Bwrdd Iechyd Prifysgol Hywel Dda University Health Board

PWYLLGOR ADNODDAU CYNALIADWY **SUSTAINABLE RESOURCES COMMITTEE**	

DYDDIAD Y CYFARFOD: **DATE OF MEETING:**	25 April 2022
TEITL YR ADRODDIAD: **TITLE OF REPORT:**	Corporate Risk Report
CYFARWYDDWR ARWEINIOL: **LEAD DIRECTOR:**	Huw Thomas, Director of Finance Andrew Carruthers, Director of Operations
SWYDDOG ADRODD: **REPORTING OFFICER:**	Charlotte Beare, Head of Assurance and Risk

| **Pwrpas yr Adroddiad** (dewiswch fel yn addas)
Purpose of the Report (select as appropriate) |
|---|
| Ar Gyfer Trafodaeth/For Discussion |

ADRODDIAD SCAA **SBAR REPORT**

Sefyllfa / Situation

The Sustainable Resources Committee is asked to request assurance from the identified Executive Director that the corporate risks in the attached report at Appendix 1, are being managed effectively.

Cefndir / Background

Effective risk management requires a 'monitoring and review' structure to be in place to ensure that risks are effectively identified and assessed, and that appropriate controls and responses are in place.
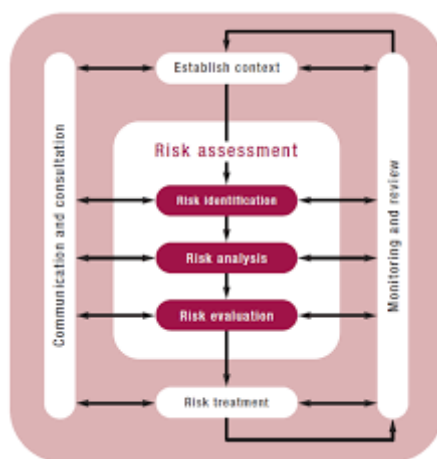
(Risk Management Process, ISO 31000)

The Board's Committees are responsible for the monitoring and scrutiny of corporate-level risks within their remit. As such, they are responsible for:

- Seeking assurance on the management of corporate risks included in the Corporate Risk Register (CRR) and providing assurance to the Board that risks are being

managed effectively, reporting areas of significant concern - for example, where risk appetite is exceeded, lack of action etc;

- Reviewing principal and operational risks over tolerance and, where appropriate, recommending the 'acceptance' of risks that cannot be brought within Hywel Dda University Health Board's (HDdUHB's) risk appetite/ tolerance to the Board through the Committee Update Report;
- Providing annual reports to Audit and Risk Assurance Committee (ARAC) on the effectiveness of the risk management process and management of risks within their remit;
- Identifying through discussions any new/ emerging risks, and ensuring these are assessed by management;
- Signposting any risks outside their remit to the appropriate HDdUHB Committee;
- Using risk registers to inform meeting agendas.

The Executive Team has agreed the content of the CRR. These risks have been identified via a top-down and bottom-up approach.

Each risk on the CRR has been mapped to a Board-level Committee to ensure that risks are being managed appropriately, taking into account gaps, planned actions and agreed tolerances, and to provide assurance regarding the management of these risks to the Board through Committee Update Reports.

The Board has delegated a proportion of its role in scrutinising assurances to its Committees in order to make the most appropriate and efficient use of expertise. Therefore, Committees should also ensure that assurance reports relating to principal risks are received and scrutinised, and an assessment made as to the level of assurance they provide. The reports should consider the validity and reliability of each assurance in terms of source, timeliness and methodology. Robust scrutiny by its Committees will enable the Board to place greater reliance on assurances and will provide the Board with greater confidence in the likelihood of achieving strategic objectives, in addition to ensuring a sound basis for decision-making. It is the role of Committees to provide challenge where missing or inadequate assurances are identified and to escalate any gaps in assurance to the Board.

Asesiad / Assessment

The Sustainable Resources Committee Terms of Reference state that it will:

2.7 Seek assurance on the management of principal risks within the Board Assurance Framework (BAF) and Corporate Risk Register (CRR) allocated to the Committee and provide assurance to the Board that risks are being managed effectively and report any areas of significant concern e.g. where risk tolerance is exceeded, lack of timely action.

2.8 Recommend acceptance of risks that cannot be brought within the UHBs risk appetite/tolerance to the Board through the Committee Update Report.

2.9 Receive assurance through Sub-Committee Update Reports and other management/task & finish group reports that risks relating to their areas are being effectively managed across the whole of the Health Board's activities (including for hosted services and through partnerships and Joint Committees as appropriate).

There are 3 risks assigned to the Committee from the 16 risks currently identified on the CRR. The principal risks to the Health Board's strategic objectives have been reported to the Board from September 2021.

The 3 corporate risks have been entered onto a '*risk on a page*' template, which includes information relating to the strategic objective, controls, assurances, performance indicators, and action plans to address any gaps in controls and assurances.

Changes Since Previous Report

Total Number of Risks	3	
New risks	2	*See Note 1*
De-escalated/Closed	4	*See Note 2*
Increase in risk score ↑	0	
No change in risk score →	1	*See Note 3*
Reduction in risk score ↓	0	

The 'heat map' below includes the risks currently aligned to the Sustainable Resources Committee.

