IT Service Management

Draft Internal Audit Report

2020/21

Cwm Taf Morgannwg University Health Board

November 2020

NHS Wales Shared Services Partnership

Audit and Assurance Services

Contents **Page**

Review reference:	CTM-2021-20
Report status:	Draft
Fieldwork commencement:	19 August 2020
Fieldwork completion:	5 November 2020
Draft report issued:	27 November 2020
Management response received:	2020
Final report issued:	2020
Auditor:	Martyn Lewis
Executive sign off:	Director of Planning and Performance
Distribution:	Mark Evans, Karen Winder
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.

Disclaimer notice - Please note:

This audit report has been prepared for internal use only. Audit & Assurance Services reports are prepared, in accordance with the Internal Audit Charter and the Annual Plan, 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 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

A review of the arrangements in place for IT Service Management within Cwm Taf Morgannwg University Health Board (the 'Health Board' or the 'organisation') has been completed in line with the 2020/21 Internal Audit Plan.

Best practice for IT service management is set out within ITIL, formally an acronym for Information Technology Infrastructure Library. This is a set of detailed practices for IT service management that focuses on aligning IT services with the needs of business. ITIL describes processes, procedures, and tasks which are not organisation-specific, but can be applied by an organisation for establishing integration with the organisation's strategy, delivering value, and maintaining a minimum level of competency.

The relevant lead for the assignment is the Director of Planning and Performance.

2. Scope and Objectives

The overall objective of the audit was to evaluate and determine the adequacy of the systems and controls in place for IT service management, in order to provide assurance to the Health Board's Audit and Risk Committee that risks material to the achievement of system objectives are managed appropriately.

The areas the review sought to provide assurance on were:

- IT services are appropriately designed, provided and managed with reference to an appropriate framework (ITIL);
- service desk provision is appropriate and appropriate request fulfilment management practices are followed;
- appropriate processes are in place for incident, event, and problem management in order to minimize the impact on users;
- processes are in place to gather, analyse, store and share knowledge and information within the organisation in order to improve efficiency by reducing the need to rediscover knowledge;
- an appropriate process is in place for change management; and
- processes are in place to review and evaluate business services and infrastructure services on a regular basis in order to improve service quality, and to identify more economical ways of providing a service where possible.

3. Associated Risks

The potential risk considered in the review is as follows:

- IT services provided do not meet the needs of the organisation.

OPINION AND KEY FINDINGS

4. Overall Assurance Opinion

We are required to provide an opinion as to the adequacy and effectiveness of the system of internal control under review. The opinion is based on the work performed as set out in the scope and objectives within this report. An overall assurance rating is provided describing the effectiveness of the system of internal control in place to manage the identified risks associated with the objectives covered in this review.

The level of assurance given as to the effectiveness of the system of internal control in place to manage the risks associated with IT service management is limited assurance.

RATING	INDICATOR	DEFINITION
Limited assurance		The Board can take **limited assurance** that arrangements to secure governance, risk management and internal control, within those areas under review, are suitably designed and applied effectively. More significant matters require management attention with **moderate impact on residual risk** exposure until resolved.

The service management processes within the ICT department are being developed and improved. The department has restructured its staffing and governance arrangements to better fit the needs of the organisation, and there is a commitment to aligning provision with ITIL.

There is a Service Management Board in place for overseeing and managing the commitment to align with ITIL, and related key indicators are reported to this group. Significant work has been undertaken regarding change management with a functioning process that ensures changes are appropriately assessed, approved and actioned, and a weekly Change Advisory Board to monitor the process.

There is a service desk in place and call handlers record and pass calls to relevant staff for action. The actions to resolve calls that we reviewed were appropriate. However, the recording of information is not always correct or consistent. There is no closure process, and a number of calls are outstanding on the system. In addition, the alerts process in place to notify managers when call response times are about to breach targets, was not always functioning properly.

Although not all aspects of service management are operational, the Health Board has started developing a problem management process and some problems are being recorded at a basic level. However, there is no formal procedure for this, and as such although problems are being recorded,

these are not being fully completed, and key information is sometimes missing.

