

## **Hywel Dda University Health Board**

### **Departmental IT System:**

### **Lilie – Sexual Health Management**

### **Final Internal Audit Report**

**November 2019**

**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              | 4  |
| 3. Associated Risks                  | 5  |
| <u>Opinion and key findings</u>      |  |
| 4. Overall Assurance Opinion         | 5  |
| 5. Assurance Summary                 | 6  |
| 6. Summary of Audit Findings         | 8  |
| 7. Summary of Recommendations        | 13   |
| Appendix A                           | Management Action Plan   |
| Appendix B                           | Assurance Opinion and Action Plan Risk Rating  |
| <b>Review reference:</b>             | HDUHB-1920-22  |
| <b>Report status:</b>                | Final Internal Audit Report  |
| <b>Fieldwork commencement:</b>       | 04/10/2019   |
| <b>Fieldwork completion:</b>         | 22/11/2019   |
| <b>Draft report issued:</b>          | 03/12/2019   |
| <b>Management response received:</b> | 04/12/2019   |
| <b>Final report issued:</b>          | 10/12/2019   |
| <b>Auditor/s:</b>                    | Kevin Seward   |
| <b>Executive sign off:</b>           | Andrew Carruthers (Director of Operations)   |
| <b>Distribution:</b>                 | Karen Miles (Director of Planning, Performance and Commissioning); Keith Jones (General Manager Women, Childrens and Cancer Services); Lisa Humphrey (Service Delivery Manager for Sexual Health and Gynecology) |
| <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**

The review of Lilie Sexual Health Management IT system within Hywel Dda University Health Board (the 'Health Board') or (the 'organisation') originates from the 2019/20 internal audit plan. The Sexual Health Management System (Lilie) is a fully-scalable Electronic Patient Record system (EPR) used to capture outpatient activity, diagnoses and treatments for genitourinary medicine (GUM) patients. While the core software has many standard features, modules are adopted on a flexible basis according service requirements.

Providing clinic team members with fast access to patient records, Lilie offers immediate and secure visibility of all patient data – such as previous consultations, test results and referrals – greatly reducing administrative functions and allowing multidisciplinary teams to streamline their service. All audit and quality measures are also incorporated automatically to reduce clinical risk and improve the quality of sexual health services.

The relevant executive lead for the assignment was Andrew Carruthers (Director of Operations) and copied to Karen Miles (Director of Planning, Performance and Commissioning) for information and action of any findings which fall within the responsibility of the Hywel Dda University Health Board Informatics Department.

## **2. Scope and Objectives**

The objective of the audit was to evaluate and determine the adequacy of the systems and controls in place for the management of the Lilie Sexual Health Management IT System, in order to provide reasonable assurance to the Health Board Audit Committee that risks material to the achievement of system objectives are managed appropriately.

The purpose of the review was to provide assurance to the Audit Committee that data held within the Sexual Health Management System is accurate, secure from unauthorised access and loss, and that the system is used fully.

The main areas that the review sought to provide assurance on were:

- An appropriate governance process is in place for the system;
- Appropriate control is maintained over the database;
- All input is authorised, complete, accurate, timely and input once only;
- Proper control is exercised over access to application systems;
- Controls ensure the accuracy, completeness, confidentiality and timeliness of output, reports and interfaces;
- A complete audit trail is maintained which allows an item to be traced from input through to its final resting place; and
- Appropriate business continuity arrangements are in place with include backing up copies of data and programs, storing and retaining them securely, and recovering applications in the event of failure.

### 3. Associated Risks

The potential risks considered in the review were as follows:

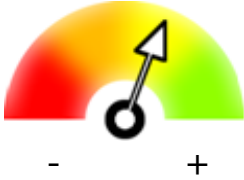
- Inappropriate access to system / data.
- Inaccurate data held in system.
- Inaccurate data reported from system.
- Loss of processing / data.
- The Health Board may not maximise the benefits from the system.

## 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 Lilie – Sexual Health Management IT system is **Reasonable** assurance.

| RATING                      | INDICATOR   | DEFINITION  |
|-----------------------------|---|---|
| <b>Reasonable assurance</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 <b>low to moderate impact on residual risk</b> exposure until resolved. |





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.

