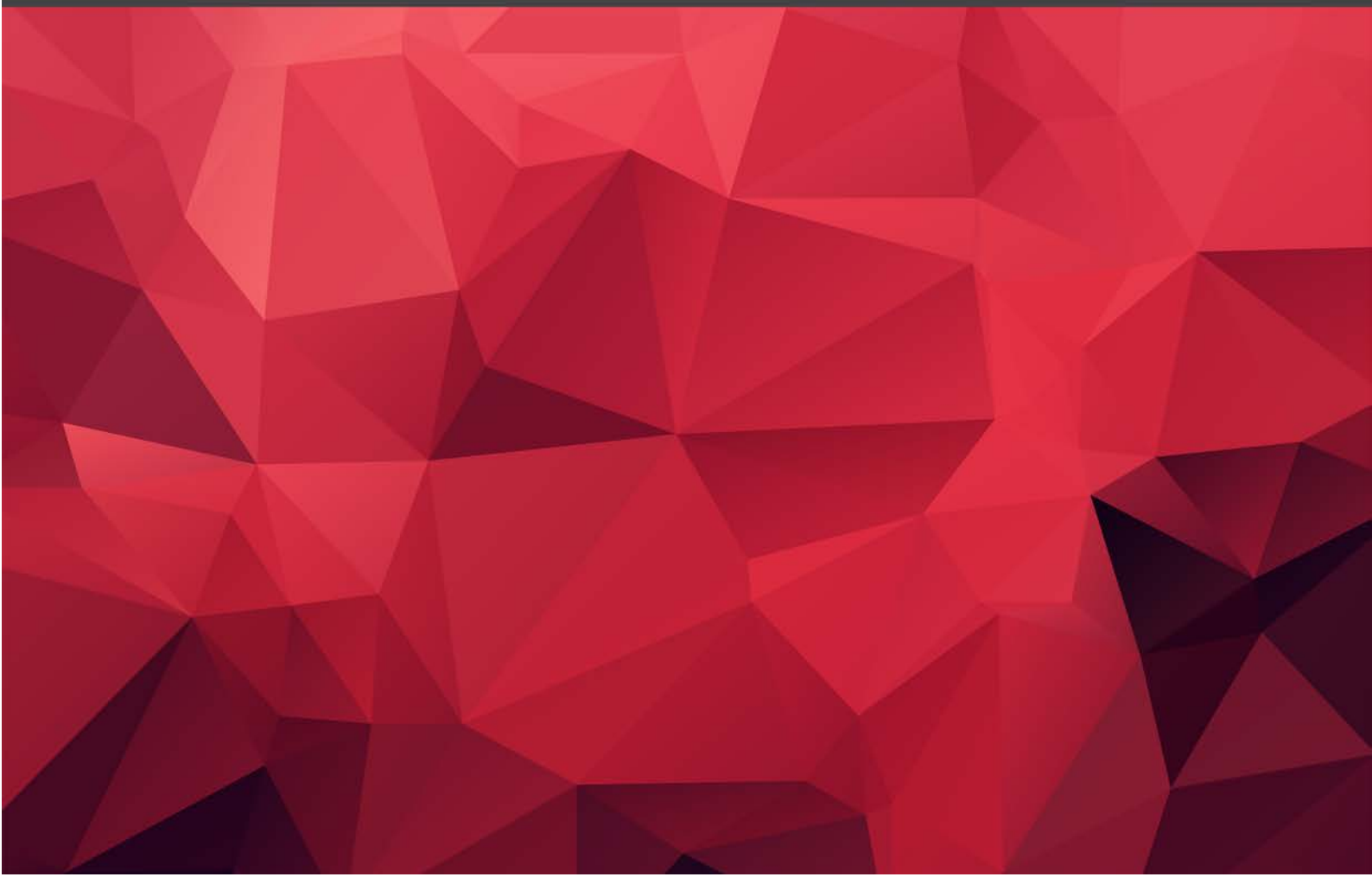
WALES AUDIT OFFICE
SWYDDFA ARCHWILIO CYMRU

Archwilydd Cyffredinol Cymru
Auditor General for Wales

Communications Technology Audits – **Abertawe Bro Morgannwg University Health Board**

Date issued: November 2016

Document reference: 324A2016



The person who delivered the work was Pauline Suchy.

Contents

The Health Board is addressing issues raised in previous ICT reviews, but slower progress in some areas, recent organisational changes and IT architecture upgrades make some further actions necessary.

Summary report

Background

1 The Wales Audit Office has previously undertaken a number of reviews covering aspects of informatics and communications technology (ICT) at the Abertawe Bro Morgannwg Health Board (the Health Board) during 2012 and 2013. Exhibit 1 summarises its conclusions.

Exhibit 1: Key conclusions from previous ICT reviews

Review name (audit year)	Key conclusions
Data quality (2012)	The Health Board has adequate data quality arrangements; however, our data analysis indicates varying degrees of effectiveness for ensuring consistent data accuracy.
IT Disaster Recovery (DR) and Business Continuity (BC) (2012)	The Health Board is well prepared in terms of ICT DR and BC arrangements, but could strengthen these in some areas. The Health Board is aware of these areas and is currently taking improvement actions.
Caldicott Arrangements (2012)	The Health Board's overall Caldicott arrangements are good and are progressing well, the Health Board is aware of the weaknesses that exist particularly around staff training and patient information.
Information Back Up (2013)	Although many of the controls we would expect to see are in place within the Health Board, there are some weaknesses. In particular, changes to back-up procedures are not always formally agreed and communicated, and the record kept of routine DR tests is incomplete. Additional controls in these areas need to be developed and implemented by 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 ICT reports'?**

3 In carrying out our follow-up review, we have taken into account the changes to the information technology architecture since our earlier ICT reviews, and the 2015 organisational restructuring of the Health Board and its management arrangements.

Our main findings

4 We concluded that the Health Board is addressing issues raised in previous ICT reviews, but slower progress in some areas, recent organisational changes and IT architecture upgrades make some further actions necessary.

5 Our detailed assessment of progress against each of our previous recommendations is set out in the main body of this report. In summary, we found:

- the Information Governance Framework is not yet fully implemented following management restructure in 2015, but is better placed to assure the Board on data quality.
- standardised Disaster Recovery (DR) and Business Continuity (BC) planning is developing, but BC plans are less well established in some clinical departments and testing of DR and BC plans is limited.
- Caldicott governance arrangements have improved but there are unresolved weaknesses in succession planning, resourcing, benchmarking and identifying sources of patient identifiable information.
- back-up arrangements have been revised to reflect the new virtual environment and will be enhanced by the new service catalogue, but there are no back-up arrangements for data held on medical devices.

Recommendations

6 The Health Board has fully completed nine of the 21 previous recommendations and partially met a further eight. A full list of the recommendations, along with the status of each, is set out in the detailed report. The Health Board needs to maintain focus on implementing the recommendations that are not yet completed. These are summarised in Appendix 1. We also raise five new recommendations, set out in Exhibit 2, to ensure these specific areas identified in 2015 are also addressed.

Exhibit 2: audit recommendations

Recommendations	
Data Quality	
R1	The Health Board should review the staffing arrangements for the Data Quality Team and ensure that staffing resources are sufficient.
DR and BC planning	
R2	The Health Board should identify any material/key clinical systems that have not been tested for DR and ensure they are tested appropriately.
Caldicott	
R3	The Health Board should identify a Senior Information Risk Officer (SIRO), as a role separate to that of the Caldicott Guardian.
R4	Information Governance staff should work closely with the electro bio-medical equipment (EBME) department to ensure data held in medical devices is fully considered under Caldicott principles.
Information Back-up	
R5	The Health Board should identify all medical devices not covered under the IT Services back-up regime, establish a back-up policy and issue appropriate guidance to staff.

7 The Health Board's management response[1] setting out how the Health Board intends responding to the issues identified in this report is included in Appendix 2.

[1] The actions and timescales identified by the Health Board to address the audit recommendations, together with the assigned responsibilities as relevant and including the ICT team, unit management teams and other departments such as EBME.

Detailed report

8 The tables below (Exhibits 3 to 6) list the recommendations from each of our four previous reviews and give our opinion on whether the recommendations have been fully implemented (Yes), partially implemented (In part) or not implemented (No).

Data Quality

The Information Governance Framework is not yet fully implemented following the management restructure in 2015, but is better placed to assure the Board on data quality

Exhibit 3: assessment of progress made implementing data quality recommendations

Reference	Implemented	Recommendation	Summary of progress made
R1	Yes	Introduce an annual report on data quality to provide organisational level assurance to the Board, which covers the effectiveness of arrangements in place to ensure data quality, and that meets both national and local data needs.	The Health Board introduced annual reporting on data quality in 2012-13. It covers data quality performance against national indicators, data quality governance, and data quality improvement work (plus the action plan for the forthcoming year). It also reviews clinical coding performance, improvement work and audits (external and internal). The Head of Information produces the report which is reviewed by the Information Governance Committee (IGC). The Board received the 2013-14 data quality report in September 2014 but the 2014-15 report was later, not being received by the Quality and Safety Committee until February 2016. Although annual reporting is now in place, more timely reporting would provide greater assurance.

