# APPENDIX 5

# 024/25 EPRR Report

| Ref | Domain | Standard | Deep Dive question | Supporting evidence- including examples of evidence | Organisational Evidence - Please provide details of arrangements in order to capture areas of good practice or further development. (Use comment column if required) | Self assessment RAG<br>Red (not compliant) = Not evidenced in EPRR arrangements.<br>Amber (partially compliant) = Not evidenced in EPRR arrangements but have plans in place to include in the next 12 months.<br>Green (fully compliant) = Evidenced in plans or EPRR arrangements and are tested/exercised as effective. | Action to be taken | Lead | Timescale | Comments |
|---|---|---|---|---|---|---|---|---|---|---|
| **Deep Dive - Cyber Security and IT related incident response (NOT INCLUDED WITHIN THE ORGANISATION'S OVERALL EPRR ASSURANCE RATING)** | | | | | | | | | | |
| DD1 | Deep Dive Cyber Security | Cyber Security & IT related incident preparedness | Cyber security and IT teams support the organisation's EPRR activity including delivery of the EPRR work programme to achieve business objectives outlined in organisational EPRR policy. | -Cyber security and IT teams engaged with EPRR governance arrangement and are represented on EPRR committee membership (TOR and minutes)<br>- Shared understanding of risks to the organisation and the population it serves with regards to EPRR - organisational risk assessments and risk registers<br>-Plans and arrangements demonstrate a common understanding of incidents in line with EPRR framework and cyber security requirements.<br>-EPRR work programme<br>-Organisational EPRR policy | 2024 - NHS - SaTH - EPRR - Core Standards - Evidence DOC 004 - EPRR002 SaTH Major Incident EPRR Policy V4.2.1<br>2024 - NHS - SaTH - EPRR - Core Standards - Evidence DOC 015 - BAF for FPAC, QSAC, ARAC and Board v1.1 Apr 24 - Q4 2023-24<br>2024 - NHS - SaTH - EPRR - Core Standards - DEEP DIVE Evidence DOC 016 - WMLRF Cyber Response Framework 2021_11_18<br>2024 - NHS - SaTH - EPRR - Core Standards - DEEP DIVE Evidence DOC 014 - SaTH_DRBC_Policy_1.1 | Partially compliant | Continue to keep Cyber risk on the EPRR Agenda<br>Contue to include Cyber Incident scenarios in BC Exercises<br>Maintain cyber related risk assessments on the Corporate Risk Register and BAF<br>Continue to work closely with the Digital Team in the development of EPRR plans, training and exercises. | | | |
| DD2 | Deep Dive Cyber Security | Cyber Security & IT related incident response arrangements | The organisation has developed threat specific cyber security and IT related incident response arrangements with regard to relevant risk assessments and that dovetail with generic organisational response plans. | Arrangements should:<br>-consider the operational impact of such incidents<br>-be current and include a routine review schedule<br>-be tested regularly<br>-be approved and signed off by the appropriate governance mechanisms<br>-include clearly identified response roles and responsibilities<br>-be shared appropriately with those required to use them<br>-outline any equipment requirements<br>-outline any staff training needs<br>-include use of unambiguous language<br>-demonstrate a common understanding of terminology used during incidents in line with the EPRR framework and cybersecurity requirements.' | 2024 - NHS - SaTH - EPRR - Core Standards - DEEP DIVE Evidence DOC 014 - SaTH_DRBC_Policy_1.1<br>2024 - NHS - SaTH - EPRR - Core Standards - Evidence DOC 122 - Cutover and early live Support Plan V6<br>DD Documents 001-014 uploaded onto futures in support of this standard | Partially compliant | risk on the EPRR Agenda<br>1. Request an agenda item at SaTH Risk Management Committee<br>2. ICB and Trust Cyber specific forum to be established. Cyber Operational Group Chaired by Sam Tilley (STW ICB). Action notes from last meeting included (Cyber Operational Group Action Notes 17 May 24)<br>3. IT DR Plans to be submitted as evidence Included IT DR Policy along with DR Plans for critical supporting infrastructure<br>4. Digital Team Training Needs Analysis<br>5. Tactical Commander and Executive on Call | | | |
| DD3 | Deep Dive Cyber Security | Resilient Communication during Cyber Security & IT related incidents | The organisation has arrangements in place for communicating with partners and stakeholders during cyber security and IT related incidents. | Arrangements should consider the generic principles for enhancing communications resilience:<br>1. look beyond the technical solutions at processes and organisational arrangements<br>2. identify and review the critical communication activities that underpin your response arrangements<br>3. ensure diversity of technical solutions<br>4. adopt layered fall-back arrangements<br>5. plan for appropriate interoperability<br>https://www.england.nhs.uk/wp-content/uploads/2019/03/national-resilient-telecommunications-guidance.pdf | 2024 - NHS - SaTH - EPRR - Core Standards - Evidence DOC 097 - SaTH - EPRR communications planv2.1<br>2024 - NHS - SaTH - EPRR - Core Standards - Evidence DOC 082 - Genesys Exercise Notification Alert 12.07.24<br>2024 - NHS - SaTH - EPRR - Core Standards - DEEP DIVE Evidence DOC 016 - WMLRF Cyber Response Framework 2021_11_18 | Fully compliant | Request that the LRF Cyber Response Framework is updated in advance of annual assurance deadline. The current version has been uploaded as evidence | | | |
