Strategic Risk owner	Strategic Objective	Risk Domain	Risk Title	Risk Description	Controls in place	Action Plan	Assuring Committees	Rating (current)	Heat Map Link (Consequence X Likelihood)	Rating (Target)	Trend	Opened	Last Reviewed	Next Review Date	Datix ID
Executive Director of Public Health - Interim Executive Lead responsible for ICT.	Provide high quality, evidence based, and accessible care.	Legal / Regulatory Statutory duty, regulatory compliance, accreditation, mandatory requirements	Ransomware Attack resulting in loss of critical services and possible extortion	**IF**: The Health Board suffers a major ransomware attack. **Then**: there could be potential data loss and subsequent loss of critical services. **Resulting in**: Catastrophic service loss to all clinical and business services impacting on population health management, patient care, business continuity, organisational relationships & substantial financial risk - culminating in a culture of mistrust of the UHB and all things digital	**Key Controls**: 1. Email filters from both Microsoft and the National email relay which scan for malicious and suspicious email types and their attachments. 2. National Checkpoint firewalls that monitor for and block suspicious network traffic, including those from known malicious geographical areas. 3. National SIEM that monitors and logs suspicious external incoming traffic. As well as monitoring local network traffic for each NHS Wales organisations. 4. Local Firewalls at each of the Health Board's geographical areas that only allows inbound trusted network traffic. 5. Anti-malware software installed on all Health Board computing devices which includes ransomware behavioural intelligence. 6. Blocking and monitoring of Internet traffic. 7. Locally systems that monitor the local network for suspicious traffic. 8. A monthly patching regime to ensure that all operating systems are up to date. 9. Regular backups of critical information and device configuration which is stored off site as part of DR/BC planning. **Gaps in Controls**: 1. Current National SIEM has presented many issues in terms of access to the Health Board for identifying issues and addressing false positives. 2. The Health Board is currently not addressing the need for the national Cyber Security training to become part of mandatory training to all staff. 3. A regular co-ordinated approach to providing Phishing campaigns as part of staff awareness to indicators of compromise. 4. A process where the Health Board can monitor where staff have read important information/cyber security policies. 5. The current network Intrusion Detection/Intrusion Protection system (IDS/IPS) is no longer licensed under the new generation firewall infrastructure.	The Health Board has purchased a Phishing tool which the ICT Department in co-operation with Information Governance and Counter Fraud are using to simulate Phishing attacks. This is to help educate staff and will be used to push the organisation to add the NHS Wales national cyber security awareness training as a mandatory core competency to all staff via ESR. The ICT Department are investigating ways to improve the security of backups to ensure that these are protected from potential ransomware attacks. The ICT Department are investigating ways to segregate the current configuration of the network infrastructure to ensure that critical clinical systems are better protected from cross infection. The ICT Department will be re-introduce Cisco FirePower which is an IDS/IPS networking software. The ICT Department will be reviewing the current local Cyber Incident Response Plan which will be escalated up to senior and board level management. The SIRO/cyber leads will be undertaking a programme of introducing the NCSC Board Level toolkit to provide knowledge of cyber to Board members. The organisation is recruiting a Director of Digital Services who will be a member of the Board. This position will enhance the complexities and needs of both service delivery and information/cyber risks.	Digital & Data Committee	20	C5 x L4	15 (C5xL3)	New Risk escalated by ICT Digital June 2021	26/05/2021	05/06/2021	25/06/2021	4664
