Hywel Dda University Health Board

IM&T Control and Risk Assessment

Final Internal Audit Report

2020/21

Private and Confidential

NHS Wales Shared Services Partnership

Audit and Assurance Services

Contents **Page**

Review reference:	HDUHB-2021-20
Report status:	Final Internal Audit Report
Fieldwork commencement:	01/07/2020
Fieldwork completion:	01/10/2020
Draft report issued:	06/10/2020
Management response received:	23/11/2020
Final report issued:	27/11/2020
Auditor/s:	Kevin Seward (Senior IM&T Auditor) Martyn Lewis (IM&T Audit Manager)
Executive sign off:	Huw Thomas (Executive Director of Finance)
Distribution:	Anthony Tracey (Assistant Director of Informatics) Paul Solloway (Head of IT) Patrycja Duszynska (Head of Information Governance) Rob Elliott (Director of Estates, Facilities and Capital Management) Sarah Brain (Informatics Business Manager)
Committee:	Audit & Risk Committee

Audit and Assurance Services conform to 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.

Disclaimer notice - 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 & Risk Committee.

Audit reports are prepared by the staff of the NHS Wales Shared Services Partnership – Audit & Risk Assurance Services, and addressed to Independent Members or officers including those designated as Accountable Officer. They are prepared for the sole use of the Hywel Dda 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

In line with the 2020/21 Internal Audit Plan for Hywel Dda University Health Board (the Health Board) a baseline review of the arrangements in place for the management and control of Information Governance (IG) and Information Communications Technology (ICT) was undertaken. The review sought to provide a baseline picture to the Audit & Risk Assurance Committee of the processes in place to manage the risks associated with IG / ICT.

The move to a digitally enabled organisation should be part of an IM&T Strategy which should support the organisational strategy and provide a holistic view of the current business and Information Technology (IT) environment, the future direction, and the initiatives required to migrate to the desired future

The relevant lead Executive for the assignment was the Director of Finance.

2. Scope and Objectives

The overall objective of the audit is 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 provide suggestions for areas of improvement or future development.

The areas considered in the review were:

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. GDPR, NIST, 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 were as follows:

- The 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.

