GIG CYMRU NHS WALES
Partneriaeth Cydwasanaethau
Gwasanaethau Archwilio a Sicrwydd
Shared Services Partnership
Audit and Assurance Services

GIG CYMRU NHS WALES
Bwrdd Iechyd Prifysgol Cwm Taf Morgannwg University Health Board

Cwm Taf Morgannwg University Health Board

IT Assessment

Final Internal Audit Report

2020/21

NHS Wales Shared Services Partnership

Audit and Assurance Services

Contents **Page**

Review reference:	CTMUHB2021.17
Report status:	Final
Fieldwork commencement:	16 July 2020
Fieldwork completion:	5 October 2020
Draft report issued:	3 November 2020
Management response received:	6 January 2021
Final report issued:	14 January 2021
Auditor:	Martyn Lewis, IT Audit Manager
Executive sign off:	Clare Williams, Director of Planning and Performance (Interim)
Distribution:	Andrew Nelson, Chief Information Officer Karen Winder, Interim ADI
Committee:	Audit and Risk Committee

Audit and Assurance Services conform with all Public Sector Internal Audit Standards as validated through the external quality assessment undertaken by the Institute of Internal Auditors.

ACKNOWLEDGEMENT

NHS Wales Audit & Assurance Services would like to acknowledge the time and co-operation given by management and staff during the course of this review.

Please note:

This audit report has been prepared for internal use only. Audit & Assurance Services reports are prepared, in accordance with the Service Strategy and Terms of Reference, approved by the Audit and Risk Committee.

Audit reports are prepared by the staff of the NHS Wales Shared Services Partnership – Audit and Assurance Services, and addressed to Independent Members or officers including those designated as Accountable Officer. They are prepared for the sole use of the Cwm Taf Morgannwg University Health Board and no responsibility is taken by the Audit and Assurance Services Internal Auditors to any director or officer in their individual capacity, or to any third party.

1. Introduction and Background

This baseline review of the arrangements in place for the management and control of Information Governance (IG) and Information Communications Technology (ICT) has been completed in line with the 2020/2021 Internal Audit Plan for Cwm Taf Morgannwg University Health Board (the 'Health Board' or the 'organisation'). The review seeks to provide a baseline picture to the Audit and Risk Committee of the processes in place to manage the risks associated with IG / ICT.

As this is a baseline review, the assignment has not been allocated an assurance rating, but observations and recommendations have been provided to facilitate change and improvement, and to focus audit work in the future.

2. Scope and Objectives

The objective of the audit was to establish the processes and mechanisms in place for management of IG/ ICT within the organisation. The review sought to provide a baseline picture of the organisation's status and provides suggestions for areas of improvement or future development.

The areas considered within the review are:

Information Governance

- The information governance process in place.
- IG policies and procedures in place.

ICT and Security

- ICT responsibilities are clear.
- ICT strategy, linked to organisational strategy.
- The ICT governance process in place.
- The funding / resource available for ICT and its sustainability.
- IT security policies and procedures.
- ICT provision and support arrangements across the organisation.
- IT continuity and disaster recovery processes.
- Compliance against obligations (e.g. General Data Protection Regulation (GDPR), Directive on Security of Network and Information Systems (NISD), Payment Card Industry Data Security Standard (PCI DSS) etc.)
- The process to track ICT assets.
- IG / ICT risk identification and management.

3. Associated Risks

The potential risks considered in this review are as follows:

- the Information Management and Technology (IM&T) strategy does not effectively support the organisation in delivery of its objectives and not supported by effective governance and/or delivery arrangements;
- un-coordinated IM&T related financial activities in both the business and IT functions, covering budget, cost and benefit management and prioritisation of spending;
- the IM&T services provided do not fully meet the needs of the organisation;
- IM&T services are subject to loss of service;
- inappropriate access to systems and data; and
- breach of legal compliance requirements.