A reasonable rating has been deemed appropriate for this review with six medium priority findings identified as potential improvements for the system, these were:

- The service agreement between the sexual health department and HDUHB ICT has exceeded its review date;
- System administrator responsibilities are not formally documented with a risk of concentration of knowledge in one member of with responsibility for the administration and upkeep of the system;
- The Lilie system has provision for strong passwords i.e. contain number, special character, length and expiry date, however this functionality is not currently activated and used by the service.
- Whilst there is an audit trail of user activity within the system, inappropriate access to patient information is not actively monitored or reported;
- The service schedule agreement between the department and HDUHB ICT which sets out the arrangements for backup of the system and testing of the process, testing of backups could not be evidenced therefore we cannot be certain this has been done successfully; and
- Departmental business continuity arrangements have been communicated to staff in the form of an email; while this is a good practice in itself, the email was sent some time ago.

## **5. Assurance Summary**

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

| Audit Objective |   | Assurance Summary*  |  |   |   |
|-----------------|---|---|--|---|---|
|                 |   |  |  |  |  |
| <b>1</b>        | Ensure that an appropriate governance process is in place for the system.   |   |  | ✓   |   |
| <b>2</b>        | Ensure appropriate control is maintained over the database.   |   |  |   | ✓   |
| <b>3</b>        | System input should be authorised, complete, accurate, timely and input once only.  |   |  |   | ✓   |
| <b>4</b>        | Proper control is exercised over access to application systems.   |   |  | ✓   |   |
| <b>5</b>        | Controls are in place to ensure the accuracy, completeness, confidentiality and timeliness of output, reports and interfaces.   |   |  |   | ✓   |
| <b>6</b>        | Ensure a complete audit trail is maintained which allows an item to be traced from input through to its final resting place.  |   |  | ✓   |   |
| <b>7</b>        | Ensure business continuity arrangements are in place with include backing up copies of data and programs, storing and retaining them securely, and recovering applications in the event of failure. |   |  | ✓   |   |

\* 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 three issues that are classified as weakness in the system control/design for the Lilie Departmental IT system.

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

## **Operation of System/Controls**

The findings from the review have highlighted nine issues that are classified as weakness in the operation of the designed system/control for the Lilie Departmental IT system.

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

## **6. Summary of Audit Findings**

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

### **OBJECTIVE 1: Ensure that an appropriate governance process is in place for the system.**

The following areas of good practice were noted:

- a contract is in place between the Health Board and the vendor for the maintenance of the system;
- the contract includes key areas and performance metrics required to monitor service and sets out required responsibilities around information governance;
- there is a service agreement for the system between the sexual health department and Health Board ICT department;
- a service call resolution tracker is maintained by the department to monitor reported issues with the system;
- upgrades for the system have been received and there are plans for future upgrades to take place;
- as part of the original implementation project a user group was established, Terms of Reference were created and meetings were minuted;
- there is a system administrator who is tasked with the admin and upkeep of the system, she extremely knowledgeable in relation to the system and responsibilities in terms of the role are understood;



- the system administrator role is supported when necessary by a small group of other members of staff classed as super users;
- when required the system administrator is supported by members of staff from the health boards ICT department for more technical aspects of the system admin role.

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

- The service agreement between the sexual health department and Health Board ICT Department has exceeded its review date; historically it was reviewed annually however documentation provided shows this was last done in 2016.
- The system administrator who is a PA to the consultants understands the responsibilities in terms of the role; however, these responsibilities are not formally documented. There is a risk associated with the concentration of knowledge in one member of staff with responsibility for the administration and upkeep of the system. Whilst the role has been supported in the past by a small group of super users, only some of the knowledge and expertise of the system administrator has been cascaded.

We note the following Low priority findings in relation to this objective:

- The ICT service agreement states that all calls relating to the system should be logged via the ICT helpdesk, this is to ensure that when it comes to review the performance all calls are considered. This is not always done as some calls are opened directly with the vendor, not a problem in itself as in some cases there is no requirement for ICT input but the department should ensure that these are logged with ICT retrospectively.
- Discussions with key staff identified that whilst the Lilie Prescribing Module had been purchased it was abandoned after testing because of the complexity of the module. Internal Audit reviewed the maintenance contract for the system and found that it still contains provision for the abandoned Prescribing Module.
- As part of the original implementation project, a user group was established with ToR and Minutes produced. However, this group fell into abeyance after 2017. While some of its duties were absorbed into other service group meetings, the service and system users would benefit from its re-establishment in order to provide a more suitable forum for identifying and improving the system and its use.