FINDINGS

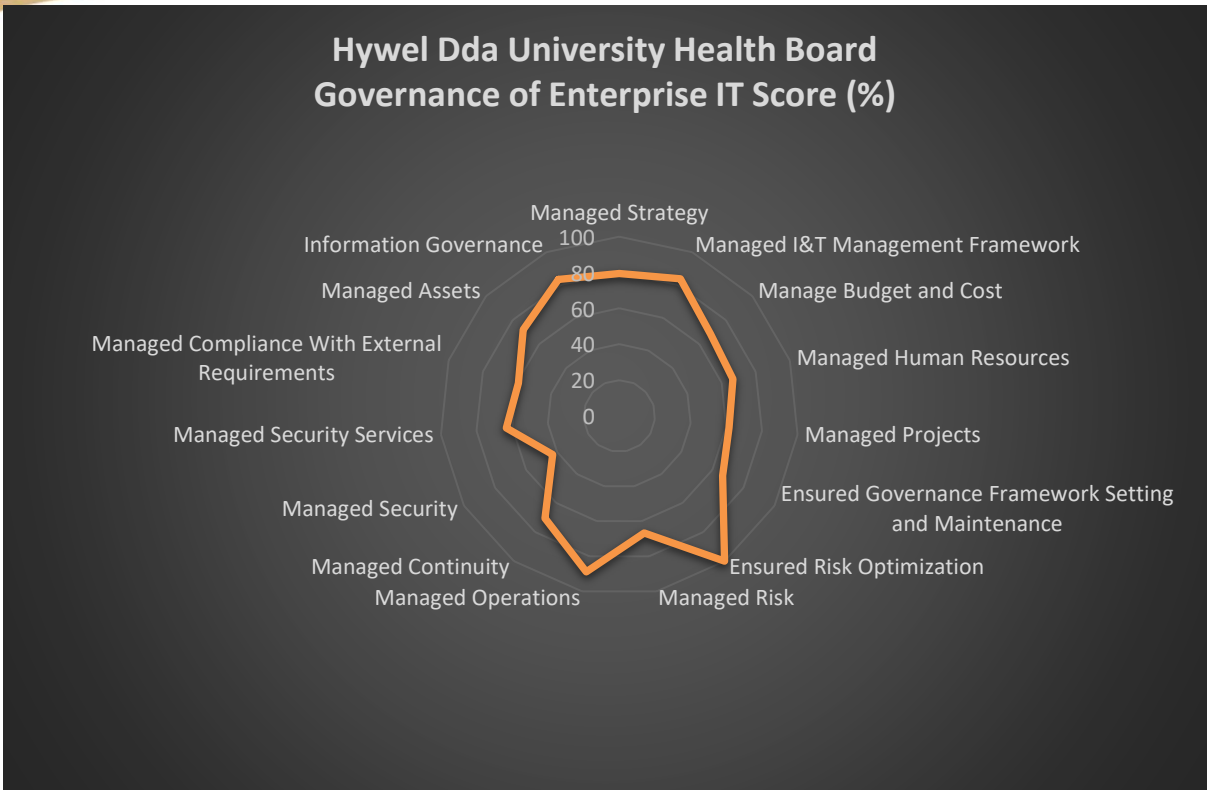
4. Key Findings

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

This baseline assessment utilised the expected controls derived from the COBIT 2019 framework and is reported using the subheadings of these processes for governing enterprise IT.

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

As part of our assessment we scored the individual controls expected 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 organisations enterprise IT arrangements.



We note that the Health Board scored well under many of the headings in particular: Managed Strategy; Information Governance; IM&T Management Framework; Managed Operations; and Ensured Risk Optimization.

Objective	Percent
Managed Strategy	79.5
Managed I&T Management Framework	83.7
Manage Budget and Cost	73.7
Managed Human Resources	66.7
Managed Projects	61.5
Ensured Governance Framework Setting and Maintenance	66.7
Ensured Risk Optimization	100.0
Managed Risk	66.7
Managed Operations	88.9
Managed Continuity	70.5
Managed Security	42.9
Managed Security Services	63.3
Managed Compliance With External Requirements	59.1
Managed Assets	72.0
Information Governance	83.3

Opportunities for improvement were noted across a number of headings, more detail on these can be found in the sections below. Two areas requiring management attention were identified from the scoring, these

were the management of compliance with external requirements and management of cyber security services.

There isn't a complete register of compliance requirements for IM&T and there is no structured process to identify IM&T compliance requirements, assess the compliance status and feed the status and consequences upwards to committee.

While the Head of ICT has oversight for cyber security as the strategic lead, there is no dedicated technical operational lead for cyber security instead these duties are currently shared throughout the department.

While this post has gone out for advert it remains vacant because of the lack of suitable candidates.

Without a dedicated cyber security role being extant and operational, the Health Board will be unable to fully reduce its cyber security risks, it cannot fully undertake all the actions needed to ensure a robust cyber security programme is maintained and will not be able to maximise the use of the security tools that have been procured nationally.

This assessment was against a wide ranging set of expected controls, although there is room for improvement, and with the exception of the weaknesses noted under security and compliance, the expected risk and control framework for the management of IM&T was found to be in place.

5. Summary of Audit Findings

The key findings are reported in the Management Action Plan at Appendix A.

OBJECTIVE 1: Information Governance

Information Governance
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.

There is an IG team to support the organisation, and a suite of IG control documentation 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 Information Governance Sub-Committee (IGSC) a Sub-Committee of the People, Planning & Performance Assurance Committee (PPPAC).

There were no findings under this objective.

OBJECTIVE 2: ICT and Security

Managed Strategy

There is a strategic plan in place for Digital, the plan's strategic direction is aligned to the Health Boards annual plan. The plan is explicitly linked to the organisational strategy and sets out the high level objectives for delivery.

There is an assessment of the underpinning requirements within the Digital plan, it is noted that the full implementation of the plan would require additional resources within the department. These additional resources have been approved in order to deliver the strategic opportunities set out in the plan.

The Digital plan sets out the current situation and the desired position around five key strategic enablers, it shows what programmes and initiatives that are required to close this gap, it references a digital baseline which was a standalone piece of work highlighting current situation and future change requirements in more detail.

The Digital plan identifies the projects needed to deliver its ambition, as well as the infrastructure items. As the organisation moves from a strategy into delivery, they have revised governance arrangements with the establishment of additional groups which feed into PPPAC. Also, given that there is a need for increasing level of engagement across the Health Board with regards to the digital agenda, it has been agreed that a specific Digital Delivery Group be established to ensure that the Digital plan is being delivered to time, and within the resource envelope.

