REPORT TO:	**NHS SOMERSET INTEGRATED CARE BOARD** **ICB Board Part A**	**ENCLOSURE:** **J**
DATE OF MEETING:	**30 January 2025**	
REPORT TITLE:	**Somerset ICS Cyber Security Strategy**	
REPORT AUTHOR:	**Sophie Hardesty, Head of Information Security and Compliance**	
EXECUTIVE SPONSOR:	**David McClay, Chief Officer of Strategy, Digital and Integration**	
PRESENTED BY:	**Sophie Hardesty, Head of Information Security and Compliance**	

PURPOSE	DESCRIPTION	SELECT (Place an 'X' in relevant box(es) below)
Approve	To formally receive a report and approve its recommendations, (authorising body/committee for the final decision)	X
Endorse	To support the recommendation (not the authorising body/committee for the final decision)	
Discuss	To discuss, in depth, a report noting its implications	
Note	To note, without the need for discussion	
Assurance	To assure the Board/Committee that systems and processes are in place, or to advise of a gap along with mitigations	

SELECT (Place an 'X' in relevant box(es) below)	LINKS TO STRATEGIC OBJECTIVES (Please select any which are impacted on / relevant to this paper)
X	Objective 1: Improve the health and wellbeing of the population
	Objective 2: Reduce inequalities
	Objective 3: Provide the best care and support to children and adults
	Objective 4: Strengthen care and support in local communities
	Objective 5: Respond well to complex needs
	Objective 6: Enable broader social and economic development
X	Objective 7: Enhance productivity and value for money

PREVIOUS CONSIDERATION / ENGAGEMENT
Somerset Cyber Forum, consisting of members from NHS Somerset, Somerset Foundation Trust, Somerset Council, St Margaret's Hospice, South West Ambulance Service Trust formed the stakeholder group which has informed the recommendations, supported by the NHS England Southwest Region Security Lead. Somerset Digital Transformation Board has discussed and agreed this strategy. ICS Digital Group has discussed and agreed this strategy.

REPORT TO COMMITTEE / BOARD
This report details the vision, objectives and recommendations of the Somerset ICS Cyber Security Strategy. It is recommended that accountability for this strategy is accepted by all ICS partners, and that it is owned and signed off by the Somerset ICB Board. The strategy will ensure the ICS is compliant with the Network and Information Security (NIS) Regulations by prioritising the protection of the operation of its essential healthcare functions. This strategy will be supported by a delivery plan that will be developed and overseen by the Digital Delivery Group. The pace of delivery against the plan will be determined by the availability of resource. Board members are asked to note however, that robust cyber defences are a fundamental building block to our wider DDaT strategy and support an approach that prioritises available resource to deliver this strategy. The prioritisation of funding will take place through the Digital Delivery Group with updates to the Board on progress, risks and mitigations. The strategy has been written to be applicable to all system partners, although recognises that some aspects will only be relevant to organisations delivering healthcare services, and specifically those that are subject to NIS Regulations. However, as this strategy is aimed at reducing the likelihood of an organisation being subject to a cyber-attack, and thereby protecting patient services, it is hoped that this strategy sets the bar for what is expected of all ICS partner organisations.

IMPACT ASSESSMENTS – KEY ISSUES IDENTIFIED (please enter 'N/A' where not applicable)	
Reducing Inequalities/Equality & Diversity	N/A
Quality	Achieving the strategic objectives helps to prevent organisations from being subject to cyber-attack, therefore preventing a negative impact on the quality of service, patient safety, patient experience and clinical effectiveness.
Safeguarding	N/A
Financial/Resource/ Value for Money	ICS partners will be required to provide appropriate funding and resource to ensure the strategy objectives are met, and to reduce the likelihood of organisations being subject to cyber-attack, therefore protecting health and social care services.
Sustainability	N/A
Governance/Legal/ Privacy	This strategy requires there to be a governance framework in place which has clear accountability, allowing for informed ICS-wide decision making which has sufficient influence to direct funding and prioritise cyber projects.
Confidentiality	N/A
Risk Description	This strategy will support ICS partners' existing cyber risk mitigating actions, alongside aiming to form an ICS-level cyber risk register to prioritise overall ICS cyber risk reduction. This strategy will use the Data Security & Protection Toolkit/Cyber Assessment Framework (DSPT/CAF) to monitor process and cyber maturity.