4. Conclusion

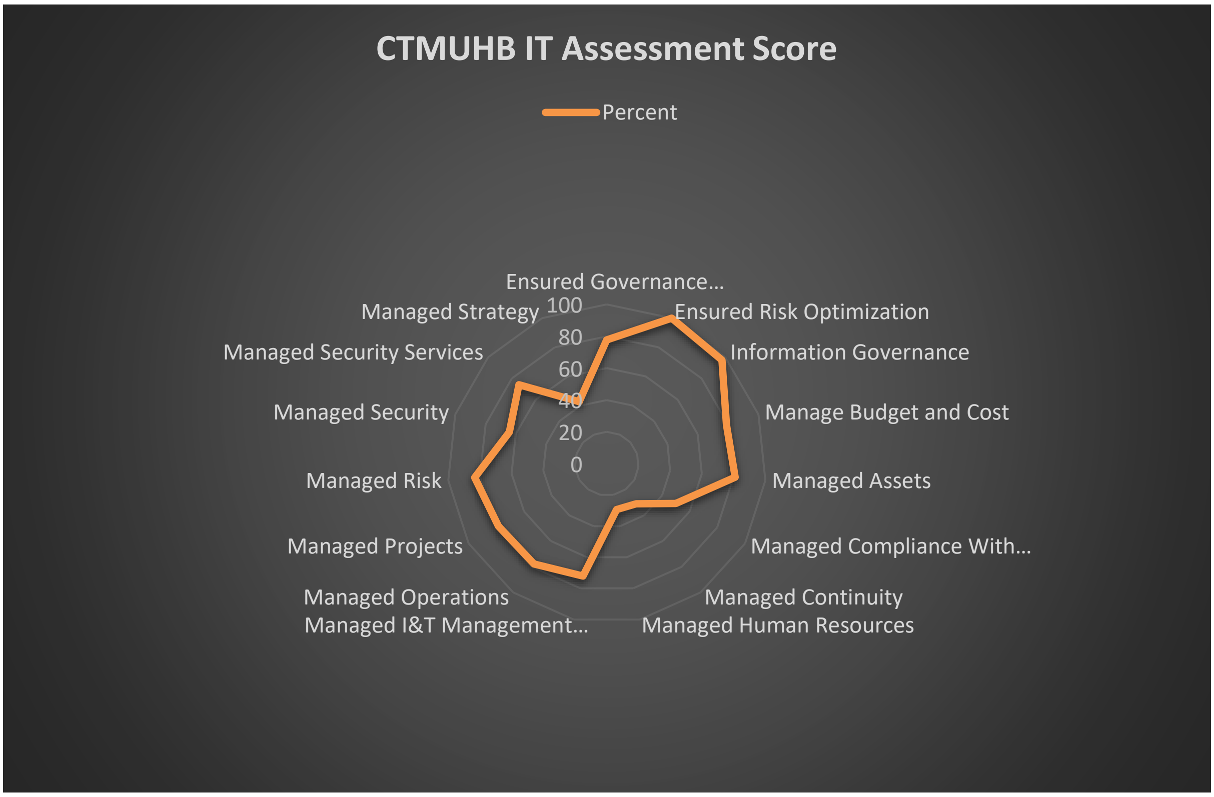
As this is a baseline review we have not allocated an assurance rating, but observations recommendations have been provided to facilitate change and improvement, and to focus audit work in the future.

For this review we used the expected controls derived from the Control Objectives for Information and Related Technologies (COBIT) 2019 framework and we have reported using the subheadings of these control processes for governing organisational IT.

COBIT is an IT management framework developed by the Information Systems Audit and Control Association (ISACA) to help organisations develop, organise and implement strategies around information management and governance.

As part of our assessment we scored the individual controls in place at the Health Board against the controls we would expect to be in place under each of the headings of the framework. These scores have been represented graphically below to illustrate the strengths and potential for improvement in the organisation’s management of IG / ICT.

The scoring reflects the level of compliance with the controls set out within the COBIT framework, and the extent to which they apply across the entire organisation.



The Health Board scored well under many of the headings, in particular against: Managed Assets; Information Governance; Governance Framework; Managed Operations; Managed Budget; Managed Projects; Managed Risk and Ensured Risk Optimization.

However, there are opportunities for improvement across a number of objectives. The key areas requiring management attention are identified from the scoring. These were: the management of compliance with external requirements; managed continuity; managed human resources; and managed strategy. More detail can be found on these opportunities in section 4 below, and in Appendix A.

The percentage score for each objective is set out in the table below:

Control area	Percentage	No. of observations/ Recommendations
Information Governance	97%	-
Ensured Governance Framework Setting and Maintenance	78%	-
Managed Compliance with External Requirements	50%	1
Ensured Risk Optimization	100%	1
Managed Risk	83%	1
Managed I&T Management Framework	72%	2
Managed Strategy	43%	6
Managed Budget and Cost	79%	1
Managed Human Resources	29%	1
Managed Security	64%	-
Managed Security Services	74%	1
Managed Assets	81%	2
Managed Operations	78%	-
Managed Continuity	31%	1
Managed Projects	79%	-
Total	**-**	**17**

5. Observations and Recommendations

<u>Objective 1: Information Governance</u>

Control Area: Information Governance (97.2%)

- There is an established process for Information Governance (IG) at the Health Board with key strategic responsibilities such as Senior Information Risk Owner (SIRO) and Caldicott guardian assigned to appropriate officers.

  There is an IG team to support the organisation, and a suite of IG control documents to support the IG agenda, these are available on the intranet, and form part of induction and organisational training.

IG issues are monitored via the Digital & Data Committee, and there is an Information Governance Group sitting below this, which takes the lead on Information Governance.

The Health Board has a publication scheme in place, along with a disclosure log and an Information Asset Register.

There are no recommendations under this objective.

Objective 2: ICT and Security

Control area: Ensured Governance Framework Setting and Maintenance (78%)

- There is a formal governance structure in place for ICT with a defined Committee (Digital & Data Committee) which has a committee work plan. The work plan includes an annual review of committee effectiveness. There are operational groups which feed into a steering group and then reporting up to committee.

