

8.14 IM&T Assurance Follow-up (Reasonable Assurance) - Draft

*Presenter: James Johns*

IM&T Assurance Follow-Up Draft IA Report

IM&T Assurance Follow-Up Draft IA Report amended

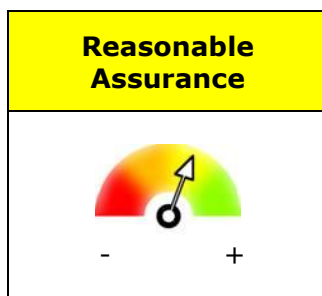
## **IM&T Assurance – Follow Up**

### **Draft Internal Audit Report 2019/20**

**Hywel Dda University Health Board**

**Private and Confidential**

**NHS Wales Shared Services Partnership  
Audit and Assurance Service**



## CONTENTS

	Page
1. Introduction and Background	4
2. Scope and Objectives	4
3. Associated Risks	5
<u>Opinion and key findings</u>	
4. Overall Assurance Opinion	5
5. Summary of Audit Findings	6
6. Audit Recommendation	8
Appendix A	Previously Agreed Management Actions
Appendix B	Audit Assurance Ratings

**Review reference:** HDUHB\_1920\_40

**Report status:** Draft Report

**Fieldwork Commencement:** 11 February 2020

**Fieldwork Completion:** 20 March 2020

**Draft Report Issued:** 27 March 2020

**Management Response Received:**

**Final Report Issued:**

**Auditor/s:** Kevin Seward

**Executive sign off** Karen Miles (Director of Finance, Planning & Performance)

**Distribution**

- Anthony Tracey (Assistant Director of Informatics)
- Sara Brain (Informatics Business Manager)

**Committee** Audit Committee



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

## ACKNOWLEDGEMENT

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

**Please note:**

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

An audit was undertaken to determine the status of previously agreed recommendations arising from the following prior IM&T assurance audits:

- IM&T/PC/Laptop Security Arrangements Follow-Up (February 2019);
- IM&T Directorate Review (January 2019);
- IM&T Security Policy & Procedures Follow-Up (August 2018); and
- Procurement and Disposal of IT Assets Follow-Up (November 2018).

The review sought to provide the Health Board with assurance that appropriate and timely action had been taken in respect of previously agreed audit recommendations arising from prior IM&T Assurance audits.

## **2. Scope and Objectives**

This audit sought to take account of the Health Board's audit tracker to determine the focus of recommendations to follow up at this audit. The process was progressed through obtaining evidence in support of each recommendation, to demonstrate sufficient action had been taken to address each recommendation.

## **3. Associated Risks**

The potential risks considered in the review were as follows:

- Management control frameworks continue to exhibit weaknesses;
- Management do not have processes in place to review and action agreed audit recommendations;


## **OPINION AND KEY FINDINGS**

### **4. Overall Assurance Opinion**

The current review considers all recommendations made (high, medium or low priority). This report does not provide assurance against the full review scopes and objectives of the original audits. The 'follow up review opinion' provides the assurance level against the implementation of the agreed action plans only.

It is pleasing to report that of the 14 recommendations that were agreed by management, eleven (79%) recommendations have been implemented, one (7%) was partially implemented and two (14%) remain outstanding. The outstanding recommendations relate to stores asset management and physical and environmental security awareness.

The level of assurance given as to the effectiveness of the system of internal control in place to manage the risks associated with the outstanding recommendations is **Reasonable Assurance**.

RATING	INDICATOR	DEFINITION
Reasonable Assurance		The Board can take <b>reasonable assurance</b> 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 <b>moderate impact on residual risk</b> exposure until resolved.

## 5. Summary of Audit Findings

The status of agreed management actions can be summarised as follows:

Audit	Implemented	Partially implemented	Outstanding / Future	Total
IM&T/PC/Laptop Security Arrangements Follow-Up	3	-	1	4
IM&T Directorate Review	6	1	1	8
IM&T Security Policy & Procedures Follow-Up	1	-	-	1
Procurement and Disposal of IT Assets Follow-Up	1	-	-	1
<b>Total</b>	<b>11</b>	<b>1</b>	<b>2</b>	<b>14</b>

Of the 14 recommendations that were agreed by management, eleven (79%) recommendations were implemented, one (7%) was partially implemented and two (14%) remain outstanding.