A roadmap is identified to support the strategy, this shows systems, cloud and infrastructure, revised information governance, Digital Governance and High level costings and resource required for delivery.

The Digital plan shows consideration how the external ecosystem can be used to support delivery. The strategy notes NWIS, but also notes wider digital opportunities such as:

- A regional Collaboration for Health (ARCH)
- City Deal
- Regional Digitisation Plan
- Transformation Fund Ambitions

There is an assessment of digital maturity contained in Digital Plan, but this is only relative to Electronic Medical Records. It doesn't cover all areas such as ability of leadership to leverage technology, level of accepted technology risk, approach to innovation, culture and knowledge level of users.

See Finding 1 at Appendix A.

The Digital Plan is well structured in terms of what it means for each stakeholder group, patient, clinician and health board Informatics staff but there is no communications plan in place to ensure the Digital Plan is formally communicated to these groups.

See Finding 2 at Appendix A.

IM&T Management Framework
The organisation has an appropriate steering structure for Digital and Information Governance.

There are defined IM&T related roles and responsibilities for the organisation which delineate responsibilities and accountabilities, with appropriate stakeholders included on the PPPAC and the steering groups.

The organisation has created and communicated suite of national and local policies to drive IT and IG control expectations on relevant key topics such as security, privacy, confidentiality, internal and usage of IM&T assets.

There were no findings under this process subheading.

Manage Budget and Cost
Standard NHS finance practice ensure all items of IM&T spend are identifiable. Funding for it is available and reported under a defined cost centre and identification of spend level for the whole organisation is achievable by the finance department upon request.

There is a standard budget monitoring process which provides the department with a monthly breakdown and includes analysis of any variances. Prioritisation of IM&T budget spend is done with a decision matrix to rank IM&T initiatives and requests for development, new build, information, IG and programmes.

While Informatics has been allocated additional resources to deliver the Digital plan, the department budget was not based on actual need. Instead it was based previous years with some changes factored in. This means it does not fully cover the financial resource needed to achieve the organisations digital ambitions and without future investment overspending may occur against budgets.

See Finding 12 at Appendix A.

Managed Human Resources
There has been a recent assessment of the skills / resource needed to support the organisation and deliver the Digital plan and funding has been secured to address the identified gaps.

Staff training for the informatics department is recorded via the NHS Electronic Staff Record (ESR) system and proposed training is identified via the Performance Appraisal and Development Review (PADR) process. This feeds into a single record of training requirements that is prioritised and provided within funding limits.

There have been exercises to determine knowledge silos within the department and measures have been taken to address this where possible, however the processes is event driven i.e. reactive not proactive.

See Finding 13 at Appendix A.

Managed Risk
There is a process for identification and collation of ICT related risks within a consistent risk register. There is a link from incident / event reporting whereby information from operational staff is communicated to senior management within the department to feed the process.

The impacts of risks are assessed and actions are defined to manage the risk within accepted tolerance levels with the risk register monitored and reported via Committee and Board.

While the department risk register is monitored via the standard health board process and reported via Committee and Board, the process could be improved with monitoring of the risks being managed at a lower level which contain a sever worst case scenario via the Digital subcommittee.

See Finding 5 at Appendix A.

Managed Security
There is a group within the Health Board who monitor the cyber security action plan with a formal Committee in place receiving cyber security KPI's and cyber security related risks being included on the organisations risk register.

Previous internal and external audit work identified two key findings related to the resources available to the informatics department to progress some actions contained in the cyber improvement plan and not having a dedicated technical operational lead for cyber security within the Health

Board. While this post has gone out for advert it remains vacant because of the lack of suitable candidates.

The lack of defined cyber security resource has meant that although the Health Board has maintained key cyber security requirements such as patching and monitoring, it hasn't been able move the cyber security agenda forward or maximise the use of the nationally procured tools such as the logarithm Security Incident and Event Management (SIEM).

The informatics department KPI's include 3 cyber related measures, it is expected that the list will be expanded once dedicated resource is in place.

During the Covid situation some Cyber awareness information was issued by the Health Board but apart from this and the section on the mandatory Information Governance module there is very little additional Cyber awareness training for staff.

See Finding 8 at Appendix A.

Managed Assets

Asset registers are in place for the health boards IT equipment. There has been an assessment critical assets within the Health Board infrastructure which has in turn been recorded as a departmental risk and escalated via the corporate risk register.