Reference	Implemented	Recommendation	Summary of progress made
R2	In part	**Ensure that Information Governance arrangements are efficient, effective and appropriately include data quality:** • ensure that accountability structures and the respective responsibilities of all staff for Data Quality are clearly communicated and understood by all; and • monitor and periodically review the Health Board's Data Quality Governance arrangements to ensure they are effective.	The informatics governance framework includes three strands: • Clinical Validation and Engagement; • Strategy and Delivery; and • Informatics Governance. Data Quality falls within the remit of the Informatics Governance strand. The Informatics Strategy and Governance Board (ISGB) was replaced by the Information Governance Committee (IGC) in 2015, with two supporting Groups planned (Clinical Data Quality Assurance Group and the Non-Clinical Data Quality Assurance Group). These two supporting groups have yet to be set up as they are being considered alongside the assessment of setting up the Information Governance (IG) toolkit. The IGC's Terms of Reference detail its scope of responsibility, which includes data quality, clinical coding, data quality of performance, quality and safety reports, health records governance, ICT security, Information Governance and Caldicott issues. The IGC has reported to the Quality and Safety Committee which provides the Health Board with advice regarding the quality and integrity, safety and security, and access and use of personal data to support high quality healthcare. The Terms of Reference confirm that the remit had not changed since our review in 2012. However, assurance reporting arrangements have been subject to recent revision with the IGC reporting to the Audit Committee from February 2016. Committee terms of reference have been revised accordingly.

Reference	Implemented	Recommendation	Summary of progress made
R2	In part	Ensure that Information Governance arrangements are efficient, effective and appropriately include data quality: • ensure that accountability structures and the respective responsibilities of all staff for Data Quality are clearly communicated and understood by all; • monitor and periodically review the Health Board's Data Quality Governance arrangements to ensure they are effective.	The Data Quality Team also report to the Clinical Outcomes Steering Group, whose responsibilities have not changed since our original report. The Service Led User Group was set up in 2013 to agree working practices for new services or change of services to ensure services/informatics/finance staff have the relevant information in order to facilitate and accurately record the patient's journey. Management restructuring within the Health Board in October 2015, has changed the Information Governance structure. The Health Board knows it needs to ensure that responsibilities for data quality specifically and information governance more generally are understood and embedded in operational unit arrangements. Plans to roll out the Information Governance toolkit will support this.

Reference	Implemented	Recommendation	Summary of progress made
R2	In part	Ensure that Information Governance arrangements are efficient, effective and appropriately include data quality: • ensure that accountability structures and the respective responsibilities of all staff for Data Quality are clearly communicated and understood by all; and • monitor and periodically review the Health Board's Data Quality Governance arrangements to ensure they are effective.	The Health Board has established a number of roles and responsibilities covering data quality: • The Information Quality and Standards Manager leads the Data Quality Team. The team is led by the Information Quality and Standards Manager and consists of one data quality co-ordinator, one information assistant, one information officer and an information clerk. This are two fewer staff members than in 2012. Informatics management believes it is inadequately resourced to fulfil its purposes, resulting in insufficient progress on data cleansing and provision of training and awareness courses. • The Health Board had also introduced data quality leads in each directorate to help ensure that standards are maintained throughout the organisation. Their roles include attendance at service level user group meetings, reviewing data quality performance reports for their own area and working with the Data Quality Team to resolve specific issues and improve data quality performance. These roles may be subject to change because of the new operational unit structures. • In recent months nine extra staff in the form of Product Specialists have been introduced for each ICT solution. The Product Specialist will be responsible for technical design development (new systems and changes to existing systems), ensuring that systems meet the needs of services and that data quality procedures and standards are implemented. • Product Specialists will be setting up System User Groups and the Myrddin group is already in place, but Terms of Reference were still being drafted at the time of our review.

Reference	Implemented	Recommendation	Summary of progress made
R2	In part	Ensure that Information Governance arrangements are efficient, effective and appropriately include data quality: • ensure that accountability structures and the respective responsibilities of all staff for Data Quality are clearly communicated and understood by all; and • monitor and periodically review the Health Board's Data Quality Governance arrangements to ensure they are effective.	The Data Quality team leader provides data quality training for administrative and clerical staff. The Data Quality Policy which includes the Information Governance Framework and responsibilities is available on the Health Board's Intranet. Admin/Clerical staff are reminded when the policy is refreshed. All staff have a general section within their Job Descriptions, which includes their individual responsibilities for confidentiality and effective records management. However, for Primary Care the Health Board is not the systems owner. This sits with General Practitioners (GPs) and the NHS Wales Informatics Service (NWIS), which are funded to provide support. The Health Board has no jurisdiction to access the systems or specify how the systems must be operated. The Informatics Directorate are also developing and implementing their own Data Assurance Framework to provide: • assurance that data is an accurate reflection of the Health Board's performance; • confidence the information used is of a high enough level to inform decision making and monitor performance; and • a visual indicator acknowledges the variability of data and makes an assessment of the quality of data. The Informatics Directorate has established a requirement to integrate the Kite Mark (as used in some NHS Trusts in England) with the monthly performance statements for the Health Board. The Kite Mark comprises the five core elements of data quality and datasets will be assessed monthly against this standard by data owners. The report was accepted and agreed at the August 2015 IGC meeting.

Reference	Implemented	Recommendation	Summary of progress made
R3	Yes	Update the Data Quality Policy so that the policy: • covers all aspects of the Health Board including primary care and locally defined data quality needs; • identifies how the Informatics Strategy and Governance Board co-ordinates and provides data quality assurance to a formal committee of the Board or the Board itself; and • defines the role and responsibility of the Data Quality Manager.	The Data Quality Policy was reviewed in September 2013, recommended by the ISGB in September 2013 and ratified by Changing for the Better (C4B) Delivery Board in February 2014. The policy specifies that it is applicable to all Health Board employed staff (including agency or contract staff) and sets out responsibility for recording, interpreting or reporting on data relating to the business of the Health Board. The policy also reflects the Health Board's recognition of its responsibilities towards primary care practitioners and offers the policy for their use to inform and support good practice. Although this is subject to the constraints mentioned in R2 above with regards to jurisdiction over primary care systems and procedures. The policy defines the annual data quality report as the means by which the Health Board receives data quality assurance and includes the responsibilities of the Information Quality and Standards Manager.

Reference	Implemented	Recommendation	Summary of progress made
R4	In part	Reduce inappropriate duplicate patient demographic data within key systems (such as PAS, RADIS, RadCentre and others) and promote the consistent use of NHS numbers and patient identifiers.	The Health Board was an early adopter of the Master Patient Index (MPI) in 2011, which links patient records and establishes patient identifiers. The MPI is currently being added to other systems. A Master Patient Index Product Specialist has recently been employed who will be examining the duplicate records and measuring the extent of the duplicate records problem. A number of IT system resolutions have taken place since the original review to help reduce duplicate records including the following: • a single Patient Administration System (PAS) was introduced in 2013 and underpinned by the MPI; • a single theatre system was implemented in 2014; • pathology systems have been migrated to the national Laboratory Information Management System (LIMS); • Fuji picture archiving and communication system (PACS), a nationally used system, will be implemented across the Health Board by the 2015-16 financial year-end; • three audiology systems have been rationalised to a single system; and • the national Emergency Department system implementation is planned for 2016. To prevent further duplicate records the Health Board led in the development of a Gold Standard' in patient identification – best practice, under the 1000 Lives campaign. Patient Search, Amend and Registration guidance was included within the Myrddin training for all staff. There is an issue with duplicate paper records as well as electronic duplicate records. A business case for a scanning solution for these is under development, but not yet in a suitable state of readiness to be shared. Duplicate records (electronic and paper) remain a notified risk on the Datix system (risk registers) with the latest updates (02 August 2015 and 02 October 2015) being scored with a residual risk of 20 and a red risk.

Disaster Recovery and Business Continuity

Standardised Disaster Recovery (DR) and Business Continuity (BC) planning is developing, but BC plans are less well established in some clinical departments and testing of DR and BC plans is limited

Exhibit 4: assessment of progress made implementing disaster recovery and business continuity recommendations

Reference	Implemented	Recommendation	Summary of progress made
R1	In part	Develop the overall co-ordination of ICT DR provision for the Health Board, ensuring clear priorities in terms of the order of system recovery in the event of a large scale failure. Test these arrangements on completion of the testing strategy to ensure they work as intended.	The IT infrastructure has changed from physical application servers to a virtual environment since the last review in 2012. Traditional DR facilities are no longer applicable, eg, a standby site or provision of a mobile data centre by an external supplier. The Health Board has multiple data centres and virtual networks so virtual servers can be restored to another server in a different datacentre fairly easily. The service catalogue currently under development (see Information Back-up below) includes details of service dependencies and each system is categorised as one of the following: • Admin – Standard • Admin – Critical • Clinical – Standard • Clinical – Critical Categories allocated to each system are agreed with the system owners. DR procedures are part of the Standard Operating Procedures for each type of system and are currently being incorporated within the Service Catalogue.

