Health Board's current compliance figure for Information Governance is 8.24 per cent. The Learning & Development Manager explained that although the figure appears to be low, they are aware that there is historical training that has not been recorded onto ESR, from which this figure is produced, and will not therefore be a true reflection of their compliance. The Health Board are aiming to be able to give an accurate picture of compliance with the competency by August 2016.

Caldicott – Key findings 2012 structured assessment (December 2012) and Annual Audit Report 2012 (March 2013, 147A2013)	
Areas reviewed	**Findings**
	Information Governance refresher training for staff is supposed to occur every two years. The Health Board will also be monitoring compliance with this training via the ESR system. As part of the evidence we received was a handout which explains the Caldicott Principles. It refers to the Caldicott Guardian as the Clinical Director, but on the next page, it refers the Director of Nursing. This is an example of inconsistencies within Health Board documentation which should be addressed. **Informing patients** In response to the 2013 Internal Audit report on Caldicott, the Health Board said that the Information Governance Team have delivered information leaflets to patient areas across the Health Board. We have not carried out a walk around the Health Board sites as part of this review to confirm this. The Health Board website has a page called 'Patient and Visitor Information'. This page contains links to the following leaflets: confidentiality (describing what patient information the Health Board collects, how it is used, and who has access to it), data protection, and FOIA. The Health Board's C-PiP scores are also on its website. The Health Board are implementing an internal broadcast system (televisions) within Health Board buildings, managed by the communications team, which will include videos relating to information governance and information confidentiality. This will help to inform the public on how their personal information is used and accessed. The Health Board's C-PiP scores are recorded on its website.

There are a number of initiatives to strengthen data quality arrangements, including a data quality audit programme, annual report and the addition of key staff but some governance arrangements require improvement

Data Quality – Annual Audit Report 2012 (March 2013, 147A2013)	
Areas reviewed	**Findings**
Is there 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?	**An annual report on data quality is in place, which would be strengthened in the future by allowing for comparisons against previous year's performance.** The annual report describes achievements made by the Data Quality Steering Group (DQSG) during 2014-15 and the risks and challenges for improvement for 2015-16. Included in an appendix is a summary of the current data quality audits undertaken by either the Data Integrity Manager or other members of the Performance and Information teams. The report would be strengthened by including comparisons against previous year's performance. This would help to clarify how well they are doing with regards to data quality, and demonstrate whether they are actually improving, or not. The report refers to both the integrated governance committee and to the information governance committee. The Health Board does not have an information governance committee, but it does have an IGG. It is unclear which of these committees the report goes to. The inconsistency of the use of these names was also identified in other documents obtained as part of this review. In addition to the annual update, a monthly performance dashboard is presented to the Executive Board, Health Board, and Finance and Performance Committee. A data quality indicator has been included as part of the report since April 2014, but recent examples of the dashboards do not explain why each indicator scored as it did. In addition, May 2015's dashboard has a section dedicated to data quality, but July 2015's does not.

Data Quality – Annual Audit Report 2012 (March 2013, 147A2013)

Areas reviewed	Findings
Are adequate IM&T and data quality governance arrangements in place?	**Health Board IM&T governance arrangements are unclear although the data quality policy does refer to the specific governance framework for the assurance of the Health Board's data quality.** Although the data quality policy displays the specific governance structure for the assurance of the Health Board's data quality, we were unable to obtain a specific diagram to explain the current arrangements with regards to the overall IM&T reporting governance structure. The IM&T steering group (set up in 2012) has not met since December 2014. As the group's functions stated in its terms of reference are not officially stated in other Health Board group/committee terms of references, there is a risk that they are not being carried out. The Health Board needs to have assurance that IM&T issues are appropriately and sufficiently dealt with. A DQSG oversees the quality of data on all systems in place within Cwm Taf LHB, and reports to the Corporate Risk Committee, via the IGG. We noted that data quality related reports also go to the Finance and Performance Committee as well as the Executive Board, although the reporting line to the Finance and Performance Committee is stated in the Data Quality Policy, it is not in the DQSG terms of reference. The Health Board should consider reviewing the DQSG's TOR and membership, because its minutes for June and September 2014 show less than half of the members on the TOR list attended. It was also highlighted that directorate managers often attend in the place of the specified directors. Before leaving the Health Board, the Head of ICT was part of the health records committee membership. The committee's TOR was due to be reviewed in April 2015, and as this has not occurred, it would be timely to review the document and to ensure that there is adequate ICT representation.