  Our internal audit work includes IM&T. Our reports and outcomes from our work is monitored both by the Digital & Data Committee and the Audit and Risk Committee.

  There were no recommendations under this objective.

Control Area: Managed Compliance with External Requirements (50%)

- The policies in place are aligned to compliance requirements as they refer to relevant legislation and standards, and are reviewed periodically or when there is a significant compliance change.

  The Digital & Data Committee has a remit to gain assurance for the Board over compliance against relevant legislation, which is set out in its terms of reference. There is identification and monitoring of some of these compliance requirements, in particular the information governance related items through the committee.

  However, there is no structure to ensure compliance with all external requirements relating to IM&T. There is no register or record of the existing compliance requirements or the consequences of non-compliance.

  In addition, there is no process to fully assess the status of compliance and report upwards to committee for items such as PCI/DSS, or NISD. Consequently, the committee may not be fully aware of the assurance it needs to seek over compliance with external requirements, or indeed how well the Health Board is complying.

  See Observation/Recommendation 1 at Appendix A.

Control Area: Ensured Risk Optimization (100%)

- There is an organisational risk management strategy in place. The policy is supported by a formally defined active risk management process which includes a structure for escalation via the Audit & Risk Committee.

  ICT risks are monitored with a clear escalation from the ICT department to the Digital & Data Committee and Audit & Risk Committee, with the greatest risks included on the organisational risk register.

  There were no recommendations under this objective.

Control Area: Managed Risk (83%)

- As noted above the risk management process works to ensure that executives and independent members are informed of the risks with the highest score. However, there is no process to formally notify senior management of risks being managed at a lower level which contain a severe or catastrophic worst-case scenario.

  See Observation/Recommendation 2 at Appendix A.

- There is a process for including risks within business cases, and the identification and collation of ICT related risks within a consistent risk register format. The impacts of risks are assessed and actions are defined to manage the risk within accepted tolerance levels.

  However, although there are processes in place to manage issues and incidents as they occur, these processes are not fully linked to the risk management process. This means that any underlying risks may not always be identified and recorded within the risk register immediately.

  See Observation/Recommendation 3 at Appendix A.

Control Area: IM&T Management Framework (72%)

- There is a management framework in place for ICT and this has recently been revised.

  There is a Digital Health Strategy Steering Group in place with stakeholder involvement. Underneath this there is the senior team meeting and operational subgroups which take the lead for specific operational areas.

  Not all of the subgroups have documented terms of reference. This may mean some lack of clarity over the function, scope and mandate of the group and the related departments within ICT.

  See Observation/Recommendation 4 at Appendix A.

- The creation of the centralised model for ICT delivery and support was part of a formal review when originally developing the structure, as such the organisation is aware of the context and placement of ICT.

The ICT department has recently restructured to ensure that departmental functions and scopes are suitable for the delivery of ICT services, with key roles for ICT in place.

Roles and responsibilities for ICT functions are made clear via job descriptions, and there is consideration of cover needs and succession planning in the operation of the department in order to minimise the potential disruption due to staff loss.

There are regular senior team meetings for ICT that allow for tracking and management of performance and progress tasks.

Policies and procedures are in place for many ICT items and there is a webpage for these. However, the webpage does not include all of the ICT procedures in place (disposal and back up procedures are both absent). In addition, there is no procedure or guidance for Bring Your Own Device (BYOD) or change management.

See Observation/Recommendation 5 at Appendix A.

Control Area: Managed Strategy (43%)

- There is a Digital Health strategy in place, which is aligned to the all Wales 'Informing Healthcare' programme. This is explicitly linked to the organisational strategy and sets out the high-level objectives for delivery. In addition, the Health Board's IMTP includes an ICT section that defines the strategic priorities for ICT.

  The Digital Health Strategy compares the current position to the target in terms of systems and infrastructure items. The Health Board has recently reviewed the implementation of the strategy and found that it lacked a 'roadmap' to deliver the strategy. The changes needed in order to implement the Digital Health Strategy are not fully explained and there has been no assessment of the implications of the gaps. In addition, there is no assessment of the value of the change action. This may mean that the Health Board is not fully aware of the changes needed and has not articulated the value in the change or the cost of not enacting these.

  See Observation/Recommendation 6 at Appendix A.

- The baselining of the current position contained within the Digital Health Strategy is incomplete. It does not cover services supplied by external suppliers, and there is no assessment of IT skills both within ICT and more widely across the organisation. In addition, although there is a maturity assessment this is only against the services provided. It does not cover all supporting areas such as the ability of leadership to leverage technology, the level of accepted technology risk, approach to innovation, culture and knowledge level of users.

The lack of a full baseline and maturity assessment means that the Health Board is not fully aware of its starting position, and so cannot appropriately plan out a roadmap to full strategic implementation.

See Observation/Recommendation 7 at Appendix A.