Reference	Implemented	Recommendation	Summary of progress made
R1	In part	Develop the overall co-ordination of ICT DR provision for the Health Board, ensuring clear priorities in terms of the order of system recovery in the event of a large scale failure. Test these arrangements on completion of the testing strategy to ensure they work as intended.	Within the current funding constraints, IT services only have sufficient resources to run live services and can not provide full DR testing across the sites. However, evidence of restores of individual files, databases and full servers is available on the IT Services Sharepoint site. Although all restores are recorded, it is not clear if all critical systems are tested on a regular basis. The Health Board should identify any material/key clinical systems that have not been tested for DR and test them appropriately.

Reference	Implemented	Recommendation	Summary of progress made
R2	In part	Strengthen BC planning by: • implementing the overall corporate BC register for the Health Board which co-ordinates all departmental plans. This process should involve active engagement with each department. • clarifying and allocating ownership of BC at clinical service department levels. • developing and documenting clinical system BC plans that: – follow a minimum standard template based on good practice in this area; – contain a risk assessment to decide on the arrangements needed to be put in place; – are formally approved by the service area senior management; – are regularly updated and communicated to those staff that may need it; and	An overall corporate BC register is not yet in place. The Health Board's Emergency Planning Officer and Emergency Planning Group have been in place since 2011. Part of the group's remit is to be 'responsible for ensuring that Emergency Plans and BC plans are in place, up to date and in line with BC Standard BS2599'. It is a sub-group of the Operational Management Group, and also reports to the Clinical Governance and Risk Management Group. The agenda and minutes of the meeting of 7 October 2015 show that the new BC process was discussed. A draft Strategy for Emergency Planning has been developed by the Emergency Planning Officer which covers the Health Board's proposed arrangements for emergency preparedness, resilience and response under the Civil Contingencies Act 2004. The Emergency Planning Officer is responsible for the maintenance and registration of corporate BC plans and is focusing initially on development of corporate BC plans such as the 'Pandemic Framework' and Telecommunications BC Plan. These support incidents that may significantly affect the Health Board in whole or in part and will be combined with specific local plans for each Directorate/Specialty and key organisational functions to manage local disruptions as well as supporting larger organisational disruptions. With the organisational restructure in October 2015, Unit Directors now have responsibility for each operational unit, in place of the previous horizontal structure of management across directorates/specialities. At the time of our fieldwork, the Emergency Planning Officer was scheduling meetings with each Director to discuss emergency planning and their responsibilities for local BC plans.

Reference	Implemented	Recommendation	Summary of progress made
R2	In part	– are tested where practical and possible, to ensure they work as intended and are fit for purpose. This test should be performed at least annually. • Completing the Pharmacy BC plan, where the section on 'unavailability of premises' has not been completed. • Finalising the IT BC plan and the BC plan testing strategy and testing the arrangements following implementation to ensure they work as intended.	Two key documents had been prepared for the new Unit Directors: • Business Continuity Management Strategic Framework – an overarching framework of business continuity principles and the business continuity arrangements for Directorates, specialties and core organisational functions. A template local BC plan is included in the appendix and instructions for development of the local plans using a business impact analysis to identify critical activities. • Complete Business Continuity Process – supports the Health Board in anticipating risks and dealing with unplanned and significant events that impact on a number of functions and defines the corporate BC plans. It also acts as a register for the corporate plans. Unit Directors will be responsible for ensuring that all local departments have developed an effective BC plan for their site, that it is tested and stored appropriately and a register of plans is maintained. Corporate BC plans are formally approved by the Emergency Planning Group, but a new 'Strategic Planning and Commissioning Board' is being established that will ratify the corporate plans in future. Testing of corporate plans is difficult, but there is a six-monthly in/out of hours communications exercise undertaken and a table-top review of whole hospital evacuation is planned.

Reference	Implemented	Recommendation	Summary of progress made
R2	In part		Our findings in relation to BC plans in various clinical departments tested are summarised below: **Pharmacy** Pharmacy and Medicines Management Delivery Service is a single delivery department hosted by the Neath Port Talbot locality, but each hospital site has a local Pharmacy Departmental Manager. Pharmacy has an overarching Pharmacy BC plan which is site-wide, but incorporates site-specific sections for the 'unavailability of premises' section. The Princess of Wales Hospital and Cefn Coed (Mental Health) section were found to be missing. The format has not changed since our last review and is not yet in the standard template as issued by the Emergency Planning Officer. However, a Business Impact Analysis was performed to decide upon the critical business functions and the arrangements that need to be put in place. There is no regular testing of BC arrangements. The only testing that takes place is of the on-call pharmacist cascade process for notifying other pharmacy staff in the event of an out-of-hours incident. This was last tested on 25 October 2015, but it is not documented and is only performed on an ad hoc basis.

Reference	Implemented	Recommendation	Summary of progress made
R2	In part		**Radiology** Radiology Services is a dual delivery department hosted in: • The West (Singleton and Morriston hospitals) by Morriston • The East (Princess of Wales and Neath Port Talbot hospitals) by Princess of Wales Each department has a Radiology Services Manager but the department has a single BC Plan. It was developed by the Radiology Services Manager (West) and the Superintendent Radiographer (Singleton), but the plan applies to both West and East services. The plan is in the corporate template format as defined in the BC Management Strategic Framework. A Business Impact Analysis is used to identify key activities, products and services along with the impact or disruption to those activities, required actions, who is responsible for taking them and when. The document management information indicates that it is reviewed annually. This version is formally approved by the Radiology Services Manager (West), but in future will also be approved by the Radiology Services Manager (East). <u>Radiology West</u> Local procedures (SOPs) have been developed and are available at each site in each of the radiography areas. They are managed by the superintendent (senior manager) of each area. All staff are trained to use these procedures when they start employment. SOPs do not have the level of document management included in the BC Plan, but are reviewed annually or after a major incident. Testing of the BC plan is ad hoc, usually when live incidents occur. For example, a power outage at Morriston hospital rendered all the CT scanners inoperable as the hospital generator did not power up as expected. Radiography services (West) currently use non-national systems. For PACs, when the services migrate to the national system (Fuji PACS), part of the user acceptance testing includes a DR test. This is scheduled for March 2016. Migration to the national system Radiology Information System (RADIS) has been delayed by NWIS.

Reference	Implemented	Recommendation	Summary of progress made
R2	In part		Radiology East Local procedures (SOPs) have been developed and are available in the 'Viewing area' of the main Radiology department in the Princess of Wales and Neath Port Talbot hospitals. Local procedures have document management and the document management on those provided indicates that they are reviewed annually or after a major incident. All radiology staff have induction but are given training in the business continuity SOPs and Major Incident procedures when they commence on-call duties. Testing of the BC plan is ad hoc, usually when live incidents occur, for example, in 2015 when a power cable was cut through by workmen. All of the generators are tested monthly. Radiography services (East) now use national systems. DR was part of the user/testing when the services migrated to Fuji PACS in October 2015.

Reference	Implemented	Recommendation	Summary of progress made
R2	In part		**Pathology** ABMU Pathology is managed Health-Board-wide from Singleton Hospital. Services have been rationalised across the Health Board into: • Laboratory Medicine (Chemical Pathology and Laboratory Haematology and Blood Transfusion) • Cellular Pathology • Mortuary Services Senior managers are responsible for functional business continuity for their disciplines. The Pathology BC Plan is managed by the Associate General Manager Pathology and Disinfection and Sterile Services, but does not follow the standard template as issued by the Emergency Planning Officer. It was designed as a generic, overarching brief to the Health Board to provide assurance that the Laboratory Departments have business continuity arrangements in place and was not intended to be a procedural document to be followed by staff. It has been in place for a long period of time, but there is limited document control. It is not clear if it was developed using a risk assessment to decide upon the arrangements needed and has no specific review dates. The underpinning procedural documents are SOPs and these are held in Q-Pulse and contain full document management control. There are 2,800 procedures, but the majority are for normal running of the service. Approval is by committee within the area and once approved the SOP is updated on Q-Pulse by the quality manager or senior manager. Users are issued with an e-update notice. Testing of the BC plan and BC SOPs is ad hoc, usually when live incidents occur. Recent examples include staff illness and a leaking ceiling at the Princess of Wales Hospital from the ward above requiring relocation of processing. Staff training, equipment and SOPs have been standardised across the Health Board so that work can easily be moved between sites.