The full audit findings are detailed at **Appendix A**.

## 6. Audit Recommendation

A summary of the recommendations remaining is outlined below by priority:

	H	M	L	Total
IM&T/PC/Laptop Security Arrangements Follow-Up	2	-	-	2
IM&T Directorate Review	1	-	-	1
<b>Total</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>3</b>

Of the three recommendations, the key issues for management are:

- 2 High priority issues (outstanding)
  - IM&T/PC/Laptop Security (Follow-up) – The Health Board should consider a wider security awareness programme. To facilitate this

the Assistant Director of Informatics should identify individuals with jurisdiction to implement the recommendation fully, drawing on their expertise and services, coordinating a programme of work to improve the security arrangements surrounding the Health Boards IT assets.

- IM&T Directorate Review – Accurate records of stores should be maintained and regularly verified with physical checks.
- 1 High priority issue (Partially implemented)
  - IM&T Directorate Review – Advice should be sought on the matter of compulsory breaks to ensure the European Working Time Directive is appropriately adhered to.

In addition to our follow-up work we would like to make an observation in relation to the tracking and reporting of agreed management actions:

The Health Boards Capital, Estates & IM&T Sub-Committee (CE&IMT) are responsible for receipt of reports from capital audit, ensuring appropriate action is taken and report findings and all follow up action is tracked and reported to the Health Boards Audit and Risk Assurance Committee and where necessary risk issues highlighted to the BP&PAC.

Whilst agreed IM&T audit management actions specifically related to Information Governance are tracked via the Information Governance Sub-Committee (IGSC) there is currently no arrangement for tracking general IM&T actions.

Currently the CE&IMT Sub-Committee receive quarterly reports from a tracker of agreed capital and estates related audit management actions, similar arrangements could support the tracking of general IM&T actions and ensure the timely implementation of future IM&T recommendations from assurance reports.



## IM&T PC/Laptop Security Arrangements Follow-Up (February 2019) Previously providing



Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
<b>High</b>				
1	<p>The Health Board should consider a wider security awareness programme. To facilitate this the Assistant Director of Informatics should identify individuals with jurisdiction to implement the recommendation fully, drawing on their expertise and services, coordinating a programme of work to improve the security arrangements surrounding the Health Boards IT assets.</p> <p>The programme should include a communications plan to better publicise good practices and individuals responsibilities</p>	<p>Assistant Director of Informatics to Coordinate</p> <p>Scoping – 1-2 months Action plan creation -2 months Resourcing gap analysis – 1 month Implementation – 10 months</p>	<p><b>Outstanding</b></p> <p>In terms of the wider awareness program and physical environmental security, initial conversations took place with stakeholders (security, estates, etc.) the intention was to set up a virtual group to carry this forward.</p> <p>This progress was reported to the Health Board governance team as being on schedule for completion, however these initial conversations</p>	<p>Assistant Director of Informatics</p> <p><b>High</b></p>

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
	<p>in relation to the physical and environmental security for IT assets such as PCs laptops and server equipment.</p> <p>Specialist assistance should be sought from the Health, Safety &amp; Security team to identify site leads and empower them with the knowledge and responsibility for IT physical and environmental security self-assessment. These self-assessments should be reviewed and followed up by visits from the Health, Safety &amp; Security team at an appropriate frequency.</p>		<p>did not progress any further.</p> <p>Now the intention is to incorporate these tasks into the new Welsh IG toolkit work stream, the rationale for this is that section 6 of the toolkit submission relates to the physical and environmental security of information and IT assets, with requirements to capture and evidence and report the Health Board's arrangements. Categories will include polices, staff awareness, technical arrangements for security etc. If this is completed properly it will adequately address the</p>	

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
			recommendation made by us.	
<b>Medium</b>				
2	Amman Valley Hospital The Health Boards Informatics department should work with leads at the site to coordinate the resolution of weaknesses identified in the security assessment, where necessary drawing on assistance from specialist departments such as Estates and Facilities.	Site Lead for Amman Valley Hospital Director of Estates and Facilities Assistant Director of Informatics 2 months	<b>Implemented</b> A site visit was carried out by us on Friday 21/02/2020 to verify the completion of the works outlined in the management response. One site was selected at random, from attending the Amman Valley hospital site we can see that the initial work to rectify the problems was completed, the cabling has been organised to fit within the cabinets and the scrap materials have been removed.	N/A