Reports are run from the KACE system and senior IT staff monitor the age and criticality of components and prioritise replacements etc. with a process in place for secure decommissioning of IT equipment which allows assets to be tracked through to disposal.

We did note some weakness around documented processes for applying regular preventive maintenance to critical assets, again this is a result of the health board not having a dedicated cyber security resource in post. This has been **recorded** as a finding under the Security subheading.

There were no findings under this process subheading.

Managed Projects

Hywel Dda has recently setup the new Digital Delivery Group, which will set direction for the department, taking into account information requirements, IT requirements, projects, clinical requirements and the 5 year strategy recently adopted by the Health Board.

There is a Programme Assurance Group which provides assurance to the Digital Delivery Group on the delivery of the Health Boards programmes and projects.

The Health Board has developed in conjunction with NWIS an agreed blueprint for the Implementation of the National Informatics Projects. This route map identifies the timescales that Hywel Dda and NWIS are working towards implementation subject to multiple dependencies both locally and nationally. The route map has been signed off and changes to it are subject to change control, either from the Health Board side or from NWIS themselves.

Members of staff within the department hold formal project management qualifications, they use a decision matrix to record and prioritise work with existing staffing limitations and funding has been secured to recruit additional support for IT project management at the Health Board.

Historically the Health Board have experienced difficulties in delivering its project work on schedule with the resources available to them. With recruitment of the additional support and the establishment of the programme delivery group in the revised governance structure a level of governance and control over the implementation of local and national projects will be achieved, allowing the Health Board to deliver at a pace it was able to demonstrate during the Covid situation.

There were no findings under this process subheading.

Managed Operations

The Health Board operate two main data centres in order to support the operation of its ICT services, in addition it has a number of smaller server rooms at various sites but key systems have been migrated from these where possible.

The data centres are propose built units situated at opposite end of the UHB in separate counties with more than one source for dependent utilities. The data centres are monitored for environmental hazards such as fire, smoke, humidity and temperature. Consideration was given to physical and environmental security and resilience as part of the procurement and implementation projects. There is also an inspection process to ensure smaller server rooms are kept tidy and physically protected.

The Digital Plan references the need to regularly test the uninterruptible power supply's mechanisms so as to ensure that power can be switched to the supply without any significant effect on business operations. We requested evidence to show that the testing of the UPS mechanisms were

taking place and being monitored by the department. We were informed that this is the responsibility of the estates department and informatics do not hold records of tests.

See Finding 6 at Appendix A.

Managed Continuity

There is a backup strategy underpinned by standard operating procedures (SOP's). Hywel Dda utilises a backup solution to protect its data both on and offsite. The private cloud backup solution, consists of a primary and a secondary vault within the Hywel Dda network. All data is backed up locally to the primary vault which resides in the Hywel Dda data centre, this data is then replicated offsite to a secondary data centre. Backups are spread between 3 windows and 3 Linux clients.

The Health Board has documented processes for ICT Major Incidents, Disaster Recovery and Backup. These are underpinned by several continuity SOPs which are used to support the recovery of key systems in the event of an incident.

The Organisation also have service management schedules for the systems they support which set out business continuity (BC), disaster recovery (DR) and backup arrangements. These individual plans identify stakeholders and are agreed with the head of IT.

The documentation sets out the severity categories and gives examples of critical problems and sets out the recovery time objectives.

Testing of IT disaster recovery has been a longstanding issue from both internal and external audit recommendations. However, the organisation has agreed that until a full test is possible, a group of systems will be selected periodically so as to minimise disruption and risk to the organisation. IT staff are aware of BC plans and have used internal SOPs to backup and recover systems as part of the process.

The BC process is set out in the Business Continuity Planning (BCP) Policy, along with a rout for monitoring at an organisational level.

There were no findings under this process subheading.

Managed Security Services

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 NHS Wales Operational Security Service

Management Board (OSSMB), the Head of IT gets regular alerts as part of this group which are then assessed and acted upon locally.

The organisation uses a process of device level authentication for the network so that only authorised devices have access to corporate information and the enterprise network. This is accompanied by the standard NHS Wales password management practices.

There are firewalls in place, the Health Board are currently undertaking a firewall replacement programme and key documentation is being created as part of this.

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

The organisation will develop and leverage a portfolio of supported technologies, services and assets once there are dedicated cyber security resources in post. Many of these have already been procured nationally and funding for the posts is in place.