Reference	Implemented	Recommendation	Summary of progress made
R2	In part		**IT Services** IT Services' BC plan is now in place and is in the format prescribed by the Business Continuity Framework document. Testing is ad hoc, usually when live incidents occur. For example,e the Service Desk element was tested successfully in a live crisis in August 2015 when workmen accidentally cut through a cable and the network was lost in headquarters.
R3	Yes	Store and make available paper copies of both the BC and DR plans, currently available through the internet site, so that they can be easily accessed in case of emergency incidents where internet access is compromised.	**Pharmacy** Paper copies of the BC plan and manual data capture forms are stored in the Major Incident File. **Radiology** Radiology West Electronic copies of the BC plans and local procedures are held on the unstructured files (G: drive) for the Department and backed up by ICT services. A paper copy of the BC plan and local procedures are held in the office of the Head of Radiology Services and are also available in all radiography departments. Radiology East Electronic copies of the Radiography BC Plan and the SOPs are held on the on a shared drive (G:) which is backed up by ICT services. Paper copies of the BC plan and local procedures are held in the 'Viewing area' of the radiography department and also held by section managers. **Pathology** Service managers hold electronic copies of the Pathology BC Plan. Electronic copies of the SOPs are held on QPulse, which resides on a corporate server managed by the Health Board's ICT services. Paper copies are not available for any SOPs other than for Blood Transfusions (which are time-critical). The Pathology manager reported that this is because if QPulse were to fail it would not be down for more than one hour. All other services could wait for that period.

Reference	Implemented	Recommendation	Summary of progress made
R3	Yes	Store and make available paper copies of both the BC and DR plans, currently available through the internet site, so that they can be easily accessed in case of emergency incidents where internet access is compromised.	**IT Services** There is no overall DR plan but work is ongoing with development of the Service Catalogue (see R1 above). The IT BC Plan is held electronically on Sharepoint and paper copies are held in the fireproof safe at each hospital site.
R4	Yes	Relocate and review the supporting infrastructure for the two network cores at both Neath Port Talbot and Princess of Wales hospitals, so that they are located in separate computer rooms, and avoid single points of failure.	All main hospital sites (Morriston, Singleton, Princess of Wales and Neath Port Talbot) have the core network switches in different rooms. Each core is on a different power circuit within the hospitals and the BT and Virgin Circuits are separated between both core switches. All edge network switches terminate on both core switches. Network core locations for each hospital site were confirmed with the Health Board's Network Manager.

Reference	Implemented	Recommendation	Summary of progress made
R5	Yes	Complete, update and finalise contractual arrangements, through the working group which is being set up for this purpose, for DR for critical third-party supplied systems. Specifically: • Finalise the support and maintenance agreement for the Ascribe system and define responsibility and processes for appropriate DR arrangements. • Define clear DR responsibilities for the JAC system. • Review the recovery procedures for the Telepath system to ensure that they are fit for purpose.	The Pharmacy system – ASCRIBE – is no longer in use. This was a legacy system inherited by the Health Board when boundaries changed and the Health Board was formed. It was only used at the Princess of Wales Hospital and Cefn Coed (Mental Health) sites. A single instance of the JAC Pharmacy Stock Control system is now in place and accessible from all sites. A formal procurement exercise was undertaken in 2013, which resulted in the implementation of JAC across the Health Board. The contract provided defines the responsibilities for the supplier and for the Health Board. Provision and maintenance of server hardware and network connectivity are the responsibility of the Health Board IT services; the suppliers are responsible for software provision, support and development. DR is not specifically listed within the Health Board's responsibilities (Schedule D), but is implicit within the requirements for maintenance of the primary/mirrored servers and responsibility for back-up. Also, in Section B – Deliverables, at B6 – Disaster Recovery, the supplier also grants the right for the Health Board to install the software on other hardware as part of DR arrangements. The JAC system is part of the virtualised server farms, and back-up/DR responsibilities sit with IT services. A Pharmacy services SOP for loss of the JAC system is also in place. Loss of the system at any one site could be temporarily managed by procurement through an alternative Health Board site. Distribution of drugs can be issued form the alternative site through the Health Board's transportation network.

Reference	Implemented	Recommendation	Summary of progress made
R5	Yes	Review these contracts and agreements 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 • DR and BC arrangements.	Telepath is no longer in use. Pathology services now utilise: TRAK (LIMS) – used to draw down demographic detail from the patient administration system (PAS) to link with the test requested – for Laboratory Medicine and Histology. This is the all-Wales system and is fully managed by NWIS. MasterLAB – used to draw down demographic detail from PAS to link with the test requested – for blood transfusions. The DR arrangements are the same as in our original review and the next test is scheduled for January 2016 at the SunGARD data centre in Leicester. This is tentative as the Health Board are due to migrate to the all-Wales LIMS Blood Transfusion system, but target dates for migration have slipped. Indigo Review – Results viewing system. The system is managed by the Health Board IT services. PSM – Analyser middleware to connect multiple analysers to one source (TRAK or Masterlab). Also acts as concentrator to manage the analysers. A shadow server is maintained in a separate location to the live server – this is updated in parallel with the live server. A document outlining the process to be performed during a system failure is held on QPulse.

Caldicott arrangements

Caldicott governance arrangements have improved but there are unresolved weaknesses in succession planning, resourcing, benchmarking and identifying sources of patient identifiable information

Exhibit 5: assessment of progress made implementing recommendations relating to Caldicott arrangements

Reference	Implemented	Recommendation	Summary of progress made
R1	No	The current Caldicott Guardian is well respected and well known by staff and management at the Health Board, it is imperative that the Health Board put in place effective succession planning to manage the replacement of the Caldicott Guardian when the current Guardian retires in December 2012. Consideration should be given to the appointment of a deputy Caldicott Guardian who could maintain continuity and progress against actions in the absence of the Caldicott Guardian, but actual Caldicott decisions should not be delegated and should remain with the Guardian.	There have been two changes of Caldicott Guardian since our review in 2012, with previous and current Guardians being the Medical Director. There is, however, no official deputy Caldicott Guardian who could maintain continuity in the absence of the Guardian. In addition to a Caldicott Guardian, it is good practice to have a separate Senior Information Risk Officer (SIRO). The Health Board recognises this but has not yet introduced a designated SIRO. There are a number of differences and potential conflicts between the SIRO and Caldicott Guardian roles that support them being distinct and separate. Both roles are concerned with ensuring that NHS data is protected and not stored, accessed or used inappropriately, but in practice, both roles are different: • The Caldicott Guardian (ideally a Board member who is a senior professional) is primarily concerned with the protection of patient and service user information by ensuring it is only shared with those with a justified need for it; and only shared through appropriately safeguarded routes. • The SIRO is a senior officer concerned with identifying and managing wider information risks to the organisation, including the overall information risk policy and risk assessment process. The role should be supported by Information Asset Owners, each with assigned responsibilities for information assets.

Reference	Implemented	Recommendation	Summary of progress made
R1	No	The current Caldicott Guardian is well respected and well known by staff and management at the Health Board, it is imperative that the Health Board put in place effective succession planning to manage the replacement of the Caldicott Guardian when the current Guardian retires in December 2012. Consideration should be given to the appointment of a deputy Caldicott Guardian who could maintain continuity and progress against actions in the absence of the Caldicott Guardian, but actual Caldicott decisions should not be delegated and should remain with the Guardian.	The Information Governance Manager has delegated responsibility for taking the lead role in maintaining the confidentiality of patient identifiable information in accordance with the 'Confidentiality: NHS Wales Code of Practice'. This includes assisting the development and co-ordination of a comprehensive information security programme and providing in depth specialist knowledge across a range of work procedures and practices to ensure compliance with the Data Protection Act 1998 and other legislative and NHS Policies. Succesion planning is needed to maintain continuity in this role, on the retirement of the current post-holder in 2016 (referred to further under R3 below).
R2	Yes	The Health Board has robust management arrangements in place but they need to document and approve the Caldicott responsibilities to provide clarity over these arrangements. This is particularly important with the impending changes to the Caldicott Guardian position at the Health Board.	The Data Protection and Confidentiality Policy version 2.6 (Sections 4 and 5) details the data protection responsibilities for all staff, from the Caldicott Guardian, through Management and to all staff. Section 4 – Compliance specifies that confidentiality is an obligation for all staff. 'Breach of confidence, inappropriate use of health records, inappropriate disclosure of Identifiable Information or abuse of computer systems may lead to disciplinary measures being taken (see Information Security Policy for further information). It may also bring into question professional registration and could result in legal proceedings.' Section 5 – specifies the additional responsibilities for specific roles/grades ie, Caldicott Guardian, Head of ICT Operations and all managers. Subsequent sections and appendices provide details of specifics regarding the data protection and Caldicott requirements.