- Although the Digital Health Strategy sets out the services required by the organisation, this is only in terms of the specific systems / applications needed. There is no consideration of wider, supporting items such as validated emerging technology or innovation ideas, reference standards, I&T capabilities, comparative benchmarks of good practice, and emerging I&T service provision. In effect, the Digital Health Strategy sets out what to deliver as a system / application, but not what needs to be done in the background to support this.

  See Observation/Recommendation 8 at Appendix A.

- Projects and infrastructure items have been identified to deliver the Digital Health Strategy. While there is a partial roadmap within the Digital Health Strategy which is focused on systems and infrastructure, there is no single full roadmap for implementation of the strategy that sets out all the projects into a prioritised programme, and identifies resource requirements, overlaps and synergies between projects. In addition, there is no consideration of using external suppliers and agencies to deliver the strategy e.g. partnerships with suppliers.

  See Observation/Recommendation 9 at Appendix A.

- While there is a business champion, the Clinical Lead for IM&T, the mechanisms for driving forward the Digital Strategy are undeveloped. The strategy is promoted by ICT, but there is no network of champions within the organisation that can act as a 'pull factor' and lead within their area. In addition, the organisation does not link business change managers into ICT projects. These issues mean that departments are not fully realising the benefits of technology and this acts as a drag on implementation.

  See Observation/Recommendation 10 at Appendix A.

- While there has been communication of the Digital Health Strategy and its aims, this was several years ago and there has been no recent communication of the Digital Health Strategy, and there is no link or page on the intranet to include it.

  See Observation/Recommendation 11 at Appendix A.

Control Area: Managed Budget and Cost (79%)

- Prioritisation of capital expenditure is against business cases to ensure the appropriate benefits and strategic fit.

  Funding is available for ICT, with all ICT expenditure routed through the ICT department which means identification of spend level is achievable.

There is a defined ICT budget and performance monitoring process. However, the ICT budget is based on the previous year, with changes factored in. The budget does not appear to link to the strategy or work plan and so does not fully reflect the organisation's requirements. This means that the Health Board may not be sighted on the financial resource needed to achieve the Digital Health Strategy, and that overspending may happen against budgets.

See Observation/Recommendation 12 at Appendix A.

Control Area: Managed Human Resources (29%)

- As noted previously the ICT department has been restructured to better fit the needs of the organisation. The department contains staff who are qualified in various IT skills. Training is provided for ICT staff, and training needs are identified via the PADR process. This feeds into a single record of training requirements that is prioritised and provided within funding limits.

  There has been no full assessment skills held within ICT, and what resource and skills are required in order to support IM&T across the organisation and to deliver the Digital Health Strategy. Consequently, there has been no identification of the skills gap and no development of a structured staff development plan in order to close the gap. Without this development plan in place ICT may struggle to implement the Digital Health Strategy.

  See Observation/Recommendation 13 at Appendix A.

Control Area: Managed Security (64%)

- The structure for cyber security has been revised, with a team now in place and a formal governing group. There is a cyber work stream action plan to improve the cyber security position of the Health Board. This action plan is monitored by the ICT Risk, Audit, Governance & Cyber Security Board.

  Guidance is available for staff on the cyber site on the intranet with reminders provided using the Health Board news page. There is cyber security training available to staff, and this is being further developed with intended training on phishing to identify areas of weakness and support the designation of the cyber security training as mandatory.

  The KPIs in place for the cyber team are being further developed to provide cyber security status related KPIs.

  The Health Board is in the early stages of enacting the Security Information and Event Management System (SIEM). Once this is in place it will enable active monitoring of cyber security within the organisation.

  There were no recommendations under this objective.

Control Area: Managed Security Services (74%)

- Systems for antivirus protection, web and mail filtering have been deployed at the Health Board. There has been increased collaboration with national cyber groups including the NHS Wales Operational Security Service Management Board (OSSMB). Regular alerts are provided as part of this group which are then assessed and acted upon locally. There is also a cyber email address which receives notifications and alerts from: Microsoft; Cisco; Solarwinds; CVE; as well as NWIS.

  There are firewalls in place. Firewall rules have recently been revised, and a process for more active management of these rules has been established.

  The network is governed by a standard NHS Wales code of connection. The Code of Connection (CoCo) process is designed to ensure that appropriate levels of assurance are provided for organisations requiring a connection to the NHS Wales Network. In order to provide this assurance the NWIS' Cyber Security Team requires documentation to be completed by any organisation wishing to connect.

  At the present time there is no device level authentication to the network, and the network is not fully segmented or split up into different sub-networks or sections in order to increase security.

  See Observation/Recommendation 14 at Appendix A.

- Vulnerability scanning and management, together with intrusion detection, is work in progress, with the use of scanning products such as Nessus, Solar Winds and CISCO ISE all being developed. At present only initial vulnerability scanning has occurred, although we note that management intend to roll this out further, along with a more developed intrusion detection capability.

  Security incidents are monitored by the cyber group and there is a Cyber Incident Response Plan in place that sets out how the organisation will react and deal with threats.