~~Executive Director of Planning & Performance (ICT).~~ Executive Director of Public Health - Interim Executive Lead for ICT Bridgend Integrated Locality Group	Ensure sustainability in all that we do, economically, environmentally and socially.	Operational: • Core Business • Business Objectives • Environmental / Estates Impact • Projects Including systems and processes, Service /business interruption	IT Systems	**IF:** The Health board is unable to deliver vital clinical information services to the Bridgend locality affecting many clinical systems that are not compatible with Cwm Taf University Morgannwg Systems. **Then:** The Health board will be unable to deliver safe, high quality care to patients without vital clinical information available. **Resulting In:** Compromised safety of patients needing treatment that are reliant on clinical test results and information being available to clinicians to plan and deliver the treatment plan.	**Key Controls** SBUHB Service Level Agreement Bridgend disaggregation and the one-CTM aggregation plan Numerous national service management boards and Technical oversight groups providing strategic, tactical and operation governance. **Gaps in Control** The business case for integration remains unfunded. There are currently a number of CTM systems that are not compatible with Bridgend systems. SBUHB have no process in place to incorporate the needs of Bridgend users in their developments.	Progress in line with the existing plans which were agreed on the primary basis of their need to be affordable, has been made over 2020/21 with a number of new systems, such as pharmacy management introduced as pan-CTM products. However there is still considerable work required to create a unified digital infrastructure for CTM = around the clinical systems and the remainder of the ICT SLA. The business case details a funding requirement of £8 million. This was discussed at the Digital cell with WG in February 2021 and a further funding request has been submitted to WG at their request, along with complimentary proposals from Digital Healthcare Wales (DHCW) for which CTM has worked with them on. Timeframe - Mid June 2021 when DPIF Funding is announced.	Digital & Data Committee	16	C4 x L4	8 (C4xL2)	↔	14.10.2020	26.5.2021	30.06.2021	4337
Executive Director of Public Health - Interim Executive Lead for ICT / Digital Chief Information Officer	Provide high quality, evidence based, and accessible care.	Operational: • Core Business • Business Objectives • Environmental / Estates Impact • Projects Including systems and processes, Service /business interruption	Absence of coded structured data & inability to improve our delivery of the national clinical coding targets and standards (target is 95% completeness within month coded, and 98% on a rolling 3 month period)	**IF:** The Health Board is not able to record information accurately and reliably & does not address the 25000 backlog of uncoded FCEs **Then:** the data informing the clinical, regional and organisational decisions we and our partners (including WG) make, will be inaccurate, out of date or incomplete **Resulting in:** Degradation in our delivery of the quadruple aim and strategic objectives and damage to our reputational standing with our population and partners. Further we will be prevented from driving forward our ambitions to become a digital organisation, an exemplar for R&D and Value etc.	**Operational controls:** Coding key performance indicators covering productivity, demand and backlog robustly monitored DHCW annual coding quality audit. 2020/21 funding addressed backlog and proposals made to extend this into 2021/22. **Tactical controls:** Digital element of the strategic programme - Culture to digitise the EPR, our communications, how we do business National Architecture Review - encompassing (NDR /CDR & Sharing arrangements) Coding transformation programme Information and Technical Standards Clinical audit **Gaps in controls** Workforce skills & development programme Insufficient resource available to address backlog Digital solutions not yet using snomed-CT/ structurally coded data	Coding Improvement and transformation plan established incorporating additional trained coding capacity, coding at source, use of data captured in other systems and e-forms implemented. Programme to address the backlog using additional sessions and agency codings ran in March and extension for 2021/22 proposed - awaiting consideration via IMTP prioritisation process **Tactical** - EPR programme with deployment of snomed-CT onotology server, WCP & E-forms etc	Digital & Data Committee	15	C3 x L5	9 (C3xL3)	New Risk escalated from Digital ICT June 2021	05.06.2021	05.06.2021	31.07.2021	4672
Executive Director of Public Health - Interim Executive Lead for ICT / Digital Chief Information Officer	Provide high quality, evidence based, and accessible care.	Operational: • Core Business • Business Objectives • Environmental / Estates Impact • Projects Including systems and processes, Service /business interruption	NHS Computer Network Infrastructure unable to meet demand	**IF**: The Health Board suffers regular local and/or national network issues and/or outages to clinical and critical business systems. **Then**: there could be a detriment to patient care, inefficiencies in care provision and loss in confidence by Health Board staff in the technology provided to them leading to them using alternative software and bespoke systems (including paper based systems) to carry out their duties which are not integrated. **Resulting in**: delays in clinical decisions and consequently treatment which may affect clinical outcomes, reduced levels of productivity and thus poorer access to services, staff appetite to work digitally and in accordance with the digital standards required to realise the full strategic benefits of an integrated record and repository not being realised. Other consequences include: Loss of information integrity and accessibility as multiple copies of clinical records. Threat of malware being introduced on to the network from unmanaged data, systems and software. Possible breaches to the GDPR, safeguarding and information governance risks.	