Reference	Implemented	Recommendation	Summary of progress made
R3	In part	The current Caldicott support teams, comprising members of the Information Governance and IT security teams, work well together and with the Guardian, but the Health Board needs to ensure the resources of these teams is sufficient to deliver the Caldicott training programme and to monitor progress against Caldicott principles.	**Resources** The Information Governance Team consists of four members of staff (3.2 Whole Time Equivalent) which is reported to be inadequate to undertake all of the tasks of the team. A meeting is to be held with the Assistant Director of Informatics about resourcing and succession planning as the Information Governance Manager will retire in spring 2016. **Training** Training is discussed under R4 below. **Monitring progress against Caldicott Principles** The Caldicott Principles into Practice (CPiP) online self-assessment tool is completed/submitted annually by the Information Governance Manager and the Information Security Manager. A report on the self-assessment is agreed by the Caldicott Guardian and presented to the IGC. The Health and Social Care Information Centre (HSCIC) which provides an external and independent Information Governance (IG) assessment in England, does not apply in Wales. Consequently, there is no benchmarking. The CPiP score for the Health Board for 2014-15 is 86 per cent (compared to 79 per cent in 2013-14). These scores fall within the category of a four-star rating, which is 76 to 90 per cent compliance. This means responses to the assessment demonstrate a good level of assurance of information governance risks; but there is still work to be done.

Reference	Implemented	Recommendation	Summary of progress made
R3	In part		Reviewing the 2014-15 assessment against the 41 CPiP standards, the Health Board was assessed as: • fully compliant with 27 standards (compared to 26 in 2013-14); • partially compliant with 13 standards (compared to 15 in 2013-14); and • non-compliant with one standard (compared to 0 in 2013-14). An action plan which supports improvement details the individual actions, who is responsible and when it should be completed by. The action plan is monitored by the Information Governance Manager on a quarterly basis and progress is reported to IGC. **IG Toolkit** The Health Board is pursuing use of the English NHS IG Toolkit, adapted for Welsh use, and has appointed staff to work towards its adoption. This should provide the Health Board with more robust evidence-based reporting, in conjunction with CPiP. A Project Manager is in place to review the IG Toolkit and undertake a self-assessment against Level 1 with a pilot initially in the Informatics department. A gap analysis has been conducted and an action plan is being developed within IT to bridge the gaps.

Reference	Implemented	Recommendation	Summary of progress made
R4	Yes	The Health Board has undertaken a range of Caldicott training but it recognises more needs to be done on general update training and job specific training.	Caldicott training for staff is mandatory every two years, with face-to-face and e-learning training available. With a 16,000 strong workforce it is not possible to provide face-to-face training for everyone within the timescale. The Information Governance (IG) team have developed a two-pronged approach to facilitate staff access to training; provision of face-to-face drop-in sessions together with an e-learning package that can be studied by the member of staff at a time suitable to them. The IG team provide the training and details of availability, but uptake and compliance with the mandated rule rest with line-managers. We have not reviewed uptake and compliance rates or the accuracy of ESR records as part of this follow-up review. **Face-to-face training** This is delivered by the Information Governance Manager and the Information Security Manager and takes the form of a drop-in session. These are run in the four main hospitals and general managers are sent a notification of when sessions are running, including a reminder that they should ensure staff attend where possible. It was reported by the Information Governance Manager that there are problems covering shift workers as training staff only work normal office hours. Departmental training sessions will also be provided on request from general managers. These sessions are tailored to the specific needs of the area. The Information Governance Team provided 82 departmental training sessions in the 2015 calendar year. Completion of training is recorded in the attendee's ESR record. **E-Learning** The Information Governance e-learning course is provided by NWIS. Although the course material with regard to the the principles is adequate, it does not contain any references to local policies or procedures. However, it is anticipated that there will be all-Wales policies in place by the end of 2016, enabling standardisation of e-leaning. Attendees' ESR records are automatically updated on completion of the package.

Reference	Implemented	Recommendation	Summary of progress made
R4	Yes		**Policies associated with Caldicott** There are a number of policies available to staff which aid awareness of information security. These are available on the Health Board's intranet. **Information Governance Helpline** The Health Board has launched a generic IG helpline e-mail address where staff can send questions and ask for advice. It became operational on 1 April 2015 and was publicised on the intranet bulletins page, with a link on the IG Intranet page. **Welsh Health Circular WHC/2015/036 – ICO report on Information Governance Training across Welsh Health Boards** The Health Board received their report from the Information Commissioner's Office (ICO) in July 2015 and developed an action plan in response. The action plan is managed by the Information Governance Manager and was submitted to the August 2015 IGC meeting for approval. Progress is reported to the IGC bi-monthly. All recommendations have an associated action, person responsible and a timescale. Progress is being made with seven of the 11 actions being reported as complete or linked to an e-learning package refresh (which is being implemented by NWIS). External IG training for information governance officers and the Caldicott Guardian was planned for the end of November 2015. Delivered by Blake Morgan in Leeds, the week-long course included a BCS[2] examination. The action plan for the ICO report confirms this as an agreed action.

[2] BCS, The Chartered Institute for IT

Reference	Implemented	Recommendation	Summary of progress made
R5	Yes	The HB is aware of the need to better inform patients on the use and access to their information.	Information leaflets about use of patient information and their access rights were distributed to departmental managers for display at reception desks. Posters on 'Your Information – Your Rights' were to be included on hospital notice boards, but we were told that these un-laminated posters had not been displayed in clinical areas due to infection control concerns about contamination risks. Copies were alternatively circulated to General Managers for distribution to departmental areas. The Health Board should periodically check the availability of information in patient areas and keep its content up to date. Advice on public access to health records is included on the Health Board's website under Patient Information and Contact Us/FOI tabs. It includes information on how to access medical records and provides contact email and postal addresses. It also provides a link to the NHS Direct website which explains what patient information is used for, how it is kept and how to gain access to it.
R6	No	The Health Board has a good understanding of its Information Confidentiality responsibilities and has identified its high-risk patient and staff information but needs to do more to identify whether there are any other information sources which need to be assessed under the Caldicott Principles.	A database of devices on which personal information which may pose a Caldicott/information security risk is being developed. Information Governance staff should work closely with electro bio-medical equipment (EBME) to ensure that data held within this equipment is fully considered under Caldicott principles. A related recommendation was raised by the 2013 Information Back-up review (R3): 'A review of the medical devices not covered within the IT systems' back-up and recovery procedures should be undertaken. These devices also pose a potential Caldicott (data security) risk.' The relevant section below provides detail.

Reference	Implemented	Recommendation	Summary of progress made
R7	In part	The Health Board completes an annual assessment and processes against actions identified in the assessment on the Caldicott Principles in Practice (CPiP) and they should seek their own internal assurance on this self assessment via internal audit.	The CPiP online self assessment tool continues to be completed annually by the Information Governance Manager and the Information Security Manager. The outturn report generated from the self-assessment is agreed by the Caldicott Guardian before being presented to the IGC. Internal Audit had some opportunity to comment on the 2015 outturn draft report due to their attendance at the IGC but there are no formalised arrangements for obtaining internal assurance on the self-assessment. In the absence of evidence being received by the IGC or Caldicott Guardian, the Health Board could consider commissioning an internal audit review. The IG Toolkit is currently being piloted within the informatics directorate and under national consideration for mandated introduction across NHS Wales. Its adoption within the health board may increase the requirement for management to provide evidence to demonstrate compliance.
R8	In part	The level of compliance with the Caldicott Principles should be effectively reported to the Board and the Caldicott Principles in Practice (CPiP) score included in the Annual Report to provide balance to any information security incidents reported in the Annual Report.	The outturn CPiP report sets out compliance and once agreed by the Caldicott Guardian is presented to IGC, as noted above. The route for providing assurance to the Board is via Board sub-Committee reporting, but the Annual Report no longer contains the CPiP score or the Information Security Incidents. The CPiP outturn report will replaced by the IG Toolkit once fully rolled out.
R9	No	The Health Board effectively uses performance information to inform improvement but needs to do more to identify ways of benchmarking its progress against other similar organisations.	There is no official benchmarking undertaken in relation to Caldicott principles at present. The Health and Social Care Information Centre (HSCIC) which provides an external Information Governance (IG) assessment and benchmarking opportunity in England does not apply in Wales. However, the adoption of the IG Toolkit across NHS Wales presents a future benchmarking opportunity. In the interim, however, the Health Board could do more to identify ways of benchmarking.