HYWEL DDA RISK HEAT MAP					
	LIKELIHOOD →				
IMPACT ↓	RARE 1	UNLIKELY 2	POSSIBLE 3	LIKELY 4	ALMOST CERTAIN 5
CATASTROPHIC 5					
MAJOR 4				1352 (NEW) 1371 (NEW)	
MODERATE 3				1335 (→)	
MINOR 2					
NEGLIGIBLE 1					

Note 1 – New Risks
Since the previous report in February 2022, 1 new risk has been added to the CRR:

Risk	Lead Director	New/ Escalated	Date	Reason
1352 - Risk of business disruption and delays in patient care due to a cyber attack	Director of Operations	New	02/03/22	This corporate risk was approved by the Executive Risk Group on 2nd March 2022 following an in-depth review of corporate risk 451 (cyber security breach) and external assessment. There are daily threats to systems which are managed by Digital Health Care Wales and HDdUHB. Cyber attacks are

				becoming more prevalent, and previously hackers were not targeting health bodies, however the recent attack in Ireland, illustrates that the possibility of an attack is ever present. Impact score is 4 as a cyber-attack has the potential to severely disrupt service provision across all sites for a significant amount of time, however the processes and controls in place have reduced the likelihood due to the improvements in patching.
1371 - Risk to the delivery of UHB's Draft Interim Financial Plan for 2022/23	Director of Finance	New	13/04/22	This corporate risk was approved by the Executive Risk Group on 13th April 2022 to reflect the risk to the delivery of the Health Board's draft interim Financial Plan for 2022/23 of a £25.0m deficit.

Financial planning assumptions have been assessed, assuming up to 12 months of "Low" COVID-19 prevalence (defined as COVID-19 circulating in the community, perhaps at levels similar to Summer 2021, but lower severity (equivalent to Omicron variant)). Whilst the operational responses and corresponding financial impact of the pandemic during 2020-2022 has provided a sound basis for modelling scenarios, it should be acknowledged that this "Low" scenario may not be the case throughout the year, which may have resource implications. Welsh Government (WG) funding streams are partly confirmed, however there will be a reliance on the success of bids for specific funding to support the Health Board's further Elective Recovery |

| | | | | Plans, specific exceptional costs, transitional COVID-19 support in response to the pandemic, and in the acceleration of the Health Board's Strategy. A strategic overhaul of the Health Board's operating model is required to make the transformational shift in services that are required to deliver workforce and finance sustainability - this is a medium term outlook, however it will impact the in-year position.

Through the Integrated Medium Term Plan (IMTP) process, operational plans to address the financial savings gap have not provided sufficient assurance to mitigate the risk, and was a key factor in the Health Board's ability to not submit an IMTP. Whilst it has been committed that the Health Board will submit a financially balanced IMTP by the end of Quarter 1 2022/23, financial assurance will need to be sought to achieve this. |
|---|---|---|---|---|

Note 2 - De-escalated/Closed Risks

Since the previous report in February 2022, the following corporate risks have been closed/de-escalated:

Risk	Lead Director	Close/De-escalated	Date	Reason
451 - Cyber Security Breach	Director of Finance	Closed	02/03/22	The Executive Risk Group agreed to the closure of this risk following a review of the risk by the Digital team. The new risk (1352 - see table above) reflects the current context and issues following an external review.
1296 - Risk that the Health Board will not deliver a financial out-turn position in line	Director of Finance	Closed	13/04/22	The Executive Risk Group agreed to the closure of this risk as it relates to the previous financial year (2021/22) and has been

with our original plan of £25m deficit				replaced by a new risk for 2022/23 (see risk 1371 above).
1297 - Risk that the Health Board's underlying deficit will increase to level not addressed by additional medium term funding	Director of Finance	Closed	13/04/22	The Executive Risk Group agreed to the closure of this risk as the new financial risk (risk 1371 above) will address this through the targeted operating model.
1307 - Risk to achieving the Capital Resource Limit 2021/22	Director of Finance	Closed	13/04/22	The Executive Risk Group agreed to the closure of this risk as the Health Board has met its statutory duty to breakeven against its Capital Resource Limit for 2021/22.

Note 3 - No change in Current Risk Score
There has been no change in the current risk score of the below risks.

Risk Reference & Title	Previous Risk Report Feb-22 (LxI)	Risk Score Apr-22 (LxI)	Date of Review	Update
1335 - Risk of being unable to access patient records, at the correct time and place in order to make the right clinical decisions	3x4=12	**3x4=12**	31/03/22	Across the Health Board, there is currently a considerable variance in both operational practice and process when utilising and dealing with the various types of records in use throughout directorates, services and departments. The current records management methodology results in a non-standardised approach to delivering effective records management arrangements. With a lack of agreed criteria regarding the management of the record during its life cycle from creation, during retention and its disposal. There is a requirement for an investment in a modern day solution and an alteration to culture and attitude, which will embrace change and

				technology associated with a digital health record (DHR), to manage the risk. The Health Board has selected its electronic document management system (EDMS) supplier.

The Committee is requested not to devolve its responsibility for seeking assurances on corporate risks; however, it can reassign risks to another Board level Committee if it is agreed that it fits better within their remit.

Argymhelliad / Recommendation

The Sustainable Resources Committee is requested to:

- Seek assurance that all identified controls are in place and working effectively;
- Seek assurance that all planned actions will be implemented within stated timescales and will reduce the risk further and/ or mitigate the impact, if the risk materialises;
- Challenge where assurances are inadequate.

Subsequently, this will enable the Committee to provide the necessary onward assurance to the Board, through its Committee Update Report, that HDdUHB is managing these risks effectively.