Somerset Integrated Care System – Cyber Security Strategy

30 January 2025

Somerset Integrated Care System Cyber Strategy

NHS Somerset

Preamble:

Integrated Care Systems have been directed by NHS England's National Chief Information Office to develop an ICS wide strategy that builds on the cyber security strategy for health and social care to 2030.

Milestones for the ICS cyber strategy are:

- Initial draft – by 30 Sept 24
- Final draft – by 18 Dec 24
- Formal sign-off by the ICB Board – 30 Apr 25

It is recommended that accountability for this strategy is accepted by all ICS partners, and that it is owned and signed off by the Somerset ICB Board. It is recommended that it provides oversight of any subsequent delivery plan detailing the work activities required to deliver the strategy.

The ICS cyber strategy has been written to be applicable to all system partners, although recognises that some aspects will only be relevant to organisations delivering health care services, and specifically those that are subject to the Network and Information Security Regulations (NIS) as operators of essential services (delivering health care services). However, as this strategy is ultimately aimed at reducing the likelihood of an organisation being subject to a cyber-attack, and thereby protecting patient services, it is hoped that this strategy sets the bar for what is expected of all ICS partner organisations.

The audience for this strategy is:

- Directors across the ICS – this will allow them to allocate appropriate funding and resource to ensure the strategic objectives are met.
- Local cyber and IT teams – with the expectation that a delivery plan will be created to provide appropriate detail around the work activities, time scales and resourcing required to deliver the strategy.

Somerset Integrated Care System Cyber Strategy

NHS Somerset

Vision

Working together to create secure digital environments that enable efficient and safe services

This Cyber Security Strategy will ensure the ICS is compliant with the Network and Information Security Regulations by prioritising the protection of the operation of its essential healthcare functions.

It will be based on the following set of core principles:

- Maximising existing capability before procuring new solutions.
- Data driven – using the data available across the ICS to help identify common risks and enabling prioritisation of effort and resource.
- Using the Data Security & Protection Toolkit/Cyber Assessment Framework (DSPT/CAF) to monitor progress and cyber maturity.

The strategy will be based on 5 themes that will be used to form a number of underpinning objectives:

- Awareness and culture
- Risk visibility and management
- Third party assurance
- Collaboration
- Ongoing resilience

Strategy objectives

NHS Somerset

Objective One: Developing and embedding a cyber aware culture

Through coordinated cyber training across the ICS, bolstering cyber governance and supporting the careers of cyber specialists within the ICS, we will ensure cyber becomes integrated into ICS core business.

Objective Two: Improving cyber risk visibility and management

The ICS will develop a clear understanding and oversight of its cyber risk through adopting a common risk reporting process that translates to a common risk language. There will be a defined risk appetite enabling effective prioritisation and management of cyber risks.

Objective Three: Building robust third-party assassurance

We recognise the risk posed by our suppliers so will prioritise identification of our critical suppliers and adopting robust assurance processes that minimise our risk exposure to the supply chain.

Objective Four: Prioritising collaboration

We will enhance the learning of individuals and teams by sharing good practice and leveraging the diverse range of skills across the ICS. We will achieve this through adopting resilient and accessible communication channels.

Objective Five: Ensuring ongoing resilience

Recognising that most cyber-attacks are opportunistic, we will focus on doing the basics well, critical review and test our processes to make sure we are the best we can be.

our SOMERSET Together we care

Objective one

NHS Somerset

Developing and embedding a cyber aware culture.