Information back-up

Back-up arrangements have been revised to reflect the new virtual environment and will be enhanced by the new service catalogue, but there are no back up arrangements for data held on medical devices

Exhibit 6: assessment of progress made implementing information back-up recommendations

Reference	Implemented	Recommendation	Summary of progress made
R1	In part	Changes to the standard operating procedures (SOPs) including changes to the back-up routines should be officially signed off to ensure all parties are aware of the changes made and agree to any new back-up routines, changes in responsibilities etc.	Most of the Health Board's servers have been virtualised and back-ups are managed by CommVault. Standard Operating Procedures (SOPs) are in place. SOPs are generic rather than system specific, eg, SOP for SQL[3] systems, although there are some individual systems eg Myrddin, the national patient administration system. The generic SOPs are signed off by local IT management. Local IT staff have no responsibility for the servers, but action a partial back-up. There are some third party systems which are fully managed by the third party and for which IT services have no part in the back-up, for example: • AGFA PACS • Carestream PACS • Fuji PACS

[3] Structured Query Language, or SQL is the standard language for relational database management systems. SQL is used to perform tasks such as updating or retrieving data on a database. Many common relational database management systems use SQL, including Oracle.

Reference	Implemented	Recommendation	Summary of progress made
R1	In part	Changes to the standard operating procedures (SOPs) including changes to the back-up routines should be officially signed off to ensure all parties are aware of the changes made and agree to any new back-up routines, changes in responsibilities etc.	There is currently a back-up Sharepoint site where CommVault back-up information is stored. System owners have sight of their own back-ups and reports are online. Back-up job success/failure reports are sent to some system owners. Changes to back-ups are recorded on the Changes Log on the IT Sharepoint site but will be recorded on the service catalogue currently being developed. Changes to back-up schedules for virtual systems very rarely concern systems owners as they are backed up daily. CommVault Back-up is disk to disk (in a separate room on the same site) with a second copy transported offsite. The nature of snapshot back-ups means the service is not affected, so back-ups can be taken at any time. Local IT services are developing a Sharepoint service catalogue that will drive the back-up and restore processes and will hold all back-up documentation for each system, workflows (being developed) and SOPS (generic and individual systems). It will also link to the back-up schedule on CommVault once fully developed. When service owners are identified, a workflow process will be developed to notify the service owner of a change to a component of the service. Back-up changes would be included in this. Back-up success/failure features in the IT services key performance indicators (KPI).

Reference	Implemented	Recommendation	Summary of progress made
R2	In part	A formal register of the DR tests carried out as part of routine system maintenance (ie creation of test systems) should be created to identify any systems which are not being DR tested at least annually. These systems should then be scheduled for routine DR tests.	Recovery of individual files, folders, databases and servers does take place on an ad hoc basis when there is an issue, on request or when new hardware is implemented. Recovery procedures (and a list of recoveries made) are held on Sharepoint and will be referred to by the service catalogue when it is complete. However, IT management reported that as there are more than 300 systems within the Health Board's network, it is not possible to schedule annual testing for all systems. The Health Board should maintain a register of the DR tests carried out as part of routine system maintenance, and schedule DR testing of key systems on a risk assessed basis.

Reference	Implemented	Recommendation	Summary of progress made
R3	No	A review of the medical devices not covered within the IT systems back-up and recovery procedures should be undertaken. These devices also pose a potential Caldicott (data security) risk.	EBME staff were not aware of this recommendation and have not been involved in any actions arising from it. As a result the Medical Devices Committee, which met for the first time under the new management arrangements on 13 November 2015, included this recommendation on the agenda. The meeting is chaired by the Medical Director and includes representatives from the four acute hospitals, primary care and mental health. There is a potential for patient-related data to be on medical equipment. The Health Board uses the company, Hilditch for the secure disposal of medical equipment. Hilditch has been the all-Wales contract provider for a number of years and the contract was renewed in May 2015 following competitive tender. Hilditch send certificates of cleansing for equipment before they sell it on. EBME have a medical equipment database of 37,823 devices and can produce a list of equipment which has the potential to hold patient identifiable data. Medical Devices containing patient identifiable data can be backed up to memory sticks, external drives or DVD writers, but the Health Board has no overall view of the current situation. The Health Board should identify all medical devices not covered under the IT Services back-up regime, establish a back-up policy and issue appropriate guidance to staff. However, there appears to be no agreement on the responsibilities of EBME for the medical equipment in this context and the IT service from an IT security perspective. This impasse has acted as a barrier to addressing the issue to date. The implications for Caldicott principles also need to be considered and accounted for as noted earlier in this report.

Appendix 1

Outstanding recommendations from 2012 and 2013 ICT reviews: key issues

Exhibit 7: key issues relating to outstanding recommendations

Recommendation	Key issues in 2015
Data Quality	
DQ R2 (met in part)	Recent changes to the information governance arrangements and current work to establish new data quality approaches (including 'kite mark') need to be fully embedded. The staff complement of the Data Quality Team has reduced since 2012. The Health Board needs to ensure that staffing resources are sufficient to adequately fulfil all tasks within their scope of responsibility, including data cleansing and provision of data quality training.
DQ R4 (met in part)	Much work has progressed to address duplicate electronic records and a business case for a scanning solution for paper records is being progressed. But currently, duplicate records (electronic and paper) remain a notified risk on the risk register.
IT Disaster Recovery (DR) and Business Continuity (BC)	
DRBC R1 (met in part)	The Health Board should identify any material/key clinical systems that have not been tested for DR and ensure they are tested appropriately.
DRBC R2 (met in part)	Documented business continuity plans and regular BC testing in operational units need to be fully embedded in the context of the new organisational structures.
Caldicott Arrangements	
CR1 (not yet met)	There is no deputy for the Caldicott Guardian to ensure continuity for a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Health Board also needs to identify a Senior Information Risk Owner (SIRO), who should not be the Caldicott Guardian.

Recommendation	Key issues in 2015
Caldicott Arrangements	
CR3 (met in part)	The Health Board is actively working to implement the IG Toolkit but the capacity of the information governance team is limited and while the CPiP assessment scores indicate a good level of assurance on information governance risks, there is still work to be done.
CR6 (not yet met)	Information Governance staff should work closely with EBME to ensure that data held within medical devices is fully considered under Caldicott principles.
CR7 (met in part)	The Health Board completes an annual assessment on the Caldicott Principles in Practice (CPiP) but there are no formalised arrangements for obtaining internal assurance on the self-assessment. In the absence of evidence being received by the IGC or Caldicott Guardian, the Health Board could consider commissioning an internal audit review. However, the IG Toolkit, when implemented, may require evidence collection and revised arrangements. The Annual Report does not contain information on the CPiP score or Information Security Incidents.
CR8 (met in part)	The outturn CPiP report sets out compliance and once agreed by the Caldicott Guardian is presented to IGC. The route for providing assurance to the Board is via Board sub-Committee reporting, but the Annual Report no longer contains the CPiP score or the Information Security Incidents.
CR9 (not yet met)	The Health Board effectively uses performance information to inform improvement but needs to do more to identify ways of benchmarking its progress and position.
Information Back Up	
IB-up R1 (met in part)	Most servers have been virtualised with back-ups managed by CommVault and Standard Operating Proceedues (SOPs) for IT systems in place. Work to develop a Sharepoint service catalogue is underway to improve on current arrangements, but is not yet complete.
IB-up R2 (met in part)	Recovery procedures are in place and a record of recoveries made is held. Annual DR testing has not proved feasible with more than 300 systems within the Health Board's network but the Health Board should maintain a register of the DR tests carried out, and schedule DR testing of key systems on a risk assessed basis.
IB-up R3 (not yet met)	The Health Board should identify all medical devices not covered under the IT services back-up regime, establish a back-up policy and issue appropriate guidance to staff.

Appendix 2

The Health Board's management response

Exhibit 8: The Health Board's management response setting out how the Health Board intends responding to the issues identified in this report is set out in this appendix.

Ref	Recommendation	Intended outcome/ benefit	Management response	Completion date	Responsible officer
2016 recommendations					
R1 2016	**Data Quality** The Health Board should review the staffing arrangements for the Data Quality Team and ensure that staffing resources are sufficient.	There are sufficient resources to Data Quality Team fulfil all responsibilities and tasks, including data cleansing/ provision of data quality training.	• The staffing arrangements for the Data Quality (DQ) Team are continuously reviewed and actions have been taken to address identified shortfalls. Due to financial constraints additional staff cannot always be allocated to the team therefore alternative ways of working have been implemented and actions taken to embed DQ principles across the Health Board. • Structure and roles and responsibilities of the wider informatics teams have been reviewed with the aim of increasing the numbers of staff who have a DQ function included in their role. • The role of product specialist has been introduced and has the responsibilities for data quality and training in good information practices.	October 2016	Helen Thomas (Head of Information Services)

