AGENDA ITEM
(2.2.2)

DIGITAL & DATA COMMITTEE

RESPONSE TO CYBER ASSURANCE LETTER FROM WELSH GOVERNMENT

Date of meeting	(15.12.2020)
FOI Status	Open/Public
If closed please indicate reason	Not Applicable - Public Report
Prepared by	Karen Winder ADI ICT Interim
Presented by	Clare Williams Executive Director of Planning and Performance
Approving Executive Sponsor	Executive Director of Planning & Performance
Report purpose	FOR NOTING

Engagement (internal/external) undertaken to date (including receipt/consideration at Committee/group)		
Committee/Group/Individuals	**Date**	**Outcome**
(Insert Name)	(DD/MM/YYYY)	Choose an item.

ACRONYMS	
CTM	Cwm Taf Morgannwg
NCSC	National Cyber Security Centre
NIS	Network and Information Security
OSSMB	Operational Security Service Management Board

RAGCSB	Risk, Audit, Governance and Cyber Security Board
IMB	Infrastructure Management Board

1. SITUATION/BACKGROUND

1.1 A letter, **Appendix** 1, was sent to all Chief Executives by Ifan Evans, Director – Technology, Digital & Transformation in October 2020. The letter required assurance from the health boards around: Cyber Security and confirmation that the organisation is in contact with NCSC and signed up to the NCSC Cyber Security.

1.2 Incident response plans are in place and updated as appropriate. If a cyber incident is detected, there is a standard NCSC incident reporting process which involves promptly reporting to the NCSC and Welsh Government, collect and share all relevant information, and involve information governance leads if there is any possibility of a data breach or loss of data.

1.3 Welsh Government have engaged a specialist cyber security consultancy firm with experience in establishing NIS regulatory frameworks in other settings to support the development of the compliance framework and governance arrangements. Engagement will start work in November and it is important that all organisations engage with this process

2. SPECIFIC MATTERS FOR CONSIDERATION BY THIS MEETING (ASSESSMENT)

2.1 OSSMB has been the forum for all the Health Boards' discussions around the cyber security discussions. The CTM Cyber Security team will be taking the lead for the Health Board in ensuring it is compliant under the regulation. It will be reported to the ICT RAGCSB at the next meeting in November as well as ensuring it is added as a standard agenda item. The Cyber Team will be working with colleagues within IG as the regulation has the type of financial penalties as in the Data Protection Act. This will also be added as standard agenda items to the national boards - IMB and OSSMB.

2.2 CTM can also confirm that all the members of the Cyber Security team are signed up to the NCSC CiSP.

3. KEY RISKS/MATTERS FOR ESCALATION TO BOARD/COMMITTEE

3.1 No escalation required

4. IMPACT ASSESSMENT

Quality/Safety/Patient Experience implications	There are no specific quality and safety implications related to the activity outined in this report.
Related Health and Care standard(s)	Governance, Leadership and Accountability
	If more than one Healthcare Standard applies please list below:
Equality impact assessment completed	Not required
Legal implications / impact	There are no specific legal implications related to the activity outlined in this report.
Resource (Capital/Revenue £/Workforce) implications / Impact	There is no direct impact on resources as a result of the activity outlined in this report.
Link to Strategic Well-being Objectives	Co-create with staff and partners a learning and growing culture

5. RECOMMENDATION

5.1 To note that CTM is compliant with the recommendations and requirements in the letter from Welsh Government