Audit Committee				
Meeting Date	**31st July 2018**		**Agenda Item**	**2a**
Report Title	**Update Report – National Data Centre Outages**			
Report Author	Matt John, Interim Chief Information Officer			
Report Sponsor	Pam Wenger, Director of Corporate Governance , SIRO			
Presented by	Matt John, Interim Chief Information Officer Carl Mustad, Head of ICT Operations			
Freedom of Information	Open			
Purpose of the Report	The purpose of this paper is to provide an update to Audit Committee Members on the recent national data centre outages; the clinical risk associated with them; and progress on the management and assurance regarding data centre outages.			
Key Issues	The availability of key clinical IT systems to ABMU clinicians and staff			
Specific Action Required ***(please ✓one only)***	**Information**	**Discussion**	**Assurance**	**Approval**
	✓			
Recommendations	The Audit Committee are asked to: • **Note** the recent national data centre outages and the impact on HB services • **Note** the effective business continuity plans enacted by HB staff • **Note** the actions undertaken to increase assurances • **Support** the further actions required			

UPDATE REPORT – NATIONAL DATA CENTRE OUTAGES

1. Background

Since January 2018, there have been three major incidents at the national data centres which have caused concurrent outages to multiple national services (Jan 24, March 21 and April 24). Each of these resulted in significant disruption to clinical services across NHS Wales and required local business continuity processes to be invoked.

There have also been a significant number of other major incidents within the national data centres which have resulted in single national system failures, for example WLIMS (Pathology) and Cancer Information System Cymru (CANISC).

The most significant multi-system incident occurred on 24 January 2018, where firewall failures at both national data centres resulted in a loss of numerous national IT systems for up to 5 hours, including Pathology (WLIMS), all GP systems, the Welsh Clinical Portal, CANISC and the Internet. This outage also caused failure for users of local systems, due to a reliance on national authentication services. The March incident affected electronic Master Patient Index (eMPI), WLIMS, email, intranet, Welsh Clinical Portal, CANISC – and as a result multiple operational services were affected across NHS Wales. In the April incident, similar services were affected but given their intermittent manner, not all users were affected.

While the impact of each multiple outage was different, an ABMU business continuity debrief, identified the following impacts:

- Risk to patients requiring timely pathology results.
- Risk to patients with consultations, creating anxiety for clinicians and patients as a result of the inability to view all patient records.
- Delays in patient flows within hospital services and GP surgeries.
- Some patients required repeat diagnostics as a result of the inability to process pathology samples.
- Rescheduling of some patient appointments as a result of the inability to view patient records/results.
- Communication challenges in contacting large number of general practices and hospital medical teams and departments.
- Recovery period prolonged in some areas as a result of retrospective re-checking of patient treatment pathways, pathology results etc.

The biggest issue identified from the incidents was the delay in processing pathology results and our review identified that some patients had to be re-bled where results were needed urgently. Our business continuity arrangements for processing urgent blood results in the event of WLIMS failure mitigated against the risk of harm. As a result of the system failure, we are aware that some patient care was delayed, but we have not received any reports from clinical staff that indicate that a delay had a negative or harmful impact on the health of patients.

The Chief Executive wrote an 'Accounting Officer' letter (Appendix 1) to Velindre on 27th April setting out the Board's concerns about the serious governance risk and patient safety risk for the organisation and this was also included in the Board's governance statement for 2017/18. The Director of NWIS, Andrew Griffiths, provided a detailed response to the letter (Appendix 2) indicating that a number of actions have/are being taken forward to offer additional assurance. Accompanying the letter were a Serious Incident Report regarding the incident that occurred on 24th January 2018 and a further Briefing Document following the incident on 21st March 2018. Andrew Griffiths also offered to meet the CEO to discuss further – this meeting took place on July 11th.

2. Further Incidents

During July there have been two further incidents. The first incident affected the WLIMS, causing disruption for approximately 4.5 hours on Saturday am 7 July 2018. The Health Board was able to cope with this incident very effectively, since there was already a planned WLIMS downtime scheduled for that afternoon. The business continuity shifted to the morning and the planned maintenance was cancelled. The second incident related to an antivirus software update that was applied at the national data centres, and blocked

access to WLIMS, the Welsh Patient Administration System (WPAS), Canisc, and integration services for just over an hour on the morning of Friday 13 July 2018.