Control Area: Managed Assets (81%)

- There is an asset register that is used to record all IT equipment. This is an 'in house' written application and links to Service Point. The register captures key information for assets including the type of asset, manufacturer, model, location and serial number.

  The asset management process includes a process for the disposal of IT equipment that ensures data is kept secure and allows assets to be tracked to disposal. Although all assets are recorded there is no clear identification of those assets that are critical to the provision of ICT services for the organisation. Accordingly, there is no formal, regular assessment of the risk of failure of these or identification of the need for replacement.

See Observation/Recommendation 15 at Appendix A.

- There is a process in place for patching and updating firmware of IT equipment. Contracts are in place for services that 'flag' the need for updates. This process however is not formally documented meaning that the organisation is reliant on staff knowledge.

  See Observation/Recommendation 16 at Appendix A.

Control Area: Managed Operations (78%)

- We identified specific risks to the operation of ICT service within the risk register, which includes the risk of fire and loss of power to servers.

  Server rooms are kept secure and there is a regular physical check to ensure that the rooms are protected and kept clear. The main server rooms have air conditioning and there is a process in place for monitoring the environment of the server rooms using equipment that ensures warnings are produced in the event of abnormal temperature, humidity or smoke conditions.

  The designed architecture is resilient with mirroring and high availability in operation, which minimises the risks associated with the loss of individual servers.

  The main rooms have dual power supplies to ensure continuity. There is an Uninterruptible Power Supply (UPS) in place for the servers, which has recently been renewed at the PCH site. Emergency generators are operational on each site and there are annual tests of these.

  There were no recommendations under this objective.

Control Area: Managed Continuity (31%)

- There are IT disaster recovery (DR) plans in place for systems managed by ICT, which consider key risks, and include contacts for enacting the plans, although we note that our report in February 2019 identified that some of these plans were out of date and remain so.

  There is no overarching Business Continuity Plan (BCP) for ICT, that covers all systems, and provides for prioritisation of system recovery based on a Business Impact Analysis (BIA), which considers agreed departmental needs for an appropriate recovery time.

  See Observation/Recommendation 17 at Appendix A.

- There is a Backup policy in place. Backups of electronic data are taken on a regular and structured basis, with a structure for testing these.

  Across the Health Board directorates appear to be generally aware of their responsibility to ensure an appropriate plan is in place to provide continuity of their services in the event of a loss of IT, and generally understand that there may be a 'lag' in recovery.

Control Area: Managed Projects (79%)

- There is a record of all IT projects underway. IT projects are run in accordance with PRINCE2 methodology and procedures / guidance for project management are place. In addition, a deployment assurance matrix has been developed to provide assurance that the key events within a PRINCE2 projects have occurred, forcing the project to comply with requirements. The ICT department includes project managers with the appropriate certification. Training is provided on project management to ICT staff.

  There were no recommendations under this objective.

6. Summary of Observations and recommendations

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

Design of Systems/Controls

Our fieldwork has highlighted one observation/recommendation that can be classified as a weakness in the system controls/design.

Operation of System/Controls

Our fieldwork has highlighted sixteen observations/recommendations that can be classified as weaknesses in the operation of the designed system/controls.

Observation 1 – Monitoring Compliance (Operation)

There is no register of compliance requirements for IM&T and there is no structured process to identify all the compliance requirements relating to IM&T, assessing the compliance status and feeding the position in relation to requirements, status and consequences upwards to committee for items such as PCI/DSS, or NISD.

Recommendation

A register of compliance requirements for all IM&T related legislation and standards should be developed along with a process for assessing status and reporting upwards to Committee.

Management Response, Responsible Officer and Deadline

Compliance requirements are managed within the UHB’s internal digital working groups and also in pan-Wales groups. These internal groups include cyber security, end user computing, architect board, IG group, with the pan Wales groups including IG Managers Advisory Group, Infrastructure Management Board and Cyber Security Board.

These groups maintain a risk register which will in future be combined and reported in to the Digital Health Strategy Steering Group DHSSG and the UHB’s Information Governance Group, both of which report into the Digital and Data Sub Committee of the Board.

Responsible Officer

Chief Information Officer

Deadline

End January 2021

Observation 2- Communicating Managed Risks (Operation)

While the department risk register is monitored via the Health Board process and reported via Committee and Board, there is no process to formally notify executives of risks being managed at a lower level which contain a severe or catastrophic worst-case scenario.

Recommendation

Management should consider providing an annual report that identifies risks that have a low likelihood, have a severe worst-case scenario. This would ensure that executives are aware of the risks and worst cases that are being managed at a lower level, but hold the potential for severe adverse effects should they materialise.

Management Response, Responsible Officer and Deadline

All ICT risks are managed in the department with those risks 15 and above escalated to the Health Board risk register. The Health Board risk register is reviewed regularly at Management Board and Board. The escalation of the ICT and Performance and Information departmental risks above 15 has been a new change to reporting since the latest review of the Health Board risk register. The risk register both the ICT and Performance and Information department, and the relevant risks on the Health Board risk register has been added as a standard agenda item for consideration by DHSSG following and the Information Governance Group.