- Improved governance. Clear accountability allowing for informed decision making. This needs to be established across the ICS as a joint group with sufficient influence to direct funding and prioritise cyber projects.
- Common and shared training baseline such that staff across the ICS develop a shared understanding of cyber risk
- Agree common training tools that maximise investment.
- Regular awareness campaigns to help improve overall staff awareness, utilising national offerings where possible and applicable.
- In line with the CAF-DSPT, focus cyber training on high risk/high impact areas.
- Developing clear training and career pathway for cyber specialists.

our SOMERSET Together we care

Objective two

NHS Somerset

Improving cyber risk visibility and management

- Adopting a common risk language and scoring across the ICS that is readily understood and is aligned and compatible with all ICS organisations.
- A clear understanding and articulation of each organisation's risk appetite, and an agreed and documented risk appetite for the ICS.
- Shared Board and Operational dashboards that gives a common and representative view of organisational and system risk.
- Agreed understanding, prioritisation and monitoring of systems delivering essential functions to the ICS.
- Robust and well understood governance process that allows for prompt escalation of identified risks and issues.
- Align organisations vulnerability management processes where possible and create an ICS wide process to understand, validate and prioritise vulnerability management activity.

our SOMERSET Together we care

Objective three

NHS Somerset

Building robust supply chain assurance

- A regularly reviewed definitive list of ICS critical suppliers.
- A set of baseline cyber security standards and requirements for all suppliers and their products/services and implementing a common assurance process for all suppliers.
- Ensuring robust risk management of ICS critical suppliers through appropriate tooling.

our SOMERSET Together we care

Objective four

NHS Somerset

Prioritising collaboration

- A formalised virtual cyber team composed of individuals within ICS organisations that provide ongoing and reactive support to risk management and cyber incident response (24hr support) across the ICS.
- Agreeing and adopting common security policies and standards.
- A common platform, used by cyber professionals, that facilitates the sharing of knowledge, lessons and best-practice.
- Develop a system wide enterprise architecture approach that incorporates cybersecurity requirements early on in the design of digital systems and ensures relevant security assurance processes are adopted.
- Support all organisations across the ICS by appropriate allocation of central funding that prioritises overall ICS risk reduction.

our SOMERSET Together we care

Objective five

NHS Somerset

Ensuring ongoing resilience

- Focusing on excellence in fundamental technical cyber security controls and practices, such as implementing MFA by default, robust configuration and hardening and regular patching.
- Regular testing and exercising of incident response, business continuity and disaster recovery plans of critical ICS systems.
- Develop an agreed and appropriately resourced cyber security programme that improves ICS wide digital maturity and interoperability.

our SOMERSET Together we care

Objective One: Developing and embedding a cyber aware culture

Objective	Where we are now	Where we want to be by 2026	How will we know when we've got there?
Improved governance. Clear accountability allowing for informed decision making. This needs to be established across the ICS as a joint group with sufficient influence to direct funding and prioritise cyber projects.	There is existing cyber governance within partner organisations in the ICS, but this isn't coordinated through a formalised governance structure. As such, whilst Somerset has established a cyber group which meets monthly, it doesn't sit within a recognised reporting structure, isn't tasked by a senior group or formally asked to report on cyber issues or risks. Consequently, decisions on cyber security are made in a vacuum outside of the formal decision-making process.	There is a formal cyber group with terms of reference, a clear mandate and boundaries, including a quick and robust escalation route to known accountable individuals when required. There is a defined and protected funding stream that is clear and understood.	• Reviewed and approved cyber group TORs that are approved by the ICB Digital Group. • The ICS cyber group is integrated into the ICS reporting structure and is formally documented. • Escalation and decisions have been tested, using real cases as evidence. • All organisations meet the 'achieved' indicated of good practice objective A1 of the DSPT-CAF Managing risk.
Common and shared training baseline such that staff across the ICS develop a shared understanding of cyber risk	Each organisation has their own cyber training which isn't coordinated with other organisations across the ICS. Training isn't based on any specific threat profile.	In accordance with DSPT-CAF, each organisation will have completed a training needs analysis that will have identified staff risk levels. ICS organisations will work together to coordinate their training campaigns tailored to staff risk levels. A shared training plan will be in place that will have defined training levels. Each campaign will be tied to current threat profiles – taken from NCSC and NHSE CSOC For cyber professionals, relevant training courses will be identified and associated with specific roles across the ICS.	• The same campaign materials are used across organisations. • Campaigns will be directly linked to threat assessments provided by NCSC and CSOC. • A common ICS staff risk profile is documented. • Cyber professionals across the ICS will have attended the same professional course.
Agree common cyber training tools that maximise investment.	No coordination of training tools, different procurement routes followed.	Common training providers are used across the ICS, and training licences to ICS organisations are shared and coordinated centrally.	• A single identified training provider is delivering training across the ICS.

