Board of Directors – Public

SUMMARY REPORT	Meeting Date:	27 November 2024
	Agenda Item:	21

Report Title:	Emergency Preparedness Resilience Response (EPRR) Assurance Framework 24-25 Submission	
Author(s):	Jean Kiyori – Emergency Planning Manager	
Accountable Director:	Neil Robertson – Executive Director of Operations	
Other meetings this paper has been presented to or previously agreed at:	**Committee/Tier 2 Group/Tier 3 Group**	Audit and Risk committee (ARC) Board of Directors Development, Planning and Strategy
	Date:	15 October 2024 23 October 2024
Key points/ recommendations from those meetings	**ARC 15th October 2024** Assurance was given that the organisation is on track against the overall trajectory to achieve full compliance, and that significant improvements have been made to the rate of compliance compared to where we've been. ARC was advised that SHSC benchmarks comparably to other Mental Health Trusts and are likely to outperform other MH Trusts against the standards, but this is yet to be seen as a result of the exercise undertaken which is in the initial stages. The committee were alerted to the risk relating to standards that are applied to universally across all Trusts which relates to the exposure of chemical, biological, radiological, and nuclear materials. It was noted that this is unlikely to occur in a mental health trust and might be more common in acute trusts and as such, there is assurance that there is sufficient mitigation in place against those risks. **Board Development, Planning and Strategy Day 23rd October 2024** The paper and framework was presented at the Board Development, Planning and Strategy session as an agenda item because of the need to meet the submission deadline to the Integrated Care Board (ICB) for review. The assurance framework was approved for submission, and it was agreed that the paper and framework will be shared and noted at the Public Board in November 2024. The board were advised about our position in relation to bolstering EPRR standards by releasing other leaders with EPRR experience as required. It was also advised that discussions are taking place to remove four of the core standards for Mental Health Trust's due to the requirement not being	

	deemed applicable. Feedback was given the Director of Finance about the cyber and digital incidents deep dive and the associated action plan. The deep dive is a self-assessment that will not be subject to any further review externally.

Summary of key points in report

Sheffield Health and Social Care NHS Foundation Trust (SHSC) needs to plan for, and respond to, a wide range of incidents and emergencies that could affect patient care. Incidents may range from extreme weather conditions, an outbreak of an infectious disease, or a hospital evacuation. The Civil Contingencies Act (2004) requires all NHS organisations, and providers of NHS-funded care to deal with such incidents while maintaining services. The EPRR core standards published annually are designed to provide assurance.

Background

The Board will be aware that the 2024/25 core standards brought with them 6 new standards and significant additional requirements to meet all the standards, together with a new process for submission that involved trusts submitting evidence against each standard to be inspected by NHS England.

In line with all trusts in the region, SHSC were non-compliant. Last year (2023-24) our overall rating was 10% compliance with 6 green core standards and 52 amber core standards. An action plan was proposed in December 2023 providing timescales for meeting those standards deemed partially compliant, that we are currently able to. However, it was agreed by the ICB that SY providers and ICB themselves, would work to overall compliance by the end of October 2025.

SHSC Current Position

We can report that we have self-assessed against the criteria that 47 core standards are now Green (74%), 15 amber core standards and 1 red core standard. This is subject to an ICB review following submission of our assessment on the 31 October 2024.

Many plans and policy have been sent to Trust Emergency Preparedness Group (TEPG) in the last months for approval and taken through to Policy Governance Group (Policy approval) and Audit and Risk Committee (Plans) for sign off:

Standards no	Standard name
14	New and Emerging Pandemics Plan
20	On Call Policy
23&48	EPRR Work Plan
28&50	Business Continuity Management System
47	New Business Continuity Plan template
CBRN	Hazmat /CBRN Awareness for Reception and Pharmacy staff

The list of documents approved and signed off that are part of our compliance are as follows:

- EPRR Core Standards Action Plan
- TEPG Terms of Reference
- Policies from PGG – EPRR Policy
- Business Continuity Policy
- Business Continuity Plan Template

- Business Continuity Management System
- Lockdown Policy
- VIP Policy
- Adverse Weather and other emergency conditions
- Heatwave Plan
- Evacuation Plan YH Low Medium Secure Plan
- CBRNe Plan
- Major and Critical Incident Plan
- Emergency Plan – Communications

SHSC will be submitting in region of 180 documents of evidence to support our submission.

Predicted Compliance Rate this year

The compliance rate (initially 74%) is highly likely to drop down. Our predicated compliance rate is likely to be between 57% and 65%. This is primarily due to a lack of clear guidance and useful information on the domain 10: CBRN Core standards, and secondarily to domain 5 which relates to training and exercising and any other requested evidence which we may not be able to provide. Regarding training plans are in place to address the minimum standard over the next 12 months, though it is important to the note that the expectations are equivalent to the current mandatory training requirements of a line manager.

NHS England Regional and South Yorkshire ICB process for 2024-25

Building on the process last year, there is no expectation of how many standards an organisation should be moving to a compliant position, however, organisations should be able to demonstrate progress they have made against their final position in 2023. Below is the proposed process and timelines for 2024:

The NHS England process this year is that ICBs will agree how local assurance will be undertaken (evidence submissions, peer reviews, check & challenge sessions etc) and system level assurance arrangements via their Local Health Resilience Partnership (LHRP), with a focus on seeking assurance that any standards assessed as Partial or Non-compliant in 2023. This has been through an internal check & challenge process and advice and support from partners to ensure reliability before submitting a self-assessment of full compliance this year. The process is as follows:

- The regional EPRR team will provide support and guidance to this process at the request of each ICB – this will be agreed via LHRPs and confirmed by ICBs to the September Regional Health Resilience Partnership (RHRP).
- Organisations will undertake a self-assessment against the 2024/25 core standards, which will be submitted to their ICB by or on 31st October. ICBs will also submit their self-assessments to NHS England NEY on this date. The self-assessment must be signed of by the board this submission date and is on the agenda.
- As normal, LHRPs will undertake formal confirm & challenge sessions post receipt of the organisation's self-assessments before submission of LHRP reports to the regional team at the end of November.
- The regional team will then work with ICBs to obtain organisational level assurance ratings and agree next steps to share learning and best practice ahead of the 2025/26 work programme being agreed, as per the timescale set out below.
- **Early November (dates and process TBC)**: Formal review meetings will be held between the ICB and each provider's AEO and EPRR teams to review their submission. Arrangements will be confirmed once it is known how many standards overall are being put forward for evidence reviews and how much time will be required for each meeting.
- **19th November –** Check & Challenge LHRP meeting will take place to allow for peer review and discussion of submissions, including agreement of monitoring process for

2025.

- **Late November, date TBC** - ICB meets with NHS England NEY team to review the South Yorkshire submissions.
- **2 Dec 2024** – the final ratings for South Yorkshire will be shared with the NEY Regional Health Resilience Partnership (RHRP). Boards should then sign off the finalised organisational positions at the earliest opportunity following this date and share the paper(s) with the ICB.

If following the discussion, there is a difference in the provider organisations' rating for a core standard and the ICB perception of what the rating should be, then the provider organisation is asked to provide details of this in their subsequent Board report on their core standards rating.

2024/25 deep dive: Cyber Security and IT Related Incidents

Each year, alongside the annual assurance process, a 'deep dive' is conducted to gain valuable additional insight into a specific area. Following recent incidents and common health risks raised as part of last year's annual assurance process, the 2024/25 EPRR annual deep dive will focus on responses to cyber security and IT related incidents. The deep dive questions are applicable to those organisations indicated within the EPRR self-assessment tool. Please note that compliance ratings against individual deep dive questions do not contribute to the overall organisational EPRR assurance rating. The outcome of the deep dive will be used to identify areas of good practice and further development and as in previous years it is expected that organisations will use their self-assessment to guide the development of local arrangements. SHSC is compliant with 1 standard, partially compliant with 9 standards and not compliant with 1 standard.

More training, exercising and testing SHSC resilience to cyber security plans will be part of action plan to be done by Emergency Planning Manager and Head of Service Delivery & Infrastructure Digital.

The table below shows where SHSC stands with this year deep dive:

Deep Dive	Total standards applicable	Fully compliant	Partially compliant	Non-compliant
Cyber Security	11	1	9	1
Total	11	1	9	1

Conclusion

In summary, we are confident that the overall compliance rate for SHSC this year will be between 57% and 65% following the check and challenge process where we anticipate being and we expect to be in a similar position to other providers in South Yorkshire.

Assurance was given to Audit and Risk committee (ARC) that the organisation is on track against the overall trajectory to achieve full compliance, and that significant improvements have been made to the rate of compliance compared to where we've been.

ARC was advised that SHSC benchmarks comparably to other Mental Health Trusts and are likely to outperform other MH Trusts against the standards, but this is yet to be seen as a result of the exercise undertaken which is in the initial stages.

The committee were alerted to the risk relating to standards that are applied universally across all Trusts which relates to the exposure of chemical, biological, radiological, and nuclear materials. It was noted that this is unlikely to occur in a mental health trust and might be more common in acute trusts and as such, there is assurance that there is sufficient mitigation in place against those risks.

Audit and Risk Committee recommend to the Board that they support this submission for sign off by the

Board of Directors in October 2024.

Appendices
Appendix 1 SHSC NHSE EPRR Core Standards Initial Self-Assessment 2024

Recommendation for the Board/Committee to consider:							
Consider for Action		**Approval**		**Assurance**		**Information**	**x**
The Board are asked to note the SHSC's core standards submission for 2024-2025, which took place in October 2024, and which followed approval at the private Board of Directors meeting in October 2024.							

