Internal Audit Baseline Review – IT Assessment – Updated Management Response (Original Report to March 2021 Digital & Data Committee)

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

Update June 2021 - In setting-out the strategic risk register we have sought to incorporate the register of controls to mitigate non-compliance with legislation and the gaps in those controls. The risk register will be presented as a working draft for consideration by the Digital and Data Committee in July and is subject to ongoing efforts to improve its value.

The risk approach is then underpinned by operational risk and assurance groups and procedures. These include the Information Governance Group, which seeks to mitigate non-compliance with data protection, freedom of information and medical records legislation, the Risk Assurance Group for cyber security (NIS-D, GDPR), and the Architecture Review Board– which advises on standards and the DPIA procedure, which operationalises the key areas of risk management.

There remains outstanding a list of technical standards which CTMUHB and NHS Wales need to agree upon and intend to do so through the national architectural work and the new office of the Chief Digital Officer. The timescales for the delivery of these will be set by the CDO.

Update February 2021 - There has been ongoing consideration as to how compliance could and should be monitored across the UHB and beyond as we look to share data and have increasingly integrated clinical and digital services and networks.

Digital is increasingly an enabler too, and element of all services, and many of these services have their own standards, of which some are digitally related. In addition to these there are a number of legislative requirements covering IM&T ranging from Common Law Duty of Confidentiality, NIS-D and the Medical Records Act to Medical Devices Legislation and layered on top of these will increasingly be added Welsh Technical and Information Standards as we move to adopt a standards based open architecture.

We remain committed to individual services and corporate departments assuring compliance and using the risk management framework to ensure that level 15+ risks associated with non-compliance are escalated through the UHB's governance processes regardless as their nature.

Of the specific digital compliance issues, RAGCSB now monitors and manages NIS-D including cyber essential risks on behalf of the organisation, with the Information Governance Management group managing Data protection and the Medical Records Group, compliance with the Medical Health Records Act.

All level 15+ risks are discussed in the regular corporate risk review meetings. Digital related risks are now notified to the Data and Digital Committee.

Responsible Officer - Senior ICT management team and DHSSG

Deadline - Completed except for standards aspect, which is to national timelines tbd.

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
Completed - All ICT risks are posted on to the Datix system. In acknowledging the intent of the recommendation is to ensure that risks of significant consequence but lower likelihood of occurrence need to be known about at board level we have attempted to consider risks at a system wide as well as an individual operational risk level through the strategic risk register. **Update February 2021 -** The Digital Risk register is now a standard agenda item for the Digital Delivery Board to consider. There is still work to do to improve the maturity of the risks identified particularly in respect to how we use governance to enable delivery of the UHB's wider strategic objectives. **Responsible Officer -** Senior ICT management team and DHSSG **Deadline -** Completed

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
Update May 2021 Completed - Digital Operational issues are now either logged on the Servicepoint site or the Datix system and jointly analysed as part of ICT service management arrangements. These are now being put into themes and discussed at the relevant SMBs and where necessary the digital risk management group (RAGCSB) and fortnightly at the Digital Senior Management Team. Operational risks are then recorded on Datix & the strategic impact of the risk is considered against the digital programme's strategic risk register. **Update February 2021 -** 50% of projects have boards established. Risks associated with these projects are systematically fed into the overall ICT risk register. Other projects which are at the BUA stage, such as the WCP programme, do not yet have a formal mechanism for recording risk. The first meeting of reconstituted programme delivery board is scheduled to meet in March, with a standard agenda item to consider all risks established. **Responsible Officer -** Senior ICT management team **Deadline -** End April 2021

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
Update February 2021 - This has been completed, with terms of reference defined **Responsible Officer -** Senior ICT management team to ensure all individual groups comply **Deadline -** End February 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
Update May 2021 - There remains outstanding policies and procedures in need of review. These are being managed based on their relative priority determined via a subjective but informed approach by the digital SMT and the Information Governance Group. **Update February 2021 -** The ICT Web site is currently being reviewed and first iteration is live. We will work to ensure that the gaps identified in the Audit are addressed **Responsible Officer -** Service manager and Server team **Deadline -** No deadline has been set as these are subject to prioritisation of resource decisions

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

Update June 2021 - The review of the strategic capabilities assessment, the infrastructure review and user feedback, including that contained within the Internal Audit report for the digital response to covid-19, indicates that whilst the potential benefits arising from the adoption of digital tools and ways of working are known, they are not being fully realised, due to a combination of cultural behaviours, variable system reliability and performance, lack of training, lack of infrastructure (both within the population and of staff) and connectivity.