Security-related event records are kept in service point and are subject to the Health Board retention periods. While event and security logs would be reviewed following an incident, this is not a standard process, again due to the absence of a cyber-security post.

The Head of ICT has oversight for cyber security as the strategic lead however, there is no dedicated technical operational lead for cyber security, instead these duties are currently shared throughout the department.

Working in this way means that the organisation cannot fully undertake all the actions needed to ensure a robust cyber security programme is maintained. Without a dedicated cyber security role being extant and operational, the Health Board will be unable to fully reduce its cyber security risks and the organisation will not be able to maximise the use of the security tools that have been procured nationally.

See Finding 7 at Appendix A.

With no dedicated resource for cyber related work the health board informatics team work very hard to distribute all protection software centrally (version and patch-level) using centralised configuration via recognised IT change management procedures. However our assessment

found some change management documentation to be significantly out of date (2010).

See Finding 9 at Appendix A.

While the Health Board have specialist tools and in the past commissioned security scans, there is no regular process of testing.

See Finding 10 at Appendix A.

The Health Board has an IT Incident Management Procedure document which was based on the Welsh Health IT Service Management Incident Management Policy and Process. However our assessment found this key document to be significantly out of date (2010).

See Finding 11 at Appendix A.

Ensured Governance Framework Setting and Maintenance
There is a formal governance structure in place for Informatics with a work plan monitored via the PPPAC Committee. There is a structure under this with operational groups feeding a steering group. The terms of reference for the committee and groups which make up the governance structure set out a frequency for review of their effectiveness.

There is an Internal Audit programme monitored by the Audit and Risk Assurance Committee (ARAC) which includes IM&T, currently IG related reports and findings are also monitored by IGSC committee as per its terms of reference. However the terms of reference for Digital group do not include monitoring internal or external audit findings.

See Finding 3 at Appendix A.

The terms of reference for the IG and Digital Sub-committees state that they are to provide assurance against regulations and standards. Reports from IGSC do specifically note the compliance position on some of these such as the GDPR and FOI, however neither committee have a full list, or is fully aware of what compliance to monitor.

See Finding 4 at Appendix A.

Ensured Risk Optimization
A risk management process is in place which is formally defined and includes a structure for escalation via committee. This is set out in the risk management policy. Risks are actively monitored by the Health Board with

clear escalation from the IT department to committee with the highest risks added to the corporate risk register

There were no findings under this process subheading.

Managed Compliance with External Requirements

Responsibility to monitor compliance is documented within the terms of reference for the Health Boards IG and Digital sub-committees. There is evidence of the identification and monitoring of some compliance requirements, in particular the IG items. Policies and maintenance contracts refer to relevant legislation and standards, and are reviewed in line with their Health Board approved review period.

The organisation performs some periodical compliance assurance work through audits for licencing, NIAS and GDPR. It also uses external audit organisations such as NWSSP Audit and Assurance Services, Audit Wales, Stratia etc. to perform assurance work prioritised by risk, this sometimes looks at compliance issues.

While there is evidence of the identification and monitoring of some compliance requirements, there isn't a complete register of compliance requirements for IM&T and there is no structured process to identify all these compliance requirements or feeding the position in relation to requirements upwards to committee.

See Finding 4 at Appendix A.

6. Summary of Recommendations

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

A summary of these recommendations is outlined below:

Priority	Total
Number of recommendations	**13**

Design of Systems/Controls

The findings from this IM&T Control & Risk baseline assessment have highlighted six issues that are classified as weakness in the system controls/design.

These are identified in the Management Action Plan as (D).

Operation of System/Controls

The findings from this IM&T Control & Risk baseline assess have highlighted seven issues that are classified as weakness in the operation of the designed system/controls.

These are identified in the Management Action Plan as (O).

Finding 1 - Assessment of digital maturity (D)
There is an assessment of digital maturity, but this is only relative to Electronic Medical Records. It doesn't cover all areas such as ability of leadership to leverage technology, level of accepted technology risk, approach to innovation, culture and knowledge level of users.
Recommendation (Medium)
The digital maturity measurement methodology should be further developed to give a more rounded view of the organisations capabilities.
Management Response, Responsible Officer and Deadline
The Health Board has committed to use the industry standard HIMSS (Healthcare Information and Management Systems Society, along with a number of other tools to assess the wider organisations digital maturity. We will commission an independent review to assess our maturity against the HIMSS standard within the next year. This is further explored in the new "Our Digital Response – 2020-2025", which outlines an ambitious path where we will choose how we navigate through these levels according to our need, priority and investment, which may mean that our progress will not be linear, however, with the right direction and strategic funding we will reach level 6 by the end of the five years. By the end of 2022, we anticipate to be at level 2, and in 2024 level 4, with Level 6 being attend the following year. **Responsible Officer** – Anthony Tracey, Assistant Director of Digital Services **Deadline(s)** – Commission independent review by December 2021