**See Finding 1-5 at Appendix A.**

**OBJECTIVE 2: Ensure appropriate control is maintained over the database.**

The following areas of good practice were noted:

- the application database sits within the organisations virtual environment and is supported with patch management under the arrangements for this environment;
- Evidence was provided to show the database had been patched at the time of audit;
- there are links with the Health Bard ICT and application vendor to address performance issues should they arise.

**No matters arising.**

**OBJECTIVE 3: System input should be authorised, complete, accurate, timely and input once only.**

The following areas of good practice were noted:

- data quality is enforced at input with controls governing what fields are mandatory, data types and upper and lower limits;
- The process for maintaining standing data items is documented and understood by the system administrator.

**No matters arising.**

**OBJECTIVE 4: Proper control is exercised over access to application systems.**

The following areas of good practice were noted:

- a process with appropriate segregation exists for granting new users access to the system;
- when a user is set up by the system admin, they in turn are only granted access to the parts of the database that are required for there are of responsibility;
- leavers are appropriately processed by the system admin by moving them from a live group to a non-live state;

- all users receive job specific training from the system admin prior to receiving their user ID and password;
- user guides are supplied by the vendor and are updated for every major release of the system;
- There is evidence that the Health Board has updated the system and the service are planning to implement a further update which was released in May 2019.

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

- The Lilie system has provision for strong passwords i.e. contain number, special character, length and expiry date, however this functionality is not currently activated.

We note the following Low priority findings in relation to this objective:

- System access is allocated on an individual basis and not using role based access. When a user is created by the system admin, they are manually granted access to the required sections of the system. This is a labour intensive exercise, as it has to be repeated for each user.
- As a result of our testing of access to the system some additional findings were noted which also require management attention:
  - 4 members of staff have multiple usernames with different roles and 2 members of staff have multiple Roles assigned to the same username. This differs from the standard practice at the Health Board it should be investigated for appropriateness.
  - 5 super users are listed in the system, this includes one band 2 member of staff, these should be assessed to ensure the level of access is appropriate for the level of responsibility within the organisation.
- Training on the system takes place in the live environment, training ID's and dummy clients are created on the system and changes are then undone for the next cohort. Training in this way presents the risk of affecting live data and clients on the system.

**See Findings 6-8 at Appendix A.**

**OBJECTIVE 5: Controls are in place to ensure the accuracy, completeness, confidentiality and timeliness of output, reports and interfaces.**

The following areas of good practice were noted:

- there are a number of reports available to the user and there is specialist support from the Health Board informatics department when needed;
- reports are checked by an appropriate member of staff before any information is published;
- there are organisation wide restrictions on moving data to physical media and where reports are printed, printer selection is predefined.

**No matters arising.**

**OBJECTIVE 6: Ensure a complete audit trail is maintained which allows an item to be traced from input through to its final resting place.**

The following areas of good practice were noted:

- the system has the ability to log user activity events in an audit trail, testing showed this functionality to have been enabled;
- system security logging has been enabled to allow the software vendors to identify incidents and correct errors.

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

- Whilst there is an audit trail of user activity within the system, inappropriate access to patient information is not actively monitored or reported.

**See Finding 9 at Appendix A.**

**OBJECTIVE 7: Ensure business continuity arrangements are in place with include backing up copies of data and programs, storing and retaining them securely, and recovering applications in the event of failure.**

The following areas of good practice were noted:

- the architecture supporting the Lilie system sits within the Health Board's virtual environment. This environment is well designed and allows resources to be shared, thus ensuring resilience;
- departmental business continuity arrangements have been communicated to staff;

- disaster recovery plans have been agreed with the ICT department, these are contained in the Lilie service schedule document;
- responsibilities in relation to disaster recovery have been clarified and communicated and mechanism exists for capturing data in downtime;
- there is a service schedule agreement between the department and Health Board ICT, this document sets out the arrangements for backup of the system.

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

- While there is a service schedule agreement between the department and HDUHB ICT which sets out the arrangements for backup of the system and testing of the process, testing of backups could not be evidenced therefore we cannot be certain this has been done successfully. This issue and its associated risk has been reported within the organisation and the ICT department have agreed a testing programme based on selecting samples of systems on a rotating basis.
- Departmental business continuity arrangements have been communicated to staff in the form of an email; while this is a good practice in itself, the email was sent some time ago.