Amcanion: (rhaid cwblhau) Objectives: (must be completed)	
Committee ToR Reference: Cyfeirnod Cylch Gorchwyl y Pwyllgor:	Contained within the report
Cyfeirnod Cofrestr Risg Datix a Sgôr Cyfredol: Datix Risk Register Reference and Score:	Contained within the report
Safon(au) Gofal ac Iechyd: Health and Care Standard(s):	Governance, Leadership and Accountability
Amcanion Strategol y BIP: UHB Strategic Objectives:	All Strategic Objectives are applicable
Amcanion Llesiant BIP: UHB Well-being Objectives: Hyperlink to HDdUHB Well-being Objectives Annual Report 2018-2019	10. Not Applicable

Gwybodaeth Ychwanegol: Further Information:	
Ar sail tystiolaeth: Evidence Base:	Underpinning risk on the Datix Risk Module from across HDdUHB's services reviewed by risk leads/ owners

Rhestr Termau: Glossary of Terms:	Explanation of terms is included in the main body of the report.
Partïon / Pwyllgorau â ymgynhorwyd ymlaen llaw y Pwyllgor Adnoddau Cynaliadwy: Parties / Committees consulted prior to Sustainable Resources Committee:	Not Applicable

Effaith: (rhaid cwblhau) Impact: (must be completed)	
Ariannol / Gwerth am Arian: Financial / Service:	No direct impacts from report, however, impacts of each risk are outlined in risk description.
Ansawdd / Gofal Claf: Quality / Patient Care:	No direct impacts from report, however, impacts of each risk are outlined in risk description.
Gweithlu: Workforce:	No direct impacts from report, however, impacts of each risk are outlined in risk description.
Risg: Risk:	No direct impacts from report, however organisations are expected to have effective risk management systems in place.
Cyfreithiol: Legal:	No direct impacts from report, however proactive risk management, including learning from incidents and events, contributes towards reducing/eliminating recurrence of risk materialising and mitigates against any possible legal claim with a financial impact.
Enw Da: Reputational:	Poor management of risks can lead to loss of stakeholder confidence. Organisations are expected to have effective risk management systems in place and take steps to reduce/mitigate risks.
Gyfrinachedd: Privacy:	No direct impacts from report, however, impacts of each risk are outlined in risk description.
Cydraddoldeb: Equality:	Has EqIA screening been undertaken? No Has a full EqIA been undertaken? No

Risk Ref	Risk (for more detail see individual risk entries)	Risk Owner	Domain	Tolerance Level	Previous Risk Score	Risk Score Apr-22	Trend	Target Risk Score	Risk on page no...
1352	Risk of business disruption and delays in patient care due to a cyber attack	Thomas, Huw	Statutory duty/inspections	8	4×4=16	4×4=16	→	3×4=12	6
1371	Risk to the delivery of UHB's Draft Interim Financial Plan for 2022/23	Thomas, Huw	Statutory duty/inspections	8	N/A	4x4=16	New	2x4=8	
1335	Risk of being unable to access patient records, at the correct time and place in order to make the right clinical decisions	Carruthers, Andrew	Quality/Complaints/Audit	8	4×3=12	4×3=12	→	2×3=6	

RISK SCORING MATRIX

Likelihood x Impact = Risk Score

Likelihood	1	2	3	4	5
Descriptor	Rare	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
Frequency - How often might it/does it happen? (how many times will the adverse consequence being assessed actually be realised?)	This will probably never happen/recur (except in very exceptional circumstances).	Do not expect it to happen/recur but it is possible that it may do so.	It might happen or recur occasionally.	It might happen or recur occasionally.	It will undoubtedly happen/recur, possibly frequently.
	Not expected to occur for years.*	Expected to occur at least annually.*	Expected to occur at least monthly.*	Expected to occur at least weekly.*	Expected to occur at least daily.*
			* time-framed descriptors of frequency		
Probability - Will it happen or not? (what is the chance the adverse consequence will occur in a given reference period?)	(0-5%*)	(5-25%*)	(25-75%*)	(75-95%*)	(>95%*)
			*used to assign a probability score for risks related to time-limited or one off projects or business objectives.		

Risk Impact Domains	Negligible - 1	Minor - 2	Moderate - 3	Major - 4	Catastrophic - 5
Safety of Patients, Staff or Public	Minimal injury requiring no/minimal intervention or treatment.	Minor injury or illness, requiring minor intervention.	Moderate injury requiring professional intervention.	Major injury leading to long-term incapacity/disability.	Incident leading to death.
	No time off work.	Requiring time off work for >3 days	Requiring time off work for 4-14 days.	Requiring time off work for >14 days.	Multiple permanent injuries or irreversible health effects.
		Increase in length of hospital stay by 1-3 days.	Increase in length of hospital stay by 4-15 days.	Increase in length of hospital stay by >15 days.	An event which impacts on a large number of patients.
			Agency reportable incident.	Mismanagement of patient care with long-term effects.	
			An event which impacts on a small number of patients.		
Quality, Complaints or Audit	Peripheral element of treatment or service suboptimal.	Overall treatment or service suboptimal.	Treatment or service has significantly reduced effectiveness.	Non-compliance with national standards with significant risk to patients if unresolved.	Totally unacceptable level or quality of treatment/service.
	Informal complaint/inquiry.	Formal complaint.	Formal complaint -	Multiple complaints/ independent review.	Gross failure of patient safety if findings not acted on.
		Local resolution.	Escalation.	Low achievement of performance/delivery requirements.	Inquest/ombudsman inquiry.
		Single failure to meet internal standards.	Repeated failure to meet internal standards.	Critical report.	Gross failure to meet national standards/performance requirements.
		Minor implications for patient safety if unresolved.	Major patient safety implications if findings are not acted on.		
		Reduced performance if unresolved.			
Workforce & OD	Short-term low staffing level that temporarily reduces service quality	Low staffing level that reduces the service quality.	Late delivery of key objective/ service due to lack of staff.	Uncertain delivery of key objective/service due to lack of staff.	Non-delivery of key objective/service due to lack of staff.