Ref	Recommendation	Intended outcome/ benefit	Management response	Completion date	Responsible officer
2016 recommendations					
R1 2016	**Data Quality** The Health Board should review the staffing arrangements for the Data Quality Team and ensure that staffing resources are sufficient.	There are sufficient resources to Data Quality Team fulfil all responsibilities and tasks, including data cleansing/ provision of data quality training.	• A band 6 product specialist in MPI (Master Patient Index) has been recruited with specific responsibilities for patient demographic reducing duplicate records and improving data quality in Patient Administration Systems. • The Health Board is piloting the Information Governance Toolkit within Informatics. Following evaluation a decision on further roll out will be taken by IGB. Embedding the use of the tool kit will increase the staff base who have responsibility and take ownership of DQ issues within their own departments. • To take the pilot forward, an IG toolkit Project Manager has been identified from within current resources.	October 2016	Helen Thomas (Head of Information Services)

Ref	Recommendation	Intended outcome/ benefit	Management response	Completion date	Responsible officer
2016 recommendations					
R1 2016	**Data Quality** The Health Board should review the staffing arrangements for the Data Quality Team and ensure that staffing resources are sufficient.	There are sufficient resources to Data Quality Team fulfil all responsibilities and tasks, including data cleansing/provision of data quality training.	**Actions:** • An assessment of the resource requirement to implement IG toolkit within Informatics will be presented to the newly formed Information Governance board in October 2016. • The Health Board has revised the role of the Information Governance Board to ensure it has sufficient authority and good representation across the Organisation. Every Delivery Unit will be represented and will provide assurance of their local priorities and reporting structures for IG and DQ issues.	October 2016	Helen Thomas (Head of Information Services)

Ref	Recommendation	Intended outcome/ benefit	Management response	Completion date	Responsible officer
2016 recommendations					
R2 2016	**Disaster Recovery (DR) and Business Continuity (BC) planning** The Health Board should identify any material/key clinical systems that have not been tested for DR and ensure they are tested appropriately.	There is appropriate DR testing for all material/key clinical systems.	• Identify all key clinical systems and create an ongoing testing schedule. • Test those systems in line with agreed testing schedule.	January 2017 TBD following assessment requirement	Carl Mustad (Head of ICT Ops)
R3 2016	**Caldicott** The Health Board should identify a Senior Information Risk Officer (SIRO), as a role separate to that of the Caldicott Guardian.	In addition to a named Caldicott guardian, there is a separate named SIRO for the organisation.	Completed SIRO Hamish Laing Medical Director. Calidicot Guardian Sara Hayes Director of Public Health.	Completed	
R4 2016	**Caldicott** Information Governance staff should work closely with the electro bio-medical equipment (EBME) department to ensure data held in medical devices is fully considered under Caldicott principles.	Caldicott principles are applied to any patient identifiable data held on medical devices.	The Medical Devices Committee updated ToR to include representation from Information Governance (IG). The newly appointed Head of IG will sit on the Medical Devices committee from January 2017.	January 2017	Sian Richards (Head of Health Records)

Ref	Recommendation	Intended outcome/ benefit	Management response	Completion date	Responsible officer
2016 recommendations					
R5 2016	**Information Back-up** The Health Board should identify all medical devices not covered under the IT Services back-up regime, establish a back-up policy and issue appropriate guidance to staff.	Back-up arrangements consider and include information held on relevant medical devices	The Medical Equipment Team is completing a review of all existing devices by the end of September 2016. The outcome will be discussed by the medical devices committee and an appropriate action plan developed.	February 2017	Mike Rowlands, (Head of MEMS), Carl Mustad (Head of ICT Ops) and Sian Richards (Health of Health Records)

Ref	Recommendation	Intended outcome/ benefit	Management response	Completion date	Responsible officer
Recommendations for continuing action from 2012 data quality audit					
DQ R2 (met in part)	Ensure that Information Governance arrangements are efficient, effective and appropriately include data quality: • ensuring that accountability structures and the respective responsibilities of all staff for Data Quality are clearly communicated and understood by all; and • monitor and periodically review the Health Board's Data Quality Governance arrangements to ensure they are effective.	Revised information governance arrangements and the new data quality approaches are fully embedded. The Data Quality Team is sufficiently resourced to fulfil all responsibilities (including data cleansing and provision of data quality training). **See 2016 R1**	**See R1 2016 above** • Information Governance Board has been designed following a workshop in July 2016. The first meeting of the revised board will meet in October 2016 and the revised ToR will be signed off. The Board will sign off the Data Quality and Information Governance annual plans and review progress. • The Board will identify leads in each of the Delivery Units to ensure that DQ and IG issues are embedded into local structures and have a regular place in local management review processes and meetings.	October 2016	Gareth Westlake (Informatics Business Manager)

Ref	Recommendation	Intended outcome/ benefit	Management response	Completion date	Responsible officer
Recommendations for continuing action from 2012 data quality audit					
DQ R4 (met in part)	Reduce inappropriate duplicate patient demographic data within key systems (such as PAS, RADIS, RadCentre and others) and promote the consistent use of NHS numbers and patient identifiers.	Duplicate records (electronic and paper) and the associated risks are minimised.	• Work has been undertaken by the Master Patient Index Product Specialist to establish the extent of the duplicate records problem and support has been given to the relevant departments in order to reduce the creation of duplicate numbers. Reports are provided to the departments on a monthly basis in order to measure progress and address areas that are creating duplicates. • A Data Set Change Notice (DSCN 2015/06 [4][1]) was issued in November 2015 to mandate the use of the NHS Number as a national operational standard. This introduces a requirement for the use of the NHS Number in all systems used to support the commissioning or provision of NHS services that hold patient demographic information by April 2020, with the aim of further reducing duplicate records and improving Data quality. Promotion of the NHS numbers is ongoing • Work dealing with the confused records, approximately 3,000 records (different patients holding the same NHS number) is ongoing, and 100 records are outstanding, therefore reducing clinical risk.	Ongoing	

[4] Welsh Information Standards Board, **Welsh Health Circular (WCH) 2015 (049) – NHS Number Operational Standard**, 6 November 2015.

Ref	Recommendation	Intended outcome/ benefit	Management response	Completion date	Responsible officer
Recommendations for continuing action from 2012 IT Disaster Recovery (DR) and Business Continuity (BC) audit					
DRBC R1 (met in part)	Develop the overall co-ordination of ICT DR provision for the Health Board, ensuring clear priorities in terms of the order of system recovery in the event of a large scale failure. Test these arrangements on completion of the testing strategy to ensure they work as intended.	Any material/key clinical systems that have not been tested for DR are tested appropriately. **See 2016 R2**	See 2016 R2	January 2017	Carl Mustad (Head of ICT Ops)

Ref	Recommendation	Intended outcome/ benefit	Management response	Completion date	Responsible officer
Recommendations for continuing action from 2012 IT Disaster Recovery (DR) and Business Continuity (BC) audit					
DRBC R2 (met in part)	Strengthen BC planning by: • implementing the overall corporate BC register for the Health Board which co-ordinates all departmental plans. This process should involve active engagement with each department. • clarifying and allocating ownership of BC at clinical service department levels. • developing and documenting clinical system BC plans. • completing the Pharmacy BC plan, where the section on 'unavailability of premises' has not been completed. • finalising the IT BC plan and the BC plan testing strategy and testing the arrangements following implementation to ensure they work as intended.	Documented business continuity plans and regular BC testing in operational units is fully embedded in the context of the new organisational structures.	• There are corporate business continuity plans and these are in place to mitigate incidences that may affect the HB wide and are included in a Corporate Business Continuity Process and mapped against key risks, therefore there is a register. Examples of these include Pandemic Framework, Contaminated Casualties, Alternative Premises for Critical Care Areas, Security Procedures, eg Lock Down, receipt of bomb threat etc.	December 2017	Joanne Davies (Assistant Director of Strategy and Partnerships, Strategy) and Karen Jones (Emergency Planning Officer)

Ref	Recommendation	Intended outcome/ benefit	Management response	Completion date	Responsible officer
Recommendations for continuing action from 2012 IT Disaster Recovery (DR) and Business Continuity (BC) audit					
DRBC R2 (met in part)	Strengthen BC planning by: • implementing the overall corporate BC register for the Health Board which co-ordinates all departmental plans. This process should involve active engagement with each department. • clarifying and allocating ownership of BC at clinical service department levels. • developing and documenting clinical system BC plans • completing the Pharmacy BC plan, where the section on 'unavailability of premises' has not been completed. • finalising the IT BC plan and the BC plan testing strategy and testing the arrangements following implementation to ensure they work as intended.	Documented business continuity plans and regular BC testing in operational units is fully embedded in the context of the new organisational structures.	**Actions** • BC Process approved by EPRR Strategy Group and includes a register of the above plans. A schedule is in place for review and update of each of these plans. IT BC is included within this register and it is noted on the schedule the assigned lead for the update. It is planned during 2017 to have an exercising programme for these plans. All these plans are included on the major incident web page and are stored in a central drive for major incidents; all email users have access. There are 'hard copies' in each of the co-ordination centres where Silver Command will be undertaken. • Emergency Preparedness Resilience and Response (EPRR) Strategy developed and approved by the Board which includes identification of the HB obligations under the Civil Contingencies Act and BC is included within this. There is a work programme in place and the Board is updated on EPRR progress.	December 2017	Joanne Davies (Assistant Director of Strategy and Partnerships, Strategy) and Karen Jones (Emergency Planning Officer)

