

Board of Directors (in Public)

Item 5.5

Subject: High Risk Report
Date of meeting: 29th April 2025
Prepared by: Helen Martin, Head of Risk Management
Purpose of report: To Note

BAF Reference	Impact on BAF
All	The report includes high level risks which continue to be considered in respect of any implications for the BAF.

Level of assurance (please tick) To be used to provide the Board / Committee with a guide on the extent of assurance and evidence of assurance provided within the report		<input checked="" type="checkbox"/>
Level of assurance	Description	
High	There is a strong system of internal control which has been effectively designed to meet the system objectives, and that controls are consistently applied in all areas reviewed.	<input type="checkbox"/>
Substantial	There is a good system of internal control designed to meet the system objectives, and that controls are generally being applied consistently.	<input checked="" type="checkbox"/>
Moderate	There is an adequate system of internal control, however, in some areas weakness in design and/or inconsistent application of controls puts the achievement and some aspects of the system objectives at risk.	<input type="checkbox"/>
Low	There is a compromised system of internal control as weaknesses in the design and / or inconsistent application of controls puts the achievement of the system objectives at risk.	<input type="checkbox"/>
No	There is an inadequate system of internal control as weaknesses in control, and/or consistent non-compliance with controls could/has resulted in failure to achieve the system objectives.	<input type="checkbox"/>

1. Executive Summary

The Risk Registers contain significant risks identified as having potential impact on the trust objectives. These include risks identified and escalated by the Clinical Divisions.

Risks are reviewed monthly at each Divisional Governance meeting and quarterly by the Risk Management Committee.

This report provides an update of risks with residual scores of 15 or higher along with the action plans in place to control and/or mitigate them.

Other highlights: Emergency Planning Resilience Response

Business continuity plans and scenario testing

EPRR KPI's are reported through the EPRR group to monitor compliance.

Key performance indicators that are being measured to ensure the BCMS is being applied effectively are:

- At least 95% of clinical areas will be subject to a scenario/exercise test annually.
- At least 95% of non-clinical areas will be subject to a scenario/exercise test annually.
- At least 90% of area business continuity plans will be updated, approved, and uploaded onto the intranet annually.
- The testing regime will be subject to an annual audit to ensure the clinical and non-clinical areas are exercised as per the KPI's.

As of April 2025:

- 100% of clinical areas have been subject to a scenario test in the last 12 months.
- 100% of non-clinical areas have been subject to a scenario test in the last 12 months.
- 90% Business continuity plans are in date (80% reported by document control)
- Scenario testing was carried out between April and June 2024, so they are due to recommence Q1 25/26.

Joint Evacuation Exercise

Meetings have taken place with the Divisional Manager at LUFHT on the Broadgreen site to commence planning for a live site exercise which will it is envisaged will take place in May and include the BGH wards/areas

Training

C&M ICB have sent a TNA to expressions of interest in specific training

- Legal Awareness Training
- Media Training
- Structured Debrief Training
- Level 3 in Education and Training

A number of the divisional leads have also enrolled on the JESIP and Joint Decision Making Model Courses. The communications team have enrolled on the EPRR Communications Awareness and Foundations of Health Command courses.

The Risk Management Coordinator attended the Structured Debrief Training in February.

Debriefs are not solely for when things go wrong, they could also be held following successes to extract learning.

A loggist training package has been developed. Sessions will be held in the next few months to train more staff and add to our number of available loggists.

Cyber Incident

The external report regarding the cyber incident (Granite Fern) that occurred in November 2024 and affected Liverpool Heart and Chest and Alder Hey Hospitals has been completed by NHS England. The report describes the event and makes a number of recommendations, which include

- Reviewing password complexity policies

- Review multi factor Authentication (MFA) policies on external access and administrative accounts
- Rebuilding of assets affected by the attacker and conducting a health check through the security provider.
- Commissioning a third party vulnerability assessment
- Creating a security strategy and defining cyber security risk appetite.

The LHCH internal cyber report has been presented to the EPRR group for discussion and information.

2. Key Issues

There are currently **three** risks that have a score of 15 or above. This report is correct as of 7th April 2025.