**See Finding 10-11 at Appendix A.**

## **7. Summary of Recommendations**

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

A summary of these recommendations 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>0</b> | <b>6</b> | <b>5</b> | <b>11</b>    |

| <b>Finding - 01 - ICT service agreement review (O)</b>   | <b>Risk</b>  |
|--|--|
| <p>The service agreement between the sexual health department and HDUHB ICT has exceeded its review date; Historically it was reviewed annually however documentation shows that this was last done in 2016.</p>   | <p>The Health Board may not maximise the benefits from the system.</p> |
| <b>Recommendation</b>  | <b>Priority level</b>  |
| <p>The service agreement between the sexual health department and the ICT department should be jointly reviewed annually; discussions should include a review of performance levels and call resolution times.</p>   | <p><b>Medium</b></p>   |
| <b>Management Response</b>   | <b>Responsible Officer/ Deadline</b>                                   |
| <p>Meeting arranged with Paul Solloway Head of ICT on 11<sup>th</sup> December 2019 to discuss annual review schedule of the service agreement and overall performance of the Sexual Health IT system Lillie. The review will include contracting arrangement, performance of system e.g. call resolution etc. and interface between HDUHB ICT and Idox.</p> | <p>Lisa Humphrey/Paul Solloway<br/>11<sup>th</sup> December 2019</p>   |

|   |  |
|---|--|
| <p><b>Finding - 02 - Calls logged via the ICT helpdesk (O)</b></p>  | <p><b>Risk</b></p>   |
| <p>The ICT service agreement states that all calls relating to the system should be logged via the ICT helpdesk, this is to ensure that when it comes to review the performance all calls are considered.</p> <p>This is not always done as some calls are opened directly with the vendor, this isn't an issue for specific calls, as in some cases there is no requirement for ICT input. However these calls will then not be factored into performance monitoring..</p> | <p>The Health Board may not maximise the benefits from the system.</p> |
| <p><b>Recommendation</b></p>  | <p><b>Priority level</b></p>   |
| <p>As stated in the ICT service agreement, all calls relating to the system should be logged via the ICT helpdesk, either initially or retrospectively.</p>   | <p><b>Low</b></p>  |
| <p><b>Management Response</b></p>   | <p><b>Responsible Officer/ Deadline</b></p>                            |
| <p>All calls will be logged via HDUHB ICT helpdesk in the first instance prior to escalation to idox.</p>   | <p>Lisa Humphrey 9<sup>th</sup> December 2019</p>                      |



|   |  |
|---|--|
| <p><b>Finding - 03 - Prescribing module not used (O)</b></p>  | <p><b>Risk</b></p>   |
| <p>Discussions with key staff identified that whilst the Lilie Prescribing Module has been purchased it was abandoned after testing because of the complexity of the module. Internal Audit reviewed the maintenance contract for the system and found that it still contains provision for the abandoned Prescribing Module.</p> | <p>the organisation does not gain full value from its investment</p> |
| <p><b>Recommendation</b></p>  | <p><b>Priority level</b></p>   |
| <p>The department should hold discussions with ICT and the system vendor to explore options for removing the prescribing module from its maintenance contract if it is no longer required.</p>  | <p><b>Low</b></p>  |
| <p><b>Management Response</b></p>   | <p><b>Responsible Officer/ Deadline</b></p>                          |
| <p>Contracting arrangement with idox will be included as part of the annual review with HDUHB ICT.</p>  | <p>11<sup>th</sup> December 2019</p>                                 |

| <b>Finding - 04 - User Group Meetings (O)</b>   | <b>Risk</b>   |
|---|---|
| <p>As part of the original implementation project, a user group was established with ToR and Minutes produced. However, this group fell into abeyance after 2017.</p> <p>While some of its duties were absorbed into other service group meetings, the service and system users would benefit from its re-establishment in order to provide a more suitable forum for identifying and improving the system and its use.</p> | <p>The Health Board may not maximise the benefits from the system.</p>    |
| <b>Recommendation</b>   | <b>Priority level</b>   |
| <p>The user group should be re-established, the service would also benefit from IT involvement to this user group to discuss upgrades, ongoing calls and poor service etc.</p>  | <p><b>Low</b></p>   |
| <b>Management Response</b>  | <b>Responsible Officer/ Deadline</b>                                      |
| <p>The user group will be re-established from January 2020, TOR will be reviewed to include representation from HDUHB ICT and Informatics team and will focus on the more technical aspects of the Lillie system.</p>   | <p>Lisa Humphrey<br/>Paul Solloway<br/>Gareth Beynon<br/>January 2020</p> |