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
			<p>However, on this visit it was noted that since the work to tidy the room was completed, Health Board staff have used the space to store a quantity of hospital mattresses and various items used by occupational therapy equipment.</p> <p>Because this is a shared room it is appreciated that IM&amp;T equipment must be stored alongside therapy equipment, we can see from our visit that the work was carried out and there is now a programme of server room visits in place where members of IT staff audits the conditions of the rooms. Therefore we consider</p>	

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
			these recommendations to have been implemented.	
3	South Pembrokeshire Hospital The Health Boards Informatics department should work with leads at the site to coordinate the resolution of weaknesses identified in the security assessment, where necessary drawing on assistance from specialist departments such as Estates and Facilities.	Site Lead for South Pembrokeshire Hospital Director of Estates and Facilities 4 months	<b>Implemented</b> A site visit was carried out by us on Friday 21/02/2020 to verify the completion of the works outlined in the management response. One site was selected at random, from attending the site we can verify that the initial work to rectify the issues was completed and there is now a programme of server room visits in place where members of IT staff audits the conditions of the rooms.	N/A

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
			Therefore we consider the recommendation to have been implemented.	
4	<p>Bro Cerwyn</p> <p>The Health Boards Informatics department should work with leads at the site to coordinate the resolution of weaknesses identified in the security assessment, where necessary drawing on assistance from specialist departments such as Estates and Facilities.</p>	<p>Director of Estates and Facilities</p> <p>3 months</p>	<p><b>Implemented</b></p> <p>A site visit was carried out by us on Friday 21/02/2020 to verify the completion of the works outlined in the management response.</p> <p>One site was selected at random, from attending the site we can verify that the initial work to rectify the issues was completed and there is now a programme of server room visits in place where members of IT staff audits the conditions of the rooms.</p>	N/A

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
			Therefore we consider the recommendation to have been implemented.	

**IM&T Directorate Review (January 2019)**

Previously providing



Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
<b>High</b>				
1	Accurate records of stores should be maintained and regularly verified with physical checks.	Anthony Tracey, Assistant Director of Informatics Start Date: November 2018 Finish Date: May 2019	<b>Outstanding</b> Verbal updates from IM&T indicate that these registers are now in place for the sites which hold stocks of assets, however the evidence provided was not sufficient to support these statements.  Instead of local stores asset registers one Kace network report was provided which showed all Health Board assets connected to the network. This report did not account for assets that were yet to be commissioned and did not evidence regular verification with physical checks.	Assistant Director of Informatics  <b>High</b>



Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
			This was queried but no clarification or additional documentation was provided. For this reason we cannot provide assurance as to whether this work has been carried out.	
4	Remind staff of the importance of accurately and completely filling in on-call claim forms.  Ensure that all claim forms are kept properly and are available to check against, claim forms should not be missing or unable to be found.	Anthony Tracey, Assistant Director of Informatics Start Date: November 2018 End Date: February 2019	<b>Implemented</b> Additional scrutiny now takes place for claim forms with the Head of IT checking and the ADI also verifying information before claims are authorised. Forms have been updated to record the authorisations and reasons for the on call work. Sample forms were received and we can verify that these changes have been implemented.	N/A
8	WOD advice should be sought on the matter of compulsory breaks to ensure the European		<b>Partially implemented</b> The business manager was able to supply a paper which was produced for the Executive Team in June 2019, this paper evidences that work is	Assistant Director of Informatics

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
	Working Time Directive is appropriately adhered to.		<p>underway to address the noncompliance of the original recommendation.</p> <p>The paper lists under option 4, temporary measures the health board is implementing while the permanent measures are implemented.</p> <p>The paper being explored, and further work to progress an OCP and Executive Paper in March 2020 evidence that this recommendation, to seek advice on the matter of compulsory breaks to ensure the European Working Time Directive is appropriately adhered to is in train.</p>	<b>Medium</b>
<b>Medium</b>				
2	Key codes should be changed on a regular basis, for example every 6 months.	Anthony Tracey, Assistant Director of Informatics May 2019 onwards	<p><b>Implemented</b></p> <p>The IT department have changed the process of changing key codes, they are also working towards replacing</p>	N/A

