

A close-up photograph of a doctor's hands and arms. The doctor is wearing a white lab coat over a light blue shirt and a dark tie. They are holding a black stethoscope against their chest. The background is a blurred hospital corridor with bright lights.

Cheshire and Merseyside ICS: Cyber Security Strategy

A large, thick blue graphic element on the right side of the page, consisting of a diagonal line that curves downwards and then back up, resembling a stylized arrow or a checkmark.

May 2023

CONTENTS

What does the ICS Cyber Security Strategy cover?

Cheshire and Merseyside



EXECUTIVE SUMMARY

03



OBJECTIVES AND
KEY ACTIVITIES

20



CONTEXT

07



GOVERNANCE AND
ACCOUNTABILITY

58



ENSURING ALIGNMENT

10



CYBER SECURITY
STRATEGY EXECUTION

62



OUR MISSION AND VISION

15



APPENDICES

69



PUTTING THE STRATEGY
TOGETHER

17

01 Executive Summary

EXECUTIVE SUMMARY (1/3)

In response to the 2019 NHS Long Term Plan, NHS England established 42 **Integrated Care Systems (ICSs)** across England, each led by an **Integrated Care Board (ICB)**, including our **Cheshire and Merseyside (C&M) ICS**. ICSs have facilitated NHS collaboration with local councils and other key stakeholders to take responsibility for improving the health and well-being of local residents, collectively coordinating services and managing resources.

We have an ambitious vision **to enable everyone in C&M to have a great start in life**, and get the support they need to stay healthy and live longer. To achieve it, we need to continue to develop and maintain a **secure health and care system** across C&M. We can achieve this by **levelling up our digital tools and services**, and ensuring they are **cyber secure and resilient** by working together.



Five-Year Cyber Security Strategy

Our vision is to become **cyber leaders amongst our peers** by contributing to developing and maintaining a **secure health and care system** across C&M. We will achieve this by **protecting our organisations**, as well as **information systems and critical assets** that support **our essential functions** from cyber threats, ensuring the safety of our staff and patients.

As a result, we have designed this **five-year C&M ICS Cyber Security Strategy** to enable us to strengthen our security posture and further improve organisational resilience. As such, this Strategy document details our:

- Proposed **cross-community cyber security initiatives**, which will enable us to take advantage of economies of scale that come from working as one;
- Approach to **minimising the impact of cyber incidents** and ensuring patient data security;
- Proposes an ICS-wide **cyber security governance structure** that maximises value; and
- Defines **clear metrics**, in a form of Key Performance Indicators (KPIs) to **measure success**.



Key considerations in developing this Strategy

We wanted to ensure that the Strategy **builds upon existing foundations** to **tackle the challenges we face**, and **take advantage of opportunities** open to us. External drivers, such as the [2023 Department of Health and Social Care \(DHSC\) Cyber Security Strategy](#), our [Digital and Data Strategy](#), as well as key NHS and cyber security frameworks, such as the NHS [‘What Good Looks Like’ framework](#) and [NIST Cybersecurity Framework](#), guided development of the Strategy to ensure our alignment with their requirements and **industry good practice**. Additionally, we have worked with **primary stakeholders** across the C&M ICS, running workshops to identify nine fundamental strategic objectives we would like to **achieve over the next five years** and ensure that the Strategy **meets the security needs of ICS partner organisations**.

EXECUTIVE SUMMARY (2/3)



Strategic objectives

At the core of this Cyber Security Strategy there are **nine strategic objectives** with corresponding **activities** to be delivered across a five-year timeline **by the ICS Regional Security Operations Centre (R-SOC) and Cyber Centre of Excellence (CCoE)**, overseen by the **Cyber Management Board**.

Working with key stakeholders across the ICS, we have identified our **current state for each objective**, defined **our target state**, and discussed a number of **detailed activities** we would need to complete to achieve each objective. In turn, each activity has been assigned **an accountable lead**, one of four **priority levels for implementation** and a **list of dependencies** that should be achieved prior to commencement. Working through these activities will enable us to level up organisational cyber security resilience throughout C&M ICS, thereby cementing our position as cyber leaders across the ICS landscape.

- 1 The first strategic objective, centred around [Cyber Governance](#), outlines our aspiration for the C&M ICS to effectively and efficiently lead, drive, and oversee cyber security activities across all ICS partner organisations. To help us achieve this, the Strategy also proposes a governance approach we can implement.
- 2 Objective two, [Cyber Risk Management](#), recommends that the C&M ICS and its partner organisations utilise a shared language when it comes to cyber risk, applying a unified approach to identifying and mitigating cyber risk to its shared critical systems and services wherever possible.
- 3 For objective three, [Cyber Incident Management](#), we want to collaboratively and consistently identify, respond to, and recover from cyber security incidents, minimising their impact on critical services, utilising the standardised incident management approaches and ICS-wide SOC capability.
- 4 The fourth objective, [Cyber Procurement](#), calls for the C&M ICS to maximise its use of nationally provisioned tools and services to eliminate procurement duplication and take advantage of economies of scale, while effectively managing third-party suppliers.
- 5 Objective number five, [Third-Party Risk Management](#), proposes that the C&M ICS uses a risk-based third-party risk management framework to effectively manage cyber security risk associated with third-party tools and services, while selecting, contracting, monitoring and off-boarding external service providers.
- 6 The sixth, [People and Culture](#), focuses on our objective to have a strong cyber security culture, backed by a robust training and awareness programme that communicates and embeds staff's security responsibilities, and allows the ICS to constantly upskill staff on cyber security.
- 7 Under objective seven, [Knowledge Sharing and Good Practice](#), we want the C&M ICS to have a robust cyber security knowledge-sharing culture, where all personnel use tools to efficiently exchange and discuss industry good practices, information, and recent cyber activities.
- 8 Meeting the eighth objective, [Cyber Security Policies and Processes](#), will help us manage cyber security across all ICS partner organisations by standardising and improving cyber security policies and processes, as well as identifying and correcting policy non-compliance.
- 9 Finally, the ninth strategic objective, [Cyber Baselines and Minimum Standards](#), focuses on the C&M ICS supporting its partner organisations in upholding robust cyber security and improving cyber resilience by developing and supporting the roll out of minimum cyber security standards across the ecosystem.

EXECUTIVE SUMMARY (3/3)



Cyber security governance

In order to move on as an ICS from the current ‘collaboration of the willing’ to a **well-functioning, ICB-led unit** and **effectively implement this ICS Cyber Security Strategy**, we require a strong **foundation of effective cyber governance and accountability** model. Consequently, we are proposing a change from how we currently operate under the Cyber Leadership Group and Cyber Group, to set up an **ICS Cyber Management Board** that will be accountable and monitor implementation of this Strategy.

Reporting to the **Digital Transformation and Clinical Improvement Board**, the Cyber Management Board will include: an **ICB Chief Technology Officer (CTO)**, which will chair the Board, an **ICS Lead Chief Information Officer (CIO)** that would fulfil the role of a Senior Information Risk Officer (SIRO), a **Data Protection Officer (DPO)** – two roles mandated by the NHS ‘What Good Looks Like’ framework for an ICS to have, an **ICS Cyber Services Managing Director**, a **Security Operations Centre Lead**, a **Cyber Centre of Excellence Lead**, as well as other cyber leadership members.

To implement the activities outlined within this ICS Cyber Security Strategy and meet our desired strategic objectives, we are also proposing installation of an **ICS Regional Security Operations Centre (R-SOC)**, which will provide a 24/7 monitoring, detection, and response capabilities to the ICS partner organisations’; and **ICS Cyber Security Centre of Excellence (CCoE)**, that will consist of a group of ICS-dedicated cyber security professionals that will drive implementation of the Strategy activities, ICS-based cyber services, and support the C&M ICS partner organisations in matters of cyber security when required.



Next steps

In order to reach our target state and implement the activities under the strategic objectives within the next five years, a certain level of **investment and buy-in** is required. Some activities would require investment into **technical solutions**, such as monitoring and alerting systems for the R-SOC to meet objective three which is focused on cyber incident management; or a knowledge management platform to meet the knowledge sharing and good practice objective.

However, majority of the identified activities would predominantly rely on **time and effort from dedicated resources** as part of the ICS R-SOC and CCoE. We are already developing a target operating model for our R-SOC and resources that would support the CCoE when it comes to cyber incident response, but to proceed with understanding the full scope of the resources we need, we need to now **agree and approve** the C&M ICS Cyber Security Strategy, the ICS cyber governance structure, as well as the services the ICS will deliver centrally to our partner organisations.