Finding 2 – Communication of Digital Plan (D)
The Digital Plan is well structured in terms of what it means for each stakeholder group, patient, clinician and Health Board Informatics staff but there is no communications plan in place to ensure the Digital Plan is formally communicated to these groups.
Recommendation (Low)
The organisation should develop a communication plan covering the required messages, target audiences, communication mechanisms/channels and schedules. Departmental leads or champions should be identified and included in the communication of the strategy, acting as a point of contact they will aid ownership of the strategy.
Management Response, Responsible Officer and Deadline
Communicating the Digital ambition will be key. The lessons learned from the Office 365 rollout, have been adopted, in that we are recruiting "Digital Champions" to assist in driving the Digital agenda forward. The recent work with the Scheduled Care Team, with the General Manager and the Assistant Director of Digital Services, being joint SROs for the adoption of digital platforms for video consultations has worked extremely well, and is a model for future projects which require service involvement. Going forward Relationship Managers will be developed who will act as a key point of contact for the sites and directorates. They will work closely with Transformation and Quality Improvement colleagues. These strategic roles will help provide guidance and technical expertise to ensure the right solutions are in place for services. **Responsible Officer** – Anthony Tracey, Assistant Director of Digital Services **Deadline(s)** – March 2021

Finding 3 - Monitoring Audit findings (D)
There is an Internal Audit programme which includes IM&T, currently Information Governance related reports and findings are monitored by the IGSC committee as per its terms of reference. However the terms of reference for Digital group do not include monitoring internal or external audit findings.
Recommendation (Medium)
Terms of reference should be updated in order to assign the responsibility of monitoring the Digital related internal and external audit reports and findings.
Management Response, Responsible Officer and Deadline
As the Information Governance Sub-Committee (IGSC) is a formal sub-committee of the Health Board, all internal and or external audit findings will be monitored through this Sub-Committee. As such the Terms of Reference for IGSC will be modified when next reviewed. Senior Members of the Digital Team also meeting corporate colleagues to discuss the audit tracker, which in turn is reported to ARAC. **Responsible Officer** – Anthony Tracey, Assistant Director of Digital Services **Deadline(s)** – May 2021. This date is reflective of the current review period. At their September 2020 meeting IGSC approved their new Terms of Reference and agreed that a further review would be undertaken in 6 months.

Finding 4 - Monitoring compliance (O)
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 e.g. for items such as PCI/DSS, NISD. The terms of reference for the IGSC and Digital Sub-committee state that they are to provide assurance against regulations and standards. Reports from IGSC do specifically note the compliance position on some of these such as the GDPR and FOI, however neither committee have a full list, or is fully aware of what compliance to monitor.
Recommendation (High)
The organisation should maintain oversight of the extent to which IM&T satisfies obligations (regulatory, legislation, common law, contractual), internal policies, standards and professional guidelines. A register of compliance requirements for all IM&T related legislation and standards should be developed along with a process for reporting status upwards via the Digital Sub-Committee and IGSC.
Management Response, Responsible Officer and Deadline
Agreed – The Digital Team acknowledges the requirement to adhere to industry standard such as COBIT (Control Objectives for Information and Related Technologies), ITIL and ISO27001. The Health Board has adopted ITIL within ICT for a number years, and we have been working towards ISO27001 for a number of years and much of the readiness work has been progressed. As this assessment was based on COBIT, the Health Board will need to fully understand the requirements, and then undertake a gap analysis. It is recognised that this is an industry standard, however, the NHS Wales approach has been progressing to the attainment of ITIL and ISO27001.

The Digital Team will therefore undertake a scoping exercise to assess and create a log of requirements, compliance which will be reported/monitored via the already established sub-committees.