Please identify which strategic priorities will be impacted by this report:				
Effective Use of Resources	*Yes*	***X***	*No*	
Deliver Outstanding Care	*Yes*	***X***	*No*	
Great Place to Work	*Yes*	***X***	*No*	
Ensuring our services are inclusive	*Yes*	***X***	*No*	

Is this report relevant to compliance with any key standards ?					**State specific standard**
Care Quality Commission Fundamental Standards	*Yes*	***X***	*No*		**Safety, Premises and equipment, Staffing, Good Governance, well led**
Data Security and Protection Toolkit	*Yes*	***X***	*No*		***Data Protection and Security Toolkit – 10 national data guardian standards***
Any other specific standard?		***X***			**NHS England EPRR – 55 core standards for mental health trusts**

Have these areas been considered ? YES/NO					If Yes, what are the implications or the impact? If no, please explain why
Service User and Carer Safety, Engagement and Experience	*Yes*	***X***	*No*		***Failure to maintain some or all of our services; increased risk to service users***
Financial (revenue &capital)	*Yes*	***X***	*No*		***Reputational risk, risk of legal action, removal of funding***
Organisational Development /Workforce	*Yes*	***X***	*No*		***Staff safety, reputation of SHSC aim to create a great place to work***
Equality, Diversity & Inclusion	*Yes*	***X***	*No*		***All EPRR policies include equality related impacts, together with the specific plans that are formed within them***
Legal	*Yes*	***X***	*No*		***Breach of regulatory standards andconditions of Provider Licence***
Environmental sustainability	*Yes*	***X***	*No*		***Loss of power. Inability to maintain our services***

Please select type of organisation: **Acute Providers**

Click button to format the workbook

Publishing Approval Reference: 000719

Core Standards	Total standards applicable	Fully compliant	Partially compliant	Non compliant
Governance	6	6	0	0
Duty to risk assess	2	2	0	0
Duty to maintain plans	11	10	1	0
Command and control	2	1	1	0
Training and exercising	4	2	2	0
Response	7	7	0	0
Warning and informing	4	3	1	0
Cooperation	4	2	2	0
Business Continuity	10	6	4	0
Hazmat/CBRN	12	7	4	1
CBRN Support to acute Trusts	0	0	0	0
Total	62	46	15	1

Deep Dive	Total standards applicable	Fully compliant	Partially compliant	Non compliant
Cyber Security	11	1	9	1
Total	11	1	9	1

Overall assessment:	Non compliant

Instructions:
Step 1: If you see a yellow ribbon at the top of the page and a button asking you to 'Enable Content' please do so.
Step 2: Select the type of organisation from the drop-down at the top of this page
Step 3: Click on the 'Format Workbook' button.
Step 4: Complete the Self-Assessment RAG in the 'EPRR Core Standards' tab
Step 5: Complete the Self-Assessment RAG in the 'Deep dive' tab
Step 6: Ambulance providers only: Complete the Self-Assessment in the 'Interoperable capabilities' tab
Step 7: In the Action Plan tab, click on the 'Format Action Plan' button.

Ref	Domain	Standard name	Standard Detail	Supporting Information - including examples of evidence	Organisational Evidence	Self assessment RAG Red (not compliant) = Not compliant with the core standard. The organisation's work programme shows compliance will not be reached within the next 12 months. Amber (partially compliant) = Not compliant with core standard. However, the organisation's work programme demonstrates sufficient evidence of progress and an action plan to achieve full compliance within the next 12 months. Green (fully compliant) = Fully compliant with core standard.	Action to be taken	Lead	Timescale	Comments
Domain 1 - Governance										
1	Governance	Senior Leadership	The organisation has appointed an Accountable Emergency Officer (AEO) responsible for Emergency Preparedness Resilience and Response (EPRR). This individual should be a board level director within their individual organisation, and have the appropriate authority, resources and budget to direct the EPRR portfolio.	Evidence • Name and role of appointed individual • AEO responsibilities included in role/job description	Role Holder: Neil Robertson: Director of Operations and Transformation	Fully compliant				
2	Governance	EPRR Policy Statement	The organisation has an overarching EPRR policy or statement of intent. This should take into account the organisation's: • Business objectives and processes • Key suppliers and contractual arrangements • Risk assessment(s) • Functions and / or organisation, structural and staff changes.	The policy should: • Have a review schedule and version control • Use unambiguous terminology • Identify those responsible for ensuring policies and arrangements are updated, distributed and regularly tested and exercised • Include references to other sources of information and supporting documentation. Evidence Up to date EPRR policy or statement of intent that includes: • Resourcing commitment • Access to funds • Commitment to Emergency Planning, Business Continuity, Training, Exercising etc.	EPRR Policy in place - updated and approved at Policy Governance Group 28/03/2022, reviewed annually by AEO/EPRR lead and goes to PGG 3 yearly or earlier if changes identified. Policy on Policies document.	Fully compliant				
3	Governance	EPRR board reports	The Chief Executive Officer ensures that the Accountable Emergency Officer discharges their responsibilities to provide EPRR reports to the Board, no less than annually. The organisation publicly states its readiness and preparedness activities in annual reports within the organisation's own regulatory reporting requirements	These reports should be taken to a public board, and as a minimum, include an overview on: • training and exercises undertaken by the organisation • summary of any business continuity, critical incidents and major incidents experienced by the organisation • lessons identified and learning undertaken from incidents and exercises • the organisation's compliance position in relation to the latest NHS England EPRR assurance process. Evidence • Public Board meeting minutes • Evidence of presenting the results of the annual EPRR assurance process to the Public Board • For those organisations that do not have a public board, a public statement of readiness and preparedness activities.	Periodic reports to Board members through Audit and Risk Committee throughout the year; Results of the annual EPRR assurance process are presented annually to Board meeting, evidenced through report and meeting minutes.	Fully compliant				
4	Governance	EPRR work programme	The organisation has an annual EPRR work programme, informed by: • current guidance and good practice • lessons identified from incidents and exercises • identified risks • outcomes of any assurance and audit processes The work programme should be regularly reported upon and shared with partners where appropriate.	Evidence • Reporting process explicitly described within the EPRR policy statement • Annual work plan	Reporting process is through Audit and Risk Committee, who review progress against the core standards at each meeting on behalf of the Board, in line with the annual work plan formed through the EPRR core standards self-assessment and the annual objectives set by the AEO.	Fully compliant				
5	Governance	EPRR Resource	The Board / Governing Body is satisfied that the organisation has sufficient and appropriate resource to ensure it can fully discharge its EPRR duties.	Evidence • EPRR Policy identifies resources required to fulfil EPRR function; policy has been signed off by the organisation's Board • Assessment of role / resources • Role description of EPRR Staff/ staff who undertake the EPRR responsibilities • Organisation structure chart • Internal Governance process chart including EPRR group	Advised Board at Board Development Presentation on 28/02/2024	Fully compliant				
6	Governance	Continuous improvement	The organisation has clearly defined processes for capturing learning from incidents and exercises to inform the review and embed into EPRR arrangements.	Evidence • Process explicitly described within the EPRR policy statement • Reporting those lessons to the Board/ governing body and where the improvements to plans were made • participation within a regional process for sharing lessons with partner organisations	Updated policy to ARC 16/01/2024 and included in EPRR Work Plan to go to TEPG 27/03/2024	Fully compliant				
Domain 2 - Duty to risk assess										
7	Duty to risk assess	Risk assessment	The organisation has a process in place to regularly assess the risks to the population it serves. This process should consider all relevant risk registers including community and national risk registers.	• Evidence that EPRR risks are regularly considered and recorded • Evidence that EPRR risks are represented and recorded on the organisations corporate risk register • Risk assessments to consider community risk registers and as a core component, include reasonable worst-case scenarios and extreme events for adverse weather	Emergency Planning risk register created on Ulysses and reviews in TOR for TEPG	Fully compliant				
8	Duty to risk assess	Risk Management	The organisation has a robust method of reporting, recording, monitoring, communicating, and escalating EPRR risks internally and externally	Evidence • EPRR risks are considered in the organisation's risk management policy • Reference to EPRR risk management in the organisation's EPRR policy document	Emergency Planning risk register created on Ulysses and reviews in TOR for TEPG	Fully compliant				
Domain 3 - Duty to maintain Plans										

Ref	Domain	Standard name	Standard Detail	Supporting Information - including examples of evidence	Organisational Evidence	Self assessment RAG Red (not compliant) = Not compliant with the core standard. The organisation's work programme shows compliance will not be reached within the next 12 months. Amber (partially compliant) = Not compliant with core standard. However, the organisation's work programme demonstrates sufficient evidence of progress and an action plan to achieve full compliance within the next 12 months. Green (fully compliant) = Fully compliant with core standard.	Action to be taken	Lead	Timescale	Comments
9	Duty to maintain plans	Collaborative planning	Plans and arrangements have been developed in collaboration with relevant stakeholders including emergency services and health partners to enhance joint working arrangements and to ensure the whole patient pathway is considered.	Partner organisations collaborated with as part of the planning process are in planning arrangements Evidence • Consultation process in place for plans and arrangements • Changes to arrangements as a result of consultation are recorded	Collaborative planning takes place both formally and informally. For example, plans such as adverse weather are shared to incorporate good practice, whereas plans such as YH Low Medium Secure Evacuation are formally consulted on as the process requires the agreement of all parties to it. Plans are also shared from time to time in advance of events with place partners e.g. public holidays; North of England MH forum for EPRR matters specific to MH Trusts.	Fully compliant				
10	Duty to maintain plans	Incident Response	In line with current guidance and legislation, the organisation has effective arrangements in place to define and respond to Critical and Major incidents as defined within the EPRR Framework.	Arrangements should be: • current (reviewed in the last 12 months) • in line with current national guidance • in line with risk assessment • tested regularly • signed off by the appropriate mechanism • shared appropriately with those required to use them • outline any equipment requirements • outline any staff training required	Major and Critical Incident Plan in place, reviewed and updated in Inauary 2024.M&CI plan was sent to ARC on 16/01/2024.BCBS was sent to TEPG on 27/03/2024	Fully compliant				
11	Duty to maintain plans	Adverse Weather	In line with current guidance and legislation, the organisation has effective arrangements in place for adverse weather events.	Arrangements should be: • current • in line with current national UK Health Security Agency (UKHSA) & NHS guidance and Met Office or Environment Agency alerts • in line with risk assessment • tested regularly • signed off by the appropriate mechanism • shared appropriately with those required to use them • outline any equipment requirements • outline any staff training required • reflective of climate change risk assessments • cognisant of extreme events e.g. drought, storms (including dust storms), wildfire.	Adverse weather and other emergencies plan reviewed, updated and signed off. 16/01/2024 SHSC Green Plan, UKHSA Adverse Weather and Health Plan 2023	Fully compliant				
12	Duty to maintain plans	Infectious disease	In line with current guidance and legislation, the organisation has arrangements in place to respond to an infectious disease outbreak within the organisation or the community it serves, covering a range of diseases including High Consequence Infectious Diseases.	Arrangements should be: • current • in line with current national guidance • in line with risk assessment • tested regularly • signed off by the appropriate mechanism • shared appropriately with those required to use them • outline any equipment requirements • outline any staff training required Acute providers should ensure their arrangements reflect the guidance issued by DHSC in relation to FFP3 Resilience in Acute setting incorporating the FFP3 resilience principles. https://www.england.nhs.uk/coronavirus/secondary-care/infection-control/ppe/ffp3-fit-testing/ffp3-resilience-principles-in-acute-settings/	Jillian Singleton - Lead Infection Prevention &Control Nurse is leading on this. Lorraine Mitchell at Sheffield City Council has prepared a Mass Treatment and Vaccination Plan that all SY Health Partners have signed up to.The plan has been tested and approved	Fully compliant				
13	Duty to maintain plans	New and emerging pandemics	In line with current guidance and legislation and reflecting recent lessons identified, the organisation has arrangements in place to respond to a new and emerging pandemic	Arrangements should be: • current • in line with current national guidance • in line with risk assessment • tested regularly • signed off by the appropriate mechanism • shared appropriately with those required to use them • outline any equipment requirements • outline any staff training required	New and Pandemics Plan was out for consultation, to TEPG 27/03/2024 before going to ARC for sign off.	Fully compliant				