Our audit fieldwork identified three issues that we consider to be high priority, these are:

- There are no procedures for the operation of the service desk and no guidance for call handlers in terms of how calls are to be logged, classified, prioritised and routed.
- Calls and incidents are not being recorded appropriately within Service Point, with incidents recorded as 'requests', and 'requests' as incidents. We also saw instances where calls had been classified and prioritised incorrectly.
- There is no procedure or guidance for chasing or ensuring activity is maintained on calls / incidents. Our testing identified numerous calls and incidents left with a status set to 'responded to', or 'awaiting user' and not being chased or closed.

5. Assurance Summary

The summary of assurance given against the individual objectives is described in the table below:

Assurance Summary					
1	IT service design			✓	
2	Service desk provision		✓		
3	Incident and problem management		✓		
4	Knowledge management		✓		
5	Change management				✓
6	Continual service improvement		✓		

** The above ratings are not necessarily given equal weighting when generating the audit opinion.*

Design of Systems/Controls

Our findings from the review have highlighted two issues that would be classified as a weakness in the system control/design of IT service management.

Operation of System/Controls

Our findings from the review have highlighted ten issues that are classified as weaknesses in the operation of the designed system/control for IT service management.

6. Summary of Audit Findings

In this section we highlight areas of good practice that we identified during our review. We also summarise the high and medium priority findings made during our audit fieldwork. The detailed findings are reported in the Management Action Plan (Appendix A).

Objective 1: IT services are appropriately designed, provided and managed with reference to an appropriate framework (ITIL).

We note the following areas of good practice:

- the ICT staffing and governance structure has recently been revised to better fit the needs of the organisation;
- the intent for ICT is to conform to ITIL and use ITIL methodologies;
- there has been significant training provision for ITIL within ICT;
- there is a service catalogue in place; and
- the service catalogue defines the service level provided to each service. These levels, and their impact, are defined within the document.

We note the following medium priority findings in relation to this objective.

- The Service Catalogue is not published on the intranet, and appears to be incomplete, with the Electronic Patient Record (EPR) not included. In addition, the definition used for prioritising incidents within the catalogue retains the national definition for the "extensive" impact and states that this can only be allocated at a national level. This means that the catalogue is not focussed on the Health Board, but nationally. (Finding 9).
- The Service Catalogue sets out the service level that ICT is providing for each service. However, this has not been formally agreed with the user departments, and they have not had the option to review or change their service level. (Finding 10).

Objective 2: Service desk provision is appropriate and appropriate request fulfilment management practices are followed.

We note the following areas of good practice:

- there is a service desk in place;

- there is a mechanism for staff to self-record a call online;
- calls are logged when received, either from a direct call or from email / web logging and these are all triaged quickly;
- call handlers use the NWIS documentation for classification and prioritisation of calls;
- organisation specific procedures for the service desk and call handling are currently being developed;
- there is an approval process in place for requests. Our testing showed that this was operating appropriately, with SON (Statement of Need) forms provided to most calls, and if not provided with all required information, then the user contacted;
- in general, actions against calls are appropriate, with user requirements being fulfilled; and
- the processes for chasing up actions on calls are being developed, with templates having been defined for calls with the 'awaiting user' status.

We note the following high and medium priority findings in relation to this objective.

- There are no procedures for the operation of the service desk and no guidance for call handlers in terms of how calls are to be logged, classified, prioritised and routed. In addition, there are no predefined calls or incident models. (Finding 1).
- Calls and incidents are not being recorded appropriately within Service Point, with incidents recorded as requests, requests as incidents, and classifications and prioritisations not applied correctly. (Finding 2).
- There is no procedure or guidance for chasing and ensuring activity is maintained on calls / incidents. Our testing identified calls and incidents being left with a status set to 'responded to' or 'awaiting user', and not being chased or closed. (Finding 3).
- There is no formal procedure or guidance for the closure of calls and incidents or the requirement for ensuring the issue is resolved. As there is nothing defined, our testing identified inconsistencies in this stage. (Finding 5).

Objective 3: Appropriate processes are in place for incident, event and problem management in order to minimize the impact on users.