Responsible Officer

Chief Information Officer

Deadline

End December 2020

Observation 3 – Link of Risks to Events (Operation)

The link from the risk management process to the event / issue / problem management process is not fully defined, with no automatic identification of underlying risks that are causing issues and addition of these onto the risk register. This means that any underlying risks may not always be recorded in good time.

Recommendation

The risk identification process should be formally linked to the issue / event / problem management process in order to ensure that underlying risks are identified.

Management Response, Responsible Officer and Deadline

Each project has its own live risk register which is managed by the project team. A Head of ICT Programmes has been appointed and will ensure that these risk registers and the proposed mitigating actions are kept as living documents and are also assessed, standardised, considered from a system wide perspective in order to ensure that causes and consequences are identified and addressed.

Responsible Officer

Assistant Director of ICT

Deadline

Mid-February 2021 (6 weeks post start date of Head of ICT programmes)

Observation 4 – ICT Sub-Groups (Operation)

There are sub-group meetings for the management of ICT, however they do not all have TORs. This may mean some lack of clarity over the function, scope and mandate of the group and the related departments within ICT.

Recommendation

Each sub-group should have a defined terms of reference.

Management Response, Responsible Officer and Deadline

All longstanding non task and finish sub-groups will have TORs developed by end of January, subject to operational pressures, such as the Covid response enabling capacity to be prioritised to this task.

Responsible Officer

Assistant Director of ICT

Deadline

End January 2021

Observation 5 – Policies (Operation)

Policies and procedures are in place for many ICT items and there is a webpage for these.

However, the webpage does not include all ICT procedures in place (Disposal and Back Up procedures absent) and there is no procedure or guidance available for Bring Your Own Device (BYOD) or change management.

Recommendation

The website should include all ICT policies and procedures and guidance developed for key areas of ICT operation.

Management Response, Responsible Officer and Deadline

The ICT Web site is currently being reviewed and first iteration is live and all relevant approved policies that are not available will be uploaded. The caveat that this should be limited to relevant policies relates to the significant change in needs and service models arising during our management of the Covid response. During this time there has been a necessity for working practices to adapt to try and maximise what is achievable to maintain care and services for our population and patients, some of which are at odds with existing policy. It is our intention to ensure that we continue to enable patients, clinicians and carers to maximise the benefits of digital ways of working and living and thus we will review and update our policies as soon as the external environment permits.

Responsible Officer

Service manager and Server team re website

Chief Information Officer re policies

Deadline

End April 2021 subject to the Covid environment allowing

Observation 6 – Strategy Gap Analysis (Operation)

The strategy, which has recently been reviewed by management, compares the current position to the target position in terms of systems and infrastructure items. However, the changes needed in order to implement the strategy are not fully explained within the strategy and there has been no assessment of the implications of the gaps. In addition, there is no assessment of the value of the changes or lack of change.

This means that the Health Board is not fully aware of the changes needed and has not articulated the value in the change or the cost of not enacting these.

Recommendation

A full gap analysis should be undertaken to highlight the changes needed, along with the value impact of these.

Management Response, Responsible Officer and Deadline

The UHB is in the process of tendering for external support review initially our infrastructure as part of the review of the digital strategy. Whilst this is being developed within ICT we are working on formalising a roadmap to be able to clearly demonstrate what is planned to be delivered, when and any gaps that need to escalate to HB. This item of work will need to be delivered as part of the response to observation 7.

Responsible Officer

Chief Information Officer

Deadline

Intention is that this will be completed by April 2021

Observation 7 –Strategy Baseline (Operation)

The strategy includes some baselining of the current strategic position, but this is incomplete. It does not specify services supplied by external suppliers versus internal provision separately, and there is no assessment of IT skills within ICT or wider organisational IT skills.

In addition, although there is an assessment of maturity, this is only against the services provided. It does not cover areas such as the 'ability of leadership to leverage technology', the 'level of accepted technology risk', or the 'approach to innovation', 'culture' and 'knowledge level of users'.

The lack of a full baseline and maturity assessment means that the Health Board is not fully aware of its starting position, and so cannot properly plan a 'roadmap' to full strategic implementation.

Recommendation

A review of the current strategic position of the Health Board in relation to its digital provision and maturity across all domains should be undertaken.

Management Response, Responsible Officer and Deadline

In refreshing its strategic for digital the UHB will complete a maturity review as recommended to baseline our position.

Responsible Officer

Chief Information Officer

Deadline

Whilst a high level baseline review should be completed by February, it is intended that given the agile nature of digital developments and requirement, the review will become a live document composed of numerous domain specific

detailed reviews, which will be completed on an ongoing cycle as it is felt they are necessary.

Observation 8 – Strategy Requirements (Operation)

Although the strategy sets out the services required, this is only the systems and applications needed. There is no consideration of validated emerging technology or innovation ideas, reference standards, I&T capabilities, comparative benchmarks of good practice, and emerging I&T service provision.