02 Context

BACKGROUND

Who are we and where are we coming from?

For years, health services and care services across England were run by separate organisations with different objectives. In 2016, health services and local authorities from across **Cheshire and Merseyside (C&M)** formed what would later become the C&M Integrated Care System (ICS), to provide a forum for NHS leaders, local authorities and other key organisations to come together, as equal partners, and **take collective action**.

The NHS Long Term Plan, published in 2019, aimed towards an even greater **integration of regional healthcare services**. Subsequently, 42 ICSs, each led by an **Integrated Care Board (ICB)**, have been established across England. The ICSs have become a driving force for the NHS to collaborate with local councils and other key stakeholders to take responsibility for improving the health and well-being of local residents, coordinating services, and managing resources collectively. One of which, the **C&M ICS**, was designated by NHS England in April 2021, with the following vision:

“ We want everyone in Cheshire and Merseyside to have a great start in life, and get the support they need to stay healthy and live longer. ”

C&M is **one of the largest ICSs** in England with a population of **2.7 million people** living across a large and diverse geographical footprint. The ICS brings together **nine places**, each with an individual **local authority**, **17 NHS Provider Trusts**, **two NHS Provider Collaboratives**, **one Ambulance Service** and **355 GP practices**.

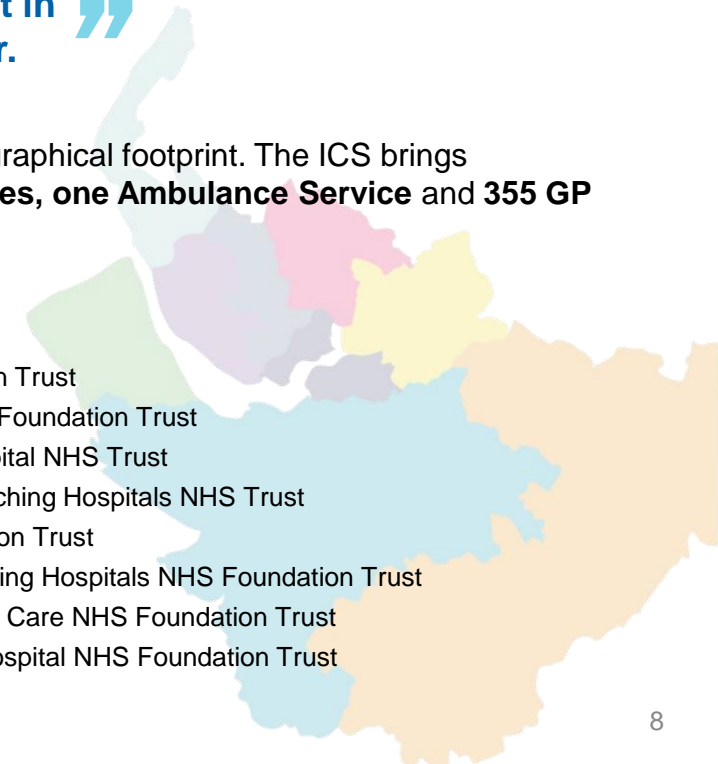
Local Authorities

- Cheshire East Council
- Cheshire West and Chester
- Halton Borough Council
- Knowsley Council
- Liverpool City Council
- St. Helens Council
- Sefton Council
- Warrington Borough Council
- Wirral Council

NHS Provider Trusts

- Alder Hey Children's Hospital NHS Foundation Trust
- Bridgewater Community Healthcare NHS Foundation Trust
- Cheshire and Wirral Partnership NHS Foundation Trust
- Countess of Chester Hospital NHS Foundation Trust
- Clatterbridge Cancer Centre NHS Foundation Trust
- East Cheshire NHS Trust
- Liverpool Heart and Chest Hospital NHS Foundation Trust
- Liverpool University Hospitals NHS Foundation Trust
- Liverpool Women's NHS Foundation Trust

- Mersey Care NHS Foundation Trust
- Mid Cheshire Hospitals NHS Foundation Trust
- Southport and Ormskirk Hospital NHS Trust
- St Helens and Knowsley Teaching Hospitals NHS Trust
- Walton Centre NHS Foundation Trust
- Warrington and Halton Teaching Hospitals NHS Foundation Trust
- Wirral Community Health and Care NHS Foundation Trust
- Wirral University Teaching Hospital NHS Foundation Trust



BACKGROUND

What do we need to do now?

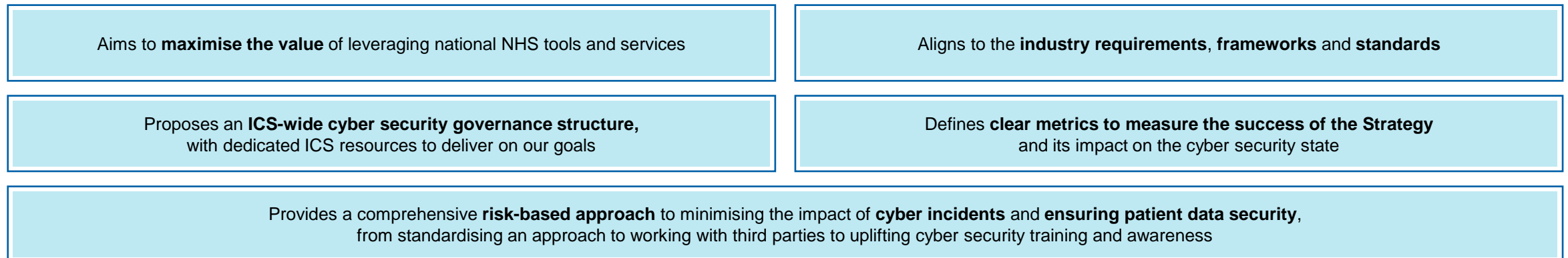
To support and enable more efficient health and care delivery, C&M has ambitious plans to **better use digital tools and data** generated across the region. To do this, we need a strong **digital infrastructure** that is **accessible, secure and resilient**.

Currently, we have an established **Cyber Group**, spearheaded by the **Cyber Leadership Group**, which came together in the aftermath of the 2017 Wannacry cyber attack that impacted the NHS across the nation. The Group began as a **'collaboration of the willing'** to explore the potential for creating closer working arrangements to mitigate the effects of a future cyber attack and improve the collective cyber security posture across the patch.

Developing a Cyber Security Strategy

With the recent establishment of the C&M ICS, we now have the opportunity to move beyond the **'collaboration of the willing'**, establish a **new governance structure**, as well as develop and deliver **cross-community cyber security initiatives to strengthen security and improve organisational resilience further**.

This document forms our **five-year C&M ICS Cyber Security Strategy**, which defines a common approach to cyber security management, and responsibilities across the ICS and partner organisations, so that we are able to deliver patient care securely and efficiently. This Strategy:



While we are keen to level up our cyber security posture across the ICS in a way that **meets the needs of our ICS partner organisations**, we also wanted to ensure alignment with the overall direction of the Department of Health and Social Care (DHSC) cyber security strategy, our overarching mission and vision, as well as the goals of the ICS Digital and Data strategy.