3. Assurance regarding Incidents

Each Health Board and Trust is currently in a different position regarding both the service unavailability from incidents at the national data centres, and also with regards to assurance. There is an active dialogue with NHS Wales Informatics Service (NWIS) Directors, an increased understanding of the causes; remedial actions taken; and actions planned. Some organisations have received a briefing report on all major incidents affecting their organisation. Others are seeking further assurance on root cause analysis, copies of Serious Incident (SI) reports to Welsh Government and to review mitigation's in order to satisfy their board and staff.

Health Board/Trust Assistant Directors of Informatics (ADIs) remain committed to working with NWIS Directors to further improve communications and the sharing of sufficient detail at an architectural and technical level to increase confidence.

4. Improvements and Further Actions Required

In response to each incident, NWIS colleagues have worked hard to achieve resolution in a timely manner and attempt to keep Health Board/Trust Informatics Leads informed of progress. NWIS investigate each serious incident and identify findings and recommendations. There are a number of actions agreed between Health Boards/Trusts and NWIS to address the issues identified, however, there are some areas where further support/action is recommended.

5. Governance and the Role of Infrastructure Management Board (IMB)

The Infrastructure Management Board (IMB) has been established for many years to discuss, plan and review infrastructure changes that are implemented across NHS Wales and also share learning and best practice that has been implemented within local services. The IMB is attended by technical infrastructure leads (who generally report to ADIs) from each Health Board/Trust and NWIS and is chaired by a Health Board/Trust technical lead.

It was recently agreed at the National Informatics Planning and Delivery Group (IPAD) that all significant infrastructure related incidents should be reported to IMB which is attended by NWIS/HB/Trust Technical Leads. IPAD also agreed that the role of the National Service Management Board (NSMB) should be reviewed and that in the interim, the IMB should report directly to IPAD.

IMB has agreed a series of actions to improve transparency on planned infrastructure changes and reporting of infrastructure related incidents. The Director of NWIS has agreed to provide a detailed timetable for implementing the agreed actions and improvements.

6. Incident Resolution Processes

In some cases the incidents have taken longer to resolve than anticipated. Understandably every incident is different, but there should be a systematic, prioritised and standardised process for incident resolution. For example, the concept of having two data centres is to provide a "failover" model, so that if a system fails in one data centre it can continue to run from the other data centre.

NWIS has undertaken a review of its "System Restoration Plan for Multiple Concurrent Service Failures" and is making some changes to improve this. Once the revised plan is complete, it will be presented to Health Board leads via the Infrastructure Management Board for further assurance.

7. National Infrastructure

NWIS has reported that some of the recent problems have occurred on equipment that is around 7 years old and that greater investment is needed to replace aging infrastructure and systems before they start to

fail. NWIS have commissioned an external review of key elements of the data centre infrastructure. The Infrastructure Management Board will support this work and make local technical leads available to work with NWIS colleagues on the review.

8. Communication and Reporting

There are NWIS and local ICT incident response plans and an NHS Wales Incident Communication Framework. When national incidents occur, NHS Wales Informatics Service (NWIS) service desk personnel inform all Health Board and Trusts service desks. These incidents are then communicated through local escalation processes. Depending on the scale of the incident, a national incident management group is initiated with representation from each Health Board and Trust, NWIS Directors and NWIS service leads. All incidents are subsequently reported to the relevant Service Management Board (SMB).

Early and regular communication between NWIS and Informatics teams is critical for all incidents. Whilst NWIS endeavour to facilitate this, there is room for improvement in terms of timeliness, consistency and communication processes.

Welsh Government have worked with NWIS and Health Board representatives to create a new communications protocol that will be used during significant outages. This protocol has been developed to ensure Welsh Government are sighted on the outages and provide a consistent message to the public working with Health Board/Trust communications teams.

NWIS have procured a new emergency communications system (Blackberry AtHoc Alerts) to enable timely notifications to multiple recipients. Health Board Informatics leads will work closely with NWIS to ensure this is implemented effectively.