There are various Service Management boards from ADIs, service delivery and infrastructure management which have representatives from each NHS Wales organisation and departments. These meet regularly with a governance structure to escalate any service delivery and security incidents and risks. SLAs are in place between DHCW and NHS Wales organisations and incidents are escalated up via the national Service Point Service Management system. The Health Board has the Risk Audit Governance & Cyber Security Board which meets monthly to discuss and take action on service delivery incidents. Local and National Infrastructure reviews are presently underway.	Infrastructure and comms actions plans were agreed 24 months ago and are being delivered as funding and staffing are available (recognising priorities changed during covid). The Health Board to develop a robust incident management process. This is to ensure that regular outages of national systems and infrastructure are escalated to the appropriate governance structures to address such issues locally and nationally.	Digital & Data Committee	15	C3 x L5	9 (C3xL3)	New Risk escalated from Digital ICT June 2021	26/05/2021	26/05/2021	25/06/2021	4671

Strategic Risk owner	Strategic Objective	Risk Domain	Risk Title	Risk Description	Controls in place	Action Plan	Assuring Committees	Rating (current)	Heat Map Link (Consequence X Likelihood)	Rating (Target)	Trend	Rationale for de-escalation	Datix ID
Executive Director of Planning & Performance (ICT)	Provide high quality, evidence based, and accessible care.	Operational: • Core Business • Business Objectives • Environmental / Estates Impact • Projects Including systems and processes, Service /business interruption	Security at the Health Board's main Medical Records & Information Hub.	**If:** The security of the Information Hub is not improved and brought up to standard there is a risk of the hub being broken into out of hours **Then:** There is a risk that patient medical records files are stolen or damaged and equipment stolen. **Resulting In:** Potential loss of a patients medical records resulting in the ICO being informed and equipment being replaced	Additional temporary measures are in place to maintain 24 hour site security whilst a longer term solution is in place. Security Plan incorporating short term short term mediations whilst the long term arrangements are being put in place has commenced. This includes: - Additional security and policy patrols, enhanced CCTV monitoring- improving response times and access controls. The Long term security arrangements have been agreed and funded following a survey of the Estate and security advice.	Long term actions to be implemented.	Digital & Data Committee	12	C4xL3	8 C4xL2	↓ 20	See update in control measures leading to a reduction in the risk rating. Will be monitored via the local ICT risk management process / risk register.	4565
Chief Operating Officer Executive Director of Planning, Performance and ICT	Provide high quality, evidence based, and accessible care.	Patient / Staff /Public Safety Impact on the safety – Physical and/or Psychological harm	Telecommunications upgrade required with operational components for cardiac arrest and emergency fire numbers.	(Facilities Risk Register Reference 11480B) **ILG:** CSO Facilities Hub **If:** The telecommunications system for cardiac arrest and emergency fire numbers is not upgraded. **Then:** Potential for system crashes. **Resulting In:** Potential delay in contacting the necessary person(s), leading to patient not having efficient and effective treatment.	Contingency plan for telecommunications in place. New telecomm system still on course to be installed across PCH and RGH by 31st July 2021 - work has commenced. Contingency plan reviewed and there is a contingency where radios are provided and all emergency calls only are communicated via this link should the system crash.	Work on the new telecomm system installation has now started and is still ongoing currently due to covid pressures. At the current stage of this work there will be a number of porting exercises taking place within switchboard RGH over the coming weeks. This will mean switchboard RGH will be out of operation for approx. 