Category					
	(< 1 day).		Unsafe staffing level or competence (>1 day). Low staff morale. Poor staff attendance for mandatory/key training.	Unsafe staffing level or competence (>5 days). Loss of key staff. Very low staff morale. No staff attending mandatory/ key training.	Ongoing unsafe staffing levels or competence. Loss of several key staff. No staff attending mandatory training /key training on an ongoing basis.
Statutory Duty or Inspections	No or minimal impact or breach of guidance/ statutory duty.	Breach of statutory legislation. Reduced performance levels if unresolved.	Single breach in statutory duty. Challenging external recommendations/ improvement notice.	Enforcement action Multiple breaches in statutory duty. Improvement notices. Low achievement of performance/delivery requirements. Critical report.	Multiple breaches in statutory duty. Prosecution. Complete systems change required. Low achievement of performance/delivery requirements. Severely critical report.
Adverse Publicity or Reputation	Rumours. Potential for public concern.	Local media coverage – short-term reduction in public confidence. Elements of public expectation not being met.	Local media coverage – long-term reduction in public confidence.	National media coverage with <3 days service well below reasonable public expectation.	National media coverage with >3 days service well below reasonable public expectation. AMs concerned (questions in the Assembly). Total loss of public confidence.
Business Objectives or Projects	Insignificant cost increase/ schedule slippage.	<5 per cent over project budget. Schedule slippage.	5–10 per cent over project budget. Schedule slippage.	Non-compliance with national 10–25 per cent over project budget. Schedule slippage. Key objectives not met.	Incident leading >25 per cent over project budget. Schedule slippage. Key objectives not met.
Finance including Claims	Small loss. Risk of claim remote.	Loss of 0.1–0.25 per cent of budget. Claim less than £10,000.	Loss of 0.25–0.5 per cent of budget. Claim(s) between £10,000 and £100,000.	Uncertain delivery of key objective/Loss of 0.5–1.0 per cent of budget. Claim(s) between £100,000 and £1 million.	Non-delivery of key objective/ Loss of >1 per cent of budget. Failure to meet specification/ slippage Claim(s) >£1 million.
Service or Business interruption or disruption	Loss/interruption of >1 hour. Minor disruption.	Loss/interruption of >8 hours. Some disruption manageable by altered operational routine.	Loss/interruption of >1 day. Disruption to a number of operational areas within a location and possible flow onto other locations.	Loss/interruption of >1 week. All operational areas of a location compromised. Other locations may be affected.	Permanent loss of service or facility. Total shutdown of operations.
Environmental	Minimal or no impact on the environment.	Minor impact on environment.	Moderate impact on environment.	Major impact on environment.	Catastrophic/critical impact on environment.

RISK MATRIX

IMPACT ↓	LIKELIHOOD →				
	RARE	UNLIKELY	POSSIBLE	LIKELY	ALMOST CERTAIN
	1	2	3	4	5
CATASTROPHIC 5	5	10	15	20	25
MAJOR 4	4	8	12	16	20
MODERATE 3	3	6	9	12	15
MINOR 2	2	4	6	8	10
NEGLIGIBLE 1	1	2	3	4	5

RISK ASSESSMENT - FREQUENCY OF REVIEW

RISK SCORED	DEFINITION	ACTION REQUIRED (GUIDE ONLY)	MINIMUM REVIEW FREQUENCY
15-25	Extreme	Unacceptable. Immediate action must be taken to manage the risk. Control measures should be put into place which will have an effect of reducing the impact of an event or the likelihood of an event occurring. A number of control measures may be required.	This type of risk is considered extreme and should be reviewed and progress on actions updated, at least monthly.
8-12	High	Very unlikely to be acceptable. Significant resources may have to be allocated to reduce the risk. Urgent action should be taken. A number of control measures may be required.	This type of risk is considered high and should be reviewed and progress on actions updated at least bi-monthly.
4-6	Moderate	Not normally acceptable. Efforts should be made to reduce risk, providing this is not disproportionate. Establish more precisely the likelihood & harm as a basis for determining the need for improved measures.	This type of risk is considered moderate and should be reviewed and progress on actions updated at least every six months.
1-3	Low	Risks at this level may be acceptable. If not acceptable, existing controls should be monitored & reviewed. No further action or additional controls are required.	This type of risk is considered low risk and should be reviewed and progress on actions updated at least annually.

Assurance Key:

3 Lines of Defence (Assurance)		
1st Line	Business Management	Tends to be detailed assurance but lack independence
2nd Line	Corporate Oversight	Less detailed but slightly more independent
3rd Line	Independent Assurance	Often less detail but truly independent

Key - Assurance Required	
▨	Detailed review of relevant information
▨	Medium level review
▨	Cursory or narrow scope of review

NB Assurance Map will tell you if you have sufficient sources of assurance not what those sources are telling you

Key - Control RAG rating	
LOW	Significant concerns over the adequacy/effectiveness of the controls in place in proportion to the risks
MEDIUM	Some areas of concern over the adequacy/effectiveness of the controls in place in proportion to the risks
HIGH	Controls in place assessed as adequate/effective and in proportion to the risk
INSUFFICIENT	Insufficient information at present to judge the adequacy/effectiveness of the controls

Date Risk Identified:	Jan-22		Executive Director Owner:	Thomas, Huw	Date of Review:	Apr-22
Strategic Objective:	6. Sustainable use of resources		Lead Committee:	Sustainable Resources Committee	Date of Next Review:	May-22

Risk ID:	1352	Principal Risk Description:	There is a risk of business disruption and intolerable delays in patient care (particularly radiology, pharmacy, laboratories and Cancer Care) and in some instances misdiagnosis. This is caused by unavailability or malfunctioning of clinical devices and systems due to a cyber-attack, and resources to implement Information Assurance and a Cyber Security culture. This could lead to an impact/affect on patient outcomes and threat to life, reputational damage, loss of patient trust, severe financial impact to Hywel Dda through regulatory fines and individual litigation (UHB's finances and reputation - ICO fines of up to 4% of Budget/Revenue for GDPR/DPA 2018, Welsh Government fines of up to £17m for NISR). In addition, a loss of clinical technologies and systems will result in extreme pressure on limited clinical resources.