The regular reporting of the root causes of incidents and the lessons learned has not always been clear or timely. Over recent incidents, the timeliness of providing an initial brief has improved. For example, following the incident that occurred on Friday 13 July 2018, NWIS submitted an executive briefing letter to Health Board/Trust CEOs and Executive Leads for Informatics on the next working day (Appendix 3). Andrew Griffiths has committed to making further improvements and will provide a reworked schedule for reporting deadlines.

9. Recommendations

The Audit Committee are asked to:

- Note the recent national data centre outages and the impact on HB services
- Note the effective business continuity plans enacted by HB staff
- Note the actions undertaken to increase assurances
- Support the further actions required

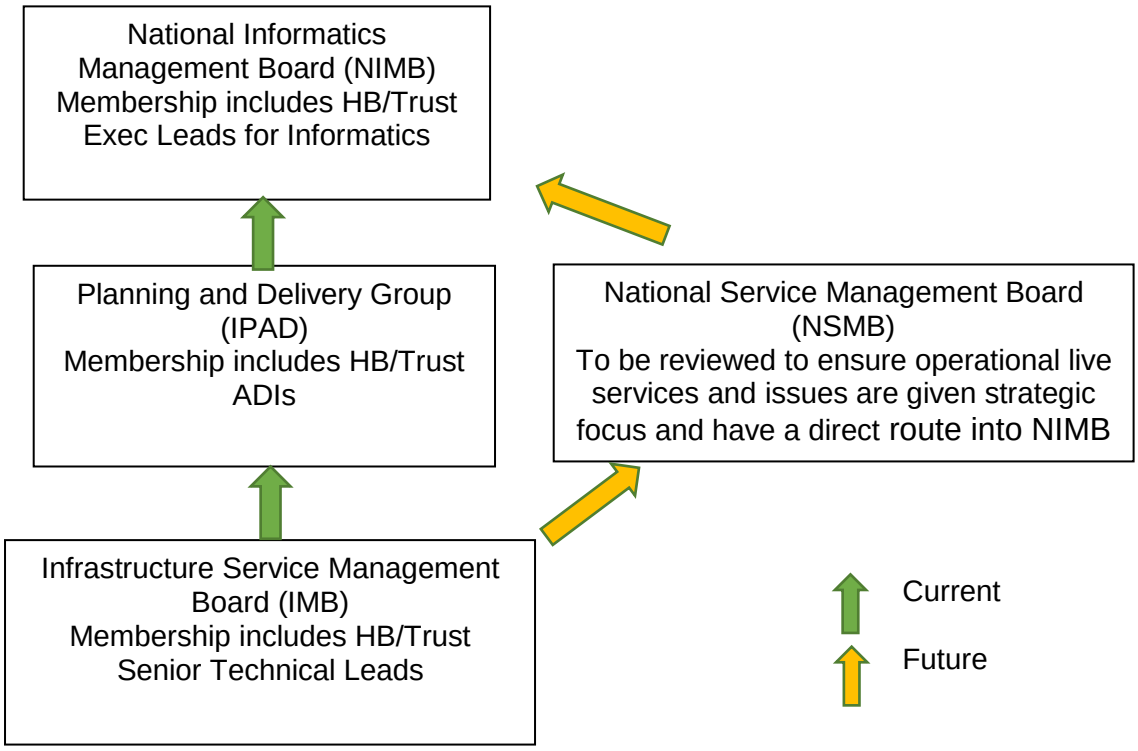
Appendix 1: Letter - ABMU CEO Accounting Officer

Appendix 2: Letter from Director of NWIS to ABMU CEO

Appendix 3: Letter from Director of NWIS re NWIS Business Continuity Incident 13 July 2018

Appendix 4: Governance of National Operational Live Services

Appendix 4: Governance of National Operational Live Services



Bwrdd Iechyd Prifysgol
Abertawe Bro Morgannwg
University Health Board

Our Ref: TCM/HL/tr

Date: 27th April 2018

ABMU Health Board
Headquarters
One Talbot Gateway, Seaway Parade,
Port Talbot
SA12 7BR

01639 683302
WHTN: 1787 3302

Steve Ham
Chief Executive
Velindre NHS Trust

Steve.Ham2@wales.nhs.uk

Dear Steve

NWIS Business Continuity Incidents

I am writing to you in your role as the accountable officer for NWIS to raise significant concerns that our Board has about the two serious incidents which occurred within NWIS on 24thJanuary and 21st March 2018. We are very disappointed to have been informed that the investigation into the incident on 24 January 2018 has not yet been concluded and that an extension for doing so has been requested from Welsh Government.