Ref	Domain	Standard name	Standard Detail	Supporting Information - including examples of evidence	Organisational Evidence	Self assessment RAG Red (not compliant) = Not compliant with the core standard. The organisation's work programme shows compliance will not be reached within the next 12 months. Amber (partially compliant) = Not compliant with core standard. However, the organisation's work programme demonstrates sufficient evidence of progress and an action plan to achieve full compliance within the next 12 months. Green (fully compliant) = Fully compliant with core standard.	Action to be taken	Lead	Timescale	Comments
14	Duty to maintain plans	Countermeasures	In line with current guidance and legislation, the organisation has arrangements in place to support an incident requiring countermeasures or a mass countermeasure deployment	Arrangements should be: • current • in line with current national guidance • in line with risk assessment • tested regularly • signed off by the appropriate mechanism • shared appropriately with those required to use them • outline any equipment requirements • outline any staff training required Mass Countermeasure arrangements should include arrangements for administration, reception and distribution of mass prophylaxis and mass vaccination. There may be a requirement for Specialist providers, Community Service Providers, Mental Health and Primary Care services to develop or support Mass Countermeasure distribution arrangements. Organisations should have plans to support patients in their care during activation of mass countermeasure arrangements. Commissioners may be required to commission new services to support mass countermeasure distribution locally, this will be dependant on the incident.	Jillian Singleton - Lead Infection Prevention &Control Nurse isleading on this. Lorraine Mitchell at Sheffield City Council has prepared a Mass treatment and vaccination Plan that all SY Health Partners have signed up to. Once approved, this will turn green.	Fully compliant				
15	Duty to maintain plans	Mass Casualty	In line with current guidance and legislation, the organisation has effective arrangements in place to respond to incidents with mass casualties.	Arrangements should be: • current • in line with current national guidance • in line with risk assessment • tested regularly • signed off by the appropriate mechanism • shared appropriately with those required to use them • outline any equipment requirements • outline any staff training required Receiving organisations should also include a safe identification system for unidentified patients in an emergency/mass casualty incident where necessary.	Embedded within the Major and Critical Incident Plan. Our plan involves working with our partners at Sheffield Teaching Hospitals to provide psychosocial support to a mass casualty incident. M&CI Plan was sent to ARC on 16/01/2024	Fully compliant				
16	Duty to maintain plans	Evacuation and shelter	In line with current guidance and legislation, the organisation has arrangements in place to evacuate and shelter patients, staff and visitors.	Arrangements should be: • current • in line with current national guidance • in line with risk assessment • tested regularly • signed off by the appropriate mechanism • shared appropriately with those required to use them • outline any equipment requirements • outline any staff training required	Evacuation and YH Low Medium Secure Plan to ARC 16/01/2024. It's been signed off by AEO for final plan and has been circulated to all partners. SHSC Evacuation Plan also approved.	Fully compliant				
17	Duty to maintain plans	Lockdown	In line with current guidance, regulation and legislation, the organisation has arrangements in place to control access and egress for patients, staff and visitors to and from the organisation's premises and key assets in an incident.	Arrangements should be: • current • in line with current national guidance • in line with risk assessment • tested regularly • signed off by the appropriate mechanism • shared appropriately with those required to use them • outline any equipment requirements • outline any staff training required	Lockdown Policy reviewed and updated. Signed off September 2022 Lockdown plans in place for all inpatient facilities .Lockdown Policy was sent to ARC 16/01/2024.	Fully compliant				
18	Duty to maintain plans	Protected individuals	In line with current guidance and legislation, the organisation has arrangements in place to respond and manage 'protected individuals' including Very Important Persons (VIPs),high profile patients and visitors to the site.	Arrangements should be: • current • in line with current national guidance • in line with risk assessment • tested regularly • signed off by the appropriate mechanism • shared appropriately with those required to use them • outline any equipment requirements • outline any staff training required	Visitors Policy reviewed and updated June 2022 includes the management of VIP visits. Protocols in place with Security Policy in the event of VIP admissions/treatment. Safeguarding Policy, individuals care plan and HM Prisons designation of high profile patients. Follow The HM Prisons and Probation Service Designation and Management of High Profile Restricted Patients in respect of Low Secure.	Partially compliant				

Ref	Domain	Standard name	Standard Detail	Supporting Information - including examples of evidence	Organisational Evidence	Self assessment RAG Red (not compliant) = Not compliant with the core standard. The organisation's work programme shows compliance will not be reached within the next 12 months. Amber (partially compliant) = Not compliant with core standard. However, the organisation's work programme demonstrates sufficient evidence of progress and an action plan to achieve full compliance within the next 12 months. Green (fully compliant) = Fully compliant with core standard.	Action to be taken	Lead	Timescale	Comments
19	Duty to maintain plans	Excess fatalities	The organisation has contributed to, and understands, its role in the multiagency arrangements for excess deaths and mass fatalities, including mortuary arrangements. This includes arrangements for rising tide and sudden onset events.	Arrangements should be: • current • in line with current national guidance in line with DVI processes • in line with risk assessment • tested regularly • signed off by the appropriate mechanism • shared appropriately with those required to use them • outline any equipment requirements • outline any staff training required	SHSC have no mortuary facilities but are a partner to the ICS and SYLRF excess death plans; represented by NHS South Yorkshire at SYLRF, ensuring excess fatality arrangements are understood and that we contribute to them as appropriate e.g. Excess Death Cell established March 2020 for the Covid-19 pandemic whereby, not a direct contributor but would work with partners where appropriate.	Fully compliant				
Domain 4 - Command and control										
20	Command and control	On-call mechanism	The organisation has resilient and dedicated mechanisms and structures to enable 24/7 receipt and action of incident notifications, internal or external. This should provide the facility to respond to or escalate notifications to an executive level.	• Process explicitly described within the EPRR policy statement • On call Standards and expectations are set out • Add on call processes/handbook available to staff on call • Include 24 hour arrangements for alerting managers and other key staff. • CSUs where they are delivering OOHs business critical services for providers and commissioners	On-call staff attend an 'Essential training for Managers' Course and receive an on-call pack, the documents of which are also contained within a shared drive folder they all have access to. Switchboard have a Major Incident Plan providing the action to take on notification to alert managers and other key staff 24/7. On call mechanism in place with two levels of on-call - Senior Manager and Executive. On call records kept via MS teams folder for on call staff On call policy out for has been sent to EPG 27/06/2024 before going to PGG and then ARC for sign off.	Fully compliant				
21	Command and control	Trained on-call staff	Trained and up to date staff are available 24/7 to manage escalations, make decisions and identify key actions	• Process explicitly described within the EPRR policy or statement of intent The identified individual: • Should be trained according to the NHS England EPRR competencies (National Minimum Occupational Standards) • Has a specific process to adopt during the decision making • Is aware who should be consulted and informed during decision making • Should ensure appropriate records are maintained throughout. • Trained in accordance with the TNA identified frequency.	All NHS leaders have attended the PHC at the appropriate level (Strategic and Tactical) as currently available. No one goes on the on-call rota until they have completed this. JESIP training is presently being rolled out to strategic leaders.	Partially compliant				
Domain 5 - Training and exercising										
22	Training and exercising	EPRR Training	The organisation carries out training in line with a training needs analysis to ensure staff are current in their response role.	Evidence • Process explicitly described within the EPRR policy or statement of intent • Evidence of a training needs analysis • Training records for all staff on call and those performing a role within the ICC • Training materials • Evidence of personal training and exercising portfolios for key staff	EPRR forms part of mandatory training on induction for all staff. Staff allocated to ICC duties receive training to carry out the actions of their role as per the Major and Critical Incident Plan. New Commander portfolios have been issued to all relevant commanders. Recent live incidents including the COVID pandemic and Industrial Action evidence some areas and work is ongoing to meet the 3 year expectation on meeting compliance that requires NHS England EPRR support. For this reason, we remain partially compliant.The requirement for a Level 3 Education and Training qualification to be included in Person Specification of EPRR lead.	Partially compliant				

Ref	Domain	Standard name	Standard Detail	Supporting Information - including examples of evidence	Organisational Evidence	Self assessment RAG Red (not compliant) = Not compliant with the core standard. The organisation's work programme shows compliance will not be reached within the next 12 months. Amber (partially compliant) = Not compliant with core standard. However, the organisation's work programme demonstrates sufficient evidence of progress and an action plan to achieve full compliance within the next 12 months. Green (fully compliant) = Fully compliant with core standard.	Action to be taken	Lead	Timescale	Comments
23	Training and exercising	EPRR exercising and testing programme	In accordance with the minimum requirements, in line with current guidance, the organisation has an exercising and testing programme to safely* test incident response arrangements, (*no undue risk to exercise players or participants, or those patients in your care)	Organisations should meet the following exercising and testing requirements: • a six-monthly communications test • annual table top exercise • live exercise at least once every three years • command post exercise every three years. The exercising programme must: • identify exercises relevant to local risks • meet the needs of the organisation type and stakeholders • ensure warning and informing arrangements are effective. Lessons identified must be captured, recorded and acted upon as part of continuous improvement. Evidence • Exercising Schedule which includes as a minimum one Business Continuity exercise • Post exercise reports and embedding learning	An Internal Communication test carried out 29/05/2024 by SY ICB to to assess the effectiveness of SHSC Trust communications arrangements when cascading information to all on Call Strategic Health Commanders via switchboard and mobiles phones Exercise Hello), supports test carried out in April 2023 internally. Table-top YH Low/Medium secure evacuation Plan exercise 05/09/2022. We have had a series of live incidents relating to Industrial Action since January 2023. programme of testing BCP's, the most recent being Power Failure in December 2022. Live Critical incident 18/08/23 re: Legionella.	Fully compliant				
24	Training and exercising	Responder training	The organisation has the ability to maintain training records and exercise attendance of all staff with key roles for response in accordance with the Minimum Occupational Standards. Individual responders and key decision makers should be supported to maintain a continuous personal development portfolio including involvement in exercising and incident response as well as any training undertaken to fulfil their role	Evidence • Training records • Evidence of personal training and exercising portfolios for key staff	Key response staff are aware, hard copy personal logs issued and available to be printed from the on-call shared drive. Loggist training has been undertaken to the required standards but Loggists are only available during working hours, so this standard remains partially complete.Training of new Loggists and refresher training for existing loggists	Fully compliant				
25	Training and exercising	Staff Awareness & Training	There are mechanisms in place to ensure staff are aware of their role in an incident and where to find plans relevant to their area of work or department.	As part of mandatory training Exercise and Training attendance records reported to Board	Major and Critical Incident Plan include action cards for key roles, BCP's for teams and Services are available both in hard copy, SHSC Extranet JARVIS and in team shared drives. EPRR is included in induction training.	Partially compliant				
Domain 6 - Response										
26	Response	Incident Co-ordination Centre (ICC)	The organisation has in place suitable and sufficient arrangements to effectively coordinate the response to an incident in line with national guidance. ICC arrangements need to be flexible and scalable to cope with a range of incidents and hours of operation required. An ICC must have dedicated business continuity arrangements in place and must be resilient to loss of utilities, including telecommunications, and to external hazards. ICC equipment should be tested in line with national guidance or after a major infrastructure change to ensure functionality and in a state of organisational readiness. Arrangements should be supported with access to documentation for its activation and operation.	• Documented processes for identifying the location and establishing an ICC • Maps and diagrams • A testing schedule • A training schedule • Pre identified roles and responsibilities, with action cards • Demonstration ICC location is resilient to loss of utilities, including telecommunications, and external hazards • Arrangements might include virtual arrangements in addition to physical facilities but must be resilient with alternative contingency solutions.	Major and Critical Incident Plan includes location of nominated ICC's. It can be scaled from working virtually to a fully functioning ICC with all key roles. Phone system upgraded on 31/07/2023, together with mobile phones. Note books and pens available in the event of power loss, kept in a trolley in readiness. Newly nominated ICC's at Centre Court and Wardsend Road tested on 23/08/2024 when new phones installed.	Fully compliant				
27	Response	Access to planning arrangements	Version controlled current response documents are available to relevant staff at all times. Staff should be aware of where they are stored and should be easily accessible.	Planning arrangements are easily accessible - both electronically and local copies	Electronic copies on SHSC extranet JARVIS and hard copies in ICC's and on-call packs.	Fully compliant				
28	Response	Management of business continuity incidents	In line with current guidance and legislation, the organisation has effective arrangements in place to respond to a business continuity incident (as defined within the EPRR Framework).	• Business Continuity Response plans • Arrangements in place that mitigate escalation to business continuity incident • Escalation processes	Annually reviewed BCP's in place for all teams and services.M & CI Plan and BCP Policy to ARC 16/01/2024, BCMS to TEPG 27/03/2024	Fully compliant				
29	Response	Decision Logging	To ensure decisions are recorded during business continuity, critical and major incidents, the organisation must ensure: 1. Key response staff are aware of the need for creating their own personal records and decision logs to the required standards and storing them in accordance with the organisations' records management policy. 2. has 24 hour access to a trained loggist(s) to ensure support to the decision maker	• Documented processes for accessing and utilising loggists • Training records	Key response staff are aware, hard copy personal logs issued and available to be printed from the on-call shared drive. Loggist training has been undertaken to the required standards but Loggists are only available during working hours, so this standard remains partially complete.Training of new Loggists and refresher training for existing loggists	Fully compliant				