We note the following areas of good practice:

- there is an SMB (Service Management Board) in place for overseeing and managing IT service provision;
- there is reporting of performance on service management to the SMB;

- incidents were picked up promptly and actions to resolve commenced;
- actions undertaken against reported incidents were reasonable i.e. investigations are undertaken;
- work has started on fully developing the problem management process; and
- when problems are identified, they are classified, investigated and contain information on RCA (root cause analysis) and workarounds, and fixes are identified.

We note the following medium priority findings in relation to this objective.

- Service Point contains a functionality that automatically alerts managers when calls and incidents are about to breach targets for response and resolution times. However, our testing identified that these were not always working for all teams. (Finding 4).
- Although we note that work has started on the problem management process, there is no formal SOP or guidance for this that sets out the various stages. As such, although problems are being recorded on Service Point, these are not being completed, and key information is sometimes missing. (Finding 6).

Objective 4: Processes are in place to gather, analyze, store and share knowledge and information within an organization in order to improve efficiency by reducing the need to rediscover knowledge.

We note the following area of good practice:

- there are folders and information stores in place with guides and relevant documents for staff to use when working on calls and information.

We note the following medium priority finding in relation to this objective.

- The structures for sharing operating knowledge within and across teams differ and are not formalised. Different processes are in place with SharePoint, Knowledgebase and network folders all being used. Although this knowledge is structured, the mechanisms for this vary and there is not always a review process to ensure that old or out of date information is removed. (Finding 7).

Objective 5: An appropriate process is in place for change management.

We note the following areas of good practice:

- there is a CAB (Change Advisory Board) that meets weekly and there is a terms of reference (ToR) for this group;
- there are defined procedures and guidance for change management within the ToR;

- stakeholders are involved in the CAB if changes are relevant to them;
- testing of changes showed that changes are categorised, prioritised and approved appropriately;
- testing of changes also confirmed that testing plans, back out plans and the potential effect on the service were evaluated;
- in general, there was segregation between responsibility for build, test and implement for changes;
- there is an appropriate process in place for emergency changes;
- the CAB ToR notes that the meeting is to review emergency changes made, and our review of documentation confirmed that this is the case;
- emergency changes are dealt with appropriately;
- the CAB tracks changes and monitors progress of the agreed changes;
- there is a KPI report in place for change management, this includes tracking of backlogged changes as well as those undertaken in month; and
- there is a review process for completed changes, with changes approved to be closed via CAB and the change record set to complete.

There are no high or medium findings identified under this objective.

Objective 6: Processes are in place to review and evaluate business services and infrastructure services on a regular basis in order to improve service quality and to identify more economical ways of providing a service where possible.

We note the following area of good practice:

- a CSI (Continual Service Improvement) framework is being developed.

We note the following medium priority finding in relation to this objective.

- Although there is performance reporting for call and incident handling, which includes response times, these are not being used to identify areas for improvement. In addition, the reported compliance figures are significantly different from those calculated from our testing, with the basis for the automatically calculated figures being unknown to the service management lead. (Finding 8).

7. Summary of Recommendations

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

A summary of these recommendations by priority are outlined below.

Priority	H	M	L	Total
Number of recommendations	**3**	**7**	**2**	**12**

Finding 1– No procedures (Control Design)	Risk
There are no procedures for the operation of the service desk and no guidance for call handlers in terms of: • how calls are to be logged, classified, prioritised and routed; • predefined calls and no procedures for predefined calls; and • incident models for most common incidents. Given the non-technical background of the call handlers this may delay the resolution of the call or result in miss-routing of calls. The organisation is not making use of the opportunity to fix calls at first contact by setting predefined calls and their resolutions.	IT services provided do not suit the needs of the organisation.
Recommendation	**Priority level**
Procedures and guidelines should be developed for the Service Desk. These should clarify how to deal with incoming calls, the information to collect, and the routing of these calls. As part of these procedures a set of predefined calls should be developed for the most common /simple calls and incidents to enable these to be resolved on first contact.	**High**