The failure of both National Data Centres on 24 January 2018 resulted in us having to declare a Level 3 Business Continuity /Significant Incident in ABMU. It resulted in a loss of 17 national IT systems including Pathology (WLIMS), all GP systems, the Welsh Clinical Portal and the Internet and intermittent failure of a further 7 local IT systems. Aside from a very brief update received after a month, the Health Board has received very little formally by way of an explanation as to what went wrong and what is being done to ensure this does not happened again.

The incident on 21 March 2018 also resulted in the Health Board declaring a Level 3 Business Continuity / Significant Incident due to intermittent disruption to key services such as WLIMS for a period of 1-2 hours. We understand that the cause this time was technical issues at one of the data centres, which raises questions for us about the adequacy of fail-over systems and processes and the design of the infrastructure.

These issues have been discussed in detail at our Audit Committee. These outages created a serious governance risk and patient safety risk for the organisation as well as undermining confidence.

In order to provide some assurance to my board it would be very helpful if you could share with me the actions NWIS has taken, the timescales for the investigation reports including the lessons learnt and plans put in place to mitigate the risks. I am also being asked to provide assurance to my board that robust business continuity arrangements are in place within NWIS and that they are doing everything they should to ensure there are no further incidents of this nature.

Whilst NWIS may being engaging with Welsh Government, I am sure that they recognise the impact on the service of such events and the need to keep their Health Board and Trust partners fully informed and updated when serious incidents occur. It seems that this is not happening and it would be very helpful if you could assist in ensuring this happens moving forward. From our perspective this would include timely receipt of any incident reports so that they can be considered in our own governance committees. We have not be able to provide such reports to date.

Hamish Laing our Medical Director is our Executive lead in this respect and responsible for giving confidence to our board which he's not felt able to do to date so a conversation or meeting with him might be helpful.

Board members here are very concerned so I'd welcome an early response so that I can keep them appraised

Thanks very much.

Yours sincerely

Tracy Myhill

TRACY MYHILL
CHIEF EXECUTIVE

c.c. Professor Hamish Laing, CIO ABMU

Tŷ Glan-yr-Afon
21 Heol Ddwyreiniol Y Bont-Faen, Caerdydd CF11 9AD
21 Cowbridge Road East, Cardiff CF11 9AD
Ffôn/Tel: 02920 500500

Tracy Myhill
Chief Executive
ABMU Health Board
Headquarters
One Talbot Gateway, Seaway Parade
Port Talbot
SA12 7BR

12th June 2018

Dear Tracy

NWIS Business Continuity Incidents

Further to your letter of 27th April 2018, addressed to Steve Ham in Velindre NHS Trust, I have set out below a response to the concerns raised from the perspective of the NHS Wales Informatics Service. As the Director of the Informatics Service, I am acutely aware of the impact of any service outage and consider myself personally responsible for ensuring that issues are addressed comprehensively and in a timely fashion. I am therefore keen to ensure that you have the information needed in order to assure yourselves that actions have been and continue to be taken in the manner that you would expect and I am happy to discuss any of these points further with you directly if that would be helpful.

Firstly, with regard to the issues themselves and the analysis of their cause and the corrective actions taken, I have attached to this letter the Serious Incident Report into the incident that occurred on 24th January 2018 and a further Briefing Document following the incident on 21st March 2018. You will note that both incidents have been fully investigated, involving the third party suppliers where applicable, and a number of corrective actions have already been undertaken.

You mention in your letter the option to failover services, in this case the WLIMs; as you would expect the design of the infrastructure allows for failover to an alternative data centre. In the case of WLIMS, the complexity of the service and the process required to failover can take a number of hours to complete and therefore a 2 hours contingency has been introduced during which time a decision is made. A decision to failover is only made if expectations of outage exceed this time.