The risks are as follows:

Risk ID ⇄	Risk Owner	Date	Review Date	Residual Score	Target Score
Corporate Services - Risk 00001067	Estates Manager	Oct 2018	Apr 2025	16	6
Description	There is a risk to the structural integrity of the surgical corridor floor				
Controls	<p>structural inspection carried out June/July 2021. TDE appointed as contractor and have completed propping works to rectify the issue.</p> <p>follow up inspection completed in 2024 to review current controls and check for any further deterioration. further works now required to install additional structural supports following receipt of report. risk increased to 16 until structural works are completed. funding for works approved at Jan 25 CMG for completion April 25</p>				
Actions	annual assessments by structural engineer				

Risk ID ⇄	Risk Owner	Date	Review Date	Residual Score	Target Score
Corporate Services - Risk 00002038	Head of IT	Jun 2024	Apr 2025	16	12
Description	There is a risk to ISCV clinical data security				
Controls	<p>Controls from risk #2046 31/7/24 In the short term, the trust IT support team have looked at various methods to reduce existing stored data or expand the available storage. This has included removing unused and unneeded data and removing the storage replication, freeing up additional space for data storage.</p> <p>Controls from risk #2046 31/7/24 An overarching infrastructure strategy is in production which will look to provide a long term solution which matches the trusts future storage requirements.</p> <p>IT are reviewing options with suppliers and hope to have them together by end of mid-Feb. Head of IT will be working up a business case once requirements and costs are finalised.</p> <p>IT have been provided with options from their supplier CDW which they are currently reviewing (Jan 2025). A business case will be generated and signed off by the end with the expectation of implementation in March.</p>				

	<p>27/01/2025 Awaiting confirmation that business case has been approved to enable the procurement of a storage solution</p> <p>13/03/2025 review of the archives by PACS Mgr/IT revealed that 70TB/119TB exist as a single copy.</p>
Actions	<p>In light of the INC cyber incident IT have been asked to take the ISCV archives offline until all remediation activities are complete and NHSE/KPMG report that no threat actors are present on the network.</p> <p>10/02/2025 In light of the disengagement of LHCH from iDigital this piece of work is unlikely to be commenced before 1st April</p>

Risk ID ⇄	Risk Owner	Date	Review Date	Residual Score	Target Score
Corporate Services - Risk 00002063	Head of IT	Jul 2024	Apr 2025	16	12
Description	<p>There is a significant risk of data loss (patient, clinical and corporate), which could severely impact patient care and clinical operations. The current backup strategy does not meet the 3-2-1 NCSC guidelines, with limited retention periods and insufficient replication. Current EPR Daily Backup retention has been reduced to 14 days from 30days, and is replicated for the production environment for 14 days, but only 7 days for Test and Dev Environments. Monthly archives exist for up to 6 months, although this is closely managed due to capacity concerns and at risk also. For all other systems being backed up on the Rubrik Backup Infrastructure, these are being backed up daily but retention is currently set to 7 days with no replication. Therefore we have no offsite/secondary location for backups in a DR scenario and unable to retrieve any data that may have been deleted/corrupted older than 7 days.</p>				
Controls	<p>Regular Testing and Monitoring: - Verifying Backups and their Integrity through regularly testing backups. - - Monitor backup processes to detect and address any issues promptly.</p>				
Actions	<p>Mitigation Plan: Enhance Backup Retention: Increase Retention Periods: Extend the retention periods for both EPR and other critical systems to ensure data is available for longer recovery windows. Implement Offsite Backups: Replicate Data Offsite: Ensure that backups are stored in multiple locations, including offsite or cloud-based solutions, to protect against site-specific disasters. Adopt Comprehensive Backup Solutions: Utilise Advanced Features: Leverage Rubrik’s advanced (Enterprise) features, such as automated backup verification and ransomware detection, to enhance data protection and recovery capabilities. Business case scoped to secure capital and revenue investment to expand the current Rubrik Infrastructure and consider enhanced options found in Rubrik’s enterprise suite offering. This business case is in production and will be submitted to Feb's Capital Board for approval. LHCH has been awarded capital funding which will support closing this risk</p>				

Static score	Increasing score	Decreasing score	New Risk
⇄	↑	↓	◆

3. Recommendation

The Board of Directors is asked to note the content of this report and be assured the Trust has systems and processes in place for the identification, management and escalation of risks.