Objective One: Developing and embedding a cyber aware culture

NHS Somerset

Objective	Where we are now	Where we want to be by 2026	How will we know when we've got there?
Regular awareness campaigns to help improve overall staff understanding of cyber security, utilising national offerings where possible and applicable.	Currently uncoordinated, utilising different outsourced companies. No coordination of themes so messaging across the ICS is mixed using different language.	There are common awareness campaigns that complements the national NHS Keep IT Confidential resource. Themes are coordinated and based on current threat intelligence. There is quarterly tracking and reporting that gets oversight by the ICB and local organisation Boards.	• There is a 12-month plan for which Cyber theme will be run across the ICS • A single coordinated themed campaign has been run across the ICS.
In line with the DSPT-CAF, focus cyber training on high risk/high impact areas.	Training campaigns are ad hoc without any focus on high-risk areas. Each organisation dictates its own priority theme.	Information is shared across the ICS and training is based on current threats to health/social care. The Cyber forum identifies high risk areas and recommends prioritisation of mitigation/remediation work activities.	• Defined ICS wide campaign strategy • All ICS organisations have achieved 6.b of the DSPT-CAF
Developing a clear training and career pathway for cyber specialists.	Differing level of skills and knowledge that can't be directly matched to ICS cyber roles. Limited support to develop cyber careers. Different cyber training tools are used and no linkage in cyber roles across the ICS.	Have common defined roles for cyber, including banding, where the required training for each role is understood. Working towards a shadowing programme where a cyber role from one organisation work alongside a similar role from another organisation within the ICS.	• At least 1 individual has worked alongside a colleague from a different organisations for a period of 2 days or more. • The ICS retains its cyber staff and there are no cyber leavers due to morale/pay, other than career progression.

Objective Two: Improving cyber risk visibility and management

Objective	Where we are now	Where we want to be by 2026	How will we know when we've got there?
Shared Board and Operational dashboards that gives a common and representative view of organisational and system risk.	Each organisation has their own reporting structure with their own metrics. No coordination or common reporting, including different risk scores.	There is an agreed dashboard that accurately reflects the ICS risk, both at a system and local level. There is a robust process for reporting that has elements of automation and is quick to update.	• The ICS partner boards, and subordinate committees are provided regularly with dashboards that they understand and can base decisions on.
Agreed understanding, prioritisation and monitoring of systems delivering essential functions to the ICS.	Each organisation doesn't fully understand their essential functions, how they are linked, and therefore doesn't understand which of these is essential for the ICS.	The ICS has documented its essential functions and supporting systems and has in place effective monitoring.	• An ICS system has gone through a BIA to evidence that this is in place. • The ICS has run an ICS wide Cyber Incident Response Exercise that prove the robustness of BC plans and ICS coordination.
Robust and well understood governance process that allows for prompt escalation of identified risks and issues.	Each organisation has their own processes, but they are not aligned with the wider ICS. Focus is protecting the individual organisation, rather than act in a coordinated manner based on ICS priorities.	Utilise the existing governance processes at the ICS level to embed cyber escalation within the process, such that decisions are made at the ICS level where necessary. There is a mapping of ICS systems such that there is clear understanding of inter-dependencies. Communication plans are in place and established such that information is rapidly available to relevant teams.	• The process is either tested or is used in response to an actual cyber incident.
A vulnerability management programme that can be adopted by all organisations across the ICS.	There is a clear understanding of each organisation's patching and vulnerability scanning schedule, but it is not coordinated across the ICS. Each exception is managed differently depending on organisation's risk profile.	There is a common high-level patching policy and change management process that is adopted across the ICS. There is a recognised method of instantly communicating patching issues enabling organisations to share learning and experience on patch updates. The NHS's vulnerability alerting (High Severity Alerts - HSA's) will be used across the system to help prioritise critical patches. Microsoft Defender for Endpoint (MDE) will be used to align patching reporting.	• A single patching policy has been agreed and adopted. • A patching dashboard, that shows all ICS organisations, is used at the ICS Cyber Group to report on patching progress/issues.