Strategically the organisation is reviewing its ways of working and its estates and digital plans as it is anticipated that we will need to structurally change our resource allocation from bricks and mortar to digital if we are to be able to balance the requirement to transform our approach to health and care whilst remaining financially solvent.

Update February 2021 - The strategy approaches this issue by identifying the benefits gained by the UHB in developing the strategic capabilities our users identified are required to enable the organisation's overarching strategic objectives to be delivered.

To inform the operational plan for 2021/22 the maturity assessment has been updated both in respect of the capabilities we wish to mature and realise benefit from and for the underlying infrastructure required to enable them to be delivered. This analysis has been shared with digital delivery board and the UHB's management board and has been used to inform some of the priorities for 2021/22. A more comprehensive assessment will be made as we refresh the strategic plan for digital as one enabling component of the organisations new strategy.

We are currently out to procurement for consultancy to review initially our infrastructure as the first part in the ICT review. 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 Health Board. This item of work will need to be delivered as part of the response to observation 7.

Responsible Officer - Senior ICT management team and DHSSG

Deadline- The strategic element is complete, the operational planning and business case developments are part of the wider IMTP programme.

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
Update June 2021 - We are continuing to assess our digital maturity as demonstrated by the 4Cs infrastructure review and the IMTP strategic capabilities assessment. These do not identify whether solutions are internally or externally supplied and nor does it identify whether we would hope that in the future these solutions will be. We have however agreed that at the present time, in the present political environment, that we would wish to proceed collaboratively with other NHS Wales organisations and as a Trusted Partner of DHCW. In respect of digital skills and ways of working, the June 2021 meeting of DDB, with 2 of the 3 Executive directors for the clinical professions present, agreed that at this time we would proceed with the all-Wales approach being led by HEIW. This is currently at the skills assessment stage with a multi-disciplinary workshop planned for the 27th July. **Update February 2021 -** The February 2021 Management Board agreed that the requirement to train and skill the workforce in the use of digital was a critical requirement to delivering our strategic mission and will supported within the IMTP planning and prioritisation process. HEIW have incorporated many of the basic requirements into their plan for 2021/22 and we are committed to aligning and taking further steps to develop the strategic plan for workforce aligned and to enable the UHB's new strategy. At the operational level there are numerous initiatives underway to support the technical knowledge and capabilities of staff, ranging from the champions network for O365 and the digital

patient notes programme, to the availability of video training for digital packages. We have bought training credits amounting to £40k with QA and Cisco (through their platinum training library) to support all ICT staff with training and professional development.

Responsible Officer - Senior ICT management team and DHSSG

Deadline - Skills work has commenced.

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
Update June 2021 - The Improvement and Innovation Board has been established to consider and horizon scope emerging technologies. The Architectural Review Board has been established to develop and publish the requisite standards. In terms of operational requirements, the new Data Privacy Impact Assessment and the Digital Portfolio Board act as enabling governance tools to support early decision making and compliance with standards and legislation. Being a 3 year programme we would anticipate that the IMTP to set out the detail, whilst the strategy provides the 10 year vision. **Update February 2021 -** Since the audit was undertaken there has been a greater emphasis on collaborating in practice across NHS Wales and acceptance of the move to the open architecture, based on standards. We would anticipate that with the changes arising from the establishment of Digital Health and Care Wales, opportunities for the UHB to mutually benefit from collaboration with other NHS organisations in undertaking these important functions should increase and we will certainly be seeking to realise these. **Responsible Officer -** Senior ICT management team **Deadline- Completed.**