In effect the strategy sets out what to deliver as a system / service, but not what needs to be done in the background to support this.

Recommendation

The organisation should develop an understanding of the underpinning requirements for strategic delivery.

Management Response, Responsible Officer and Deadline

The digital element of the IMTP which underpins delivery of the corporate strategy and the digital strategic plan will set out the macro level tactical approach to ensuring that the solutions proposed have solid foundations and are achievable

Responsible Officer

Assistant Director of ICT

Deadline

March 2021

Observation 9 – Strategy Roadmap (Operation)

There is no single full roadmap for the implementation of the Digital Strategy that sets out all the projects into a prioritised programme that identifies resource requirements, overlaps and synergies between projects.

In addition, there is no consideration of using external providers to deliver the strategy in terms of partnerships with suppliers.

Recommendation

The Health Board should develop a single roadmap to help deliver the Digital Strategy.

Management Response, Responsible Officer and Deadline

The UHB will be refreshing its digital strategy and as identified above will set out our approach to its delivery. As part of this each technical domain will further refine and formalise a programme register of their projects approved or at the advance stage of being planned. Oversight of these is provided by the various sub groups, such as the architectural group and the project portfolio board where each major project is discussed and any interdependencies discussed and addressed.

Responsible Officer

Chief Information Officer

Deadline

End of March 2021

Observation 10 – Strategy Leads (Operation)

The mechanisms for driving forward the Digital Strategy are undeveloped. The current position is that the strategy is pushed by ICT, however there is no network of champions within the organisation that can act as a pull and take a lead within their area. In addition, the organisation is not linking business change managers into ICT projects.

These issues mean that departments are not fully realising the benefits of technology and this acts as a drag on implementation.

Recommendation

A network of champions across the organisation should be developed alongside the use of change managers for projects.

Management Response, Responsible Officer and Deadline

The gap with digital champions has been fully recognised. The O365 project emphasised this issue and we are working to rectify with now 150+ digital champions engaging with ICT around O365 and the Digitisation Patients Notes also building a clinical team. Champions can only delivery so much and wider more formal Digital roles are also required. The HB now has a CCIO, CNIO and CIO in post and there are plans to ensure that digital roles are embedded within each ILG.

Responsible Officer

Chief Information Officer, Chief Nursing Information Officer and Chief Clinical Information Officer

Deadline

O365 champions currently being recruited, with ILG roles aiming to be in place by end March 2021

Observation 11 – Strategy Communication (Operation)

There has been no recent communication of the Digital Strategy and its aims and there is no link or page on the intranet to include it.

Recommendation

The Digital Strategy should be re-issued alongside the roadmap. This should form the basis for engaging the network of champions to drive the Strategy forward.

Management Response, Responsible Officer and Deadline

The Health Board is presently refreshing its digital strategy. In doing so, there will be engagement across the organisation and with partners as to the direction of travel and priorities and a key output will actions that set out how the organisation will continue to become an increasingly digital organisation, achievement of which is hugely dependent on achieving a digital culture and supporting staff to be effective and efficient users of an increasingly effective digital offer.

Responsible Officer

Director of Planning and Performance

Deadline

March 2021

Observation 12 – ICT Budget (Operation)

The ICT budget is based on the previous year's, with inflationary uplift i.e. incrementally produced. It does not appear to be closely linked to the strategy or work plan. As an example, the funding in the budget for refresh of kit is less than the actual need.

This means that the Health Board is unable to fully track and may not be aware of the financial resource needed to achieve the Digital Strategy meaning that overspending may happen against budgets.

Recommendation

Consideration should be given to aligning the ICT budget to the needs of the organisation and the digital strategy.

Management Response, Responsible Officer and Deadline

Capital funding and decisions relating to digital technologies are increasingly subject to national decision making, with discretionary capital to HBs failing to keep up with inflation. As such the UHB has taken a tactical approach to maximise its digital capabilities by seeking to maximise the national offerings, be they resource allocations or digital tools and applications. This preference of WG to ring fence funding for national initiatives, will be a key factor in the UHB's thinking on how it can achieve its objectives.

It is worth noting that where discretionary capital has been made available the UHB has supported the delivery of digital priorities, as evidenced by the recent financial uplift in both capital and revenue budgets. As part of this uplift it was accepted by the organisation that there will be an increase in the funding requirements of the rolling replacement programmes and licensing fees.

Responsible Officer Director of Planning and Performance **Deadline** End March 2021

Observation 13 – ICT Resource Demand (Operation)

There has been no full assessment of what skills are held within ICT and the skills and resource needed to support organisational IM&T and implement the Digital Strategy. Consequently, there has been no identification of the skills gap and no development of a structured staff development plan in order to close the gap. Without this development plan in place ICT may struggle to implement the strategy.