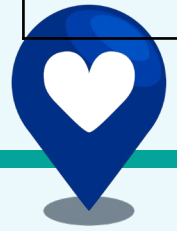
NHS Somerset

our SOMERSET Together we care

Objective Three: Building robust third-party assurance

NHS Somerset

Objective	Where we are now	Where we want to be by 2026	How will we know when we've got there?
A regularly reviewed definitive list of ICS critical suppliers.	Local organisations have different methods of measuring/identifying important suppliers. ICS has not agreed what the definition of a critical supplier is. There is no single list of critical suppliers. There is no annual review of local or ICS critical suppliers.	A documented process for identifying ICS critical suppliers. ICS critical suppliers are centrally managed, with a robust assurance process in place. This will include sharing of review responsibilities. All ICS organisations will look to align their management of suppliers to CAF principles.	• Critical suppliers are listed and the ICB Board are regularly briefed on assurance status of critical suppliers. • Critical suppliers have all been reviewed as part of an annual review.
There is a set of baseline cyber security standards and requirements for all suppliers and their products/services and implementing a common assurance process for all suppliers.	Each org. has its own method for providing assurance with different templates and standards applied. There is flexibility in supplier standards used. Shadow IT remains a problem for all organisations.	Organisations across the ICS use the same wording/requirements (common clauses) for suppliers. Consistent assurance with appropriate governance. Procurement teams are readily engaged with cyber teams having early engagement with project teams.	• Evidence is provided that all procurements use the same template for cyber assurance. • Supplier risk is reduced to a manageable level (i.e. medium/low).
Ensuring robust risk management of suppliers through appropriate tooling.	No tooling used for risk management – currently managed as an operational risk on an ad hoc basis. No dedicated resource to focus on supplier risk.	Supplier risk is prioritised across the ICS with dedicated funding to address the risk. Common and consistent process used across the ICS, done by each organisation but reported centrally to the ICB. A single 3rd party supplier management tool is centrally procured and used by all organisations in the ICS	• Cyber funding is used to procure a cyber risk management tool. • All organisations in the ICS are reporting on supplier risk through a single reporting tool.



our SOMERSET Together we care

Objective Four: Prioritising collaboration

Objective	Where we are now	Where we want to be by 2026	How will we know when we've got there?
A formalised virtual cyber team composed of individuals within ICS organisations that provide ongoing and reactive support to risk management and cyber incident response (24hr support) across the ICS.	Each 'tier 1 org' has a nominated lead for cyber and through MSP or nationally has a 24/7 capability. There is no centrally coordination of these teams. No common threshold for alerting used by Managed Service Providers/Cyber Security Operating Centre (CSOC).	Creation of a Cyber Technical Advice Cell (CTAC) which outlines the process of response. A consistent and coordinated response to a cyber incident affecting an ICS organsiation, where the skills and experience across the ICS can be leveraged as necessary. The CTAC is used to provide enduring support should the cyber incident take several weeks to resolve.	• Documented CTAC operating procedures. • CTAC has been tested (either exercised or for a real incident).
Agreeing and adopting common security policies and standards.	The Cyber Assurance Framework (CAF) (and DSPT-CAF for NHS organisations) is used for Tier 1 organisation (such as Trusts and Local Authority (LA), small organisations align where possible. LA have used ISO27001 as basis for policy template. NHS working towards ISO standard. Voluntary sector have used Cyber Essential Plus (CE+). ICB uses their IT service provider (South Central and West Commissioning Support Unit) policies.	ISO27001 is used as the high-level structure for security policies. CAF (and the DSPT-CAF) is used as the common language and the standard to which all ICS organisations look to meet.	• All ICS organisations (DSPT Category 1, 2 and 3 organisations) meet DSPT-CAF standards met.
A common platform, used by cyber professionals, that facilitates the sharing of knowledge, lessons and best-practice.	There is no common platform used across the ICS, some using the NCSC platform, others using those provided by the NHS England. Generally ad hoc using various channels.	There is formalised structure to the ICS Group forum, with approved TORs and a sharing platform that is secure and properly funded.	• Evidence of the ICS cyber leads regularly communicating on cyber matters (daily).