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 IMTP for 2021/22 is intended to provide a high level road map for the next 12 months, considering inter-dependencies, costs, benefits and sequencing and how these will be managed. In a dynamic, agile and uncertain environment, having definitive plans for much further into the future could be considered to carry more opportunity cost than benefit. The detailed programme catalogue that provides the granularity is presently under construction, and will piece together all the various initiatives underway – ranging from systems implementation and management, to infrastructure and workforce and skills development. Capacity however remains a constraint A component of the national and UHB programme for next year incorporates the provision of third party support, as per the agreed outcomes of the national architecture review. Interestingly, a number of the digital professions across NHS Wales are identifying the increasing use of external providers as a risk to sustainability and incompatible with the Wellbeing of Future Generations Act, so there is a fine balancing act to manage in this area. **Responsible Officer -** Senior ICT management team, CNIO, CCIO and CIO **Deadline -** Work has commenced and it is intended to have a reasonable first cut by August 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. Due to financial constraints we are seeking to build networks through the establishment of 4 strategic capability groups, a proposal for which is to be considered by the Digital Delivery Board in July **Responsible Officer -** Senior ICT management team for digital champions, CNIO and CCIO for the ILG clinical leads **Deadline:** July 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
Update June 2021 – CTMUHB's corporate and clinical strategies are presently being developed by the Board, our staff, population and wider stakeholders. Until this has been completed we have remained focussed on delivering the 2017 CT digital strategy and continued to build our services and assets around this programme. Options for Strengthening of our governance and operating models to improve delivery and communications of both the strategy and the benefits of digital are being discussed by DDB in July 2021 – with the recommendation being that we remain with the existent strategy until the new corporate strategy requires. **Update February 2021 -** DHSSG has asked that the Strategy is reviewed with the help of external consultancy before communicating out to the HB that the Strategy is available on the intranet. When the strategy was originally developed it was actively pushed out to HB for review and discussion. From formal exec sign off and departmental comments. The strategy was recently covered in a presentation to management board, many of whom are new to the senior leadership team of CTM UHB. The intention is for the strategy to be refreshed in order that it supports and enables delivery of the overarching corporate strategy of the uHB. **Responsible Officer** Senior ICT management team and DHSSG **Deadline -** July 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
Update June 2021 - The financial requirements of the all Wales digital strategy have never been met by WG despite the strategy and the UHB's strategic plans being in line with their guidance. As a result the UHB has made a tactical approach to seek to support and maximise the benefits of national developments whilst investing at a steady pace that balanced the mitigation of all risks, with the requirement to meet clinical and delivery standards and the benefits realisation of digital and other innovative programmes. **February 2021 update -** The financial requirements for the 2021/22 digital programme will be set out as part of the IMTP programme. Where the organisation faces financial constraints and prioritisation decisions, the impact of these decisions to the delivery of the organisation's objectives will be articulated to the Board to ensure that options may be objectively appraised. **Responsible Officer -** Senior ICT management team **Deadline -** Resource dependent

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
Update June 2021 - This is a recognised weakness in some but not all digital professions both locally within CTM and nationally and is despite numerous initiatives. A training budget is available, however the challenge being faced is one of both resource availabilities and capabilities. This is rightly identified as a risk and constraint to delivery, and we will look to put in place a skills and resource plan once the changes to the target operating model are agreed **Responsible Officer -** Senior ICT management team **Deadline -** August 2021

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

Device level authentication is 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 Organisational Unit 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's fully operational and utilising the toolsets to identify and rectify any vulnerabilities.

Update February 2021: The project to install Cisco Firepower is being reviewed, as the switch to active monitoring 12 months ago resulted in unexpected effects and detriment to the normal operational of the network. It is presently in monitoring mode, to inform the controls necessary to mitigate risk whilst avoiding disruption to our users.

Responsible Officer - Senior ICT management team and server team

Deadline - This needs to revisited following the infrastructure review to ensure there is a validated plan including costing going forward

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
The UHB has a formal rolling replacement programme for PC, Igels and servers. eg windows 7 to 10 in place. Funding has been requested from the Executive Capital Management Group with greater detail of the assets being replaced being provided. **Responsible Officer -** Senior ICT management team **Deadline -** Completed

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 in place 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. A patch management policy is in the process of being developed which will document approaches to patch management. This should be completed as capacity enables. **Responsible Officer:** Senior ICT management team **Deadline** August 2021 – in line with patching policy

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

Business continuity documents have and continue to be developed in line with the requirements of NIS-D. Progress is being managed by RAGCSB on a risk basis

Responsible Officer: Senior ICT management team

Deadline: Process is defined and now being implemented