Ref	Domain	Standard name	Standard Detail	Supporting Information - including examples of evidence	Organisational Evidence	Self assessment RAG Red (not compliant) = Not compliant with the core standard. The organisation's work programme shows compliance will not be reached within the next 12 months. Amber (partially compliant) = Not compliant with core standard. However, the organisation's work programme demonstrates sufficient evidence of progress and an action plan to achieve full compliance within the next 12 months. Green (fully compliant) = Fully compliant with core standard.	Action to be taken	Lead	Timescale	Comments
30	Response	Situation Reports	The organisation has processes in place for receiving, completing, authorising and submitting situation reports (SitReps) and briefings during the response to incidents including bespoke or incident dependent formats.	• Documented processes for completing, quality assuring, signing off and submitting SitReps • Evidence of testing and exercising • The organisation has access to the standard SitRep Template	SOP in place for submitting sitreps, tailored to particular incidents e.g COVID-19 still operating. SHSC have access to the standard template, included as an appendix to the Major and Critical Incident Plan. Submission depends on the incident e.g. COVID sitreps ICC, Lateral Flow sitreps Information Team as BAU, Industrial Action sitreps to ICB, BCP sitreps to incident lead and EPRR lead.	Fully compliant				
31	Response	Access to 'Clinical Guidelines for Major Incidents and Mass Casualty events'	Key clinical staff (especially emergency department) have access to the 'Clinical Guidelines for Major Incidents and Mass Casualty events' handbook.	Guidance is available to appropriate staff either electronically or hard copies		Fully compliant				
32	Response	Access to 'CBRN incident: Clinical Management and health protection'	Clinical staff have access to the 'CBRN incident: Clinical Management and health protection' guidance. (Formerly published by PHE)	Guidance is available to appropriate staff either electronically or hard copies	A CBRN Plan is now in place and is avalable on Jarvis, shered Drive and hard copies are in the IOR Boxes.	Fully compliant				
Domain 7 - Warning and informing										
33	Warning and informing	Warning and informing	The organisation aligns communications planning and activity with the organisation's EPRR planning and activity.	• Awareness within communications team of the organisation's EPRR plan, and how to report potential incidents. • Measures are in place to ensure incidents are appropriately described and declared in line with the NHS EPRR Framework. • Out of hours communication system (24/7, year-round) is in place to allow access to trained comms support for senior leaders during an incident. This should include on call arrangements. • Having a process for being able to log incoming requests, track responses to these requests and to ensure that information related to incidents is stored effectively. This will allow organisations to provide evidence should it be required for an inquiry.	Communications Team are integral to Major Incident Plans and are contactable out of hours to on-call staff. They are aligned also to Adverse weather and heatwave Plans, providing alerts through the SHSC extranet JARVIS and social media. Updates to incidents are dated so that staff know they're following the most up to date situation.	Partially compliant				
34	Warning and informing	Incident Communication Plan	The organisation has a plan in place for communicating during an incident which can be enacted.	• An incident communications plan has been developed and is available to on call communications staff • The incident communications plan has been tested both in and out of hours • Action cards have been developed for communications roles • A requirement for briefing NHS England regional communications team has been established • The plan has been tested, both in and out of hours as part of an exercise. • Clarity on sign off for communications is included in the plan, noting the need to ensure communications are signed off by incident leads, as well as NHSE (if appropriate).	Incident Communications Plan to ARC 16/01/2024.A communication exercise " Exercise Hello was conducted on 29/05/2024	Fully compliant				
35	Warning and informing	Communication with partners and stakeholders	The organisation has arrangements in place to communicate with patients, staff, partner organisations, stakeholders, and the public before, during and after a major incident, critical incident or business continuity incident.	• Established means of communicating with staff, at both short notice and for the duration of the incident, including out of hours communications • A developed list of contacts in partner organisations who are key to service delivery (local Council, LRF partners, neighbouring NHS organisations etc) and a means of warning and informing these organisations about an incident as well as sharing communications information with partner organisations to create consistent messages at a local, regional and national level. • A developed list of key local stakeholders (such as local elected officials, unions etc) and an established a process by which to brief local stakeholders during an incident • Appropriate channels for communicating with members of the public that can be used 24/7 if required • Identified sites within the organisation for displaying of important public information (such as main points of access) • Have in place a means of communicating with patients who have appointments booked or are receiving treatment. • Have in place a plan to communicate with inpatients and their families or care givers. • The organisation publicly states its readiness and preparedness activities in annual reports within the organisations own regulatory reporting requirements	Incident Communications Plan to ARC 16/01/2024	Fully compliant				
36	Warning and informing	Media strategy	The organisation has arrangements in place to enable rapid and structured communication via the media and social media	• Having an agreed media strategy and a plan for how this will be enacted during an incident. This will allow for timely distribution of information to warn and inform the media • Develop a pool of media spokespeople able to represent the organisation to the media at all times. • Social Media policy and monitoring in place to identify and track information on social media relating to incidents. • Setting up protocols for using social media to warn and inform • Specifying advice to senior staff to effectively use social media accounts whilst the organisation is in incident response	Media Policy to PGG 18/12/2023 and ARC 16/01/2024. Published on JARVIS.	Fully compliant				
Domain 8 - Cooperation										
37	Cooperation	LHRP Engagement	The Accountable Emergency Officer, or a director level representative with delegated authority (to authorise plans and commit resources on behalf of their organisation) attends Local Health Resilience Partnership (LHRP) meetings.	• Minutes of meetings • Individual members of the LHRP must be authorised by their employing organisation to act in accordance with their organisational governance arrangements and their statutory status and responsibilities.	MTV activation group; Evacuation Plan; YH Low medium Secure Evacuation Plan; MOU with SY 2015 (updated version requested); NEY Escalation and Mutual Aid plan 2020. Requires ICB support to maintain.MH EPRR leads have MOU's in place. The MOU has been signed off by AEO's	Fully compliant				

