

**Hywel Dda University Health Board**

**Cyber Security (Stratia Report)**

**Final Internal Audit Report**

**February 2020**

**Private and Confidential**

**NHS Wales Shared Services Partnership**

**Audit and Assurance Services**



<b>Contents</b>	<b>Page</b>
1. Introduction and Background	4
2. Scope and Objectives	5
3. Associated Risks	5
<u>Opinion and key findings</u>	
4. Overall Assurance Opinion	6
5. Assurance Summary	7
6. Summary of Audit Findings	8
<u>Conclusion and Recommendation</u>	
7. Summary of Recommendations	11

Appendix A  
Appendix B

Management Action Plan  
Assurance Opinion and Action Plan Risk Rating

<b>Review reference:</b>	HDUHB-1920-20
<b>Report status:</b>	Final Internal Audit Report
<b>Fieldwork commencement:</b>	11 <sup>th</sup> October 2019
<b>Fieldwork completion:</b>	29 <sup>th</sup> November 2019
<b>Draft report issued:</b>	14 <sup>th</sup> January 2020
<b>Management response received:</b>	05 <sup>th</sup> February 2020
<b>Final report issued:</b>	07 <sup>th</sup> February 2020
<b>Auditor/s:</b>	Kevin Seward
<b>Executive sign off:</b>	Karen Miles (Director of Planning, Performance & Commissioning)
<b>Distribution:</b>	Anthony Tracy (Assistant Director of Informatics) Paul Solloway (Head of ICT)
<b>Committee:</b>	Audit & 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 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**

A review of the cyber security arrangements in place within Hywel Dda University Health Board (the 'Health Board' or the 'organisation') was completed in line with the 2019/20 Internal Audit Plan.

The relevant lead Executive Director for the assignment was the Director of Planning, Performance & Commissioning.

Cyber security is defined as the protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems. It is the protection of computer systems from the theft or damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide.

Cyber security includes controlling physical access to the hardware, as well as protecting against harm that may come from malware, viruses and unauthorised or inappropriate software.

A strong cyber awareness culture is one of the best defences against cyber-attacks. Regulations such as the Network and Information Security (NIS) Directive and the General Data Protection Regulation (GDPR) will increase the burden on organisations to ensure they have effective cyber-security strategies and culture in place, in addition to robust controls and policies, to prevent and remediate attacks.

In October 2017, Stratia Consulting was commissioned by Velindre NHS Trust, on behalf of NHS Wales, to carry out external cyber security assessments for its organisations.

For each organisation, a cyber-security assessment report and security improvement plan (SIP) was produced. This review of sought to provide the Hywel Dda University Health Board with assurance regarding the progress in implementing its security improvement plan.

Additionally, an overarching security assessment and SIP for NHS Wales as a whole was produced. The audit is set in the context of the resources that have been assigned and deployed for this area of activity and also the further guidance awaited from Welsh Government.

## 2. Scope and Objectives

The overall objective of this review was to evaluate the adequacy of the systems and controls in place for cyber-security, in order to provide reasonable assurance to the organisation's Audit & Risk Assurance Committee that risks material to the achievement of system's objectives are managed appropriately.

The specific purpose of the review was to establish if the mechanisms in place for ensuring cyber security are appropriately designed, and procedures and controls have been implemented as outlined in the SIP derived from the external review of cyber security.

To do this we reviewed the assessment report and SIP and evaluated the evidence to support the organisation's current positional statement. Where an action plan had been developed from the SIP, we reviewed the progress in addressing the recorded actions.

The main control objectives reviewed were:

- i. Governance: An appropriate governance and management structure is in place to ensure cyber-security.
- ii. External review awareness: Information contained within the Health Board's cyber-security assessment report and SIP has been discussed and monitored by an appropriate group or committee.
- iii. Implementing actions: any actions contained within the cyber-security SIP have been completed within reasonable timeframes, or where there is significant variance from plan, this is clear within assurance reported to the monitoring group / committee.

## 3. Associated Risks

The potential risks considered in the review are as follows:

- Poor or non-existent stewardship in relation to cyber-security.
- Failure to comply with regulations such as the NIS Directive.
- Loss of data and inappropriate access to information from entities internal to the organisation.
- Risk of loss of IT services as a result of attack from entities external to the organisation, exploiting common vulnerabilities.


- Inappropriate unauthorised software installed / increased risk of infection from introduction of malware.
- Breach of licensing arrangements, leading to potential financial penalties and reputational damage.