| DD4 | Deep Dive Cyber Security | Media Strategy | The organisation has Incident communication plans and media strategies that include arrangements to agree media lines and the use of corporate and personal social media accounts during cyber security and IT related incidents | - Incident communications plans and media strategy give consideration to cyber security incidents activities as well as clinical and operational impacts.<br>- Agreed sign off processes for media and press releases in relation to Cyber security and IT related incidents.<br>- Documented process for communications to regional and national teams<br>- Incident communications plan and media strategy provides guidance for staff on providing comment, commentary or advice during an incident or where sensitive information is generated. | 2024 - NHS - SaTH - EPRR - Core Standards - Evidence DOC 097 - SaTH - EPRR communications planv2.1<br>2024 - NHS - SaTH - EPRR - Core Standards - Evidence DOC 082 - Genesys Exercise Notification Alert 12.07.24<br>2024 - NHS - SaTH - EPRR - Core Standards - DEEP DIVE Evidence DOC 016 - WMLRF Cyber Response Framework 2021_11_18 | Fully compliant | | | | |
| DD5 | Deep Dive Cyber Security | Testing and exercising | The exercising and/ or testing of cyber security and IT related incident arrangements are included in the organisations EPRR exercise and testing programme. | - Evidence of exercises held in last 12 months including post exercise reports<br>- EPRR exercise and testing programme | 2024 - NHS - SaTH - EPRR - Core Standards - Evidence DOC 084 - 2023 10 06 Business Continuity Summit_Opening and EJB Slides AM<br>2024 - NHS - SaTH - EPRR - Core Standards - Evidence DOC 086 - 2024 02 28 EPR Desktop Review V1.1 | Fully compliant | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **DD6** | Deep Dive Cyber Security | Continuous Improvement | The organisation's Cyber Security and IT teams have processes in place to implement changes to threat specific response arrangements and embed learning following incidents and exercises | - Cyber security and IT colleagues participation in debriefs following live incidents and exercises<br>- lessons identified and implementation plans to address those lessons<br>-agreed processes in place to adopt implementation of lessons identified<br>- Evidence of updated incident plans post-incident/exercise | 2024 - NHS - SaTH - EPRR - Core Standards - Evidence DOC 011 - SaTH MASTER Post Incident and Exercise Learning Log July 2024 | Fully compliant | |
| **DD7** | Deep Dive Cyber Security | Training Needs Analysis (TNA) | Cyber security and IT related incident response roles are included in an organisation's TNA. | - TNA includes Cyber security and IT related incident response roles<br>- Attendance/participant lists showing cybersecurity and IT colleagues taking part in incident response training. | TNA needs to be amended to incude the Digital Team | Partially compliant | Training Needs Analysis to be amended to include Cyber awareness and Digital Team |
| **DD8** | Deep Dive Cyber Security | EPRR Training | The oranisation's EPRR awareness training includes the risk to the organisation of cyber security and IT related incidents and emergencies | -Cyber security and IT related incidents and emergencies included in EPRR awareness training package | 2024 - NHS - SaTH - EPRR - Core Standards - Evidence DOC 084 - 2023 10 06 Business Continuity Summit_Opening and EJB Slides AM<br>2024 - NHS - SaTH - EPRR - Core Standards - Evidence DOC 086 - 2024 02 28 EPR Desktop Review V1.1 | Partially compliant | |
| **DD9** | Deep Dive Cyber Security | Business Impact Assessments | The Cyber Security and IT teams are aware of the organisations's critical functions and the dependencies on IT core systems and infrastrucure for the safe and effective delivery of these services | -robust Business Impact Analysis including core systems<br>-list of the organisations critical services and functions<br>-list of the organisations core IT/Digital systems and prioritisation of system recovery | 2024 - NHS - SaTH - EPRR - Core Standards - Evidence DOC 112 - Business Continuity Policy v10 2024<br>2024 - NHS - SaTH - EPRR - Core Standards - DEEP DIVE Evidence DOC 014 - SaTH_DRBC_Policy_1.1<br>See also DD Evidence Documents 001-015 on NHS Futures | Fully compliant | |
| **DD10** | Deep Dive Cyber Security | Business Continuity Management System | Cyber Security and IT systems and infrastructure are considered within the scope and objectives of the organisation's Business Continuity Management System (BCMS) | -Reflected in the organisation's Business Continuity Policy<br>-key products and services within the scope of BCMS<br>-Appropriate risk assessments | 2024 - NHS - SaTH - EPRR - Core Standards - Evidence DOC 026 - BCP & SaTH BC Management System (BCMS) consultation (EPRR Core standard 44-54)<br>2024 - NHS - SaTH - EPRR - Core Standards - Evidence DOC 015 - BAF for FPAC, QSAC, ARAC and Board v1.1 Apr 24 - Q4 2023-24<br>2024 - NHS - SaTH - EPRR - Core Standards - Evidence DOC 021 - SaTH - 2024 07 19 All EPRR Related Risks | Fully compliant | |
| **DD11** | Deep Dive Cyber Security | Business Continuity Arrangments | IT Disaster Recovery arrangements for core IT systems and infrastructure are included with the organisation's Business Continuity arrangements for the safe delivery of critical services identified in the organisation's business impact assessments | - Business Continuity Plans for critical services provided by the organisation include core systems<br>-Disaster recovery plans for core systems<br>-Cyber security and IT departments own BCP which includes contacts for key personnel outside of normal working hours | See DD Documents 001-015 for evidence on NHS Futures | Fully compliant | |