Ref	Domain	Standard name	Standard Detail	Supporting Information - including examples of evidence	Organisational Evidence	Self assessment RAG Red (not compliant) = Not compliant with the core standard. The organisation's work programme shows compliance will not be reached within the next 12 months. Amber (partially compliant) = Not compliant with core standard. However, the organisation's work programme demonstrates sufficient evidence of progress and an action plan to achieve full compliance within the next 12 months. Green (fully compliant) = Fully compliant with core standard.	Action to be taken	Lead	Timescale	Comments
38	Cooperation	LRF / BRF Engagement	The organisation participates in, contributes to or is adequately represented at Local Resilience Forum (LRF) or Borough Resilience Forum (BRF), demonstrating engagement and co-operation with partner responders.	• Minutes of meetings • A governance agreement is in place if the organisation is represented and feeds back across the system	SYLRF Information sharing protocol; SYLRF Constitution October 2022, information sharing agreements in place. Some are covered in individual contracts. Also requires ICB support to maintain.	Partially compliant				
39	Cooperation	Mutual aid arrangements	The organisation has agreed mutual aid arrangements in place outlining the process for requesting, coordinating and maintaining mutual aid resources. These arrangements may include staff, equipment, services and supplies. In line with current NHS guidance, these arrangements may be formal and should include the process for requesting Military Aid to Civil Authorities (MACA) via NHS England.	• Detailed documentation on the process for requesting, receiving and managing mutual aid requests • Templates and other required documentation is available in ICC or as appendices to IRP • Signed mutual aid agreements where appropriate	A Mutaual Aid between SHSC and SYLRF and LHRP partners is in place.	Fully compliant				
43	Cooperation	Information sharing	The organisation has an agreed protocol(s) for sharing appropriate information pertinent to the response with stakeholders and partners, during incidents.	• Documented and signed information sharing protocol • Evidence relevant guidance has been considered, e.g. Freedom of Information Act 2000, General Data Protection Regulation 2016, Caldicott Principles, Safeguarding requirements and the Civil Contingencies Act 2004	SYLRF Information sharing protocol; SYLRF Constitution October 2022, information sharing agreements in place. Some are covered in individual contracts. Also requires ICB support to maintain.Still waiting for katie Hunter and John John Wolstenholme.	Partially compliant				
Domain 9 - Business Continuity										
44	Business Continuity	BC policy statement	The organisation has in place a policy which includes a statement of intent to undertake business continuity. This includes the commitment to a Business Continuity Management System (BCMS) that aligns to the ISO standard 22301.	The organisation has in place a policy which includes intentions and direction as formally expressed by its top management. The BC Policy should: • Provide the strategic direction from which the business continuity programme is delivered. • Define the way in which the organisation will approach business continuity. • Show evidence of being supported, approved and owned by top management. • Be reflective of the organisation in terms of size, complexity and type of organisation. • Document any standards or guidelines that are used as a benchmark for the BC programme. • Consider short term and long term impacts on the organisation including climate change adaption planning	Business Continuity Policy. BCP to ARC 16/01/2024	Fully compliant				
45	Business Continuity	Business Continuity Management Systems (BCMS) scope and objectives	The organisation has established the scope and objectives of the BCMS in relation to the organisation, specifying the risk management process and how this will be documented. A definition of the scope of the programme ensures a clear understanding of which areas of the organisation are in and out of scope of the BC programme.	BCMS should detail: • Scope e.g. key products and services within the scope and exclusions from the scope • Objectives of the system • The requirement to undertake BC e.g. Statutory, Regulatory and contractual duties • Specific roles within the BCMS including responsibilities, competencies and authorities. • The risk management processes for the organisation i.e. how risk will be assessed and documented (e.g. Risk Register), the acceptable level of risk and risk review and monitoring process • Resource requirements • Communications strategy with all staff to ensure they are aware of their roles • alignment to the organisations strategy, objectives, operating environment and approach to risk. • the outsourced activities and suppliers of products and suppliers. • how the understanding of BC will be increased in the organisation	Business Continuity Policy; Risk Management Strategy; Communications Policy.BCMS prepared and subitted to TEPG 27/03/2024, then to ARC for information	Fully compliant				
46	Business Continuity	Business Impact Analysis/Assessment (BIA)	The organisation annually assesses and documents the impact of disruption to its services through Business Impact Analysis(es).	The organisation has identified prioritised activities by undertaking a strategic Business Impact Analysis/Assessments. Business Impact Analysis/Assessment is the key first stage in the development of a BCMS and is therefore critical to a business continuity programme. Documented process on how BIA will be conducted, including: • the method to be used • the frequency of review • how the information will be used to inform planning • how RA is used to support. The organisation should undertake a review of its critical function using a Business Impact Analysis/assessment. Without a Business Impact Analysis organisations are not able to assess/assure compliance without it. The following points should be considered when undertaking a BIA: • Determining impacts over time should demonstrate to top management how quickly the organisation needs to respond to a disruption. • A consistent approach to performing the BIA should be used throughout the organisation. • BIA method used should be robust enough to ensure the information is collected consistently and impartially.	Business Continuity Policy; Business Impact Assessment	Partially compliant				
47	Business Continuity	Business Continuity Plans (BCP)	The organisation has business continuity plans for the management of incidents. Detailing how it will respond, recover and manage its services during disruptions to: • people • information and data • premises • suppliers and contractors • IT and infrastructure	Documented evidence that as a minimum the BCP checklist is covered by the various plans of the organisation. Ensure BCPS are Developed using the ISO 22301 and the NHS Toolkit. BC Planning is undertaken by an adequately trained person and contain the following: • Purpose and Scope • Objectives and assumptions • Escalation & Response Structure which is specific to your organisation. • Plan activation criteria, procedures and authorisation. • Response teams roles and responsibilities. • Individual responsibilities and authorities of team members. • Prompts for immediate action and any specific decisions the team may need to make. • Communication requirements and procedures with relevant interested parties. • Internal and external interdependencies. • Summary Information of the organisations prioritised activities. • Decision support checklists • Details of meeting locations • Appendix/Appendices	All teams / Services have Business Continuity Plans in place that are reviewed annually or following an incident (whichever is earlier)New BCP template was submitted to TEPG on 27/03/2024	Fully compliant				

Ref	Domain	Standard name	Standard Detail	Supporting Information - including examples of evidence	Organisational Evidence	Self assessment RAG Red (not compliant) = Not compliant with the core standard. The organisation's work programme shows compliance will not be reached within the next 12 months. Amber (partially compliant) = Not compliant with core standard. However, the organisation's work programme demonstrates sufficient evidence of progress and an action plan to achieve full compliance within the next 12 months. Green (fully compliant) = Fully compliant with core standard.	Action to be taken	Lead	Timescale	Comments
48	Business Continuity	Testing and Exercising	The organisation has in place a procedure whereby testing and exercising of Business Continuity plans is undertaken on a yearly basis as a minimum, following organisational change or as a result of learning from other business continuity incidents.	Confirm the type of exercise the organisation has undertaken to meet this sub standard: • Discussion based exercise • Scenario Exercises • Simulation Exercises • Live exercise • Test • Undertake a debrief Evidence Post exercise/ testing reports and action plans	Scenario based exercise and discussion based learning to complete BIA on minimum staffing requirements. Live incidents in respect of Industrial Action and legionella. Discussion based exercise in respect of power outage.BCMS to go to TEPG 27/03/2024, EPRR work plan includes exercise programme	Fully compliant				
49	Business Continuity	Data Protection and Security Toolkit	Organisation's Information Technology department certify that they are compliant with the Data Protection and Security Toolkit on an annual basis.	Evidence • Statement of compliance • Action plan to obtain compliance if not achieved	Waiting for Adam and Katie to respond	Partially compliant				
50	Business Continuity	BCMS monitoring and evaluation	The organisation's BCMS is monitored, measured and evaluated against established Key Performance Indicators. Reports on these and the outcome of any exercises, and status of any corrective action are annually reported to the board.	• Business continuity policy • BCMS • performance reporting • Board papers	Business Continuity Policy; Board reports; ARC reports	Fully compliant				
51	Business Continuity	BC audit	The organisation has a process for internal audit, and outcomes are included in the report to the board. The organisation has conducted audits at planned intervals to confirm they are conforming with its own business continuity programme.	• process documented in EPRR policy/Business continuity policy or BCMS aligned to the audit programme for the organisation • Board papers • Audit reports • Remedial action plan that is agreed by top management. • An independent business continuity management audit report. • Internal audits should be undertaken as agreed by the organisation's audit planning schedule on a rolling cycle. • External audits should be undertaken in alignment with the organisations audit programme	Needs to be arranged - would suggest 360 Assurance - to discuss with Neil	Partially compliant				
52	Business Continuity	BCMS continuous improvement process	There is a process in place to assess the effectiveness of the BCMS and take corrective action to ensure continual improvement to the BCMS.	• process documented in the EPRR policy/Business continuity policy or BCMS • Board papers showing evidence of improvement • Action plans following exercising, training and incidents • Improvement plans following internal or external auditing •Changes to suppliers or contracts following assessment of suitability Continuous Improvement can be identified via the following routes: • Lessons learned through exercising. • Changes to the organisations structure, products and services, infrastructure, processes or activities. • Changes to the environment in which the organisation operates. • A review or audit. • Changes or updates to the business continuity management lifecycle, such as the BIA or continuity solutions. • Self assessment • Quality assurance • Performance appraisal • Supplier performance • Management review • Debriefs • After action reviews • Lessons learned through exercising or live incidents	Annual audit of BCP's, debriefs following BC incidents, lessons learned through exercising.EPRR Work Plan, EPRR and BCP Polic	Fully compliant				
53	Business Continuity	Assurance of commissioned providers / suppliers BCPs	The organisation has in place a system to assess the business continuity plans of commissioned providers or suppliers; and are assured that these providers business continuity arrangements align and are interoperable with their own.	• EPRR policy/Business continuity policy or BCMS outlines the process to be used and how suppliers will be identified for assurance • Provider/supplier assurance framework • Provider/supplier business continuity arrangements This may be supported by the organisations procurement or commercial teams (where trained in BC) at tender phase and at set intervals for critical and/or high value suppliers	Waiting for Julie Rice	Partially compliant				
Domain 10 - CBRN										
55	Hazmat/CBRN	Governance	The organisation has identified responsible roles/people for the following elements of Hazmat/CBRN: - Accountability - via the AEO - Planning - Training - Equipment checks and maintenance Which should be clearly documented	Details of accountability/responsibility are clearly documented in the organisation's Hazmat/CBRN plan and/or Emergency Planning policy as related to the identified risk and role of the organisation	CBRNe Plan reviewed and updated June 2023, staff training on induction, equipment held in Pharmacy for distribution against action cards for staff to follow and in line with guidance.CBRN Plan to ARC 16/01/2024	Fully compliant				
56	Hazmat/CBRN	Hazmat/CBRN risk assessments	Hazmat/CBRN risk assessments are in place which are appropriate to the organisation type	Evidence of the risk assessment process undertaken - including - i) governance for risk assessment process ii) assessment of impacts on staff iii) impact assessment(s) on estates and infrastructure - including access and egress iv) management of potentially hazardous waste v) impact assessments of Hazmat/CBRN decontamination on critical facilities and services	CBRNe Plan reviewed and updated January 2024, clinical waste contingency plan.RA added to Ulysses	Fully compliant				
57	Hazmat/CBRN	Specialist advice for Hazmat/CBRN exposure	Organisations have signposted key clinical staff on how to access appropriate and timely specialist advice for managing patients involved in Hazmat/CBRN incidents	Staff are aware of the number / process to gain access to advice through appropriate planning arrangements. These should include ECOSA, TOXBASE, NPIS, UKHSA Arrangements should include how clinicians would access specialist clinical advice for the on-going treatment of a patient	Conats number in the CBRN Plan and Hazmat/CBRN Training Package	Fully compliant				