Ref	Recommendation	Intended outcome/ benefit	Management response	Completion date	Responsible officer
Recommendations for continuing action from 2012 IT Disaster Recovery (DR) and Business Continuity (BC) audit					
DRBC R2 (met in part)	Strengthen BC planning by: • implementing the overall corporate BC register for the Health Board which co-ordinates all departmental plans. This process should involve active engagement with each department. • clarifying and allocating ownership of BC at clinical service department levels. • developing and documenting clinical system BC plans. • completing the Pharmacy BC plan, where the section on 'unavailability of premises' has not been completed. • finalising the IT BC plan and the BC plan testing strategy and testing the arrangements following implementation to ensure they work as intended.	Documented business continuity plans and regular BC testing in operational units is fully embedded in the context of the new organisational structures.	• Business Continuity for all services will include the following process; approval of the Business Continuity Framework which has recently been updated as the standard for all services, within each Unit they will now need to progress BCs for their respective services. • Each Unit has identified Emergency Planning leads and consequently represent the Units at the EPRR Strategy Group. In addition they have identified the process for discussion and progression of EPRR within each of their Units. Responsibility for BC development and consequent maintenance of a register per Unit will fall with the respective Unit management teams, as well as having a central drive for access of the BCs and also to ensure each service has 'hard copies' in place.	December 2017	Joanne Davies (Assistant Director of Strategy and Partnerships, Strategy) and Karen Jones (Emergency Planning Officer)

Ref	Recommendation	Intended outcome/ benefit	Management response	Completion date	Responsible officer
Recommendations for continuing action from 2012 IT Disaster Recovery (DR) and Business Continuity (BC) audit					
DRBC R2 (met in part)	Strengthen BC planning by: • implementing the overall corporate BC register for the Health Board which co-ordinates all departmental plans. This process should involve active engagement with each department. • clarifying and allocating ownership of BC at clinical service department levels. • developing and documenting clinical system BC plans. • completing the Pharmacy BC plan, where the section on 'unavailability of premises' has not been completed. • finalising the IT BC plan and the BC plan testing strategy and testing the arrangements following implementation to ensure they work as intended.	Documented business continuity plans and regular BC testing in operational units is fully embedded in the context of the new organisational structures.	• As part of the EPRR work programme, the next step is the progression of BCs for each service within the Units, utilising the BC Framework as the standard. A recent paper to the Board highlighted the need for additional resources to support this work and there has been agreement in principle for an increase in the EPRR Team. Following appointment the priority will be to work with the Units to support BC development for the respective services. In the interim, I will be liaising with the Units in term to commence this process. This has been delayed due to the organisational changes and waiting for the structures below the triumvirate to be established, particularly with the service leads.	December 2017	Joanne Davies (Assistant Director of Strategy and Partnerships, Strategy) and Karen Jones (Emergency Planning Officer)

Ref	Recommendation	Intended outcome/ benefit	Management response	Completion date	Responsible officer
Recommendations for continuing action from 2012 IT Disaster Recovery (DR) and Business Continuity (BC) audit					
DRBC R2 (met in part)	Strengthen BC planning by: • implementing the overall corporate BC register for the Health Board which co-ordinates all departmental plans. This process should involve active engagement with each department. • clarifying and allocating ownership of BC at clinical service department levels. • developing and documenting clinical system BC plans • completing the Pharmacy BC plan, where the section on 'unavailability of premises' has not been completed. • finalising the IT BC plan and the BC plan testing strategy and testing the arrangements following implementation to ensure they work as intended.	Documented business continuity plans and regular BC testing in operational units is fully embedded in the context of the new organisational structures.	• The BC Framework includes a standardised format, a risk assessment process and business impact analysis; all as part of the process for BC development. • Following the development, a schedule will be required for awareness training and a programme for exercising for each Unit. • The BC Framework also includes the 5 key areas for mitigation of risk – staffing, premises, equipment, service disruption and maintenance, therefore, as an example, Pharmacy on each Unit will have BCs in place to address each of these 5 key areas. The audit notes the premises section to be missing for the Pharmacy BCs.	December 2017	Joanne Davies (Assistant Director of Strategy and Partnerships, Strategy) and Karen Jones (Emergency Planning Officer)

Ref	Recommendation	Intended outcome/ benefit	Management response	Completion date	Responsible officer
Recommendations for continuing action from 2012 review of Caldicott Arrangements					
CR1 (not yet met)	The current Caldicott Guardian is well respected and well known by staff and management at the Health Board, it is imperative that the Health Board put in place effective succession planning to manage the replacement of the Caldicott Guardian when the current Guardian retires in December 2012. Consideration should be given to the appointment of a deputy Caldicott Guardian who could maintain continuity and progress against actions in the absence of the Caldicott Guardian but actual Caldicott decisions should not be delegated and should remain with the Guardian.	There are clear arrangements to ensure continuity for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing in the absence of the Caldicott guardian, and a separate Senior Information Risk Owner (SIRO). See 2016 R3	See R3 2016	Completed	

Ref	Recommendation	Intended outcome/ benefit	Management response	Completion date	Responsible officer
Recommendations for continuing action from 2012 review of Caldicott Arrangements					
CR3 (met in part)	The current Caldicott support teams, comprising members of the Information Governance and IT security teams, work well together and with the Guardian but the Health Board needs to ensure the resources of these teams are sufficient to deliver the Caldicott training programme and to monitor progress against Caldicott principles.	There is an appropriately resourced information governance team to support rollout of the IG and provide assurance on information governance risks.	A new role of the Head of IG is being appointed in October 2016; this has been possible due to a retirement in the team. Once in post the team structure will be reviewed to ensure it is fit for purpose. Resource requirements will be presented to IGB.	January 2017 for the review	Sian Richards (Head of Health Records)
CR6 (not yet met)	The Health Board has a good understanding of its Information Confidentiality responsibilities and has identified its high risk patient and staff information but needs to do more to identify whether there are any other information sources which need to be assessed under the Caldicott Principles.	Data held within medical devices is fully considered under Caldicott principles. **See 2016 R4**	R4 2016 above.		

Ref	Recommendation	Intended outcome/ benefit	Management response	Completion date	Responsible officer
Recommendations for continuing action from 2012 review of Caldicott Arrangements					
CR7 (met in part)	The Health Board completes an annual assessment and progress against actions identified in the assessment on the Caldicott Principles in Practice (CPiP) and they should seek their own internal assurance on this self-assessment via internal audit.	Arrangements are in place for assurance on the CPiP self-assessment and the evidence requirements for of the IG Toolkit roll-out are identified.	These will be presented to the newly formed Information Governance Board and continued to be reviewed by internal Audit.	Ongoing	Sian Richards (Head of Health Records)
CR8 (met in part)	The level of compliance with the Caldicott Principles should be effectively reported to the Board and the Caldicott Principles in Practice (CPiP) score included in the Annual Report to provide balance to any information security incidents reported in the Annual Report.	The IGC provides effective scrutiny and assurance to the Board regarding compliance with Caldicott principles and Information governance and security.	Information Governance Committee (IGC) is replaced by Information Governance Board (IGB) and will continue to provide this assurance. IGB will report to the Audit Committee.	October 2016	Gareth Westlake (Informatics Business Manager)
CR9 (not yet met)	The Health Board effectively uses performance information to inform improvement but needs to do more to identify ways of benchmarking its progress against other similar organisations.	Performance information and benchmarking inform improvement.	IGB will review opportunities for benchmarking on Information Governance.	April 2017	Head of Information Governance

Ref	Recommendation	Intended outcome/ benefit	Management response	Completion date	Responsible officer
Recommendations for continuing action from 2013 information back-up audit					
IB-up R1 (met in part)	Changes to the standard operating procedures (SOPs) including changes to the back-up routines should be officially signed off to ensure all parties are aware of the changes made and agree to any new back-up routines, changes in responsibilities etc.	Development of a SharePoint service catalogue is completed and effectively underpins arrangements.	Completed		Carl Mustad (Head of ICT Ops)
IB-up R2 (met in part)	A formal register of the DR tests carried out as part of routine system maintenance (ie creation of test systems) should be created to identify any systems which are not being DR tested, at least annually. These systems should then be scheduled for routine DR tests.	The Health Board has a register of the DR tests carried out, and schedules DR testing of all key systems on a risk assessed basis.	Completed		Carl Mustad (Head of ICT Ops)
IB-up R3 (not yet met)	A review of the medical devices not covered within the IT systems back-up and recovery procedures should be undertaken. These devices also pose a potential Caldicott (data security) risk.	There is a back-up policy for medical devices with guidance provided to staff. **See 2016 R5**	See 2016 R5		

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