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
			the key code entry doors with contactless cards which can be automatically updated and cancelled when employees leave or a card is lost/stolen.	
3	Remind staff of the importance of accurately and completely filling in on-call sheets.	Anthony Tracey, Assistant Director of Informatics Start Date: November 2018 End Date: November 2018	<b>Implemented</b> Staff have been reminded of the requirement and forms have been updated to support the recording of this information. Additional verification steps are now in place to check the information is recorded when authorising claims.	N/A
5	On-call payment claims should briefly detail the reason for the call-out being claimed for.	Anthony Tracey, Assistant Director of Informatics Start Date: November 2018	<b>Implemented</b> Staff have been reminded of the requirement and forms have been updated to support the recording of this information. Additional verification steps are now in place to	N/A

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
		End Date: November 2018	check the information is recorded when authorising claims.	
6	Ensure that all shifts are agreed and properly documented prior to the shifts taking place.	Anthony Tracey, Assistant Director of Informatics Start Date: November 2018 End Date: December 2018	<b>Implemented</b> On call rotas are now completed and published to the Departments SharePoint site.	N/A
<b>Low</b>				
7	Remind staff of the importance of accurately and completely filling in variation sheets.	Anthony Tracey, Assistant Director of Informatics Start Date: November 2018 End Date: December 2018	<b>Implemented</b> Staff have been reminded of the requirement and forms have been updated to support the recording of this information. Additional verification steps are now in place to check the information is recorded when authorising claims.	N/A

## IM&T Security Policy & Procedures Follow-Up (August 2018)

Previously providing



Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
<b>Low</b>				
1	Management should ensure that the outline for the programme of work is delivered to the August 2018 meeting of the IGSC who should ensure that the policy awareness programme is undertaken and that staff are aware of their responsibilities.	<p>Anthony Tracey, Assistant Director of Informatics / Sarah Brain, Informatics Business Manager</p> <p>Start Date: August 2018 End Date: September 2018</p> <p>The next IGSC is September, where the plan will be presented, the</p>	<p><b>Implemented</b></p> <p>The outline for the Informatics Policy Awareness Programme was agenda item 12 of the September 2018 IGSC meeting, the item was supported by attachment 10 of the paper bundle which was an SBAR outlining the scheduled communications awareness programme and schedule for policy review. This was presented by the Informatics business manager. Review of the confirmed minutes of the meeting show the report and update was received.</p>	N/A

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
		implementation of the plan will not be completed within the timescales approve.	A global was email sent 14/01/2019 stating the Informatics Department will be running its Policy Awareness Programme commencing in February 2020. Each month there will be a spotlight on each of the 17 policies within the Informatics suite.	

## Procurement and Disposal of IT Assets Follow-Up (November 2018)

Previously providing



Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
<b>High</b>				
1	As a matter of urgency, the Health Board should revisit its arrangements for the disposal of IT assets, documenting and communicating the process to correspond with the Health Board approved Policy, ensuring adequate documentation maintained and proper notification received from its third party partners to constitute a meaningful audit trail for disposed IT assets.	<p>Anthony Tracey, Assistant Director of Informatics</p> <p>Paul Solloway, Head of ICT</p> <p>30th November 2018 1st January 2019</p>	<p><b>Implemented</b></p> <p>From discussions with the ADI and ICT business manager it was noted that the recommendation has now been completed however the initial target dates of November 2018 and January 2019 were missed.</p> <p>Discussion with the Health Board governance team clarified that the progress was reported to the Health Board governance team by the interim ICT business manager and a revised completion date of September 2019 was agreed with the Director of Planning, Performance and Commissioning.</p>	N/A

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
			As part of our follow-up, copies of the asset management reports and disposal reports compiled by the HB were requested and received to support the positional statement.	



## 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 has **no assurance** that arrangements to secure governance, risk management and internal control, within those areas under review, are suitably designed and applied effectively. Action is required to address the whole control framework in this area 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
<b>High</b>	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*
<b>Medium</b>	Minor weakness in control design OR limited non-compliance with established controls. PLUS Some risk to achievement of a system objective.	Within One Month*
<b>Low</b>	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.