Responsible Officer – Anthony Tracey, Assistant Director of Digital Services

Deadline(s) – Scoping exercise to begin March 2021, with an aim to report in June 2021

Finding 5 – Communicating managed risks (O)
While the department risk register is monitored via the standard health board process and reported via Committee and Board, the process could be improved with monitoring of the risks being managed at a lower level which contain a sever worst case scenario via the Digital sub-committee. In doing so, the Digital sub-committee shall contribute to the integration of good governance across the organisation, ensuring that all sources of assurance are incorporated into the Board's overall risk and assurance framework.
Recommendation (Low)
Consideration should be given to providing reports to the Digital sub-committee identifying risks that are not scored to escalation level due to low likelihood, however contain a severe worst case scenario. In doing so, the Digital sub-committee shall contribute to the integration of good governance across the organisation, ensuring that all sources of assurance are incorporated into the Board's overall risk and assurance framework.
Management Response, Responsible Officer and Deadline
Agreed – The combined risk register for digital will be considered at required groups, with the necessary reporting. **Responsible Officer** – Anthony Tracey, Assistant Director of Digital Services **Deadline(s)** – December 2020

Finding 6 - Testing of power supply (D)
The Digital plan references the need to regularly test the uninterruptible power supply's mechanisms so as to ensure that power can be switched to the supply without any significant effect on business operations. We requested evidence to show that the testing of the UPS mechanisms were taking place and being monitored by the department. We were informed that this is the responsibility of the estates department and informatics do not hold records of tests.
Recommendation (High)
Schedules and results of uninterruptible power supply tests should be held and monitored by Informatics, providing assurance that power can be switched to the supply without any significant effect on business operations.
Management Response, Responsible Officer and Deadline
Partially agree – The Digital Team will work with our Data Centre suppliers to explore monitoring of the uninterruptible power supply (UPS) during the generation tests. As outlined above the electrical testing is the responsibility of Estates, Digital can only monitor the health check of the UPS. The Committee should also note constant checking and switching of the UPS would greatly affect the lifespan of the batteries, which will incur additional costs. **Responsible Officer** – Anthony Tracey, Assistant Director of Digital Services / Rob Elliot, Director of Estates and Facilities **Deadline(s)** – March 2021

Finding 7 - Cyber security resource (O)
The Head of ICT has oversight for cyber security as the strategic lead however, there is no dedicated technical operational lead for cyber security instead these duties are currently shared throughout the department. Working in this way means that the organisation cannot fully undertake all the actions needed to ensure a robust cyber security programme is maintained. Without a dedicated cyber security role being extant and operational, the Health Board will be unable to fully reduce its cyber security risks and the organisation will not be able to maximise the use of the security tools that have been procured nationally.
Recommendation (High)
The Health Board should develop sufficient resources in order to implement the cyber agenda.
Management Response, Responsible Officer and Deadline
Agreed – The Committee should note that we have advertised twice for the Cyber post but have been unsuccessful in appointing. As a result we have increased the banding of the post to see whether we are able to appoint a suitable candidate. In parallel to the recruitment process we are also looking to hire agency staff to progress the work plan. The Committee should also be aware that other Health Boards / Trusts and the NHS Wales Informatics Service (NWIS) have had difficulties appointing suitable candidates. **Responsible Officer** – Anthony Tracey, Assistant Director of Digital Services **Deadline(s)** – Commencement Date - March 2021 (Dependent upon a suitable candidate being appointed) Agency Staff – December 2020 (Dependent upon a suitable candidate being identified)

Finding 8 - Cyber awareness training (D)
Apart from the section on the mandatory Information Governance training there is very little additional Cyber awareness information for staff.
Recommendation (Medium)
The Health Board should consider leveraging the national cyber security training, either for all staff or targeted groups.
Management Response, Responsible Officer and Deadline
Agreed. The national cyber security training is currently optional, and is not part of mandatory training. Hywel Dda University Health Board has requested that this be reconsidered due to the importance of cyber security training. However, as part of the Health Board response to Cyber Security, the Information Governance Sub-Committee (IGSC) will be presented with a number of options on how this will be communicated across the Health Board in order to leverage the adoption. **Responsible Officer** – Anthony Tracey, Assistant Director of Digital Services **Deadline(s)** – Communication / Implementation Options to be considered at the November 2020 IGSC Meeting with a rollout plan and phased improvement targets to be agreed.