Risk Rating:(Likelihood x Impact)

Domain:	Statutory duty/inspections
Inherent Risk Score (L x I):	5×5=25
Current Risk Score (L x I):	4×4=16
Target Risk Score (L x I):	3×4=12
Tolerable Risk:	8

Legend: Current Risk Score; Target Risk Score; Tolerance Level. X-axis: Feb-22, Apr-22. Y-axis: 0 to 25.

Does this risk link to any Directorate (operational) risks?		Trend:	↔

Rationale for CURRENT Risk Score:	Rationale for TARGET Risk Score:
There are daily threats to systems which are managed by Digital Health Care Wales and UHB. Cyber attacks are becoming more prevalent, and previously hackers were not targeting health bodies, but the recent attack in Ireland, means that the possibility of an attack is ever present. Impact score is 4 as a cyber-attack has the potential to severely disrupt service provision across all sites for a significant amount of time, however the processes and controls in place have reduced the likelihood due to the improvements in patching.	Increased diligence, and monitoring of the cyber incidents will limit the impact upon the organisation. However this work is continuous and is dependent on obtaining the appropriate level of resources to undertake the patching anti-virus work at pace.

Key CONTROLS Currently in Place: (The existing controls and processes in place to manage the risk)	Gaps in CONTROLS				
	Identified Gaps in Controls : (Where one or more of the key controls on which the organisation is relying is not effective, or we do not have evidence that the controls are working)	How and when the Gap in control be addressed Further action necessary to address the controls gaps	By Who	By When	Progress
Hywel Dda's Corporate Risk Register (CRR) and Board Assurance Framework are reviewed 3 times a year. Cyber Security Risks are owned by an Executive Director, Finance Director and SIRO and delegated to Director of Digital and Deputy SIRO. Process in place to review and manage all critical cyber security risks in line with existing risk management framework. There is an Independent Board Member for Digital.	Lack of comprehensive patching across all systems used in UHB. Lack of staffing capacity to undertake continuous patching at pace. Lack of dedicated maintenance windows for updating critical clinical systems. Lack of business continuity and	Establish and publish an Organisation of Cyber Security with clearly defined roles and escalation points to the business that include Board members.	Tracey, Anthony	30/06/2022	On track - a number of programmes of work have been drafted and will be approved at the first meeting of the Cyber Resilience Sub-Group of IGSC.
		Build and deliver a communications plan on Cyber Security to the Hywel Dda workforce.	Tracey, Anthony	31/07/2022	On track - this is a programme of work within the wider Cyber Programme which will be discussed at the first meeting of IGSC.

| The Deputy SIRO chairs an Information Governance Sub Committee and the Information Asset Owners Group.

IG Risks are captured, well documented and reviewed monthly.

Mandatory IG Training .

IG policies and processes including DPIA and Privacy Notices in place (These are due for review and uplift to include data security and NISR requirements).

The following technologies are utilised in ensuring that the threat of a cyber attack is reduced:
 - Defender for Endpoint
 - SolarWinds and Kaseya
 - Email Phishing
 - Sophos
 - National Tools

Funding allocated to Cyber Security and Information Governance

Service Business Continuity Plans with fall back to manual and administrative processes.	Lack of business continuity and disaster recovery plans for key clinical systems	Train all Hywel Dda Board Members in Cyber Security including current threats to NHS Wales. The National Cyber Security Centre (NCSC) recommend their Board Toolkit https://www.ncsc.gov.uk/collection/board-toolkit	Tracey, Anthony	31/08/2022	On track - a formal training programme (e-learning) is being explored for Board members
		Restate the Board's intent on cyber security to the Hywel Dda workforce.	Tracey, Anthony	31/08/2022	On track - as above. Following a successful adoption by the Board, the eLearning package will be rolled out across the Health Board. Discussions around the mandating of such training still require to be completed.
		Carry out a yearly table top exercise to practice the Hywel Dda's response to a National Cyber Security Incident and a Major Cyber Security Incident	Tracey, Anthony	31/03/2023	On track. It has been agreed that a national exercise will be developed which will run across all Health Boards and Trusts. However, guidance will be sent to all departments of the Health Board requesting that they review their Business Continuity Plans, given the increase risk of a Cyber Attack as a result of the current Ukraine situation.
		Implement an Information Security Management System (i.e. ISO27001).	Tracey, Anthony	31/12/2022	On track
		Conduct cyber security risk and vulnerability assessments of critical systems and supporting network infrastructure to capture and remediate risks to business continuity.	Tracey, Anthony	30/06/2022	A number of vulnerabilities have been identified and reported to IGSC, and the digital team are working through the mitigation of said vulnerabilities.
		Include cyber security (Secure by design) in all maintenance, new digital and clinical initiatives (including procurement) to ensure confidentiality, integrity and availability within the maximum tolerance of the services business continuity plans and resourcing constraints.	Tracey, Anthony	30/09/2022	On track
		Implement a robust supply chain security process with controls appropriate to risk including financial penalties for clinical and business impact and appropriate insurances (public liability and indemnity, business continuity, cyber etc.).	Tracey, Anthony	31/10/2022	On track

Action	By Who	By When	Progress
Ensure that contracts are clear on cyber security and business continuity requirements and standards for products and services (GDPR/DPA 2018, NISR 2018, CIW Regulations and NHS Wales Standards 3.1 and 3.4).	Tracey, Anthony	31/07/2022	A full review of all historic contracts is underway to ensure that cyber security is included and at the forefront. All new contracts are assessed for cyber assurance before awarding.
Review all business continuity plans in light of COVID-19, new ways of working, resourcing constraints, operational targets/KPIs and reliance on networked devices and digital (inc Cloud) technologies.	Tracey, Anthony	30/06/2023	On track - A work programme has been developed and will be discussed with the Emergency Planning Team to ensure that all systems comply. Where the system is under the direct management of Digital Services, a formal update to the business continuity plans will be produced and adopted.
Review all Connections, Firewalls, Web Proxies, Switches, VLANS and implement technical segregation to minimise business impact as a result of a cyber security incident .i.e Radiology, Pharmacy, Labs, Cancer Care.	Tracey, Anthony	31/07/2022	On track
Review relative responsibilities for cyber security across the Health Board	Tracey, Anthony	30/11/2022	On track
Update the Corporate Risk Register on cyber security to include risks around data theft, lack of data integrity leading to clinical safety risk, business disruption including risk to clinical safety and patient care and regulatory fines under GDPR/DPA, NISR, CIW and PCI-DSS. Consider the impact to Revenue/Budget, Reputation, Regulation and Health and Safety.	Tracey, Anthony	Completed	New corporate risk on cyber security approved by Executive Risk Group on 02Mar22.