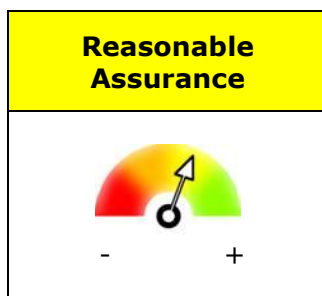
## **IM&T Assurance – Follow Up**

### **Draft Internal Audit Report 2019/20**

**Hywel Dda University Health Board**

**Private and Confidential**

**NHS Wales Shared Services Partnership  
Audit and Assurance Service**



## CONTENTS

	Page
1. Introduction and Background	4
2. Scope and Objectives	4
3. Associated Risks	5
<u>Opinion and key findings</u>	
4. Overall Assurance Opinion	5
5. Summary of Audit Findings	6
6. Audit Recommendation	8
Appendix A	Previously Agreed Management Actions
Appendix B	Audit Assurance Ratings

**Review reference:** HDUHB\_1920\_40

**Report status:** Draft Report

**Fieldwork Commencement:** 11 February 2020

**Fieldwork Completion:** 20 March 2020

**Draft Report Issued:** 27 March 2020

**Management Response Received:**

**Final Report Issued:**

**Auditor/s:** Kevin Seward

**Executive sign off** Karen Miles (Director of Planning, Performance & Commissioning)

**Distribution**

- Anthony Tracey (Assistant Director of Informatics)
- Sara Brain (Informatics Business Manager)

**Committee** Audit Committee



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

## ACKNOWLEDGEMENT

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

**Please note:**

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

An audit was undertaken to determine the status of previously agreed recommendations arising from the following prior IM&T assurance audits:

- IM&T/PC/Laptop Security Arrangements Follow-Up (February 2019);
- IM&T Directorate Review (January 2019);
- IM&T Security Policy & Procedures Follow-Up (August 2018); and
- Procurement and Disposal of IT Assets Follow-Up (November 2018).

The review sought to provide the Health Board with assurance that appropriate and timely action had been taken in respect of previously agreed audit recommendations arising from prior IM&T Assurance audits.

## **2. Scope and Objectives**

This audit sought to take account of the Health Board's audit tracker to determine the focus of recommendations to follow up at this audit. The process was progressed through obtaining evidence in support of each recommendation, to demonstrate sufficient action had been taken to address each recommendation.

## **3. Associated Risks**

The potential risks considered in the review were as follows:

- Management control frameworks continue to exhibit weaknesses;
- Management do not have processes in place to review and action agreed audit recommendations;


## **OPINION AND KEY FINDINGS**

### **4. Overall Assurance Opinion**

The current review considers all recommendations made (high, medium or low priority). This report does not provide assurance against the full review scopes and objectives of the original audits. The 'follow up review opinion' provides the assurance level against the implementation of the agreed action plans only.

It is pleasing to report that of the 14 recommendations that were agreed by management, eleven (79%) recommendations have been implemented, one (7%) was partially implemented and two (14%) remain outstanding. The outstanding recommendations relate to stores asset management and physical and environmental security awareness.

The level of assurance given as to the effectiveness of the system of internal control in place to manage the risks associated with the outstanding recommendations is **Reasonable Assurance**.

RATING	INDICATOR	DEFINITION
Reasonable Assurance		The Board can take <b>reasonable assurance</b> 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 <b>moderate impact on residual risk</b> exposure until resolved.

## 5. Summary of Audit Findings

The status of agreed management actions can be summarised as follows:

Audit	Implemented	Partially implemented	Outstanding / Future	Total
IM&T/PC/Laptop Security Arrangements Follow-Up	3	-	1	4
IM&T Directorate Review	6	1	1	8
IM&T Security Policy & Procedures Follow-Up	1	-	-	1
Procurement and Disposal of IT Assets Follow-Up	1	-	-	1
<b>Total</b>	<b>11</b>	<b>1</b>	<b>2</b>	<b>14</b>

Of the 14 recommendations that were agreed by management, eleven (79%) recommendations were implemented, one (7%) was partially implemented and two (14%) remain outstanding.

The full audit findings are detailed at **Appendix A**.