Ref	Domain	Standard name	Standard Detail	Supporting Information - including examples of evidence	Organisational Evidence	Self assessment RAG Red (not compliant) = Not compliant with the core standard. The organisation's work programme shows compliance will not be reached within the next 12 months. Amber (partially compliant) = Not compliant with core standard. However, the organisation's work programme demonstrates sufficient evidence of progress and an action plan to achieve full compliance within the next 12 months. Green (fully compliant) = Fully compliant with core standard.	Action to be taken	Lead	Timescale	Comments
58	Hazmat/CBRN	Hazmat/CBRN planning arrangements	The organisation has up to date specific Hazmat/CBRN plans and response arrangements aligned to the risk assessment, extending beyond IOR arrangements, and which are supported by a programme of regular training and exercising within the organisation and in conjunction with external stakeholders	Documented plans include evidence of the following: •command and control structures •Collaboration with the NHS Ambulance Trust to ensure Hazmat/CBRN plans and procedures are consistent with the Ambulance Trust's Hazmat/CBRN capability •Procedures to manage and coordinate communications with other key stakeholders and other responders •Effective and tested processes for activating and deploying Hazmat/CBRN staff and Clinical Decontamination Units (CDUs) (or equivalent) •Pre-determined decontamination locations with a clear distinction between clean and dirty areas and demarcation of safe clean access for patients, including for the off-loading of non-decontaminated patients from ambulances, and safe cordon control •Distinction between dry and wet decontamination and the decision making process for the appropriate deployment •Identification of lockdown/isolation procedures for patients waiting for decontamination •Management and decontamination processes for contaminated patients and fatalities in line with the latest guidance •Arrangements for staff decontamination and access to staff welfare •Business continuity plans that ensure the trust can continue to accept patients not related/affected by the Hazmat/CBRN incident, whilst simultaneously providing the decontamination capability, through designated clean entry routes •Plans for the management of hazardous waste •Hazmat/CBRN plans and procedures include sufficient provisions to manage the stand-down and transition from response to recovery and a return to business as usual activities •Description of process for obtaining replacement PPE/PRPS - both during a protracted incident and in the aftermath of an incident	CBRNe Plan reviewed and updated June 2023. Clinical waste contingency arrangements. PPE order form	Fully compliant				
59	Hazmat/CBRN	Decontamination capability availability 24 /7	The organisation has adequate and appropriate wet decontamination capability that can be rapidly deployed to manage self presenting patients, 24 hours a day, 7 days a week (for a minimum of four patients per hour) - this includes availability of staff to establish the decontamination facilities There are sufficient trained staff on shift to allow for the continuation of decontamination until support and/or mutual aid can be provided - according to the organisation's risk assessment and plan(s) The organisations also has plans, training and resources in place to enable the commencement of interim dry/wet, and improvised decontamination where necessary.	Documented roles for people forming the decontamination team - including Entry Control/Safety Officer Hazmat/CBRN trained staff are clearly identified on staff rotas and scheduling pro-actively considers sufficient cover for each shift Hazmat/CBRN trained staff working on shift are identified on shift board Collaboration with local NHS ambulance trust and local fire service - to ensure Hazmat/CBRN plans and procedures are consistent with local area plans Assessment of local area needs and resource		Partially compliant				
60	Hazmat/CBRN	Equipment and supplies	The organisation holds appropriate equipment to ensure safe decontamination of patients and protection of staff. There is an accurate inventory of equipment required for decontaminating patients. Equipment is proportionate with the organisation's risk assessment of requirement - such as for the management of non-ambulant or collapsed patients • Acute providers - see Equipment checklist: https://www.england.nhs.uk/wp-content/uploads/2018/07/eprr-decontamination-equipment-check-list.xlsx • Community, Mental Health and Specialist service providers - see guidance 'Planning for the management of self-presenting patients in healthcare setting': https://webarchive.nationalarchives.gov.uk/20161104231146/https://www.england.nhs.uk/wp-content/uploads/2015/04/eprr-chemical-incidents.pdf	This inventory should include individual asset identification, any applicable servicing or maintenance activity, any identified defects or faults, the expected replacement date and any applicable statutory or regulatory requirements (including any other records which must be maintained for that item of equipment). There are appropriate risk assessments and SOPs for any specialist equipment Acute and ambulance trusts must maintain the minimum number of PRPS suits specified by NHS England (24/240). These suits must be maintained in accordance with the manufacturer's guidance. NHS Ambulance Trusts can provide support and advice on the maintenance of PRPS suits as required. Designated hospitals must ensure they have a financial replacement plan in place to ensure that they are able to adequately account for depreciation in the life of equipment and ensure funding is available for replacement at the end of its shelf life. This includes for PPE/PRPS suits, decontamination facilities etc.	CBRNe Plan reviewed and updated January 2024, staff training on induction, equipment held in Pharmacy for distribution against action cards for staff to follow and in line with guidance. PPE order form.	Partially compliant				
61	Hazmat/CBRN	Equipment - Preventative Programme of Maintenance	There is a preventative programme of maintenance (PPM) in place, including routine checks for the maintenance, repair, calibration (where necessary) and replacement of out of date decontamination equipment to ensure that equipment is always available to respond to a Hazmat/CBRN incident. Equipment is maintained according to applicable industry standards and in line with manufacturer's recommendations The PPM should include where applicable: - PRPS Suits - Decontamination structures - Disrobe and rerobe structures - Water outlets - Shower tray pump - RAM GENE (radiation monitor) - calibration not required - Other decontamination equipment as identified by your local risk assessment e.g. IOR Rapid Response boxes There is a named individual (or role) responsible for completing these checks	Documented process for equipment maintenance checks included within organisational Hazmat/CBRN plan - including frequency required proportionate to the risk assessment • Record of regular equipment checks, including date completed and by whom • Report of any missing equipment Organisations using PPE and specialist equipment should document the method for it's disposal when required Process for oversight of equipment in place for EPRR committee in multisite organisations/central register available to EPRR Organisation Business Continuity arrangements to ensure the continuation of the decontamination services in the event of use or damage to primary equipment Records of maintenance and annual servicing Third party providers of PPM must provide the organisations with assurance of their own Business Continuity arrangements as a commissioned supplier/provider under Core Standard 53	CBRNe Plan reviewed and updated June 2023, staff training on induction, equipment held in Pharmacy for distribution against action cards for staff to follow and in line with guidance.	Fully compliant				

Ref	Domain	Standard name	Standard Detail	Supporting Information - including examples of evidence	Organisational Evidence	Self assessment RAG Red (not compliant) = Not compliant with the core standard. The organisation's work programme shows compliance will not be reached within the next 12 months. Amber (partially compliant) = Not compliant with core standard. However, the organisation's work programme demonstrates sufficient evidence of progress and an action plan to achieve full compliance within the next 12 months. Green (fully compliant) = Fully compliant with core standard.	Action to be taken	Lead	Timescale	Comments
62	Hazmat/CBRN	Waste disposal arrangements	The organisation has clearly defined waste management processes within their Hazmat/CBRN plans	Documented arrangements for the safe storage (and potential secure holding) of waste Documented arrangements - in consultation with other emergency services for the eventual disposal of: - Waste water used during decontamination - Used or expired PPE - Used equipment - including unit liners Any organisation chosen for waste disposal must be included in the supplier audit conducted under Core Standard 53		Partially compliant				
63	Hazmat/CBRN	Hazmat/CBRN training resource	The organisation must have an adequate training resource to deliver Hazmat/CBRN training which is aligned to the organisational Hazmat/CBRN plan and associated risk assessments	Identified minimum training standards within the organisation's Hazmat/CBRN plans (or EPRR training policy) Staff training needs analysis (TNA) appropriate to the organisation type - related to the need for decontamination Documented evidence of training records for Hazmat/CBRN training - including for: - trust trainers - with dates of their attendance at an appropriate 'train the trainer' session (or update) - trust staff - with dates of the training that that they have undertaken Developed training programme to deliver capability against the risk assessment	EPM need to attend a Hazmat/CBRN Train the Traner cousre. However, EPM has already gained Level 3 in Teaching and training	Partially compliant				
64	Hazmat/CBRN	Staff training - recognition and decontamination	The organisation undertakes training for all staff who are most likely to come into contact with potentially contaminated patients and patients requiring decontamination. Staff that may make contact with a potentially contaminated patients whether in person or over the phone, are sufficiently trained in Initial Operational Response (IOR) principles and isolation when necessary. (This includes (but is not limited to) acute, community, mental health and primary care settings such as minor injury units and urgent treatment centres) Staff undertaking patient decontamination are sufficiently trained to ensure a safe system of work can be implemented	Evidence of trust training slides/programme and designated audience Evidence that the trust training includes reference to the relevant current guidance (where necessary) Staff competency records	3 Hazmat /CBRN training sessions have been provide to receptionist Staff and 1 for pharmacy staff	Fully compliant				
65	Hazmat/CBRN	PPE Access	Organisations must ensure that staff who come in to contact with patients requiring wet decontamination and patients with confirmed respiratory contamination have access to, and are trained to use, appropriate PPE. This includes maintaining the expected number of operational PRPS available for immediate deployment to safely undertake wet decontamination and/or access to FFP3 (or equivalent) 24/7	Completed equipment inventories; including completion date Fit testing schedule and records should be maintained for all staff who may come into contact with confirmed respiratory contamination Emergency Departments at Acute Trusts are required to maintain 24 Operational PRPS	Nee to double chaeck with Jillian	Fully compliant				
66	Hazmat/CBRN	Exercising	Organisations must ensure that the exercising of Hazmat/CBRN plans and arrangements are incorporated in the organisations EPRR exercising and testing programme	Evidence • Exercising Schedule which includes Hazmat/CBRN exercise • Post exercise reports and embedding learning		Non compliant				

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 Red (not compliant) = Not evidenced in EPRR arrangements. Amber (partially compliant) = Not evidenced in EPRR arrangements but have plans in place to include in the next 12 months. 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) - Shared understanding of risks to the organisation and the population it serves with regards to EPRR - organisational risk assessments and risk registers -Plans and arrangements demonstrate a common understanding of incidents in line with EPRR framework and cyber security requirements. -EPRR work programme -Organisational EPRR policy	Head of Service Delivery & Infrastructure and IG Manager are both members of the Trusts Emergency Planning Group. Limited shared understanding of potential risks which needs to be reviewed. EPRR policy and related cyber incident response plans are being written and aligned.	Partially compliant	Emergency Planning manager and Head of Service Delivery & Infrastructure to review potential risks.	Adam Handley Jean Kiyori	Jan-25	
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: -consider the operational impact of such incidents -be current and include a routine review schedule -be tested regularly -be approved and signed off by the appropriate governance mechanisms -include clearly identified response roles and responsibilities -be shared appropriately with those required to use them -outline any equipment requirements -outline any staff training needs -include use of unambiguous language -demonstrate a common understanding of terminology used during incidents in line with the EPRR framework and cybersecurity requirements.'	Cyber Incident Response Plan is currently in draft phase and is being reviewed and aligned with the trusts emergency planning policy Regional Cyber review has been conducted by ANS to review all NHS and Council organisations in South Yorkshire ICS to advise on potential improvements and areas for investment.	Partially compliant	Finalise and approve Cyber Incident Response Plan and cyber playbooks Review results from regional cyber assessment and next steps in terms of documentation and investment in infrastructure	Adam Handley	Mar-25	
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: 1. look beyond the technical solutions at processes and organisational arrangements 2. identify and review the critical communication activities that underpin your response arrangements 3. ensure diversity of technical solutions 4. adopt layered fall-back arrangements 5. plan for appropriate interoperability https://www.england.nhs.uk/wp-content/uploads/2019/03/national-resilient-telecommunications-guidance.pdf	Our updated communications plan for emergency preparedness, resilience and response (EPRR) covers the principles of how we will communicate in a cyber or IT related incident.	Partially compliant	Updated communications plan with Cyber Security addition to be approved at the Trusts Emergency Planning Group in January 2025	Holly Cubitt	Jan-25	
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. - Agreed sign off processes for media and press releases in relation to Cyber security and IT related incidents. - Documented process for communications to regional and national teams - 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.	There are specific references to SHSCs communications activities and media handling plans in the updated communications plan for emergency preparedness, resilience and response (EPRR) Section 9 of SHSCs updated plan gives detail on spokespeople and how media enquiries will be handled. Section 11 of SHSCs plan details how we will report in the effectiveness of our communications activity and how we will liaise with regional and national teams as appropriate for the incident. Appendix C and D of SHSCs plan provides a draft statement for internal and external use in event of a cyber related incident. There is also detailed guidance in section 9 on spokespeople.	Partially compliant	Updated communications plan with Cyber Security additions to be approved at the Trusts Emergency Planning Group in January 2025	Holly Cubitt	Jan-25	