ASSURANCE MAP				Control RAG Rating (what the assurance is telling you about your controls	Latest Papers (Committee & date)	Gaps in ASSURANCES				
Performance Indicators	Sources of ASSURANCE	Type of Assurance	Required Assurance			Identified Gaps in Assurance:	How are the Gaps in ASSURANCE will be addressed	By Who	By When	Progress
		(1st, 2nd, 3rd)	Current Level				Further action necessary to address the gaps			

No of cyber incidents. Current patching levels in UHB. No of maintenance windows agreed with system owners. Removal of legacy equipment. Number of staff trained in Cyber Essentials	Department monitoring of KPIs	1st			Cyber Assurance Framework (CAF) - IGSC (Monthly)				
	IGSC monitoring of cyber security workplan addressing recent internal and external audits/assessments	2nd			Cyber Resilience and Security (SRC) Apr22				
	IGSC monitoring of National External Security Assessment	2nd							
	Follow-up Information Backup, Disaster Recovery & Business Continuity and Data Quality: Update on Progress	3rd							
	NHS Wales External Security Assessment - Assessment Report and Security Improvement Plan	3rd							
	Audit reviews (Internal / Cyber Resilience Unit (CRU) / Wales Audit Office (WAO)	3rd							

Date Risk Identified:	Apr-22		Executive Director Owner:	Thomas, Huw	Date of Review:	Apr-22
Strategic Objective:	6. Sustainable use of resources		Lead Committee:	Sustainable Resources Committee	Date of Next Review:	May-22

Risk ID:	1371	Principal Risk Description:	There is a risk to the delivery of the Health Board's draft interim Financial Plan for 2022/23 of a £25.0m deficit. This is caused by 1. The savings requirement within the Plan is £29.4m, which is significantly greater than the Health Board has historically achieved within an annual cycle; further there is currently insufficient assurance that identified opportunities can be converted into deliverable operational schemes. 2. In line with guidance, the Plan currently assumes Welsh Government (WG) funding to meet the planned costs of addressing our continued local COVID-19 activities, however this funding has not yet been secured centrally by WG; further, the needs may exceed the planned funding available from UHB, Regional and WG sources if decommissioning of areas of the COVID-19 response is not delivered within the planned timescales; 3. In line with guidance, the Plan currently assumes WG funding to meet the planned costs of addressing specific exceptional costs from FY23, namely energy costs, the impact of the increase in National Insurance (Health and Social Care Levy) and the increased cost in commissioned services driven by the Real Living Wage. However, this funding has not yet been secured centrally by WG and therefore poses a risk to the position if funding is not fully available. This could lead to an impact/affect on the Health Board's underlying deficit position, reduction in stakeholder confidence and increased scrutiny from WG.

Risk Rating:(Likelihood x Impact)		No trend information available.
Domain:	Statutory duty/inspections	
Inherent Risk Score (L x I):	4×5=20	
Current Risk Score (L x I):	4×4=16	
Target Risk Score (L x I):	2×4=8	
Tolerable Risk:	8	
Trend:	*New risk*	

Does this risk link to any Directorate (operational) risks?	

Rationale for CURRENT Risk Score:	Rationale for TARGET Risk Score:
Financial planning assumptions have been assessed assuming up to 12 months of "Low" COVID-19 prevalence (defined as COVID-19 circulating in the community, perhaps at levels of Summer 2021, but lower severity (equivalent to Omicron variant)). Whilst the operational responses and corresponding financial impact of the pandemic during 2020-2022 has provided a sound basis for modelling scenarios, it should be acknowledged that this "Low" scenario may not be the case throughout the year, which may have resource implications. WG funding streams are partly confirmed, however there will be a reliance on the success of bids for specific funding to support the Health Board's further Elective Recovery Plans, specific exceptional costs, transitional COVID-19 support in response to the pandemic and in the acceleration of the Health Board's Strategy. A strategic overhaul of our operating model is required to make the transformational shift in services that are required to deliver workforce and finance sustainability - this is a medium term outlook, but will impact the in-year position. Through our IMTP process, operational plans to address the financial savings gap have not provided sufficient assurance to mitigate the risk, and was an key factor in the Health Board's ability to not submit an IMTP. Whilst it has been committed that the Health Board will submit a financially balanced IMTP by the end of Quarter 1 2022/23, financial assurance will need to be sought to achieve this.	The Health Board needs to demonstrate that it is able to manage its financial position effectively, cognisant of the risks which are inherent in the delivery of safe and timely care. As the actual activity in the Health Board manifests, the level of risk may be considered to be reduced, however further clarity is required by partner organisations and WG as to funding arrangements. Given the challenge in delivering the financial position this year, it is unlikely that the Health Board will achieve a risk which is in line with the tolerable risk for the year. Consequently, the target risk score exceeds the tolerable risk at this point. This is not an acceptable position, and further work is ongoing to manage this risk.