## 6. Audit Recommendation

A summary of the recommendations remaining is outlined below by priority:

	H	M	L	Total
IM&T/PC/Laptop Security Arrangements Follow-Up	2	-	-	2
IM&T Directorate Review	1	-	-	1
<b>Total</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>3</b>

Of the three recommendations, the key issues for management are:

- 2 High priority issues (outstanding)
  - IM&T/PC/Laptop Security (Follow-up) – The Health Board should consider a wider security awareness programme. To facilitate this

the Assistant Director of Informatics should identify individuals with jurisdiction to implement the recommendation fully, drawing on their expertise and services, coordinating a programme of work to improve the security arrangements surrounding the Health Boards IT assets.

- IM&T Directorate Review – Accurate records of stores should be maintained and regularly verified with physical checks.
- 1 High priority issue (Partially implemented)
  - IM&T Directorate Review – Advice should be sought on the matter of compulsory breaks to ensure the European Working Time Directive is appropriately adhered to.

In addition to our follow-up work we would like to make an observation in relation to the tracking and reporting of agreed management actions:

The Health Boards Capital, Estates & IM&T Sub-Committee (CE&IMT) are responsible for receipt of reports from capital audit, ensuring appropriate action is taken and report findings and all follow up action is tracked and reported to the Health Boards Audit and Risk Assurance Committee and where necessary risk issues highlighted to the BP&PAC.

Whilst agreed IM&T audit management actions specifically related to Information Governance are tracked via the Information Governance Sub-Committee (IGSC) there is currently no arrangement for tracking general IM&T actions.

Currently the CE&IMT Sub-Committee receive quarterly reports from a tracker of agreed capital and estates related audit management actions, similar arrangements could support the tracking of general IM&T actions and ensure the timely implementation of future IM&T recommendations from assurance reports.



## IM&T PC/Laptop Security Arrangements Follow-Up (February 2019) Previously providing



Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
<b>High</b>				
1	<p>The Health Board should consider a wider security awareness programme. To facilitate this the Assistant Director of Informatics should identify individuals with jurisdiction to implement the recommendation fully, drawing on their expertise and services, coordinating a programme of work to improve the security arrangements surrounding the Health Boards IT assets.</p> <p>The programme should include a communications plan to better publicise good practices and individuals responsibilities</p>	<p>Assistant Director of Informatics to Coordinate</p> <p>Scoping – 1-2 months Action plan creation -2 months Resourcing gap analysis – 1 month Implementation – 10 months</p>	<p><b>Outstanding</b></p> <p>In terms of the wider awareness program and physical environmental security, initial conversations took place with stakeholders (security, estates, etc.) the intention was to set up a virtual group to carry this forward.</p> <p>This progress was reported to the Health Board governance team as being on schedule for completion, however these initial conversations</p>	<p>Assistant Director of Informatics</p> <p><b>High</b></p>

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
	<p>in relation to the physical and environmental security for IT assets such as PCs laptops and server equipment.</p> <p>Specialist assistance should be sought from the Health, Safety &amp; Security team to identify site leads and empower them with the knowledge and responsibility for IT physical and environmental security self-assessment. These self-assessments should be reviewed and followed up by visits from the Health, Safety &amp; Security team at an appropriate frequency.</p>		<p>did not progress any further.</p> <p>Now the intention is to incorporate these tasks into the new Welsh IG toolkit work stream, the rationale for this is that section 6 of the toolkit submission relates to the physical and environmental security of information and IT assets, with requirements to capture and evidence and report the Health Board's arrangements. Categories will include policies, staff awareness, technical arrangements for security etc. If this is completed properly it will adequately address the</p>	

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
			recommendation made by us.	
<b>Medium</b>				
2	Amman Valley Hospital The Health Boards Informatics department should work with leads at the site to coordinate the resolution of weaknesses identified in the security assessment, where necessary drawing on assistance from specialist departments such as Estates and Facilities.	Site Lead for Amman Valley Hospital Director of Estates and Facilities Assistant Director of Informatics 2 months	<b>Implemented</b> A site visit was carried out by us on Friday 21/02/2020 to verify the completion of the works outlined in the management response. One site was selected at random, from attending the Amman Valley hospital site we can see that the initial work to rectify the problems was completed, the cabling has been organised to fit within the cabinets and the scrap materials have been removed.	N/A