## **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 the process of cyber security is Reasonable assurance.

<b>RATING</b>	<b>INDICATOR</b>	<b>DEFINITION</b>
<b>Reasonable</b>		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.

This review of cyber security arrangements within the Health Board focused on the governance and visibility of the Stratia assessment report and SIP. We evaluated evidence to support the organisation's current positional statement on its action plan developed from the SIP; as such, our follow-up work was limited to the areas contained in the original Stratia report.

The overall level of assurance that can be assigned to a review is dependent on the severity of the findings as applied against the specific review objectives and should therefore be considered in that context.

There is an appropriate subcommittee within the Health Board for monitoring 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.





The Stratia report included actions for improvement, having reviewed the actions we can confirm that in the main, actions have been progressed and progress has been made on implementing many of these, including improving the patching documentation and the identification of machines running on old operating systems with an associated plan in place remove where possible.

Our audit fieldwork identified two key findings. These related to the resources available to the ICT department to progress some actions contained in the Stratia improvement plan and having no dedicated technical operational lead for cyber security within the Health Board.

The lack of defined cyber security resource has meant that although the Health Board has security tools, it hasn't been able to maximise the use of these.

## 5. Assurance Summary

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

Audit Objective		Assurance Summary*			
					
1	Governance			✓	
2	External review awareness				✓
3	Implementing actions		✓		

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

### Design of Systems/Controls

The findings from the review have highlighted no issues that are classified as a weakness in the system control/design for cyber security.

### Operation of System/Controls

The findings from the review have highlighted two issues that are classified as a weakness in the operation of the designed system/control for cyber security. These are identified in the Management Action Plan as (O).

## 6. Summary of Audit Findings

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

### **OBJECTIVE 1 - Governance: An appropriate governance and management structure is in place to ensure cyber-security**

The following areas of good practice were noted:

- locally, cyber security is overseen by a formal Subcommittee of the Board and is also included within working groups;
- nationally, security is overseen by the National Informatics Management Board (NIMB);
- cyber security compliance is also reported routinely in the Integrated Performance Assurance Report (IPAR) via the Business Planning and Performance Assurance Committee (BPPAC);
- the Health Board has a range of corporate control documents, relating to ICT;
- an annual overview of related written control documentation is submitted to the IGSC for information;
- dashboards are also being developed within Power BI to give management an overview of the current state of cyber security at the Health Board;
- a cyber security improvement action plan is in place at the Health Board; and
- the organisation has an established structure. There are Strategic Leads/Board Champions with defined roles relating to information security for the period 2019/20.

We note the following Medium priority finding in relation to this objective:

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 01 at Appendix A**

**OBJECTIVE 2 - External review awareness: Information contained within the Health Board's cyber-security assessment report and SIP has been discussed and monitored by an appropriate group or committee.**

The following areas of good practice were noted:

- the Stratia report was formally received by the organisation;
- the report was submitted at an appropriate group at sufficient level of influence to implement the actions and monitor compliance;
- the report from Stratia contained in its appendix, a security improvement plan (SIP), this was extracted to form the report and was monitored via the IGSC; and
- updates on the implementation of the external security assessment recommendations were provided to BPPAC in the annual report from the IGSC.

**No matters arising.**

**OBJECTIVE 3 - Implementing actions: any actions contained within the cyber-security SIP have been completed within reasonable timeframes.**

The following areas of good practice were noted:

- as a result of the assessment, Hywel Dda ICT produced a work plan to address the shortfalls identified;
- papers have been submitted to IGSC which have provided updates on the progress of the health boards cyber security improvement plan; and
- there is evidence that the action plan has been progressed, many items have been completed or are in train with updates provided to IGSC / health board.

We note the following High priority finding in relation to this objective:

There is evidence that many of the improvement plan actions relating to the issues raised in the Stratia report have been completed or are being progressed and form part of the Health Board cyber work plan communicated via the IGSC.

Key policies have been reviewed and approved by IGSC. Patching documentation has been improved and work has taken place to reduce the number of machines running on old operating systems with an associated plan in place remove where possible.

It is however acknowledged that there is still significant amount of work to be completed against the improvement plan actions in order to fully mitigate the risks associated with cyber security within the Health Board.

The lack of recourse to carry out cyber security related activities at the Health Board was a theme in the recommendations of the Stratia report; A11.1, A12.2, A12.6 and A18.2 all refer to additional resources being made available to carry out cyber security related work.

This has been reported via the IGSC, highlighting that some issues remain un-actioned as ICT are unable to progress without additional funding / resource from WG or other Health Board sources.