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 - EPRR exercise and testing programme	Annual desktop exercises are conducted as part of the DSPT to review any potential issues. Cyber documentation is new and limited in places due to no dedicated cyber resource so further testing and exercises are needed to review and follow new documentaiton to make sure its clear of roles, responsibilities and potential scenarios that may occur during a potential cyber incident.	Partially compliant	Review annual EPRR Exercise and testing programme Align DSPT and EPRR Exercises Conduct exercise with cyber incident response plan.	Jean Kiyori	Jan-25	
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 - lessons identified and implementation plans to address those lessons -agreed processes in place to adopt implementation of lessons identified - Evidence of updated incident plans post-incident/exercise	CARECert processes in place to respond to any potential threats or vulnerabilities. No previous requirement for incident plans needing to be updated but new documentation and exercises will make sure this occurs in the future. ITIL Major Incident and lessons learnt processes in place for all major incidents.	Fully compliant		Adam Handley		
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 - Attendance/participant lists showing cybersecurity and IT colleagues taking part in incident response training.	No dedicated resource for Cyber Security within the Digital department. Development is ongoing within Digital to provide some cyber security training to staff in technical roles who would potentially be involved in supporting a cyber incident.	Non compliant	Incorporated into Digitals Target Operating Model to review roles and responsibilties and potential dedicated resource for cyber security.	Adam Handley	Mar-25	
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	EPRR Risk Register informs SHSC Emergency and Busir	Partially compliant	Review current EPRR training Review potential improvements to include Cyber Security and IT related Incidents	Jean Kiyori Adam Handley	Mar-25	
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 -list of the organisations critical services and functions -list of the organisations core IT/Digital systems and prioritisation of system recovery	Disaster Recover plan outlines SHSC critical services and functions and prioritises those services above others in the event of a DR scenario	Partially compliant	Conduct business impact analysis which will require clinical involvement to support.	Adam Handley	Mar-25	
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 -key products and services within the scope of BCMS -Appropriate risk assessments	BCMS is in place. More training needed	Partially compliant	Further business continuity training sessions required across the trust and specifically on call managers	Jean Kiyori	Mar-25	
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 -Disaster recovery plans for core systems -Cyber security and IT departments own BCP which includes contacts for key personnel outside of normal working hours	Disaster recover plan in place but is not specific to each core system. Cyber incident response plan has a list of key personnel and contact details. Digitals BCP is currently being reviewed.	Partially compliant	Finalise Cyber Incident response plan which lists key personnel details. Finalise reviewing Digitals BCP Document Disaster Recovery plans (Playbooks) for core systems	Adam Handley	Mar-25	

Overall self assesment rating:										
Ref	Domain	Standard name	Standard Detail	Supporting Information - including examples of evidence	Organisational Evidence :	Self assessment RAG Red (not compliant) = Not compliant with the core standard. The organisation's work programme shows compliance will not be reached within the next 12 months. Amber (partially compliant) = Not compliant with core standard. However, the organisation's work programme demonstrates sufficient evidence of progress and an action plan to achieve full compliance within the next 12 months. Green (fully compliant) = Fully compliant with core standard.	Action to be taken	Lead	Timescale	Comments
Domain 1 - Governance										
Domain 2 - Duty to risk assess										
Domain 3 - Duty to maintain Plans										
18	Duty to maintain plans	Protected individuals	In line with current guidance and legislation, the organisation has arrangements in place to respond and manage 'protected individuals' including Very Important Persons (VIPs),high profile patients and visitors to the site.	Arrangements should be: • current • in line with current national guidance • in line with risk assessment • tested regularly • signed off by the appropriate mechanism • shared appropriately with those required to use them • outline any equipment requirements • outline any staff training required	Visitors Policy reviewed and updated June 2022 includes the management of VIP visits. Protocols in place with Security Policy in the event of VIP admissions/treatment. Safeguarding Policy, individuals care plan and HM Prisons designation of high profile patients. Follow The HM Prisons and Probation Service Designation and Management of High Profile Restricted Patients in respect of Low Secure.	Partially compliant				
Domain 4 - Command and control										
21	Command and control	Trained on-call staff	Trained and up to date staff are available 24/7 to manage escalations, make decisions and identify key actions	• Process explicitly described within the EPRR policy or statement of intent The identified individual: • Should be trained according to the NHS England EPRR competencies (National Minimum Occupational Standards) • Has a specific process to adopt during the decision making • Is aware who should be consulted and informed during decision making • Should ensure appropriate records are maintained throughout. • Trained in accordance with the TNA identified frequency.	All NHS leaders have attended the PHC at the appropriate level (Strategic and Tactical) as currently available. No one goes on the on-call rota until they have completed this. JESIP training is presently being rolled out to strategic leaders.	Partially compliant				
Domain 5 - Training and exercising										
22	Training and exercising	EPRR Training	The organisation carries out training in line with a training needs analysis to ensure staff are current in their response role.	Evidence • Process explicitly described within the EPRR policy or statement of intent • Evidence of a training needs analysis • Training records for all staff on call and those performing a role within the ICC • Training materials • Evidence of personal training and exercising portfolios for key staff	EPRR forms part of mandatory training on induction for all staff. Staff allocated to ICC duties receive training to carry out the actions of their role as per the Major and Critical Incident Plan. New Commander portfolios have been issued to all relevant commanders. Recent live incidents including the COVID pandemic and Industrial Action evidence some areas and work is ongoing to meet the 3 year expectation on meeting compliance that requires NHS England EPRR support. For this reason, we remain partially compliant.The requirement for a Level 3 Education and Training qualification to be included in Person Specification of EPRR lead.	Partially compliant				
25	Training and exercising	Staff Awareness & Training	There are mechanisms in place to ensure staff are aware of their role in an incident and where to find plans relevant to their area of work or department.	As part of mandatory training Exercise and Training attendance records reported to Board	Major and Critical Incident Plan include action cards for key roles, BCP's for teams and Services are available both in hard copy, SHSC Extranet JARVIS and in team shared drives. EPRR is included in induction training.	Partially compliant				
Domain 6 - Response										
Domain 7 - Warning and informing										
33	Warning and informing	Warning and informing	The organisation aligns communications planning and activity with the organisation's EPRR planning and activity.	• Awareness within communications team of the organisation's EPRR plan, and how to report potential incidents. • Measures are in place to ensure incidents are appropriately described and declared in line with the NHS EPRR Framework. • Out of hours communication system (24/7, year-round) is in place to allow access to trained comms support for senior leaders during an incident. This should include on call arrangements. • Having a process for being able to log incoming requests, track responses to these requests and to ensure that information related to incidents is stored effectively. This will allow organisations to provide evidence should it be required for an inquiry.	Communications Team are integral to Major Incident Plans and are contactable out of hours to on-call staff. They are aligned also to Adverse weather and heatwave Plans, providing alerts through the SHSC extranet JARVIS and social media. Updates to incidents are dated so that staff know they're following the most up to date situation.	Partially compliant				
Domain 8 - Cooperation										
38	Cooperation	LRF / BRF Engagement	The organisation participates in, contributes to or is adequately represented at Local Resilience Forum (LRF) or Borough Resilience Forum (BRF), demonstrating engagement and co-operation with partner responders.	• Minutes of meetings • A governance agreement is in place if the organisation is represented and feeds back across the system	SYLRF Information sharing protocol; SYLRF Constitution October 2022, information sharing agreements in place. Some are covered in individual contracts. Also requires ICB support to maintain.	Partially compliant				
43	Cooperation	Information sharing	The organisation has an agreed protocol(s) for sharing appropriate information pertinent to the response with stakeholders and partners, during incidents.	• Documented and signed information sharing protocol • Evidence relevant guidance has been considered, e.g. Freedom of Information Act 2000, General Data Protection Regulation 2016, Caldicott Principles, Safeguarding requirements and the Civil Contingencies Act 2004	SYLRF Information sharing protocol; SYLRF Constitution October 2022, information sharing agreements in place. Some are covered in individual contracts. Also requires ICB support to maintain.Still waiting for katie Hunter and John John Wolstenholme.	Partially compliant				
Domain 9 - Business Continuity										
46	Business Continuity	Business Impact Analysis/Assessment (BIA)	The organisation annually assesses and documents the impact of disruption to its services through Business Impact Analysis(es).	The organisation has identified prioritised activities by undertaking a strategic Business Impact Analysis/Assessments. Business Impact Analysis/Assessment is the key first stage in the development of a BCMS and is therefore critical to a business continuity programme. Documented process on how BIA will be conducted, including: • the method to be used • the frequency of review • how the information will be used to inform planning • how RA is used to support. The organisation should undertake a review of its critical function using a Business Impact Analysis/assessment. Without a Business Impact Analysis organisations are not able to assess/assure compliance without it. The following points should be considered when undertaking a BIA: • Determining impacts over time should demonstrate to top management how quickly the organisation needs to respond to a disruption. • A consistent approach to performing the BIA should be used throughout the organisation. • BIA method used should be robust enough to ensure the information is collected consistently and impartially.	Business Continuity Policy; Business Impact Assessment	Partially compliant				
49	Business Continuity	Data Protection and Security Toolkit	Organisation's Information Technology department certify that they are compliant with the Data Protection and Security Toolkit on an annual basis.	Evidence • Statement of compliance • Action plan to obtain compliance if not achieved	Waiting for Adam and Katie to respond	Partially compliant				