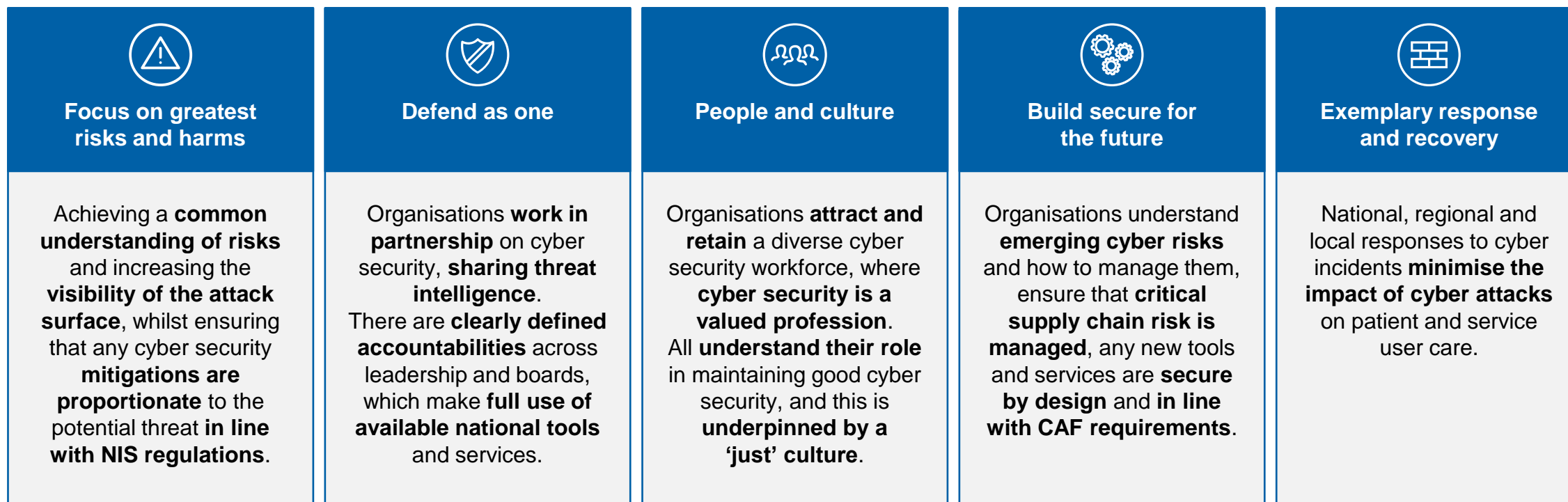
03 Ensuring Alignment

Health & Social Care Cyber Security Strategy

Aligning with national direction (1/2)

In March 2023, **DHSC** published its cyber security strategy in response to the HM Government's cyber security strategy, titled 'A cyber resilient health and adult social care system in England: cyber security strategy to 2030', setting out **an approach to cyber security with a vision of a health and social care sector that is resilient to cyber attack**, in turn improving the safety of patients and service users through good cyber security.






The strategy is centred **around five pillars**, underpinned by the Cyber Assessment Framework (CAF) and its four key objectives. As part of the strategy, each pillar is supported by desired outcomes:



Health & Social Care Cyber Security Strategy

Aligning with national direction (2/2)

Each of the five pillars details an **approach as to how each of the desired outcomes will be achieved**. A number of those approaches **fall upon the ICSs** to drive and implement. All of these requirements and obligations are embedded within our ICS Cyber Security Strategy and its underlying activities.

 Focus on greatest risks and harms	 Defend as one	 People and culture	 Build secure for the future	 Exemplary response and recovery
<ol style="list-style-type: none">1. Identify and record risks within the ICS, including supplier cyber risks, that would affect the local system's ability to function.2. Engage with a plan at ICS level to mitigate risks, invest and review progress.3. Ensure cyber risk is reviewed as part of corporate risk management.4. Ensure providers maintain an understanding of their suppliers' cyber security controls and risks.	<ol style="list-style-type: none">1. Create an ICS-wide cyber security strategy to drive security across the system.2. Allocate funding to deliver the strategy, establishing governance to review and align plans and ensuring member and wider partner involvement.3. Align with agreed cyber security standards when using existing and new cross-organisational systems.	<ol style="list-style-type: none">1. Develop an appropriately resourced and accountable cyber security function.2. Develop strategies to recruit and maintain an adequate cyber support function.3. Embed cyber security decisions into multi-disciplinary forums across the ICS.4. Encourage collaboration across organisations to share good practice and address deficiencies.5. Lead by example in implementing a 'just culture' at ICS level in approaching any identified cyber vulnerabilities.	<ol style="list-style-type: none">1. Build systems and services cyber secure by design, including engaging suppliers on their cyber security in alignment with national engagement.2. Regularly engage organisations on compliance with standards and frameworks.3. Develop a cyber security programme underpinning the objectives of the strategy and outline milestones and metrics.	<ol style="list-style-type: none">1. Outline responsibilities and expectations of partner organisations for response and recovery, as well as for a central accountable function.2. Ensure the ICS have a plan for responding to, managing, and recovering from a cyber attack.3. Lead on ICS-wide incident response exercising.4. Understanding the outcomes from dry-runs and post-incident reviews, identifying and responding to common themes.5. Develop ICS resilience with the impact of loss or unavailability of critical ICS-wide systems understood and mitigations agreed.

C&M ICS Strategy 2021-2025

Aligning with our regional direction (1/2)

In June 2021, we agreed an overarching **five-year strategy for improving health and wellbeing in Cheshire and Merseyside** in response to the NHS Long Term Plan published in 2019. As part of the strategy, we have defined a clear **mission, vision and strategic objectives**:

C&M ICS Mission

We will tackle health inequalities and improve the lives of the poorest fastest. We believe we can do this best by working in partnership.

C&M ICS Vision

We want everyone in Cheshire and Merseyside to have a great start in life, and get the support they need to stay healthy and live longer.

Strategic Objectives

➤ We have set four strategic objectives within the five-year strategy:



1. Improve population health and healthcare



2. Tackling health inequality, improving outcomes and access to services



3. Enhancing quality, productivity and value for money



4. Helping the NHS to support broader social and economic development

We recognised that the aspirations, objectives and activities defined within our new ICS Cyber Security Strategy needed to **align with the overarching mission, vision and strategic objectives** of the ICS strategy, while interlinking key success measures outlined in the **‘What Good Looks Like’ framework**. This is important for us to ensure that our approach to cyber is commensurate with our approach to improving health and care outcomes across C&M more broadly. For example:

- As part of the overall mission, we want to **work collaboratively and effectively as a partnership** and so we have **defined a clear governance approach** that will enable us to do so.
- To be able to **provide the support to everyone in C&M** to stay healthy to achieve our overall vision, we want to **build strong foundations** by agreeing on **baseline security controls and minimum standards** that would ensure continued security of health services and products.
- In line with objective three, we want to **streamline our cyber procurement practices** to **increase the value for money** of working with third party providers.

C&M ICS Digital and Data Strategy 2022-2025

Aligning with our regional direction (2/2)

To meet the overarching ICS mission, vision and objectives, we have also defined a **three-year Digital and Data Strategy**, as the investment into and the use of **digital solutions and data** will help us **generate insights** to support care planning, improve our services, tackle inequalities, and in turn **support better health and care delivery for all**. As such, **we want to be the most digitally advanced and data driven ICS in England by 2025**. This underpins **our vision**, where we want to see:

A digitally empowered C&M population taking increased control of their own physical and mental health and well-being.

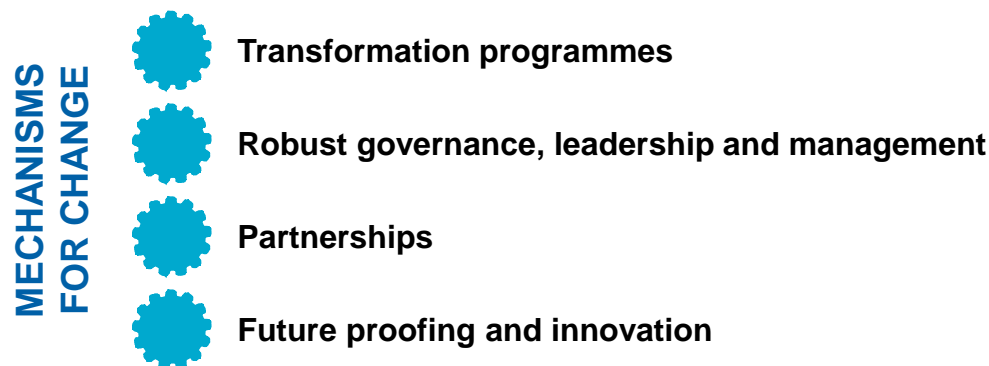
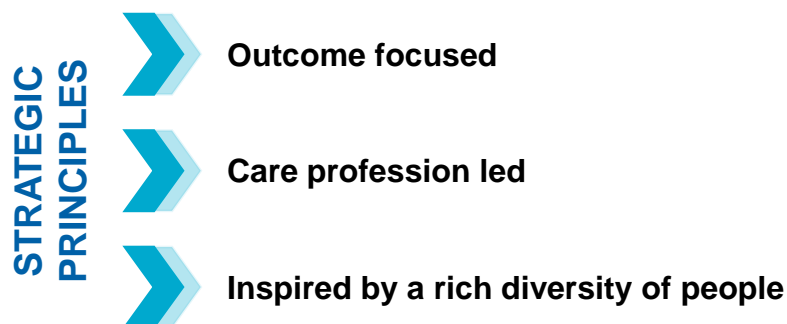
A data and digital confident and competent workforce able to deliver safe, effective and efficient care.