Key CONTROLS Currently in Place:	Gaps in CONTROLS				
(The existing controls and processes in place to manage the risk)	Identified Gaps in Controls : (Where one or more of the key controls on which the organisation is relying is not effective, or we do not have evidence that the controls are working)	How and when the Gap in control be addressed Further action necessary to address the controls gaps	By Who	By When	Progress
1. Modelling of anticipated patient flows, and the resultant workforce, equipment and operational requirements is managed through operational teams. 2. Financial modelling and forecasting is co-ordinated on a regular basis. 3. Timely financial reporting to Directorates, Finance Committee, Board and Welsh Government on local costs incurred as a result of Covid-19 to inform central and local scrutiny, feedback and decision-making. 4. Oversight arrangements in place at Board level and through the Executive Team structure. 5. Exploration of a number of funding streams, including: Local Health Board funding arrangements; Funding arrangements through the Regional Partnership Board and Local Authority partners. Funding from WG's own sources or from HM Treasury via WG.	The costs of addressing the Health Board's local needs may exceed available funding or the organisation my fail to deliver the required level of transformational change during the year through which the opening cost base is expected to be rationalised. This is in relation to the continuation of core and other services, the direct and transitional response to COVID-19, specific exceptional costs and the delivery of Recovery and Sustainability Plans.	Feedback/clarity from WG as to levels of additional revenue and capital funding available	Thomas, Huw	30/06/2022	WG feedback is awaited.
		Develop Target Operating Models across key identified themes, linked to the identified savings opportunities, in line with the Health	Carruthers, Andrew	22/06/2022	Work underway.
		Develop Target Operating Models across key identified themes, linked to the identified savings opportunities, in line with the Health Board's strategy, "A Healthier Mid and West Wales€ and align to the design assumptions set out in that. Follow the "Enquire, Discover, Design, Deliver, Evaluate" workplan set by the Executive Team in line with the key milestones. Themes: CHC packages, Primary Care and OOH.	Paterson, Jill	22/06/2022	Work underway.

		Develop Target Operating Models across key identified themes, linked to the identified savings opportunities, in line with the Health Board's strategy, "A Healthier Mid and West Wales†€• and align to the design assumptions set out in that. Follow the "Enquire, Discover, Design, Deliver, Evaluate" workplan set by the Executive Team in line with the key milestones. Theme: Workforce redesign.	Gostling, Lisa	22/06/2022	Work underway.
6. Opportunities Framework and Roadmap to Financial Sustainability, refreshed to identify alternative ways of working in response to COVID-19 that may result in cost reductions/formal savings schemes identified. Linked to Target Operating Model (TOM) workplan, which will be shaped by the Health Board's strategy, "A Healthier Mid and West Wales†€• and align to the design assumptions set out in that.					
7. Accountability statements in relation to the Opening Directorate Budgets underpinning the draft interim Financial Plan for 2022/23 will issued to all budget holders in April 2022. The letters clarify that it is expected that all budget holders manage their services within their allocated budgetary envelope; that it is incumbent on all to ensure that expenditure, including the operational response to COVID-19, represents best value; and, that there is the expectation that these operational needs can be clearly demonstrated and that additional costs will reduce as and when decisions are made.		Develop Target Operating Models across key identified themes, linked to the identified savings opportunities, in line with the Health Board's strategy, "A Healthier Mid and West Wales†€• and align to the design assumptions set out in that. Follow the "Enquire, Discover, Design, Deliver, Evaluate" workplan set by the Executive Team in line with the key milestones. Theme: Digital Transformation.	Thomas, Huw	22/06/2022	Work underway.
8. Performance against plan monitored through System Engagement Meetings with Services, including Performance, Quality and Financial information. To be improved through Improving Together.					
9. Implementation of systems for efficiency (Malinko, WellSky, Nurse Documentation system) are driving financial systems for control (Symbiotics, Caf M in Facilities and Estates, Allocate), alongside the Digital Strategy improving grip and control.		Develop Target Operating Models across key identified themes, linked to the identified savings opportunities, in line with the Health Board's strategy, "A Healthier Mid and West Wales†€• and align to the design assumptions set out in that. Follow the "Enquire, Discover, Design, Deliver, Evaluate" workplan set by the Executive Team in line with the key milestones. Theme: Clinical Support Services.	Shakeshaft, Alison	22/06/2022	Work underway.
		Develop Target Operating Models across key identified themes, linked to the identified savings opportunities, in line with the Health Board's strategy, "A Healthier Mid and West Wales†€• and align to the design assumptions set out in that. Follow the "Enquire, Discover, Design, Deliver, Evaluate" workplan set by the Executive Team in line with the key milestones. Theme: Community and non-clinical estates strategy.	Davies, Lee	22/06/2022	Work underway.

ASSURANCE MAP				Control RAG Rating (what the assurance is telling you about your controls	Latest Papers (Committee & date)	Gaps in ASSURANCES				
Performance Indicators	Sources of ASSURANCE	Type of Assurance (1st, 2nd, 3rd)	Required Assurance / Current Level			Identified Gaps in Assurance:	How are the Gaps in ASSURANCE will be addressed / Further action necessary to address the gaps	By Who	By When	Progress
Performance against planned response to COVID-19

In-month financial monitoring | Performance against plan monitored through System Engagement Meetings with | 1st | | | * Mth 12 Finance Report Sustainable Resources Committee April 2022 | None | | | | |
	Sustainable Resources Committee oversight of current performance	2nd								
	Transformation & Financial Report to Board & SRC	2nd								
	WG scrutiny through monthly monitoring returns	3rd								
	WG scrutiny through revised monthly Monitoring Returns (specific COVID-19 template) and through Finance Delivery Unit	3rd								
	Audit Wales Structured Assessment 2022	3rd								

Date Risk Identified:	Oct-21		Executive Director Owner:	Carruthers, Andrew	Date of Review:	Mar-22
Strategic Objective:	5. Safe and sustainable and accessible and kind care		Lead Committee:	Sustainable Resources Committee	Date of Next Review:	May-22

Risk ID:	1335	Principal Risk Description:	There is a risk of clinical services being unable to access patient records, at the correct time and place in order to make the right clinical decisions and provide effective patient care. This is caused by not having a fit for purpose records management infrastructure along with organisational management arrangements which are insufficient in capacity and scope. This could lead to an impact/affect on the interruption to clinical services, ability to provide effective patient care including compliance with and attainment of nationally agreed Cancer, RTT and Stroke targets, review and fine by the ICO (<£17.5m - £35m fine per episode), increased litigation and negligence claims, complaints and possible redress, non-compliance with GDPR in regards access to patient information, underutilisation of clinical staff, outpatient facilities and day case areas and theatres, inappropriate disclosure of confidential information, missing patient information and confidential documentation, and non-compliance with nationally agreed retention timescales.