Management Response	Responsible Officer/ Deadline

Finding 2– Recording of information (Operating effectiveness)	Risk
Our testing identified that calls and incidents are not being recorded appropriately within Service Point: • incidents are being recorded as requests, and requests as incidents; • 15 calls not classified correctly (from 27). With both wrong classification and 'n/a' used; • calls are not prioritised correctly or consistently; and • there were calls where priority had been changed late into the handling process (including just before closure). Without classifying and prioritising calls correctly, there is a risk that resource will be expended in the wrong area, that reporting figures will be incorrect and that underlying issues may not be identified.	IT services provided do not suit the needs of the organisation.
Recommendation	**Priority level**
Procedures and guidance should be finalised and issued with training provided as appropriate. Staff should be instructed to ensure that calls and incidents are classified and prioritised correctly.	**High**
Management Response	**Responsible Officer/ Deadline**

Finding 3– Call progress (Operating effectiveness)	Risk
There is no procedure or guidance for chasing and ensuring activity is maintained on calls / incidents. Our testing identified calls and incidents being left with a status set to 'responded to' or 'awaiting user' and not being chased or closed. For some of these we assume that the request had been completed, but the call not closed. Our analysis of call records identified calls and (incidents) open with the following status: • awaiting 3rd party - 59 with 47 over 30 days; • escalated out 61 (37) with 26 (20) over 30 days and one over one year old; • responded to 311 (232), with many over 30 days and six over one year; • resolved - 30 (17) with 22 (10) over 30 days; and • team processes - 534 (331) with lots over 30 days. If activity on calls is not maintained, then users may not receive an appropriate service and if calls are not closed promptly then any reporting will not be accurate.	IT services provided do not suit the needs of the organisation.
Recommendation	**Priority level**
A formal process to ensure call activity is maintained should be established, and calls closed appropriately.	**High**

Management Response	Responsible Officer/ Deadline

Finding 4– Alerts (Operating effectiveness)	Risk
Service Point contains a functionality that automatically alerts managers when calls and incidents are about to breach targets for response and resolution times. However, our testing identified that these were not always working for all teams. Without these alerts being active there is a risk that managers and team leaders may miss breaches.	IT services provided do not suit the needs of the organisation.
Recommendation	**Priority level**
The process for alerts should be maintained and re-established for each team.	**Medium**
Management Response	**Responsible Officer/ Deadline**

Finding 5– Closure process undefined (Operating effectiveness)	Risk
There is no formal procedure or guidance for the closure of calls and incidents or the requirement for ensuring the issue is resolved. As there is nothing defined our testing identified inconsistencies in this stage: • some handlers obtain 'user agreement' of closure (may or may not be included in service point); • some handlers are sending closure email, and so assume user approval by default; • some handlers closed without user contact; and • some calls left in a semi-complete status, such as work done but call not closed. Without an appropriate closure process there is a risk that issues will not be resolved as per user requirements and that calls will be left open and skew monitoring reports.	IT services provided do not suit the needs of the organisation.
Recommendation	**Priority level**
A formal closure process should be defined that sets out that: • all calls should be closed when finished; and	**Medium**

• the extent to which user approval should be sought to close different types of calls.	
Management Response	**Responsible Officer/ Deadline**

Finding 6– Problem Management (Control Design)	Risk
Although work has started on the problem management process, there is no formal SOP or guidance for this that sets out the various stages. We would expect these to include: • identification and classification; • investigation, diagnosis and resolution; • creation of known errors; and • proactive problem management. As such although problems are being recorded on Service Point, these are not being completed, and key information is sometimes missing.	IT services provided do not suit the needs of the organisation.
Recommendation	**Priority level**
The process should be fully defined with an associated SOP and guidance.	**Medium**
Management Response	**Responsible Officer/ Deadline**

Finding 7– Knowledge management (Operating effectiveness)	Risk
The structures for sharing operating knowledge within and across teams differ and are not formalised. Different processes are in place with SharePoint, Knowledgebase and network folders all being used. Although this knowledge is structured, the mechanisms for this vary and there is not always a review process to ensure that old or out of date information is removed.	IT services provided do not suit the needs of the organisation.
Recommendation	**Priority level**
Service management should consider defining a standard mechanism and process for operational knowledge management.	**Medium**
Management Response	**Responsible Officer/ Deadline**