Updates identifying the need for additional resources have fed into the organisations reporting structure, however the resources have not been agreed, this means that the organisation cannot fully undertake the actions needed to complete the Stratia action plan and ensure a robust cyber security programme is maintained at the Health Board.

Consequently key areas of a functioning cyber security regime are not currently present, such as regular vulnerability scanning and intrusion detection.

**See Finding 02 at Appendix A.**

## 7. Summary of Recommendations

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

A summary of these recommendations by priority is outlined below.

<b>Priority</b>	<b>H</b>	<b>M</b>	<b>L</b>	<b>Total</b>
<b>Number of recommendations</b>	<b>1</b>	<b>1</b>	<b>0</b>	<b>2</b>

<b>Finding 1 – Dedicated ICT cyber security specialists (O)</b>	<b>Risk</b>
<p>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.</p> <p>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.</p>	<p>Poor or non-existent stewardship in relation to cyber-security; and</p> <p>Risk of loss of IT services as a result of attack from entities external to the organisation, exploiting common vulnerabilities</p>
<b>Recommendation 1</b>	<b>Priority level</b>
<p>A cyber security role for the Health Board should be properly defined and operating appropriately so to enable the Health Board ICT department to fully use the security products available to them.</p>	<b>Medium</b>
<b>Management Response</b>	<b>Responsible Officer/ Deadline</b>
<p>Agreed</p> <p>Following the announcement of the Digital Priorities Invest Fund (DPIF) from Welsh Government, the Health Board secured resources to appoint a Band 6 Cyber Security post. However, due to the funding letter only arriving in December 2019, and the requirement to spend the investment by March 2020, the funding for 2019/20 was utilised to strengthen the cyber tools within the Health Board. The recurring funding will be directed towards funding a full time</p>	<p>Assistant Director of Informatics and Head of ICT</p> <p>July 2020</p>


<p>post for cyber security, to provide the monitoring of the tool sets purchased, both at a national and local level. The post has been through the appropriate governance mechanisms within the Health Board and is due to be advertised in March 2020, with an anticipated start date of May 2020.</p>	
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--


<p><b>Finding 2 – Implementing actions (O)</b></p>	<p><b>Risk</b></p>
<p>There is still significant amount of work to be completed against the improvement plan actions in order to fully mitigate the risks associated with cyber security within the Health Board.</p> <p>The lack of recourse to carry out cyber security related activities at the Health Board was a theme in the recommendations of the Stratia report; A11.1, A12.2, A12.6 and A18.2 all refer to additional resources being made available to carry out cyber security related work.</p> <p>This has been reported via the IGSC, highlighting that some issues remain un-actioned as ICT are unable to progress without additional funding / resource from WG or other Health Board sources.</p> <p>Updates identifying the need for additional resources have fed into the organisations reporting structure, however the resources have not been agreed, this means that the organisation cannot fully undertake the actions needed to complete the Stratia action plan and ensure a robust cyber security programme is maintained at the Health Board.</p> <p>Consequently key areas of a functioning cyber security regime are not currently present, such as regular vulnerability scanning and intrusion detection.</p>	<p>Poor or non-existent stewardship in relation to cyber-security; and</p> <p>Risk of loss of IT services as a result of attack from entities external to the organisation, exploiting common vulnerabilities</p>
<p><b>Recommendation 2</b></p>	<p><b>Priority level</b></p>
<p>The Health Board ICT department should formally define the cyber security tasks that cannot be undertaken within the current resource envelope and the associated risks. This should be reported through the organisational governance structure so that a decision on risks and priorities can be made.</p>	<p style="text-align: center;"><b>High</b></p>


<b>Management Response</b>	<b>Responsible Officer/ Deadline</b>
<p>Agreed</p> <p>In conjunction with Recommendation 1, a detailed assessment of the gaps / tasks will be identified which in turn will form the work plan of the newly appointed cyber security resource. A cyber security risk is already included Corporate Risk Register (Risk Ref. 451). This risk is reviewed on a monthly basis and any additional mitigations or actions are updated accordingly. As required any new risks identified through the gap analysis will be added to the ICT Risk Register and assessed for escalation.</p>	<p>Assistant Director of Informatics and Head of ICT</p> <p>June 2020</p>


## Appendix B - Assurance opinion and action plan risk rating

### 2019/20 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** arrangements in place to secure governance, risk management and internal control, within those areas under review, which 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.





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

Contact details: 01267 239780