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
			<p>However, on this visit it was noted that since the work to tidy the room was completed, Health Board staff have used the space to store a quantity of hospital mattresses and various items used by occupational therapy equipment.</p> <p>Because this is a shared room it is appreciated that IM&amp;T equipment must be stored alongside therapy equipment, we can see from our visit that the work was carried out and there is now a programme of server room visits in place where members of IT staff audits the conditions of the rooms. Therefore we consider</p>	

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
			these recommendations to have been implemented.	
3	South Pembrokeshire Hospital The Health Boards Informatics department should work with leads at the site to coordinate the resolution of weaknesses identified in the security assessment, where necessary drawing on assistance from specialist departments such as Estates and Facilities.	Site Lead for South Pembrokeshire Hospital Director of Estates and Facilities 4 months	<b>Implemented</b> A site visit was carried out by us on Friday 21/02/2020 to verify the completion of the works outlined in the management response. One site was selected at random, from attending the site we can verify that the initial work to rectify the issues was completed and there is now a programme of server room visits in place where members of IT staff audits the conditions of the rooms.	N/A

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
			Therefore we consider the recommendation to have been implemented.	
4	<p>Bro Cerwyn</p> <p>The Health Boards Informatics department should work with leads at the site to coordinate the resolution of weaknesses identified in the security assessment, where necessary drawing on assistance from specialist departments such as Estates and Facilities.</p>	<p>Director of Estates and Facilities</p> <p>3 months</p>	<p><b>Implemented</b></p> <p>A site visit was carried out by us on Friday 21/02/2020 to verify the completion of the works outlined in the management response.</p> <p>One site was selected at random, from attending the site we can verify that the initial work to rectify the issues was completed and there is now a programme of server room visits in place where members of IT staff audits the conditions of the rooms.</p>	N/A

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
			Therefore we consider the recommendation to have been implemented.	

**IM&T Directorate Review (January 2019)**

Previously providing



Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
<b>High</b>				
1	Accurate records of stores should be maintained and regularly verified with physical checks.	Anthony Tracey, Assistant Director of Informatics Start Date: November 2018 Finish Date: May 2019	<b>Outstanding</b> Verbal updates from IM&T indicate that these registers are now in place for the sites which hold stocks of assets, however the evidence provided was not sufficient to support these statements.  Instead of local stores asset registers one Kace network report was provided which showed all Health Board assets connected to the network. This report did not account for assets that were yet to be commissioned and did not evidence regular verification with physical checks.	Assistant Director of Informatics  <b>High</b>



Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
			This was queried but no clarification or additional documentation was provided. For this reason we cannot provide assurance as to whether this work has been carried out.	
4	Remind staff of the importance of accurately and completely filling in on-call claim forms.  Ensure that all claim forms are kept properly and are available to check against, claim forms should not be missing or unable to be found.	Anthony Tracey, Assistant Director of Informatics Start Date: November 2018 End Date: February 2019	<b>Implemented</b> Additional scrutiny now takes place for claim forms with the Head of IT checking and the ADI also verifying information before claims are authorised. Forms have been updated to record the authorisations and reasons for the on call work.  Sample forms were received and we can verify that these changes have been implemented.	N/A
8	WOD advice should be sought on the matter of compulsory breaks to ensure the European		<b>Partially implemented</b> The business manager was able to supply a paper which was produced for the Executive Team in June 2019, this paper evidences that work is	Assistant Director of Informatics

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
	Working Time Directive is appropriately adhered to.		<p>underway to address the noncompliance of the original recommendation.</p> <p>The paper lists under option 4, temporary measures the health board is implementing while the permanent measures are implemented.</p> <p>The paper being explored, and further work to progress an OCP and Executive Paper in March 2020 evidence that this recommendation, to seek advice on the matter of compulsory breaks to ensure the European Working Time Directive is appropriately adhered to is in train.</p>	<b>Medium</b>
<b>Medium</b>				
2	Key codes should be changed on a regular basis, for example every 6 months.	Anthony Tracey, Assistant Director of Informatics May 2019 onwards	<p><b>Implemented</b></p> <p>The IT department have changed the process of changing key codes, they are also working towards replacing</p>	N/A