Ref	Domain	Standard name	Standard Detail	Supporting Information - including examples of evidence	Organisational Evidence	Self assessment RAG Red (not compliant) = Not compliant with the core standard. The organisation's work programme shows compliance will not be reached within the next 12 months. Amber (partially compliant) = Not compliant with core standard. However, the organisation's work programme demonstrates sufficient evidence of progress and an action plan to achieve full compliance within the next 12 months. Green (fully compliant) = Fully compliant with core standard.	Action to be taken	Lead	Timescale	Comments
51	Business Continuity	BC audit	The organisation has a process for internal audit, and outcomes are included in the report to the board. The organisation has conducted audits at planned intervals to confirm they are conforming with its own business continuity programme.	• process documented in EPRR policy/Business continuity policy or BCMS aligned to the audit programme for the organisation • Board papers • Audit reports • Remedial action plan that is agreed by top management. • An independent business continuity management audit report. • Internal audits should be undertaken as agreed by the organisation's audit planning schedule on a rolling cycle. • External audits should be undertaken in alignment with the organisations audit programme	Needs to be arranged - would suggest 360 Assurance - to discuss with Neil	Partially compliant				
53	Business Continuity	Assurance of commissioned providers / suppliers BCPs	The organisation has in place a system to assess the business continuity plans of commissioned providers or suppliers; and are assured that these providers business continuity arrangements align and are interoperable with their own.	• EPRR policy/Business continuity policy or BCMS outlines the process to be used and how suppliers will be identified for assurance • Provider/supplier assurance framework • Provider/supplier business continuity arrangements This may be supported by the organisations procurement or commercial teams (where trained in BC) at tender phase and at set intervals for critical and/or high value suppliers	Waiting for Julie Rice	Partially compliant				
Domain 10 - CBRN										
59	Hazmat/CBRN	Decontamination capability availability 24 /7	The organisation has adequate and appropriate wet decontamination capability that can be rapidly deployed to manage self presenting patients, 24 hours a day, 7 days a week (for a minimum of four patients per hour) - this includes availability of staff to establish the decontamination facilities There are sufficient trained staff on shift to allow for the continuation of decontamination until support and/or mutual aid can be provided - according to the organisation's risk assessment and plan(s) The organisations also has plans, training and resources in place to enable the commencement of interim dry/wet, and improvised decontamination where necessary.	Documented roles for people forming the decontamination team - including Entry Control/Safety Officer Hazmat/CBRN trained staff are clearly identified on staff rotas and scheduling pro-actively considers sufficient cover for each shift Hazmat/CBRN trained staff working on shift are identified on shift board Collaboration with local NHS ambulance trust and local fire service - to ensure Hazmat/CBRN plans and procedures are consistent with local area plans Assessment of local area needs and resource		Partially compliant				
60	Hazmat/CBRN	Equipment and supplies	The organisation holds appropriate equipment to ensure safe decontamination of patients and protection of staff. There is an accurate inventory of equipment required for decontaminating patients. Equipment is proportionate with the organisation's risk assessment of requirement - such as for the management of non-ambulant or collapsed patients • Acute providers - see Equipment checklist: https://www.england.nhs.uk/wp-content/uploads/2018/07/eprr-decontamination-equipment-check-list.xlsx • Community, Mental Health and Specialist service providers - see guidance 'Planning for the management of self-presenting patients in healthcare setting': https://webarchive.nationalarchives.gov.uk/20161104231146/https://www.england.nhs.uk/wp-content/uploads/2015/04/eprr-chemical-incidents.pdf	This inventory should include individual asset identification, any applicable servicing or maintenance activity, any identified defects or faults, the expected replacement date and any applicable statutory or regulatory requirements (including any other records which must be maintained for that item of equipment). There are appropriate risk assessments and SOPs for any specialist equipment Acute and ambulance trusts must maintain the minimum number of PRPS suits specified by NHS England (24/240). These suits must be maintained in accordance with the manufacturer's guidance. NHS Ambulance Trusts can provide support and advice on the maintenance of PRPS suits as required. Designated hospitals must ensure they have a financial replacement plan in place to ensure that they are able to adequately account for depreciation in the life of equipment and ensure funding is available for replacement at the end of its shelf life. This includes for PPE/PRPS suits, decontamination facilities etc.	CBRNe Plan reviewed and updated January 2024, staff training on induction, equipment held in Pharmacy for distribution against action cards for staff to follow and in line with guidance. PPE order form.	Partially compliant				
62	Hazmat/CBRN	Waste disposal arrangements	The organisation has clearly defined waste management processes within their Hazmat/CBRN plans	Documented arrangements for the safe storage (and potential secure holding) of waste Documented arrangements - in consultation with other emergency services for the eventual disposal of: - Waste water used during decontamination - Used or expired PPE - Used equipment - including unit liners Any organisation chosen for waste disposal must be included in the supplier audit conducted under Core Standard 53		Partially compliant				
63	Hazmat/CBRN	Hazmat/CBRN training resource	The organisation must have an adequate training resource to deliver Hazmat/CBRN training which is aligned to the organisational Hazmat/CBRN plan and associated risk assessments	Identified minimum training standards within the organisation's Hazmat/CBRN plans (or EPRR training policy) Staff training needs analysis (TNA) appropriate to the organisation type - related to the need for decontamination Documented evidence of training records for Hazmat/CBRN training - including for: - trust trainers - with dates of their attendance at an appropriate 'train the trainer' session (or update) - trust staff - with dates of the training that that they have undertaken Developed training programme to deliver capability against the risk assessment	EPM need to attend a Hazmat/CBRN Train the Traner cousre. However, EPM has already gained Level 3 in Teaching and training	Partially compliant				
66	Hazmat/CBRN	Exercising	Organisations must ensure that the exercising of Hazmat/CBRN plans and arrangements are incorporated in the organisations EPRR exercising and testing programme	Evidence • Exercising Schedule which includes Hazmat/CBRN exercise • Post exercise reports and embedding learning		Non compliant				
Deep Dive - Cyber Security and IT relate	0	0	0	0						
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) - Shared understanding of risks to the organisation and the population it serves with regards to EPRR - organisational risk assessments and risk registers -Plans and arrangements demonstrate a common understanding of incidents in line with EPRR framework and cyber security requirements. -EPRR work programme -Organisational EPRR policy	Head of Service Delivery & Infrastructure and IG Manager are both members of the Trusts Emergency Planning Group. Limited shared understanding of potential risks which needs to be reviewed. EPRR policy and related cyber incident response plans are being written and aligned.	Partially compliant	Emergency Planning manager and Head of Service Delivery & Infrastructure to review potential risks.	Adam HandleyJean Kiyori	45658	
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: -consider the operational impact of such incidents -be current and include a routine review schedule -be tested regularly -be approved and signed off by the appropriate governance mechanisms -include clearly identified response roles and responsibilities -be shared appropriately with those required to use them -outline any equipment requirements -outline any staff training needs -include use of unambiguous language -demonstrate a common understanding of terminology used during incidents in line with the EPRR framework and cybersecurity requirements.'	Cyber Incident Response Plan is currently in draft phase and is being reviewed and aligned with the trusts emergency planning policy Regional Cyber review has been conducted by ANS to review all NHS and Council organisations in South Yorkshire ICS to advise on potential improvements and areas for investment.	Partially compliant	Finalise and approve Cyber Incident Response Plan and cyber playbooks Review results from regional cyber assessment and next steps in terms of documentation and investment in infrastructure	Adam Handley	45717	

Ref	Domain	Standard name	Standard Detail	Supporting Information - including examples of evidence	Organisational Evidence	Self assessment RAG Red (not compliant) = Not compliant with the core standard. The organisation's work programme shows compliance will not be reached within the next 12 months. Amber (partially compliant) = Not compliant with core standard. However, the organisation's work programme demonstrates sufficient evidence of progress and an action plan to achieve full compliance within the next 12 months. Green (fully compliant) = Fully compliant with core standard.	Action to be taken	Lead	Timescale	Comments
DD3	Deep Dive Cyber Security	Resilient Communication during Cyber Security & IT related incider	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: 1. look beyond the technical solutions at processes and organisational arrangements 2. identify and review the critical communication activities that underpin your response arrangements 3. ensure diversity of technical solutions 4. adopt layered fall-back arrangements 5. plan for appropriate interoperability https://www.england.nhs.uk/wp-content/uploads/2019/03/national-resilient-telecommunications-guidance.pdf	Our updated communications plan for emergency preparedness, resilience and response (EPRR) covers the principles of how we will communicate in a cyber or IT related incident.	Partially compliant	Updated communications plan with Cyber Security addition to be approved at the Trusts Emergency Planning Group in January 2025	Holly Cubitt	45658	
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. - Agreed sign off processes for media and press releases in relation to Cyber security and IT related incidents. - Documented process for communications to regional and national teams - 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.	There are specific references to SHSCs communications activities and media handling plans in the updated communications plan for emergency preparedness, resilience and response (EPRR) Section 9 of SHSCs updated plan gives detail on spokespeople and how media enquiries will be handled. Section 11 of SHSCs plan details how we will report in the effectiveness of our communications activity and how we will liaise with regional and national teams as appropriate for the incident. Appendix C and D of SHSCs plan provides a draft statement for internal and external use in event of a cyber related incident. There is also detailed guidance in section 9 on spokespeople.	Partially compliant	Updated communications plan with Cyber Security additions to be approved at the Trusts Emergency Planning Group in January 2025	Holly Cubitt	45658	
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 - EPRR exercise and testing programme	Annual desktop exercises are conducted as part of the DSPT to review any potential issues. Cyber documentation is new and limited in places due to no dedicated cyber resource so further testing and exercises are needed to review and follow new documentaiton to make sure its clear of roles, responsibilities and potential scenarios that may occur during a potential cyber incident.	Partially compliant	Review annual EPRR Exercise and testing programme Align DSPT and EPRR Exercises Conduct exercise with cyber incident response plan.	Jean Kiyori	45658	
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 - Attendance/participant lists showing cybersecurity and IT colleagues taking part in incident response training.	No dedicated resource for Cyber Securily within the Digital department. Development is ongoing within Digital to provide some cyber securily training to staff in technical roles who would potentially be involved in supporting a cyber incident.	Non compliant	Incorporated into Digitals Target Operating Model to review roles and responsibilities and potential dedicated resource for cyber security.	Adam Handley	45717	
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	EPRR Risk Register informs SHSC Emergency and Business Continuity Plans	Partially compliant	Review current EPRR training Review potential improvements to include Cyber Security and IT related Incidents	Jean Kiyori Adam Handley	45717	
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 -list of the organisations critical services and functions -list of the organisations core IT/Digital systems and prioritisation of system recovery	Disaster Recover plan outlines SHSC critical services and functions and prioritises those services above others in the event of a DR scenario	Partially compliant	Conduct business impact analysis which will require clinical involvement to support.	Adam Handley	45717	
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 -key products and services within the scope of BCMS -Appropriate risk assessments	BCMS is in place. More training needed	Partially compliant	Further business continuity training sessions required across the trust and specifically on call managers	Jean Kiyori	45717	
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 -Disaster recovery plans for core systems -Cyber security and IT departments own BCP which includes contacts for key personnel outside of normal working hours	Disaster recover plan in place but is not specific to each core system. Cyber incident response plan has a list of key personnel and contact details. Digitals BCP is currently being reviewed.	Partially compliant	Finalise Cyber Incident response plan which lists key personnel details. Finalise reviewing Digitals BCP Document Disaster Recovery plans (Playbooks) for core systems	Adam Handley	45717	

Ref	Domain	Standard name	Standard Detail	Supporting Information - including examples of evidence	Organisational Evidence	Self assessment RAG Red (not compliant) = Not compliant with the core standard. The organisation's work programme shows compliance will not be reached within the next 12 months. Amber (partially compliant) = Not compliant with core standard. However, the organisation's work programme demonstrates sufficient evidence of progress and an action plan to achieve full compliance within the next 12 months. Green (fully compliant) = Fully compliant with core standard.	Action to be taken	Lead	Timescale	Comments