We recognise that in the event of any loss of service pro-active communications are key and that was certainly the case with the two incidents in the data centre. At a senior management level we link in with the Assistant Directors of Informatics, in these two cases arranging regular telephone calls to update on the situation, and subsequently to share the outcome of the investigations via the Informatics Planning and Delivery Group (IPAD) forum; As well as issuing a notification as soon as the

Tŷ Glan-yr-Afon
21 Heol Ddwyreiniol Y Bont-Faen, Caerdydd CF11 9AD
21 Cowbridge Road East, Cardiff CF11 9AD
Ffôn/Tel: 02920 500500

incident occurs and regular updates via our Service Desk to the Health Board Service Desks for local escalation.

I note in the ABMU Debrief Report the point was raised about the lack of any notification to the Health Board Communications Team *"and therefore, dealing with media enquiries was difficult, particularly with regard to the queries in relation to Cyber Security."* This is currently being considered as part of the procedural review with Welsh Government, as this is not currently an action assigned to NWIS; In the majority of cases I would anticipate that the Health Board will be better placed to understand the specific impact on their services of any issues with their IT Services and we respect your decisions in terms of wider communications.

The Infrastructure Management Board, whose members include representatives from all of the Health Boards and Trusts, in ABMU's case Carl Mustad, has discussed these issues in detail and has overseen all activities in terms of both the remedial actions as well as the additional measures that we are taking for further assurance.

In addition to regular audits in relation to our ISO Accreditation status for ISO 20000-1 IT Service Management Systems, NWIS already has a number of external technical audits that are undertaken periodically on key components of the infrastructure. These include an Active Directory Risk Assessment, Exchange (Email) risk assessment and Microsoft SQL (Database) supportability reviews. Work to commission external reviews of the following is also now underway:

- Data Centre Networks and Firewalls
- NWIS Citrix estate (used in the delivery of LIMS, WPAS, CANISC and others).
- Backup systems

To provide additional assurance and identify any further remedial actions.

In summary we have had very few incidents in the provision of data centre services across NHS Wales but we are very aware of the impact of any disruption in service provision and have taken actions not only to ensure that the specific issues have been addressed but also to ensure that the resilience of these services is robustly tested and any additional measures taken. In doing so, we work closely with the Health Boards through the Infrastructure Management Board, Service Management Boards, IPAD and the National Informatics Management Board and I will ensure that we continue to do so.

I am happy to discuss any of these points further when we meet on 11th July 2018.

Yours Sincerely

Tŷ Glan-yr-Afon
21 Heol Ddwyreiniol Y Bont-Faen, Caerdydd CF11 9AD
21 Cowbridge Road East, Cardiff CF11 9AD
Ffôn/Tel: 02920 500500

Andrew Griffiths

Chief Information Officer NHS Wales
Director of NHS Wales Informatics Service

cc: Hamish Laing
Matt John

Tŷ Glan-yr-Afon
21 Heol Ddwyreiniol Y Bont-Faen, Caerdydd CF11 9AD
21 Cowbridge Road East, Cardiff CF11 9AD
Ffôn/Tel: 02920 500500

To: HB/Trust Chief Executives
CC: NIMB Members
ADIs

16th July 2018

Dear Chief Executive,

Executive Briefing: Informatics Business Continuity Incident

Further to my letter of 25 June 2018 regarding incidents affecting our National Data Centres and recognising the potential impact that these incidents can have on the delivery of Health Services, I will for the foreseeable future send a specific update to yourselves on any such incidents. The incidents themselves will continue to be managed through the usual processes with the Service Management and Infrastructure Management Boards.

Incident: Friday 13th July 2018
On Friday 13th July 2018 at 09:11, around 250 servers were affected by an antivirus update which enabled individual firewalls on servers. This update prevented users from accessing the following systems:

- Canisc
- WLIMS
- WPAS – some instances
- Integration Services (some feeds between systems)

In accordance with our change control procedures, this update had previously been deployed within the test environment without issue. To resolve the issue the patch was rolled back and access to systems were restored at 10:23, with confirmation of closure of the incident at 10:41. In total approximately 100 calls were received in relation to this outage, and the outage lasted approximately 1 hour and 24 minutes.

An update was provided to your Assistant Director of Informatics on Friday and a full Major Incident (MI) review will be undertaken in due course. If you require any more information, or would like further clarification, please do not hesitate to contact me

Yours Sincerely,

Andrew Griffiths

Chief Information Officer NHS Wales
Director of NHS Wales Informatics Service