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
			the key code entry doors with contactless cards which can be automatically updated and cancelled when employees leave or a card is lost/stolen.	
3	Remind staff of the importance of accurately and completely filling in on-call sheets.	Anthony Tracey, Assistant Director of Informatics Start Date: November 2018 End Date: November 2018	<b>Implemented</b> Staff have been reminded of the requirement and forms have been updated to support the recording of this information. Additional verification steps are now in place to check the information is recorded when authorising claims.	N/A
5	On-call payment claims should briefly detail the reason for the call-out being claimed for.	Anthony Tracey, Assistant Director of Informatics Start Date: November 2018	<b>Implemented</b> Staff have been reminded of the requirement and forms have been updated to support the recording of this information. Additional verification steps are now in place to	N/A

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
		End Date: November 2018	check the information is recorded when authorising claims.	
6	Ensure that all shifts are agreed and properly documented prior to the shifts taking place.	Anthony Tracey, Assistant Director of Informatics Start Date: November 2018 End Date: December 2018	<b>Implemented</b> On call rotas are now completed and published to the Departments SharePoint site.	N/A
<b>Low</b>				
7	Remind staff of the importance of accurately and completely filling in variation sheets.	Anthony Tracey, Assistant Director of Informatics Start Date: November 2018 End Date: December 2018	<b>Implemented</b> Staff have been reminded of the requirement and forms have been updated to support the recording of this information. Additional verification steps are now in place to check the information is recorded when authorising claims.	N/A

## IM&T Security Policy & Procedures Follow-Up (August 2018)

Previously providing



Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
<b>Low</b>				
1	Management should ensure that the outline for the programme of work is delivered to the August 2018 meeting of the IGSC who should ensure that the policy awareness programme is undertaken and that staff are aware of their responsibilities.	<p>Anthony Tracey, Assistant Director of Informatics / Sarah Brain, Informatics Business Manager</p> <p>Start Date: August 2018 End Date: September 2018</p> <p>The next IGSC is September, where the plan will be presented, the</p>	<p><b>Implemented</b></p> <p>The outline for the Informatics Policy Awareness Programme was agenda item 12 of the September 2018 IGSC meeting, the item was supported by attachment 10 of the paper bundle which was an SBAR outlining the scheduled communications awareness programme and schedule for policy review. This was presented by the Informatics business manager. Review of the confirmed minutes of the meeting show the report and update was received.</p>	N/A

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
		implementation of the plan will not be completed within the timescales approve.	A global was email sent 14/01/2019 stating the Informatics Department will be running its Policy Awareness Programme commencing in February 2020. Each month there will be a spotlight on each of the 17 policies within the Informatics suite.	

## Procurement and Disposal of IT Assets Follow-Up (November 2018)

Previously providing



Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
<b>High</b>				
1	As a matter of urgency, the Health Board should revisit its arrangements for the disposal of IT assets, documenting and communicating the process to correspond with the Health Board approved Policy, ensuring adequate documentation maintained and proper notification received from its third party partners to constitute a meaningful audit trail for disposed IT assets.	<p>Anthony Tracey, Assistant Director of Informatics</p> <p>Paul Solloway, Head of ICT</p> <p>30th November 2018 1st January 2019</p>	<p><b>Implemented</b></p> <p>From discussions with the ADI and ICT business manager it was noted that the recommendation has now been completed however the initial target dates of November 2018 and January 2019 were missed.</p> <p>Discussion with the Health Board governance team clarified that the progress was reported to the Health Board governance team by the interim ICT business manager and a revised completion date of September 2019 was agreed with the Director of Planning, Performance and Commissioning.</p>	N/A

Ref	Recommendation	Responsibility & Timescale	Action/Status	Updated responsibility, timescale & rating
			As part of our follow-up, copies of the asset management reports and disposal reports compiled by the HB were requested and received to support the positional statement.	



## 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 has **no assurance** that arrangements to secure governance, risk management and internal control, within those areas under review, are suitably designed and applied effectively. Action is required to address the whole control framework in this area 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
<b>High</b>	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*
<b>Medium</b>	Minor weakness in control design OR limited non-compliance with established controls. PLUS Some risk to achievement of a system objective.	Within One Month*
<b>Low</b>	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.