| <b>Finding - 05 - System Administrator role (D)</b>   | <b>Risk</b>  |
|---|--|
| <p>The system administrator who is a PA to the consultants understands the responsibilities in terms of the role; however, these responsibilities are not formally documented.</p> <p>There is a risk associated with the concentration of knowledge in one member of with responsibility for the administration and upkeep of the system. Whilst the role has been supported in the past by a small group of super users, only some of the knowledge and expertise of the system administrator has been cascaded.</p>  | <p>The Health Board may not maximise the benefits from the system.</p> |
| <b>Recommendation</b>   | <b>Priority level</b>  |
| <p>Responsibilities in relation to the system administrator and super users should be formally documented and communicated. Additionally, opportunities to share knowledge and upskill the super user group should be explored.</p>   | <p><b>Medium</b></p>   |
| <b>Management Response</b>  | <b>Responsible Officer/ Deadline</b>                                   |
| <p>The roles and responsibility and job profile of the system administrator will be formally documented and shared with the team. It is recognised that not all super users have the technical skill of the system administrator however a formal training program will be developed to improve knowledge and skills of the super users to allow continuity in the absence of the system administrator. To improve technical support a more integrated approach with HDUHB ICT should be agreed and will be formally discussed at the meeting on 11<sup>th</sup> December 2019.</p> | <p>Lisa Humphrey<br/>31<sup>st</sup> January 2020</p>                  |

| <b>Finding - 06 - Training on live system (D)</b>   | <b>Risk</b>  |
|---|--|
| <p>Training on the system takes place in the live environment, training ID's and dummy clients are created on the system and changes are then undone for the next cohort. Training in this way presents the risk of affecting live data and clients on the system.</p>  | <p>Loss or corruption of data.</p>                                       |
| <b>Recommendation</b>   | <b>Priority level</b>  |
| <p>The service should explore options of creating a training and testing environment separate to the main live system, changes to these environments could be rolled back by IT saving the system administrator time and reducing the risk of affecting live data and clients on the system.</p>                                      | <p style="text-align: center;"><b>Low</b></p>                            |
| <b>Management Response</b>  | <b>Responsible Officer/ Deadline</b>                                     |
| <p>Historically a training platform was provided by Idox however this was withdrawn during a system upgrade in 2018. Idox will only reinstate at a cost to the service. Contacting arrangement will be reviewed on 11<sup>th</sup> December 2019 with HDUHB ICT to include negotiating purchase of a dedicated training platform.</p> | <p>Lisa Humphrey<br/>Paul Solloway<br/>11<sup>th</sup> December 2019</p> |

| Finding - 07 - user access by role (O)  | Risk   |
|---|--|
| <p>As a result of our testing of access to the system some additional findings were noted which also require management attention:</p> <ul style="list-style-type: none"> <li>• 4 members of staff have multiple usernames with different roles and 2 members of staff have multiple Roles assigned to the same username. This differs from the standard practice at the Health Board it should be investigated for appropriateness.</li> <li>• 5 super users are listed in the system, this includes one band 2 member of staff, these should be assessed to ensure the level of access is appropriate for the level of responsibility within the organisation.</li> </ul> | <p>Inappropriate access to system / data; and</p> <p>The Health Board may not maximise the benefits from the system.</p> |
| Recommendation  | Priority level   |
| <p>The health board should use the functionality of the system to develop and implement role-based access of the system for groups of users instead of individually.</p> <p>The department should also review the minor issues identified above following Internal Audits testing of access to the system.</p>  | <p style="text-align: center;"><b>Low</b></p>  |

| <b>Management Response</b>  | <b>Responsible Officer/ Deadline</b>                   |
|---|--|
| <p>The 4 members staff with multiple usernames with different roles will be investigated and addresses as different roles only require one user name per person.</p> <p>The band 2 member of staff is a super user with the appropriate level of responsibility. That staff member is currently undergoing a pay band review to reflect the responsibility.</p> | <p>Lisa Humphrey<br/>28<sup>th</sup> February 2020</p> |