A secure and reliable insight and intelligence provision, underpinning joined up care planning and able to understand and help meet evolving population need.

To achieve this vision, we have identified **three key goals** we want to meet:

- 01** Strong digital and data foundations
- 02** 'At scale' digital and data platforms
- 03** System wide digital and data tools and services

In turn, to meet these goals, we identified **three strategic principles** that inform and underpin the changes we want to see, and **four mechanisms for change**:



Our **C&M ICS Cyber Security Strategy** inherently builds upon this vision, goals and strategic principles – **from overarching mission and vision**, down to **strategic objectives and activities** that sit at the heart of the Strategy.

04 Our Mission and Vision

C&M ICS CYBER SECURITY STRATEGY

Where are we going from a cyber perspective?

Aligning with the mission, vision and strategic objectives outlined within the DHSC Cyber Security Strategy, C&M ICS five-year Strategy, the three-year Digital and Data Strategy, as well as considering key NHS frameworks and requirements, such as those outlined within the **'What Good Looks Like' framework**, we have developed this **five-year C&M ICS Cyber Security Strategy**.

We have designed this Cyber Security Strategy to enable us to **continue to develop and maintain a secure health and care system** across C&M. We can achieve this by **levelling up our digital tools and services** and **ensuring they are cyber secure and resilient**.

The following **mission, vision** and **strategic objectives** sit at the heart of the Strategy and form a solid foundation for levelling up our organisational cyber position:

Cyber Security Mission

To level up organisational cyber security across C&M ICS we will:

- Establish a **shared governance model** built on **smart foundations**
- Champion **safe and secure practices**
- Encourage **collaboration** within a **supportive cyber security culture**.

Cyber Security Vision

We want to become **cyber leaders amongst our peers** by contributing to developing and maintaining a **secure health and care system** across C&M. We will achieve this by **protecting our organisations**, as well as **information systems and critical assets** that support **our essential functions** from cyber threats, ensuring the safety of our staff and patients.

Cyber Security Strategic Objectives



At the core of this Cyber Security Strategy there are **nine strategic objectives** with corresponding **activities** to achieve them, to be delivered across a five-year timeline that we will use to deliver on this mission. These objectives, which are designed to guide the C&M ICS in uplifting our cyber security maturity, are detailed across pages 21-57. Each objective has been assigned one of four **priority levels for implementation** (immediate-term, short-term, medium-term or long-term). Working through these activities will enable us to level up organisational cyber security resilience throughout C&M ICS, thereby cementing our position as cyber leaders across the ICS landscape.

05 Putting the Strategy Together

CYBER SECURITY STRATEGY DEVELOPMENT

What have we considered?

There were several **considerations and key drivers** that influenced the development of the C&M ICS Cyber Security Strategy. We wanted to ensure that the Strategy **builds upon existing foundations** to **tackle the challenges similar organisations face**, and **take advantage of opportunities** open to us:

EXISTING FOUNDATIONS



Established Cyber Programme

Two Cyber Groups currently drive the cyber programme across the C&M ICS:

1. Wider 'Cyber Group' open to all cyber leads from C&M ICS organisations.
2. 'Cyber Leadership Group' comprising of a CIO and cyber leads from several ICS partner organisations.



Existing Collaboration Model

Members from several ICS partner organisations come together to collaborate on cyber security matters, as well as share knowledge and experience, as part of the 'collaboration of the willing'.

CHALLENGES



People, Process and Technology Challenges

As with other health care industry organisations, C&M ICS faces a number of challenges. Some of these challenges include cyber governance, attraction and retention of suitably qualified resources, efficient procurement and effective incident management.



Resource Constraints

The funding streams available to ICSs are still in the process of being finalised, against a backdrop of a broader funding squeeze across the NHS. This is expected to limit the financial resources available for investment in improving cyber maturity.

OPPORTUNITIES



Economies of Scale

The C&M ICS aims to build robust cyber resilience by managing cyber security investments and limited resources at the ICS level. This should enable us to properly leverage the economic benefits that come from our regional size and scale.



Working with NHS England


NHS England supports its organisations across the NHS with comprehensive cyber tools and services, including advice, assessments, and training. It's critical that we use them to avoid duplication and missed opportunities across ICS partner organisations.

CYBER SECURITY STRATEGY DEVELOPMENT

How have we put the Strategy together?

Keeping in mind the foundations we have built, our challenges and opportunities, existing ICS cyber security-related documentation and an understanding of **our current cyber security state** served as the starting point for this Cyber Security Strategy. External drivers, such as the **DHSC and other ICS security and digital strategies, key NHS and cyber security frameworks** guided development of the Strategy to ensure our alignment with their requirements and **industry good practice**. Lastly, we have worked with **primary stakeholders across the C&M ICS** to identify fundamental strategic objectives we would like to **achieve over the next five years** and ensure that the Strategy **meets the security needs of ICS partner organisations**.


Existing Documentation



C&M ICS existing documentation served as foundational understanding of the current ICS state from both an overall strategic and a cyber current state perspective.


This included previous HCP cyber strategy, existing cyber policies and plans, such as Incident Response Plan and governance committees' Terms of Reference.

Other Strategies



Key strategies, such as the DHSC Cyber Strategy, the ICS overarching Strategy, the ICS Digital and Data Strategy, and all their underlying visions and objectives, set the direction for our Cyber Security Strategy and its structure, as well as helped to identify and align our strategic objectives.


Stakeholder Workshops



We invited key stakeholders across the C&M ICS and NHS Digital to a series of workshops to discuss the ICS's cyber security current state, prioritise what we would like to achieve over the next five years in uplifting our cyber security position, and identify key ways we would be able to achieve the desired state.

These activities ranged from technical elements such as third party risk management to people-driven initiatives, including celebrating individual staff contributions towards organisational cyber security culture.

Frameworks and Good Practice



The success measures detailed within the NHS 'What Good Looks Like' framework were incorporated in our Strategy alongside the National Data Guardian's Data Security Standards, detailed in the Data Security and Protection Toolkit (DSPT).

Our knowledge of the cyber security good practice, such as the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) and Security of Networks & Information Systems (NIS) CAF, was similarly foundational in defining key activities that would help us achieve our strategic objectives.

06 Objectives and Key Activities

STRATEGIC OBJECTIVES

How will we meet our ICS Cyber Security Strategy mission and vision? **Cheshire and Merseyside**

To achieve the **ICS cyber security mission and vision**, we have defined **nine cyber security objectives** to guide our efforts to uplift our cyber security state. As outlined on page 19, these objectives were identified through discussions with key stakeholders, documentation review and consideration of industry good practice, while considering the goals and guiding principles of wider relevant strategies. They are:

1	Cyber Governance	The C&M ICS leads, drives, and oversees cyber security activities across all ICS partner organisations, underpinned by a clear governance and efficient reporting structures.
2	Cyber Risk Management	The C&M ICS and its partner organisations utilise a shared language when it comes to cyber risk, applying a unified approach to managing and mitigating cyber risk to its shared critical systems and services wherever possible.
3	Cyber Incident Management	The C&M ICS collaboratively and consistently identifies, responds to, and recovers from cyber security incidents, minimising their impact on critical services, utilising the standardised incident management approaches and ICS-wide SOC capability.
4	Cyber Procurement	The C&M ICS maximises its use of nationally provisioned tools and services to eliminate procurement duplication and takes advantage of economies of scale, while effectively managing third-party suppliers.
5	Third-Party Risk Management	The C&M ICS uses a risk-based third-party risk management framework to effectively manage cyber security risk associated with third-party tools and services, while effectively selecting, contracting, monitoring and off-boarding external service providers.
6	People and Culture	The C&M ICS has a strong cyber security culture, backed by a robust training and awareness programme that communicates and embeds staff's security responsibilities, and allows the ICS to constantly upskill staff on cyber security.
7	Knowledge Sharing and Good Practice	The C&M ICS has a robust cyber security knowledge-sharing culture where all personnel use tools to efficiently exchange and discuss industry good practices, information, and recent cyber activities.
8	Cyber Security Policies and Processes	The C&M ICS manages cyber security across all ICS partner organisations by standardising and improving cyber security policies and processes, as well as identifying and correcting policy non-compliance.
9	Cyber Baseline and Minimum Standards	The C&M ICS supports its partner organisations in upholding robust cyber security and improving cyber resilience by developing and supporting the roll out of minimum cyber security standards across the ecosystem.