6 minutes, however there is a possibility that it could not work which could result in being out of use for a longer period. Contingency has been put in place for this work as the contractors will be on site as well as our IT Comms team, however it has been included together with the contingency within this risk as it will affect the Cardiac arrest line. Action: New telecomm system to be installed across PCH and RGH. Timescale: 31/07/2021	Digital & Data Committee	12	C3 x L4	6	↓ 15	The rationale for de-escalation is that the Health Board has recently experienced the system failing. Rather than being a complete failure of telecoms and the bleep system it was an isolated incident, which did not affect the critical element. Secondly the Health Board were able to fail over in a very quick time scale. Thus as a relative risk, it is considered that based on this experience if we looked at consequence and likelihood together the risk rating could be reduced. Will be monitored via the local Facilities risk management process / risk register.	4286
Chief Operating Officer Executive Director of Planning, Performance and ICT	Provide high quality, evidence based, and accessible care.	Patient / Staff /Public Safety Impact on the safety – Physical and/or Psychological harm	Potential cyber security risk relating to brand of medical device monitoring system.	(Facilities Risk Register Reference S9) **ILG:** CSO Facilities Hub **If:** Potential cyber security risk (CVE-2020-1472) identified relating to a specific brand of medical device monitoring system. Should a threat be successful. **Then:** Potential changes and disruption to the operation of monitoring equipment could occur. **Resulting In:** Service/business interruption and potential harm to patients being treated.	The medical device system is protected by firewalls but these will not prevent access. Clinical Engineering have discussed with manufacturer about software patching to find and implement a solution. Contacted manufacturer and problem now identified on the manufacturers online support portal as a vulnerability. Received response from the manufacture that the software patch will be available in January. Once patch has been installed by manufacturer Clinical Engineering will install the patch on the two servers and equipment affected within the Health Board and check issue has been resolved for compliance. Clinical Engineering has reviewed all other medical device systems and has identified no other medical device systems that are vulnerable to this threat.	The Specialist Healthcare Scientist in Clinical Engineering has continued to chase the manufacturer for a solution. Following a meeting with them held on 13/01/2021, the manufacturer has accepted fault and has agreed to installing a newer version of software as a solution. The solution will involve a significant amount of downtime of equipment in all critical areas which is not viable during covid pressures. Supplier has confirmed a date in June 2021 to install a new software patch. Facilities Team advised that the mitigation plan is close to being completed and weekly surveillance checking on the systems are in place and therefore support the ICT assessment that the risk can be de-escalated.	Digital & Data Committee	12	C3 x L4	4	↓ 15	Based on the update in the Action Plan column the risk has been reduced to likelihood 4 as the operating system remains supported at this time. Will be monitored via the local Facilities risk management process / risk register.	4306

Executive Director of Planning, Performance & ICT	Ensure sustainability in all that we do, economically, environmentally and socially	Operational: • Core Business • Business Objectives • Environmental / Estates Impact • Projects Including systems and processes, Service /business interruption	Shortage of IT Storage space. (The ground and first floor work at PCH requires the ICT store and build areas to be relocated to alternative accommodation. As yet a suitable area has area has not been found. The accommodation will need to be suitable for large delivery trucks to deliver ICT equipment and either ground floor or lift access to the area.)	**IF:** The lack of enough storage space for ICT equipment is not sufficient. **Then:** Equipment will be required to be stored in temporary locations which are not designed for storage. **Resulting In**: a risk to the Health and Safety of ICT staff and the risk to the equipment being either damaged, lost or stolen.	1. Ensuring regular disposal of old redundant hardware using third party company, to keeping stock down to a minimum 2. Vigorous and robust procedures in place for the procurement of new equipment. 3. identifying fully any additional storage requirements of every new system requested. 4. Due to the progression of Ground and first discussions are underway around possible areas that ICT can move into for build and storage which is key to be able to deliver a service	1. To identify extra/sufficient storage space for obsolete and new equipment. Completed extra storage space secured. 2. The temporary storage of the ECC area now under discussion. 3. Move to Pontypridd Health Centre and potential fir warehouse facility identified as a target model.	Digital & Data Committee	9	C3 x L3	3 3x1	↓ 15	This risk has been de-escalated as a new location has been identified, Pontypridd Health Centre. ICT should be able to transfer the equipment to this location prior to the existing location in ECC at PCH being no longer available.	632