|   |  |
|---|--|
| <p><b>Finding - 08 - strong passwords (O)</b></p>   | <p><b>Risk</b></p>   |
| <p>The Lilie system has provision for strong passwords i.e. contain number, special character, length and expiry date, however this functionality is not currently activated and used by the service.</p> | <p>Inappropriate access to system / data; and<br/><br/>The Health Board may not maximise the benefits from the system.</p> |
| <p><b>Recommendation</b></p>  | <p><b>Priority level</b></p>   |
| <p>The service should activate the system functionality in relation to strong passwords.</p>  | <p style="text-align: center;"><b>Medium</b></p>   |
| <p><b>Management Response</b></p>   | <p><b>Responsible Officer/ Deadline</b></p>  |
| <p>The strong password function will be activated with immediate effect.</p>  | <p>Lisa Humphrey<br/>16<sup>th</sup> December 2019</p>   |

| <b>Finding - 09 - Inappropriate access to patient information (D)</b>  | <b>Risk</b>   |
|--|---|
| <p>Whilst there is an audit trail of user activity within the system, inappropriate access to patient information is not actively monitored or reported.</p>   | <p>Inappropriate access to system / data.</p>         |
| <b>Recommendation</b>  | <b>Priority level</b>                                 |
| <p>Because of the sensitive nature of the information held within the Lilie PAS system the department should seek advice from the Health Board Information Governance Department as to whether the current level of audit trail is sufficient to monitor inappropriate access to patient information.</p> <p>Consideration should be given to whether or not the system could be included in the list of systems monitored by the NIIAS (National Intelligent Integrated Audit Solution) or if this is unfeasible, explore options with the vendor to monitor inappropriate patient record access.</p> | <p><b>Medium</b></p>                                  |
| <b>Management Response</b>   | <b>Responsible Officer/ Deadline</b>                  |
| <p>Option to audit user activity will be explored with the NIIAS (National Intelligent Integrated Audit Solution) to reflect the governance process of the health board.</p>   | <p>Lisa Humphrey<br/>31<sup>st</sup> January 2019</p> |



| <b>Finding - 10 - Testing backup process (O)</b>   | <b>Risk</b>  |
|--|--|
| <p>While there is a service schedule agreement between the department and HDUHB ICT which sets out the arrangements for backup of the system and testing of the process, testing of backups could not be evidenced therefore we cannot be certain this has been done successfully.</p> <p>This issue and its associated risk has been reported within the organisation and the ICT department have agreed a testing programme based on selecting samples of systems on a rotating basis.</p> | <p>Loss of processing / data.</p>                      |
| <b>Recommendation</b>  | <b>Priority level</b>                                  |
| <p>In order to ensure the data for the Lilie system is recoverable the system owner should request that the backup of the system be tested for validity and re-tested at a frequency deemed appropriate.</p>   | <p><b>Medium</b></p>                                   |
| <b>Management Response</b>   | <b>Responsible Officer/ Deadline</b>                   |
| <p>Testing backups process will be included in the annual review discussed with the Head of HDUHB ICT on 11<sup>th</sup> December 2019.</p>  | <p>Paul Solloway<br/>11<sup>th</sup> December 2019</p> |

| <b>Finding - 11 - Continuity process (O)</b>   | <b>Risk</b>   |
|--|---|
| <p>Departmental business continuity arrangements have been communicated to staff in the form of an email; while this is a good practice in itself, the email was sent some time ago.</p> | <p>Loss of processing / data.</p>                     |
| <b>Recommendation</b>  | <b>Priority level</b>                                 |
| <p>Local business continuity arrangements for the loss of the Lilie system should be formally documented and reviewed annually to ensure they are still applicable and feasible.</p>     | <p style="text-align: center;"><b>Medium</b></p>      |
| <b>Management Response</b>   | <b>Responsible Officer/ Deadline</b>                  |
| <p>The business continuity arrangement process will be documented and reviewed by the user group prior to cascading to the sexual health team.</p>                                       | <p>Lisa Humphrey<br/>31<sup>st</sup> January 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.

| <b>Priority Level</b> | <b>Explanation</b>  | <b>Management action</b> |
|-----------------------|---|--------------------------|
| <b>High</b>           | Poor key control design OR widespread non-compliance with key controls.<br>PLUS<br>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.<br>PLUS<br>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.<br>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