STRATEGIC OBJECTIVES

How are our strategic objectives structured?

For each of the **nine objectives** within our Strategy, we have identified our current state in each of the areas, and discussed with our key stakeholders where we want to give to. To help us get there, each of the objectives is underpinned by a **set of actionable activities** to be delivered over the **next five years**, by the **ICS Regional Security Operations Centre (R-SOC) and Cyber Centre of Excellence (CCoE)**, led by the **Cyber Management Board** (as outlined on pages 60-62).

For each of the underlying activities, we have defined an **accountable lead group** that would commission and oversee each task, delegating it as appropriate, to the R-SOC, CCoE, or individual partner organisations.

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
-----------	----	------------	------------------	-----------------------------	-----------------------------------

We have also assigned each activity a **priority for implementation**. This would assist us with sequencing of activities over the five year timeline and help us achieve easy wins first.

We envision that any activity with **'immediate'** priority, we would look to implement within the first six months; **'short-term'** within the second half of the first year; **'medium term'** within year two and three; and **'long term'** within year four and five.

However, to bring these activities to life, we require **dedicated ICS resources** as part of the ICS Cyber Management Board, the **ICS R-SOC** and the **ICS CCoE**, and consequently, these timelines would be dependent on the level of resourcing available.

Where an activity may have a **dependency** on another, we have added the relevant references as well, to help us with sequencing of activities.



STRATEGIC OBJECTIVES

1. Cyber Governance

A clear ICS cyber governance structure that defines accountabilities for cyber security and establishes well-defined lines of responsibility provides the necessary foundation and oversight for effective cyber risk management.

Where are we now?

The C&M ICS has established a strategic and an operational cyber security group in a form of 'Cyber Steering Group' and the 'Cyber Group'. Furthermore, each ICS partner organisation has developed its own approaches to regularly report to their respective boards on cyber security matters and cyber risk. However:

- Membership of ICS Cyber Group and the Cyber Steering Group currently relies on a 'collaboration of willing'. As such, there is no clear governance arrangements and underpinning processes in place to ensure coordination and collaboration between ICS partner organisations to manage cyber security effectively and minimise cyber risk exposure.
- The ICS has no formal process to oversee each ICS partner organisation's cyber investments, nor formal discussion on estimating expenses of cyber security measures and loss associated with cyber incidents to support the decision-making of budgeting at board level.



Where do we want to get to?

The ICS sets the tone from the top and cultivates **strong capabilities to lead, drive, and oversee** cyber security activities across ICS partner organisations.

Importantly, oversight of **cyber security programme** across the ICS is underpinned by a well-defined governance structure, **clear accountability and efficient reporting processes** that apply across all ICS partner organisations.

How do we get there?

▶ **Key activities to assist the C&M ICS with resolving the existing gaps and reach the desired state:**



Agree, maintain, and implement a Cyber Security Strategy across the ICS.



Agree a new ICS cyber governance structure and develop an ICS cyber target operating model.



Establish a reporting mechanism to communicate effectively with executive management on cyber security.



STRATEGIC OBJECTIVES

1. Cyber Governance Activities (1/3)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Cyber Governance**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
Cyber Governance	1a	Share, review and agree the ICS Cyber Security Strategy with the ICS leadership and the ICB, securing the necessary buy-in. As part of this, agree on the proposed ICS cyber governance approach, amending as required. This may include a review what services and capabilities the ICS should centrally provide to ICS partner organisations to maintain robust cyber security across the board, and what dedicated ICS resources may be required to achieve this.	ICS Cyber Management Board	Immediate	
	1b	Implement the agreed governance arrangements between the ICS, the ICB and the ICS partner organisations, communicating roles and responsibilities with relevant groups and individuals, including the ICS Data Protection Officer (DPO), Senior Information Risk Officer (SIRO) and Clinical Safety Officer (CSO).	ICS Cyber Management Board	Short-Term	<u>1a</u>
	1c	Review, update, or where necessary develop, the Terms of Reference for the key ICS governance groups to set clear responsibilities and accountabilities of the ICS cyber function. The responsibilities should cover the requirements of the 'What Good Looks Like' framework, including a responsibility to regularly review all ICS partner organisations' local digital strategies, cyber security plans and programmes.	ICS Cyber Management Board	Short-Term	
	1d	Develop a target operating model defining the capabilities, skills and resources required for an effective ICS cyber function per the agreed governance structure. The model shall consider the collaboration with other departments (e.g., legal, finance, HR) on cyber security matters.	ICS Cyber Management Board	Medium-Term	<u>1a, 1b</u>

STRATEGIC OBJECTIVES

1. Cyber Governance Activities (2/3)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Cyber Governance**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
Cyber Governance	1e	Share the ICS Cyber Security Strategy for input with key clinical representatives across the ICS, making changes to strategic objectives and actions where required based on clinical representatives' feedback.	ICS Cyber Management Board	Short-Term	<u>1a</u>
	1f	Review and agree the implementation timelines, as well as owners of strategic objectives activities (including identification of a named individual, where appropriate) outlined within this Cyber Security Strategy.	ICS Cyber Management Board	Short-Term	<u>1a</u>
	1g	Implement this Cyber Security Strategy, setting direction for ICS partner organisations regarding cyber security and track progress against key objectives.	ICS Cyber Management Board	Medium-Term	<u>1a</u>
	1h	Establish a mechanism review the Strategy on a regular basis to ensure it is still aligned with the C&M ICS and its partner organisations' requirements, as well as with any new requirements from NHS England.	ICS Cyber Management Board	Long-Term	
	1i	Document and publish a set of cyber security requirements for the ICS partner organisations to comply with based on the objectives outlined within this Cyber Security Strategy, communicating the value of an organised approach to cyber security management. As part of this: <ul style="list-style-type: none"> Identify accountable roles for meeting the cyber security requirements within the ICS partner organisations. Define escalation paths and consequences for not complying with the set requirements. Define a system (responsibilities, expertise, investment) for providing support to ICS partner organisations to build and enhance local cyber security arrangements, where appropriate. 	ICS Cyber Management Board	Long-Term	<u>1g</u>

STRATEGIC OBJECTIVES

1. Cyber Governance Activities (3/3)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Cyber Governance**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
Cyber Governance	1j	Develop an approach to, and perform an assessment of the cyber security capabilities at each ICS partner organisation, including but not limited to risk management, vulnerability management and data security.	ICS Cyber Management Board	Long-Term	<u>1i</u>
	1k	Identify and manage investments into cyber security at the ICS-level, including for cyber security resources and investments in modern infrastructure to retire old, unsupported systems, while defining responsibilities for budget management.	ICS Cyber Management Board	Long-Term	
	1l	Develop a report template (including a set of cyber security metrics, e.g., risk metrics) to be populated and shared with ICS executive management boards on the overall status of the cyber across the ICS on a regular basis, e.g., quarterly.	ICS Cyber Management Board	Long-Term	<u>1j</u>
	1m	Establish a mechanism to collate relevant data and populate the cyber report to be shared with ICS executive management boards on a regular basis.	ICS Cyber Management Board	Long-Term	<u>1l</u>

STRATEGIC OBJECTIVES

2. Cyber Risk Management

Cyber security can have a significant impact on clinical care of patients. To ensure the most critical cyber security threats and risks facing the ICS are managed in a timely manner, a centralised view of the biggest cyber security risks is crucial, so that they can be managed in the most efficient and effective way.

Where are we now?

We understand that each ICS partner organisation has an approach to identifying, recording and reporting cyber security risk. However:

- There is no one common risk assessment approach or tracking tool used by ICS partner organisations to record and track cyber security risks in a consistent manner. Organisations use several tools to record risks, such as Datix and Ulysses.
- As different ICS partner organisations have a different approach to cyber risk identification, assessment and management, there is no consistent risk language used across the ICS.
- There is currently no central view of the biggest risks facing the ICS as a whole, and no agreed ICS cyber risk appetite.
- At the moment, there is no accurate and complete view of the ICS operating environment (including IT assets) and attack surface (including external connections).



Where do we want to get to?

The ICS and its partner organisations have a **common understanding of cyber security risks** facing the ICS and are able to obtain a **single view** of the biggest cyber risk facing its **essential systems and services**.