Recommendation

A full assessment of the current skills within ICT, alongside the required resource and skills for the Digital Strategy should be undertaken. Once the gaps in skills have been identified a formal plan to upskill staff should be developed.

Management Response, Responsible Officer and Deadline

The ICT structure has been under review by the ICT senior management to ensure it has the correct teams and skill set in place to deliver a service. This is nearly complete and will identify gaps in positions that require JD and then funding to be agreed to support ICT in both business as usual and delivery of the HB strategy.

Responsible Officer

Assistant Director of ICT

Deadline

The review will be completed by end January 2021 but any identified gaps will need funding which will require papers and IMTP planning.

Observation 14 – Network Security (Operation)

The network is not fully secured. At present there is no device level authentication to the network and the network is not fully segmented or split up to increase security.

However, although some work is in progress for these items, the vulnerability identification and management and intrusion detection functionality are not fully operational.

Recommendation

Work should continue to improve network security.

Management Response, Responsible Officer and Deadline

The device level authentication is all managed at the Active Directory level where a PC/Laptop/ Server needs to be added to the CYMRU domain before being able to communicate with any other devices on the network/domain. When a device is added to the domain it also needs to be moved from a centralised/shared OU within the Active Directory tree into the relevant Health boards OU container where it will then receive relevant group policies and configuration etc.

At present the network isn't fully segmented, however different departments within the health board sit within their own VLAN/DHCP Scope but there are no specific rules around communication between the VLAN's inside of our Firewalls in terms of "sandboxing" or ACL's at the network level however ICT are looking to implement measures for Servers and End user devices using Windows Firewall for an added layer of protection.

ICT are now fully operational in terms of Vulnerability management, we've implemented and on-boarded with the national Nessus programme and have three of our own scanner servers setup which gives us the ability to scan for vulnerabilities across our end user devices, servers and network equipment within all sites. Although this project is in its infancy, it is now fully operational, utilising the toolsets to identify and rectify any vulnerabilities.

With regards to configuring the Cisco Firepower it is in the early stages of implementing but this is a priority as the importance of getting this fully functional in line with the sanitation of the current firewall rulesets.

Responsible Officer

Chief Information Officer

Deadline

Actions have been operationalised and are now being monitored, Identification and mitigation of new threats and requirements are part of the departments normal working activities.

Observation 15 – Business Critical Assets (Operation)

Although IT assets are recorded and tracked, there is no identification of those assets that are critical to the provision of ICT services for the organisation. Accordingly, there is no formal, regular assessment of the risk of failure of these or the need for replacement.

Recommendation

Critical assets should be identified and be subject to enhanced monitoring an assessment for risk / replacement.

Management Response, Responsible Officer and Deadline

We do have a formal rolling replacement programme for pc, igels and servers. e.g. windows 7 to 10. Funding is requested from ECMG and is acknowledge that ICT manage the funds ECMG do not require a detailed list of items replaced under the rolling replacement programme.

The IT assets application is an in house development and modification to include the recommendation can be reviewed and discussed internally

Responsible Officer

Assistant Director Of ICT

Deadline

To review the option of modification of the in house application end January 2021

Observation 16 – Patching SOP (Operation)

There is a patch / firmware update process in place, but this is not formalised within a document. This means that the organisation is reliant on staff knowledge.

Recommendation

An SOP / guide to the process should be developed to ensure the knowledge is retained within the organisation.

Management Response, Responsible Officer and Deadline

As part of the roles of Comms, voice and server managers there is an expectation that the knowledge and experience to identify, plan and install these type of updates is within the skillsets.
ICT has support arrangements with the majority of our main suppliers to ensure that the team are notified and have access to the latest updates. Procedures to install will be provided by vendor and also plans will be taken to the ICT Change Advisory Board.
For the server estate, applying updates is a function of the daily rota. SAN, Network and telephony is managed on a less frequent schedule.
The use of the NESSUS vulnerability assessment tool will also give a view on this and will flag any anomalies.

Responsible Officer

Assistant Director of ICT

Deadline

End February 2021

Observation 17 – Continuity (Design)

Although there are individual system disaster recovery plans, there is no overall BCP/DR plan for ICT as a whole that considers all the systems supported, the controls in place to provide resilience, and recovery mechanisms. As a result, there has not been a full business impact analysis. ICT are focussing on their perception of the higher risk systems without any feed in from the system users / business.

In addition, there is no consideration of Recovery Time Objective / Recovery Point Objective (RTO / RPO) within the plans with ICT taking a 'do the best' approach. Without consultation with the business there is a risk that the plans in place do not fully meet the business needs.

Recommendation

The organisation should develop an overarching BCP / DR process. This should:

- consider all the systems and use a business impact analysis to prioritise the systems for recovery;
- the business (Directorates / Departments) should be involved in the process; and
- should be consulted in order to define appropriate RTO / RPOs.

Management Response, Responsible Officer and Deadline

Accepted, the UHB will seek to have an outline overall BC/DR plan by the end of April 2021

Responsible Officer: Assistant Director of ICT

Deadline : End April 2021