Datix ID	Executive Portfolio	Risk Domain	Risk Title	Risk Description	Controls in place	Action Plan	Assuring Committees	Rating (current)	Rating (Target)	Trend	Opened	Last reviewed	Comments
4109 Chief Operating Officer Executive Director of Public Health - Interim Executive Lead for Digital Rhondda Taf Ely Locality - as host Medical Records	Provide high quality, evidence based, and accessible care.	Legal / Regulatory Statutory duty, regulatory compliance, accreditation, mandatory requirements	Increase requirement to store the paper patient record for longer due to: *Delay in the DPN project & the Increased retention period due to the Infected Blood Inquiry*	**IF:** The Health Board fails to ensure there is sufficient storage capacity to safely and securely store paper patient records as destruction of the files is delayed. **Then:** there could be potential data loss and poor records management processes and communication. Health, Safety and Fire risks will escalate due to overcrowded and inappropriate storage. **Resulting in:** possible breaches to the GDPR, safeguarding and information governance risks. Possible injuries to staff due to manual handling/trip hazards and breaches of Fire Safety procedures. These hazards extend to record stores across the Health Board as capacity to accept their excess records is compromised.	Digitisation of general patient records commenced on 18/3/21. This will gradually create storage space at the central records hub over 2 years, to ensure a sustainable, safe and secure storage solution. Interim storage may be required in the meantime, due to the impact of delayed digitisation and Infected Blood Inquiry embargo on managed record destruction until late 2023. Impact being closely monitored as areas outside the Hub are being affected due to compromised capacity to store additional records and destroy their excess. An Electronic Document Management System, Clinical Portal interface have been introduced; E-forms will follow as part of the project over the next year. Ensure Records management processes fully applied in all record stores to maximise use of available physical capacity. N.B. Limited opportunity for this, as destruction procedure cannot be applied to non-digitised records. Ensure no temporary storage solutions are agreed, without full consideration of the Executive.	Digital Patient Notes (Phase 1) was delayed but has now gone live. This will enable a limited regular destruction of digitised notes from this point forward, despite the continued record destruction embargo, as the content is held digitally. All other non-digital records are still under embargo until late 2023. This overarching record storage risk now also incorporates Bridgend Medical Records stores, where no digitisation can begin for at least 2 years, hence the overall consequence of 3 and likelihood of 5. The impact being closely monitored. Areas outside Medical Records are also being affected, due to inability to destroy their archived records at the Hub; this prevents them transferring their excess records to this site. All possible measures are being taken to manage the storage areas and maximise use of the space. Digitisation of general patient records commenced on 18/3/21. This will gradually create storage space at the central records hub over 2 years, to ensure a sustainable, safe and secure storage solution . An Electronic Document Management System and Clinical Portal interface have been introduced via this programme; E-forms will follow over the next year. To date, @13,500 deceased and live records have been digitised and @244 consultant and nurse-led teams are live on the use of the DPN software. Procurement of digital dictation for 400 users will	Digital & Data Committee	15	C1 x L3	To Close	02.07.2018	7.6.2021	Closed as target score met. The risk is described as the potential to run out of space, not that the Health Board has ran out of space, so when first described it was probably thought that the default consequence would be records left in unsecure places where they were not tracked - however, the Health Board has controls in place as outlined in the "control measures" column and staff receive Information Governance training and therefore it is considered that the likelihood and consequence of this occurring is low.