The ICS supports its partner organisations by **investing** into the necessary tools and processes to **mitigate and manage the biggest risks**.

How do we get there?

Key activities to assist the C&M ICS with resolving the existing gaps and reach the desired state:



Establish a central ICS-level cyber risk coordination function and select a risk assessment methodology.



Develop ICS-wide guidance and templates for identifying and managing cyber risk consistently.



Create an ICS-level centralised cyber risk repository and establish a mechanism to enable accurate risk reporting.

STRATEGIC OBJECTIVES

2. Cyber Risk Management Activities (1/4)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Cyber Risk Management**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
Cyber Risk Management	2a	Establish a central ICS-level cyber risk coordination function, identifying key roles required to coordinate identification of the highest cyber risks facing the ICS and where necessary, organise appropriate ICS-wide mitigating actions to manage the biggest cyber risks facing the ICS effectively and efficiently.	ICS Cyber Management Board	Short-Term	1b
	2b	Assess whether it would be necessary for the ICS to define, agree and communicate a cyber risk appetite.	ICS Cyber Management Board	Short-Term	
	2c	Select a cyber security risk identification and assessment methodology (e.g., CRAMM, IRAM2) that would meet requirements of an established framework (e.g., ISO 27001) that could be used by ICS partner organisations to identify, score and collate cyber risks in a consistent manner. The methodology should aim to be flexible enough to meet the needs of the ICS partner organisations, while allowing the ICS to use a consistent language and obtain a consolidated view of cyber risk.	ICS Cyber Management Board	Short-Term	
	2d	Share the cyber security risk identification and assessment methodology with the ICS partner organisations.	ICS Cyber Management Board	Short-Term	2c
	2e	Develop and deliver the necessary training on the chosen risk identification and assessment framework for all individuals involved in cyber risk management across the ICS to ensure consistency in implementation of the framework.	ICS Cyber Management Board	Medium-Term	2c , 2d

STRATEGIC OBJECTIVES

2. Cyber Risk Management Activities (2/4)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Cyber Risk Management**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
Cyber Risk Management	2f	<p>Develop and share with each ICS partner organisation the necessary templates and guidance for cyber risk identification and assessment in line with the chosen methodology and framework for the ICS partner organisations to implement as required. This could include:</p> <ul style="list-style-type: none"> Guidance for identifying cyber security risks facing each ICS partner organisation, utilising information including, but not limited to: <ul style="list-style-type: none"> Threat intelligence from wider NHS sources (such as NHS England); Information from the ICS Secure Operations Centre (SOC) and other tools available to each organisation for identification and management of vulnerabilities and incidents; Results of Business Impact Assessments (BIAs) and asset prioritisation activities; and Outputs from third party risk assessments. Guidance for scoring cyber security risks (including a risk scoring matrix and accompanying definitions of ratings). Cyber security risk response strategies. This may include defining an approach to: <ul style="list-style-type: none"> Identifying and implementing security controls to mitigate identified cyber security risks. Wherever possible, it should ensure that assets and services are 'secure by design'. Accepting risks (including templates to log and guidance for approving risk acceptance). Transferring risks. Guidance for review of identified cyber security risks, their ratings and risk owners on a regular basis, including following major changes and incidents. 	ICS Cyber Management Board	Medium-Term	<u>2c, 2g</u>

STRATEGIC OBJECTIVES

2. Cyber Risk Management Activities (3/4)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Cyber Risk Management**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
Cyber Risk Management	2g	<p>Develop and provide each ICS partner organisation with guidance to identify, assess and prioritise IT assets in a standardised manner. This may include:</p> <ul style="list-style-type: none"> • A framework for prioritising IT assets for cyber security protection based on their data classification, criticality and business value, linking this to the BIAs. • Guidance for documenting, regularly reviewing and maintain the IT asset inventories to identify new, relocated, re-purposed and outdated IT assets. • A processes to detect and manage shadow IT. • A process to proactively identify and manage systems when they approach their end-of-life phase (e.g., unsupported or outdated software). 	ICS Cyber Management Board	Short-Term	
	2h	<p>Centrally collate and identify assets and services that are shared across the ICS, mapping out the ecosystem, identifying interdependencies. This should include the nationally provisioned NHS tools and systems, as well as services provided by individual ICS partner organisations to others. As part of this, identify the services and assets that are of highest criticality and importance to the ICS as a whole, using a standardised ICS approach.</p>	ICS Cyber Management Board	Medium-Term	<u>2g</u>
	2i	<p>Create an ICS-level centralised cyber risk repository to be able to identify and track cyber risks that come up across multiple organisations to enable the ICS to obtain a complete picture of cyber risk and align on cyber risk mitigation.</p>	ICS Cyber Management Board	Long-Term	<u>2c, 2d, 2e</u>

STRATEGIC OBJECTIVES

2. Cyber Risk Management Activities (4/4)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Cyber Risk Management**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
Cyber Risk Management	2j	Use the ICS-level centralised cyber risk register to identify any common gaps across the ICS in current security controls (preventative, detective, and corrective). Identify, where possible, mitigating controls (tools, services or processes etc.) that can be centralised and rolled out across the ICS to close the identified gaps and support mitigation of common risks.	ICS Cyber Management Board	Long-Term	
	2k	Determine and agree risk metrics and indicators to be consistently reported by the ICS partner organisations to the ICS across the ICS to track cyber risk. This may include number of cyber security risks outside the agreed risk appetite.	ICS Cyber Management Board	Long-Term	<u>2c</u> , <u>2d</u> , <u>2i</u> , <u>2f</u>
	2l	Establish a mechanism to collate required information in a timely manner to enable accurate cyber risk reporting.	ICS Cyber Management Board	Long-Term	<u>2k</u>
	2m	To assist with meaningful cyber risk reporting to executive management boards, develop guidance and examples for reporting cyber risk posture, such as by using storytelling methods to communicate cyber risk, its likelihood and possible impact that relates to patient experience and safety.	ICS Cyber Management Board	Long-Term	<u>2k</u> , <u>2l</u>

STRATEGIC OBJECTIVES

3. Cyber Incident Management

Effective cyber incident management and response that is grounded in cyber security risk management can help organisations effectively respond to and recover from cyber attacks, minimising the adverse impact of cyber events on essential functions.

Where are we now?

The C&M ICS has drafted an incident management plan and runs incident management desktop exercises. Moreover, most ICS partner organisations have their patch and remediation activities tracked and recorded in in IT Health Assurance Dashboard after scanning for vulnerabilities and monitoring system configuration. However:

- There is currently no 24/7 coverage for incident response, particularly where ICS partner organisations consume shared services, and there are improvements to be made within the rate at which critical information about incidents is shared across the ICS partner organisations.
- There is a lack of standardisation in Disaster Recovery, Business Continuity and Incident Management Plans across the ICS.
- There is currently no centralised tool, such as a Security Information and Event Management tool (SIEM) or a SOC, to monitor the cyber security state and detect cyber incidents across the ICS.



Where do we want to get to?

The C&M ICS **identifies, responds and recovers** effectively from cyber security incidents, **minimising their impact** on the delivery of essential services, **utilising a regional SOC capability**. The ICS has a **standardised approach** to Incident Management, Disaster Recovery and Business Continuity Planning, facilitating **collaboration between ICS partner organisations** to effectively manage incidents and disaster events.

How do we get there?

➔ **Key activities to assist the C&M ICS with resolving the existing gaps and reaching the desired state:**



Develop ICS-wide Disaster Recovery, Business Continuity, Incident Management policies, processes, plans and templates.



Establish an ICS-wide SOC and centralised ICS monitoring systems.



Establish a mechanism for testing cyber incident management plans engaging a variety of stakeholders.