Finding 9 - Change Management documentation (O)
With no dedicated resource for cyber related work the Health Board informatics team work very hard to distribute all protection software centrally (version and patch-level) using centralised configuration via recognised IT change management procedures. However our assessment found the Change Advisory Board (CAB) Terms of Reference to be significantly out of date (2010).
Recommendation (Medium)
The Health Board CAB Terms of Reference should be reviewed to ensure they reflect current practices.
Management Response, Responsible Officer and Deadline
Agreed – The terms of reference will be reviewed, and modified to reflect current practices. **Responsible Officer** – Anthony Tracey, Assistant Director of Digital Services **Deadline(s)** – November 2020

Finding 10 - Periodic security testing (O)
While the health board have in the past commissioned security scans, there is no regular process of testing.
Recommendation (High)
Once in post, the health board cyber security staff should carry out periodic testing of system security to determine adequacy of system protection.
Management Response, Responsible Officer and Deadline
Agreed – The completion of this recommendation is dependent on the appointment of the specific Cyber Security resource. Once appointed then they will utilise the national product (Nessus) to undertake a full vulnerability scan of the Health Board. **Responsible Officer** – Anthony Tracey, Assistant Director of Digital Services **Deadline(s)** – August 2021 (Dependent upon a suitable candidate being appointed in March 2021)

Finding 11 - IT Incident Management documentation (O)
The Health Board has an IT Incident Management Procedure document which was based on the Welsh Health IT Service Management Incident Management Policy and Process. However our assessment found this key document to be significantly out of date (2010).
Recommendation (Medium)
The incident management process should be strengthened by updating the Health Board IT Incident Management Procedure document to reflect current practices.
Management Response, Responsible Officer and Deadline
Agreed – The incident process will be reviewed, and modified to reflect current practices. **Responsible Officer** – Anthony Tracey, Assistant Director of Digital Services **Deadline(s)** – December 2020

Finding 12 - Budget creation (O)
While Informatics has been allocated additional resources to deliver the Digital plan, the department budget was not based on actual need. Instead it was based previous years with some changes factored in. This means it does not fully cover the financial resource needed to achieve the organisations digital ambitions and without future investment overspending may occur against budgets.
Recommendation (Medium)
Consideration should be given to allocating budget on need to ensure that the trajectory for strategy delivery is maintained.
Management Response, Responsible Officer and Deadline
The compliance with this recommendations is linked to the organisations prioritisation of its allocations. However, future discussions between digital and the resources team in relation to the digital budget planning will give consideration to allocating budget on need to ensure that the trajectory for strategy delivery is maintained. This will feed into the next round of budget setting for 2021/2022. **Responsible Officer** – Anthony Tracey, Assistant Director of Digital Services **Deadline** – As part of budget setting round for 2021/2022

Finding 13 – Staff resilience (O)
There have been exercises to determine knowledge silos within the department and measures have been taken to address this where possible, however the processes is event driven i.e. reactive not proactive.
Recommendation (Medium)
The department should regularly seek out opportunities for knowledge sharing, succession planning, staff backup, cross-training and job rotation initiatives to minimise reliance on individuals performing critical job functions.
Management Response, Responsible Officer and Deadline
Agree – The Digital Team will utilise the PADR process to undertake a skills review. Any opportunities identified through this process will be prioritised. The Digital Team have been developing relationships with local Colleges, Universities and third party companies in order to provide a hybrid approach to the training of digital staff. Currently we have the following staff undertaken specific qualifications, and also a significant number of technical courses undertaken during 2020: • 5 doing Digital Apprenticeship Level 4 (this includes Sarah Ashton who emailed yesterday to come off) • 3 doing Digital Degrees in Cyber Security • 2 doing digital degrees in Analytics We are also exploring, ILM and Project Management, through the HB for staff. **Responsible Officer** – Anthony Tracey, Assistant Director of Digital Services **Deadline(s)** – To be reviewed by September 2021

Appendix B - Assurance action plan risk rating

Prioritisation of Recommendations

In order to assist management in using our reports, we categorise our recommendations according to their level of priority as follows:

Priority Level	Explanation	Management action
High	Poor key control design OR widespread non-compliance with key controls. PLUS Significant risk to achievement of a system objective OR evidence present of material loss, error or misstatement.	Immediate*
Medium	Minor weakness in control design OR limited non-compliance with established controls. PLUS Some risk to achievement of a system objective.	Within One Month*
Low	Potential to enhance system design to improve efficiency or effectiveness of controls. These are generally issues of good practice for management consideration.	Within Three Months*

* Unless a more appropriate timescale is identified/agreed at the assignment.

Office details: St Brides
St David's Park
Carmarthen
Carmarthenshire
SA31 3HB

Contact details: 01267 239785 – james.johns@wales.nhs.uk