Objective Four: Prioritising collaboration

NHS Somerset

Objective	Where we are now	Where we want to be by 2026	How will we know when we've got there?
Develop a system wide enterprise architecture approach that incorporates cybersecurity requirements early on in the design and ensures relevant security assurance processes are adopted.	Whilst each organisation will have its own process, there has been limited need for these to be coordinated across the ICS. No common setting of standards.	The ICS Cyber Group is part of an authoritative governance process that reviews ICS wide initiatives (particularly if using AI). Identifying and agreeing common cyber security standards that should be used (certificates etc).	• The ICS Cyber Group minutes a decision made to approve or reject an ICS wide initiative.
Support all organisations across the ICS by appropriate allocation of central funding that prioritises overall ICS risk reduction.	Previous central funding has been focused on local NHS organisations to mitigate specific risk. LA/Voluntary sector not often considered or access separate funding streams.	There is more of a focus on overall ICS cyber risk and central funding from NHS is managed by the ICB and allocated on cyber projects that benefit the wider ICS. The ICS Cyber Group have developed a cyber risk register and a 'list' of priorities that funding can be used to mitigate ICS risk.	• NHS central cyber funding for 24/25 is used to procure a product/services that mitigates ICS wide cyber risk, not just an individual NHS organisation.

Objective Five: Ensuring ongoing resilience

NHS Somerset

Objective	Where we are now	Where we want to be by 2026	How will we know when we've got there?
Focusing on excellence in fundamental technical cyber security controls and practices, such as implementing MFA by default, robust configuration and hardening and regular patching.	There is general alignment of guidelines. Each ICS organisation has its own build/imaging standards. Different policies and different guidelines followed (central government vs NHS).	All organisations agree and align to the same standards and policies – i.e. such as Centre for Internet Security / MFA, enabling users across the ICS to have a similar experience irrespective of what organisation they are employed by.	• The same set of standards and policies are in place and used as evidence in compliance audits. • Staff satisfaction surveys indicate positive experience of staff working across the ICS.
Regular testing and exercising of incident response, business continuity and disaster recovery plans of critical ICS systems.	Each org as its own exercise schedule, and has completed an ICS exercise, although scenario was health focused and therefore did not involve LA.	There is a planned schedule of ICS wide testing that has the correct audience (participants as well as organisations). ICB board have had oversight and some involvement in the exercise.	• A common and joined up exercising schedule is coordinated by the ICB. This includes an ICS wide exercise once a year that involves all ICS organisations.
Develop an agreed cyber security programme that improves ICS wide digital maturity and interoperability.	Varied maturity of cyber programme within organisations. No central ICS cyber programme.	Individual cyber programmes are shared, improving alignment. An ICS cyber programme is created that takes into account individual cyber programmes and is focused on reducing ICS risk exposure. The ICS Cyber Programme is centrally managed and resourced and overseen by the ICB Board.	• ICS cyber strategy created and approved by ICB Board, after sign-off from each ICS organisation. • An ICB dashboard created to report on progress of ICS cyber programme.

Glossary

AI – Artificial Intelligence

BC Plans – Business Continuity Plans

BIA – Business Impact Assessment

CE+ - Cyber Essentials Plus

DSPT-CAF – Data Security & Protection Toolkit/Cyber Assessment Framework

HSAs – High Severity Alerts

ICB – Integrated Care Board

ICS – Integrated Care System

LA – Local Authority

MDE – Microsoft Defender for Endpoint

MFA – Multifactor Authentication

MSP – Managed Service Providers

NCSC – National Cyber Security Centre

NHSE CSOC – NHS England Cyber Security Operations Centre

NIS Regulations - Network and Information Security Regulations

TOR – Terms of Reference