STRATEGIC OBJECTIVES

3. Cyber Incident Management (1/4)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Cyber Incident Management**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
Cyber Incident Management	3a	<p>Establish an ICS-level incident management policy that would outline the ICS's approach to cyber incident management. The policy should consider how the ICS partner organisations should work together to identify and respond to incidents that may impact more than one ICS partner organisation. The policy should also:</p> <ul style="list-style-type: none"> Define and document clear accountabilities and responsibilities (including decision making) for cyber incident management within the ICS, as well as outline clear lines of command and escalation paths to ensure timely and appropriate communication and decision making. In addition, define an approach to working with other relevant departments, such as Legal and Information Governance. Define the approach for cyber incident management, that links to wider Emergency Preparedness, Resilience and Response (EPRR) planning. This should include identification and analysis (including a standardised incident severity and impact rating scale), coordination, escalation and communication (including external, such as law enforcement, providers and suppliers), digital forensics, mitigation, and recovery. 	ICS Cyber Management Board	Immediate	
	3b	<p>Develop ICS-level response and recovery documents, plans and playbooks that provide well-defined, organised, cross-community approaches for cyber incident response activities, including criteria for activating the measures and actions to be taken during the most critical period (i.e., initial hours and days of a cyber incident).</p>	ICS Cyber Management Board	Immediate	<u>3a</u>



STRATEGIC OBJECTIVES

3. Cyber Incident Management (2/4)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Cyber Incident Management**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
Cyber Incident Management	3c	<p>The ICS should additionally develop and share cyber incident management and response guidance and documentation templates for ICS partner organisations to use where appropriate. This should include:</p> <ul style="list-style-type: none"> • Templates for local business continuity policy, disaster recovery procedure and incident response plans. • Guidance on data backup and restoration programmes to recover assets that support critical operations in accordance with recovery objective(s) (e.g., Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)) following a cyber incident. 	ICS Cyber Management Board	Medium-Term	<u>3a</u> , <u>3b</u> , <u>7b</u>
	3d	Agree and select a communications mechanism to use across the C&M ICS partner organisations in an event of an incident to coordinate responses, where necessary.	ICS Cyber Management Board	Immediate	
	3e	Request and collate a list of incident management and incident response individuals, their responsibilities (per requirements of the ICS-wide cyber incident management policy) and contact information within the ICS partner organisations across C&M. This will enable swift, 24/7 communications and response across the ICS in an event of a wide-spread incident.	ICS Cyber Management Board	Immediate	<u>3a</u>
	3f	Assess whether the current individuals with assigned responsibilities for cyber incident response have the necessary knowledge and tools to perform their assigned tasks. As part of the exercise, identify whether there is a requirement to obtain a cyber incident response retainer with an external third party to perform incident response activities.	ICS Cyber Management Board	Medium-Term	<u>3e</u>

STRATEGIC OBJECTIVES

3. Cyber Incident Management (3/4)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Cyber Incident Management**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
Cyber Incident Management	3g	Establish an ICS-wide, R-SOC with cyber-surveillance and incident response capability, or an other equivalent service, to centralise and coordinate security processes and technologies. As part of this, establish an ICS-wide process for reviewing and responding to relevant safety recommendations and alerts from NHS England, the Medicines and Healthcare products Regulatory Agency (MHRA) and the Healthcare Service Investigation Branch (HSIB).*	ICS Cyber Management Board	Long-Term	
	3h	Establish centralised ICS monitoring systems that would enable the ICS to monitor for abnormal or malicious activity within the ICS systems and networks to proactively identify potential cyber security incidents. The monitoring solutions should be backed by sufficient resources, with clearly defined roles and responsibilities.*	ICS Cyber Management Board	Long-Term	
	3i	Develop and conduct regular training on the cyber incident management and response, as well as business continuity and disaster recovery arrangements. This should include: <ul style="list-style-type: none"> Tailored training to crisis and incident response teams on the steps to take in an event of an incident per the developed policies, plans and playbooks. Cyber threat simulations and business continuity exercises for executive management board members, IT personnel, front line and other relevant departments across all ICS partner organisations to educate on common cyber threat scenarios, ways to appropriately identify and respond to cyber incidents and events, and the impact they may have on the ICS and patient care. 	ICS Cyber Management Board	Medium-Term	<u>3a, 3b</u>

* Would require investment into technical solutions to deliver.

STRATEGIC OBJECTIVES

3. Cyber Incident Management (4/4)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Cyber Incident Management**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
Cyber Incident Management	3j	<p>Develop ICS-level improvement processes and mechanisms to identify opportunities to improve response and recovery capabilities, and update incident management policies, processes, plans and templates, from past cyber incidents, simulations and table-top exercises. This could include:</p> <ul style="list-style-type: none"> Lessons learned from ongoing incident handling activities, past cyber incidents, and from incident replated training, and simulation/table-top exercises. A mechanism to regularly review the assigned roles and responsibilities for cyber incident response to ensure all key cyber incident response roles remain filled by skilled individuals. 	ICS Cyber Management Board	Medium-Term	<u>3a,3b,3c,3d, 3f, 3g, 3h, 3i</u>

STRATEGIC OBJECTIVES

4. Cyber Procurement

Established processes for procuring tools and services that place cyber security at its core can not only help manage cyber security risk but similarly improve efficiency of services the C&M ICS can deliver while minimising costs.

Where are we now?

In some partner organisations across the C&M ICS, IT and cyber security teams have developed close relationships with procurement teams to acquire cyber security software and services. However:

- There is currently no single view of all cyber tools and services suppliers and third parties working with the ICS and ICS partner organisations.
- There are inconsistencies within the supplier screening and onboarding process across the ICS partner organisations.
- Procurement is conducted by ICS partner organisations in isolation. This often leads to duplication of tools and software purchased (e.g. Nessus, IT Health Dashboard), leading to greater costs where valuable funds could have been allocated elsewhere (e.g. towards improving patient care).



Where do we want to get to?

The ICS has a **complete view of all its cyber tools and services suppliers**, and is able to **manage them in a consistent manner** that enables the ICS to effectively **examine and manage associated risks**.

The ICS **leverages the nationally provisioned tools and services** wherever possible and is able to capitalise on the **economies of scale** and extract value from minimising duplication in procurement.

How do we get there?

Key activities to assist the C&M ICS with resolving the existing gaps and reach the desired state:



Develop a centralised cyber vendors and suppliers register into the ICS.



Develop an ICS-wide framework and guidance for procurement of new cyber and tools.



Define an approach to consistently implement and use NHS-provided national systems.



STRATEGIC OBJECTIVES

4. Cyber Procurement (1/2)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Cyber Procurement**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
IT Procurement	4a	Request ICS partner organisations identify and share a list of all current suppliers and third parties they are working with that provide cyber services and tools. This should also include NHS-provisioned tools, systems and services.	ICS Cyber Management Board	Immediate	
	4b	Develop a centralised register of all cyber suppliers into the ICS, using the information collected from individual ICS partner organisations. The register should include: who the suppliers are, what services and tools they provide, and how long the existing contracts are for. This may be achieved by leveraging NHS England's RiskLedger platform once it goes live.*	ICS Cyber Management Board	Short-Term	4a
	4c	Identify an individual within the ICS that will own and maintain the centralised register of cyber suppliers into the ICS if necessary. Grant access to key contacts within the individual ICS partner organisations to the centralised register and request ICS partner organisations to log new supplier relationships within the register.	ICS Cyber Management Board	Short-Term	4b
	4d	Investigate whether sharing information about supplier pricing across the ICS is permissible to provide cost transparency to partner organisations (subject to any contractual confidentiality prohibitions). Where possible, include the information within the central supplier register.	ICS Cyber Management Board	Short-Term	
	4e	Using the centralised supplier register, identify common cyber suppliers that are used by multiple ICS partner organisations. Where appropriate, upon existing contracts expiry, work to set up ICS-wide contractual agreements with those third parties and vendors to benefit from economies of scale. Where centralised contracts are created, identify a key contact within the ICS to act as the relationship and contract owner with each supplier, as well as to assist ICS partner organisations with joining in on the central agreement.	ICS Cyber Management Board	Medium-Term	4b

STRATEGIC OBJECTIVES

4. Cyber Procurement (2/2)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Cyber Procurement**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
IT Procurement	4f	Develop an ICS-wide framework and guidance for procurement of new cyber services and tools. This framework should mandate, where appropriate, that ICS partner organisations consult the centralised supplier register when selecting suppliers to encourage consistency in tools used across the ICS and benefit from economies of scale. The framework should outline the steps to be taken and approvals required where none of the listed suppliers meet the requirements of the ICS partner organisation.	ICS Cyber Management Board	Medium-Term	
	4g	Define an approach to consistently implement and use NHS-provided national systems, tools and services across the ICS partner organisations (e.g. NHS login and NHS app, other digital communication and self-service tools, as well as systems that would enable development of an ICS-wide shared care record). As part of this approach: <ul style="list-style-type: none"> • Use the list of all national tools, systems and services in use across the ICS provided by the ICS partner organisations to identify gaps in usage. • Provide support to those ICS partner organisations currently not using the NHS-wide tools, systems and services to implement them. 	ICS Cyber Management Board	Long-Term	

STRATEGIC OBJECTIVES

5. Third-Party Risk Management (TPRM)

Working with third parties can introduce vulnerabilities and cyber security risks into the ICS ecosystem. As such, a standardised third-party risk management approach to assessing and managing third party goods and services is crucial.