Risk Rating:(Likelihood x Impact)

Domain:	Quality/Complaints/Audit
Inherent Risk Score (L x I):	4×4=16
Current Risk Score (L x I):	4×3=12
Target Risk Score (L x I):	2×3=6
Tolerable Risk:	8

Does this risk link to any Directorate (operational) risks?		Trend:	⬌

Rationale for CURRENT Risk Score:

Currently across the Health Board there is a considerable variance in both practice and process, operationally when utilising and dealing with the various types of records in use throughout directorates, services and departments. The current records management methodology, results in a non-standardised approach to delivering effective records management arrangements. With a lack of agreed criteria in terms of managing the record during its life cycle from creation, during retention and to disposable. There is a requirement for an investment in a modern day solution and an alteration to culture and attitude that will embrace change and technology associated with a digital health record (DHR), to manage the risk. The Health Board has selected its electronic document management system (EDMS) supplier.

Rationale for TARGET Risk Score:

The implementation of a full DHR will support and resolve a number of issues currently being experienced across the Health Board. Prior to making a record digital all services and identified IAO's will have to undertake a full review of their records management arrangements and work in conjunction with a robust criteria to ensure processes follow a standardised approach. A DHR resolves any issues we may currently be experiencing with regards the lack of storage capacity, provision of records in line with GDPR requirements, the ability to facilitate additional clinical requests, the transition to a virtual world, cost benefits, as well as many others. To assist implementation a requirement for adaptation to working practice and a considerable change in culture for future success.

Key CONTROLS Currently in Place:	Gaps in CONTROLS				
(The existing controls and processes in place to manage the risk)	Identified Gaps in Controls : (Where one or more of the key controls on which the organisation is relying is not effective, or we do not have evidence that the controls are working)	How and when the Gap in control be addressed Further action necessary to address the controls gaps	By Who	By When	Progress
Health Board Information Asset Register	An absence of a sustainable long term solution for records management and storage	Acquisition of a electronic document management system (EDMS) suited to receive the management document retrieval on an searchable basis	Tracey, Anthony	Completed	Complete - Civica Cito has been selected as the Health Boards EMDS supplier.
Identified Information Asset Owners (IAOs)					

Health Records Policies, Procedures and SOPs Some digitalisation projects commenced, eg, physiotherapy, A&E cards Health Board e-nursing documentation implementation Electronic systems including: WPAS (Welsh Patient Administration System), WCP (Welsh Clinical Portal), PACS (Radiology), LIMS (Pathology), WAP e-referrals (Welsh Admin Portal), CANIS (Cancer), Diabetes 3, Selma Acquired additional storage facilities to both accommodate excess paper records and establishing a scanning bureau Reduced understanding or records types (across various services) and those appropriate for scanning, long term storage or destruction, leading to a non-consistent criteria for records management during the records life cycle from creation, to retention and ultimate destruction. With the requirement to implement and standardise health records protocols across all services. Acquisition of a electronic document management system (EDMS).	In its paper form, the health record is not under teh accountability of any one Executive and hence the degree of influence is potentially compromised. Reduced understanding or records types (across various services) and those appropriate for scanning, long term storage or destruction, leading to a non-consistent criteria for records management during the records life cycle from creation, to retention and ultimate destruction. With the requirement to implement and standardise health records protocols across all services.	Develop and implement scanned health record solution over the next 5-7 years depending on the split between determination of scanning and deep storage (DHR).	Carruthers, Andrew	31/03/2028	£300k per annum for three years made available to prime the project to include acquiring premises to facilitate a scanning bureau along with appointment of a project manager. A paper outlining the direction of travel and key steps to be taken was presented to executive team 28 July 2021 and this was broadly supported. A project implementation plan along with specification for acquiring scanners is being progressed.
		Review current records management arrangements for records that are not within the scope and responsibility of the Central Health Records function. This will require agreement on future record management arrangements, required resources and project support going forward as an essential precursor to the delivering the scanning phase of the project plan. This will be largely driven by individual information asset owners providing comprehensive schedules of information assets under their responsibility.	Carruthers, Andrew	30/04/2022	A proposal will be submitted to Executive Team by 30/04/22.

ASSURANCE MAP				Control RAG Rating (what the assurance is telling you about your controls	Latest Papers (Committee & date)	Gaps in ASSURANCES				
Performance Indicators	Sources of ASSURANCE	Type of Assurance (1st, 2nd, 3rd)	Required Assurance Current Level			Identified Gaps in Assurance:	How are the Gaps in ASSURANCE will be addressed Further action necessary to address the gaps	By Who	By When	Progress
	Information Asset Owner Registers Group	1st			Records Storage SBAR - Executive Team (Jul21)		Agree formal reporting arrangements with Head of Corporate Governance	Rees, Gareth	Completed	Following Mar22 Board where the 3 year Annual Plan 2022/25 was agreed, the planning objectives are in the process of being aligned to Committee Workplans for 2022/23. 5M has been aligned to SDODC.
	Digital Health Records Project Group to oversee delivery of enabling work	2nd								

SDODC overseeing delivery of Planning Objective 5M	2nd		
IA Records Management Report (limited - follow up (reasonable) in Health Records only	3rd		