Finding 8– Performance management (Operating effectiveness)	Risk
Although there is performance reporting for call and incident handling, which includes response times, these are not being used to identify areas for improvement. In addition, the compliance figures being reported for resolution in time for incidents (96%) and requests (92%) are significantly different from those we calculated based on our sample testing, with the basis for the automatically calculated figures being unknown to the service management lead.	IT services provided do not suit the needs of the organisation.
Recommendation	**Priority level**
The basis for the compliance figures should be established, and if necessary, amended to fully reflect the situation within the Health Board. As part of the reporting process, areas for improvement should be identified and improvement plans developed.	**Medium**
Management Response	**Responsible Officer/ Deadline**

Finding 9– Service catalogue (Operating effectiveness)	Risk
The service catalogue sets out the service level that ICT is providing for each service. The service catalogue is not published on the intranet, and appears to be incomplete, with the Electronic Patient Record (EPR) not included. In addition, the catalogue, which was based on an NWIS service catalogue, has not been tailored for the needs of the Health Board. For example, the definition used for prioritising incidents within the catalogue retains the national definition for the "extensive" impact, and states that this can only be allocated at a national level, but with a tailored catalogue the definition of 'extensive' would be more localised to the Health Board. As such, the catalogue is not focussed on the Health Board, but nationally. From a Health Board perspective there may be a system where the outage would have an extensive impact on the organisation's operational delivery such as patient records or scanning. The service catalogue in place with the Health Board should reflect this position.	IT services provided do not suit the needs of the organisation.
Recommendation	**Priority level**
The Health Board should define their own impact and service levels for use within their Service Management framework.	**Medium**
Management Response	**Responsible Officer/ Deadline**

Finding 10– Service levels (Operating effectiveness)	Risk
The service catalogue sets out the service level that ICT is providing for each service. However, this has not been formally agreed with the user departments, and they have not had the option to review or change their service level. The lack of a formal agreement means that not all staff may be aware of the expectations and responsibilities.	IT services provided do not suit the needs of the organisation.
Recommendation	**Priority level**
The service levels provided should be issued and agreed with each user department. As part of this process an agreement setting out the responsibilities and expectations should be defined.	**Medium**
Management Response	**Responsible Officer/ Deadline**

Finding 11– Service desk (Operating effectiveness)	Risk
The operating hours of the service desk are 9am-5pm, Monday - Friday, with an on-call rota for emergencies. Calls can also be logged online by users. We understand that the basis of these hours is historical. The hours have not been discussed or agreed with the organisation, and as such they may not fully meet the needs of the organisation.	IT services provided do not suit the needs of the organisation.
Recommendation	**Priority level**
The operational hours of the service desk should be re-considered to ensure they fit with the wider organisational needs.	**Low**
Management Response	**Responsible Officer/ Deadline**

Finding 12– Changes (Operating effectiveness)	Risk
Our testing sampled a number of IT changes enacted within the financial year. From this, a small number of changes did not fully comply with the process: • some (5 from our sample of 14) did not have full segregation between build, test, and implement responsibilities; and • one change identified during our fieldwork noted that there was 'no documentation to change'. However, NADEX names were changed, so it is likely that documentation would need changing.	IT services provided do not suit the needs of the organisation.
Recommendation	**Priority level**
Care should be taken to ensure the process is followed.	**Low**
Management Response	**Responsible Officer/ Deadline**

Appendix B - Assurance opinion and action plan risk rating

Audit Assurance Ratings

 **Substantial assurance** - The Board can take **substantial assurance** that arrangements to secure governance, risk management and internal control, within those areas under review, are suitably designed and applied effectively. Few matters require attention and are compliance or advisory in nature with **low impact on residual risk** exposure.

 **Reasonable assurance** - The Board can take **reasonable assurance** that arrangements to secure governance, risk management and internal control, within those areas under review, are suitably designed and applied effectively. Some matters require management attention in control design or compliance with low to **moderate impact on residual risk** exposure until resolved.

 **Limited assurance -** The Board can take **limited assurance** that arrangements to secure governance, risk management and internal control, within those areas under review, are suitably designed and applied effectively. More significant matters require management attention with **moderate impact on residual risk** exposure until resolved.

 **No assurance** - The Board can take **no assurance** that arrangements to secure governance, risk management and internal control, within those areas under review, are suitably designed and applied effectively. More significant matters require management attention with **high impact on residual risk** exposure until resolved.

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.