Data Quality – Annual Audit Report 2012 (March 2013, 147A2013)	
Areas reviewed	**Findings**
Is there, for each system, a named individual who is responsible for data quality?	**Although the Health Board is in the process of compiling a list of Information asset owners, named individuals responsible for data quality are not in place for all systems.** A new information asset register is currently under development, with a draft version planned for the completion by the end of November 2015. The Head of Clinical Systems is compiling data collection forms for each of the Health Board's clinical systems. Included in the forms are the information owners for each IT system. The Health Board's work to compile an information asset register is part of a three-staged approach; 1st stage – Capturing the UHB wide clinical systems, 2nd stage – Capturing directorate level systems, 3rd stage – Capturing departmental team level systems. Some of the information assets register data collection forms we saw as part of this review did not refer to specific individuals as the information owner, but to departments, or stated them as 'unknown'. By not having named individuals as information asset owners, the Health Board cannot easily assign responsibility for its data quality. It is not yet clear how the Health Board plans to keep the information asset register up to date.

Data Quality – Annual Audit Report 2012 (March 2013, 147A2013)	
Areas reviewed	**Findings**
Is there appropriate staff attendance at IGG meetings, and is data quality a standing item on the agenda?	Data quality is a standing agenda item at IGG meetings; but attendance at these meetings needs improvement. As per the IGG's terms of reference, the group meets three times a year, and is directly accountable to the Corporate Risk Committee. Its key role is to provide: • 'evidence based and timely advice to the Corporate Risk Committee to assist it in discharging its functions and meeting its responsibilities with regard to the quality and integrity; safety and security and appropriate access and use of information (including patient and staff information) to support the provision of high quality healthcare; • assurance to the Board via the Corporate Risk Committee in relation to the Health Board's arrangements for creating, collecting, storing, safeguarding, disseminating, sharing, using and disposing of information in accordance with its stated objectives; legislative responsibilities, including the monitoring of compliance against the Data Protection Act including Data Subject Access Requests and Freedom of Information Act; and any relevant requirements and standards determined for the NHS in Wales; and • advice and support to the Caldicott Guardian to ensure that they are able to discharge their functions in an appropriate and effective manner.' The IGG has established the following steering groups: • IM&T Steering, (which has not met since December 2014) • DQSG Agendas for the last year demonstrate that data quality is a standing item on the agenda with updates from appropriate members of staff. A review of IGG action logs highlighted that the group acted upon the need to review the lack of attendance at meetings, in relation to the IGG in November 2013, with the aim of improving attendance by March 2014. As of September 2014, the group recognised that attendance had been improving, and the status of the action was 'complete'. However, upon reviewing the action points (which also state the attendance of the group meeting) from meetings over the last year, attendance does not appear to have changed considerably.

Data Quality – Annual Audit Report 2012 (March 2013, 147A2013)	
Areas reviewed	**Findings**
Does the Data Quality Management Policy to refer to the IM&T governance structure and include: • use of patient administration records; • security and confidentiality; • clinical coding; and • data quality of information used for performance reporting to the Board. This policy should also refer to other key clinical and business systems and be subject to regular review.	**The data quality policy was updated in January 2013, but needs further amendments.** We have already described the lack of clarity around the overall IM&T governance structure at the Health Board. The current data quality policy does not state how regularly the policy is or should be reviewed. It also refers to the information governance committee, as opposed to the IGG.
Is there an internal programme of data quality audit for key information areas?	A data quality audit programme is in place, decided upon by the data quality steering group. The Annual Data Quality report states that 'The work programme of the DQSG will continue to address all identified data quality issues and to ensure that any data quality concerns are included and addressed within the data quality audit programme.' The audit programme has evolved since 2013, and as demonstrated within the Annual Data Quality report 2014-15, it now consists of a total of 23 data quality related audits. The frequency for testing the data depends on the type of data and the reason for commissioning the audits. To aid in coding audits, the Health Board now has a qualified coding auditor clerk (since 2014).

Data Quality – Annual Audit Report 2012 (March 2013, 147A2013)	
Areas reviewed	**Findings**
Are actions taken to address multiple PAS registrations and records with missing NHS numbers?	Procedures are in place that aim to address multiple PAS registrations and records with missing NHS numbers, however it is difficult to assess how effective these procedures are. The annual data quality report 2014-15 explains that the Myrddin team undertake a number of data quality reviews daily, weekly, and monthly, depending on the data item, to ensure that data held on Myrddin PAS is of sufficient quality to support the activity it is intended to be reporting ie, monthly comparisons of duplicate registrations, and missing NHS numbers. These are monitored by the data quality steering group. The medical records department has documented procedures to explain how a member of its staff should deal with merging duplicate registrations. Having documented procedures should allow Health Board staff to deal with these issues in a consistent manner. The Data Quality team run reports on incomplete data fields and place reports on SharePoint so that the appropriate teams can rectify any issues.

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