Where are we now?

All ICS partner organisations must use and comply with the DSPT, which details a number of assertions for managing third-party risk. Additionally, the Information Governance teams complete Data Protection Impact Assessments (DPIAs) for new systems. However:

- Where DPIAs are completed, they are completed after the tender stage, and there is limited involvement from cyber security teams.
- There is currently no standardised set of clauses and penalties to be included within supplier contracts to address cyber security and non-compliance with agreed arrangements.
- There is limited due diligence over third-party service providers and their subcontractors' cyber security capability, security controls and infrastructure resiliency.
- There is currently no standardised approach for ongoing monitoring of third-party risk, performance, and issues experienced across the ICS.



Where do we want to get to?

The ICS utilises a **comprehensive, risk-based TPRM framework** across all ICS partner organisations that **provides transparency and visibility** into third-party relationships and associated risks.

Each ICS partner organisation is equipped with **sufficient tools and capabilities to mitigate third-party risk** while identifying, selecting, contracting with, monitoring and delivering timely off-boarding of external service providers.

How do we get there?

Key activities to assist the C&M ICS with resolving the existing gaps and reach the desired state:



Develop a TPRM framework to be used across all ICS partner organisations.



Develop a template of security clauses for contractual agreements with all suppliers into the ICS.



Develop a platform to share information about supplier performance and issues experienced across the ICS.



Develop TPRM reporting metrics to obtain a full view of risk posed by third parties.



STRATEGIC OBJECTIVES

5. Third-Party Risk Management (TPRM) (1/3)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Third-Party Risk Management**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
Third-Party Risk Management	5a	<p>Develop and roll out across the ICS a TPRM framework that would mandate third parties working with the ICS to meet the requirements of an established standard (e.g., ISO 27001). The framework should detail guidance that would enable all ICS partner organisations to:</p> <ul style="list-style-type: none"> Assess the risks associated with working with each third party provider and consuming their tools and services, identifying 'high', 'medium' and 'low' risk suppliers; Manage the risks associated with the third party tools and services dependent on the assigned risk rating. This should ensure that any standard the providers are required to meet is appropriate to the needs of the procuring ICS partner organisation(s). Gain assurance that third parties uphold their contractual obligations and security arrangements to minimise risk to critical infrastructure and data. This may include regular assurance reviews, depending on the assigned risk rating (e.g., a self assessment regime for those classed as 'low' risk, or annual security controls review for 'high' risk third parties). 	ICS Cyber Management Board	Short-Term	
	5b	<p>Develop the standard template(s) of security clauses, including penalty clauses for non-compliance, to be included within contractual agreements with suppliers into the ICS. The standard security clauses may cover a number of cyber security arrangements, including but not limited to, staff screening and clearance requirements, vulnerability management, as well as incident response approaches, in a way that covers how a supplier should work with the relevant ICS partner organisations and other relevant bodies, such as NHS England.</p>	ICS Cyber Management Board	Short-Term	
	5c	<p>Share the security clauses template(s) with ICS partner organisations and mandate their inclusion within each new contract, per the third-party risk management framework.</p>	ICS Cyber Management Board	Medium-Term	<u>5b</u>

STRATEGIC OBJECTIVES

5. Third-Party Risk Management (TPRM) (2/3)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Third-Party Risk Management**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
Third-Party Risk Management	5d	Develop a platform for ICS partner organisations to share information about supplier performance and issues experienced across the ICS, so organisations can factor any issues into their approach to supplier management (as discussed in workshops as a 'TripAdvisor' solution for ICS suppliers). This may be achieved by leveraging NHS England's RiskLedger platform once it goes live, or the supplier register developed as part of activity 4b.*	ICS Cyber Management Board	Long-Term	<u>4b</u> , <u>7b</u>
	5e	Investigate whether sharing of third-party audit reports and other forms of third-party assurance (e.g., SOC2 reports) received across the ICS is possible. Where possible, establish a mechanism to share this intelligence across the ICS (e.g., through the solution developed as part of activity 5d).	ICS partner organisations	Long-Term	<u>5d</u> , <u>7b</u>
	5f	Develop a mechanism for feeding the supplier risk assessment results into the wider cyber risk management approach and cyber risk registers, both ICS-wide and within individual ICS partner organisations per the Risk Management actions.	ICS Cyber Management Board	Long-Term	<u>2c</u> , <u>2f</u> , <u>2g</u>

* May require investment into technical solutions to deliver.

STRATEGIC OBJECTIVES

5. Third-Party Risk Management (TPRM) (3/3)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Third-Party Risk Management**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
Third-Party Risk Management	5g	Develop third party risk management reporting metrics to obtain a full view of risk posed by third parties. This could include number of high risk-rated suppliers into the ICS, number of legacy contracts without standard security clauses, etc. These metrics should be reported and discussed on a regular basis during the Cyber Steering Group and mitigating measures identified to uplift the third-party risk position across the ICS.	ICS Cyber Management Board	Long-Term	<u>5a</u>
	5h	If deemed necessary, develop and share across the ICS partner organisations guidance for executive management board reporting on third party risk management metrics.	ICS Cyber Management Board	Long-Term	<u>5g</u>

STRATEGIC OBJECTIVES

6. People and Culture

People and culture sit at the heart of every organisation. By ensuring that staff are appropriately trained, aware and actively contributing towards cyber security culture, cyber security incidents, such as phishing attacks can be minimised.

Where are we now?

Every staff member across the ICS is required to complete annual training, as mandated by DSPT. Some ICS partner organisations take part in the Cyber Savvy awareness campaign and have Cyber Digital Champions (Bright Sparks) to uplift cyber security culture. However:

- Cyber security is not currently part of the onboarding training within all ICS partner organisations and there is no comprehensive staff cyber training programme across the ICS, and so cyber security training is performed by each individual organisation in isolation.
- IT staff who upskill by undertaking cyber security training, accreditations and certifications paid for by ICS partner organisations are not financially incentivised to stay, leading to retention challenges.
- Currently, the impact of training is not tracked, preventing the identification of improvements in user awareness and additional training needs are not monitored following initial training.



Where do we want to get to?

The ICS has a **strong cyber security culture**, supported by a comprehensive staff **training and awareness programme** that embeds the responsibilities for keeping the ICS **secure** amongst all staff, and enables the ICS to **consistently identify gaps** in cyber knowledge and **upskill staff** as required.

How do we get there?

➤ **Key activities to assist the C&M ICS with resolving the existing gaps and reach the desired state:**



Publicise a list of free cyber training resources and opportunities across the ICS.



Assess the existing cyber security skills across the ICS, hiring or upskilling staff to close the gaps.



Establish an ICS-wide cyber training baseline standard and a system to continuously monitor staff training needs.



STRATEGIC OBJECTIVES

6. People and Culture (1/3)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **People and Culture**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
People and Culture	6a	Identify and collate a list of the current cyber security roles/positions across the ICS, identifying gaps that may exist. As part of this, identify what skills and knowledge are required to effectively fulfil these roles.	ICS Cyber Management Board	Medium-Term	
	6b	Conduct an assessment of skills, competencies and essential cyber qualifications currently possessed by ICS cyber security practitioners. Compare those against the roles, and their skills and knowledge requirements, identified under activity 6a, identifying gaps.	ICS Cyber Management Board	Medium-Term	<u>6a</u>
	6c	Identify and allocate central training funding to upskill staff with cyber security responsibilities (e.g., developers) across the C&M ICS in line with the skills and competencies required to fulfil those roles. The funding should also cover periodically renewing the required qualifications for performing the necessary cyber security responsibilities Identify where external recruitment may be necessary to close the gaps in skills, competencies and knowledge to perform key cyber security roles across the ICS.	ICS Cyber Management Board	Medium-Term	<u>6b</u>
	6d	Develop a comprehensive list of resources and/or cyber security staff training ideas, including making use of free and already available training resources (e.g., Microsoft ESI programme & Skills Development Network) for wider staff. Publicise this resource across the ICS (e.g., via the Cyber Bulletin, or using the knowledge sharing platform outlined in Knowledge Sharing actions).	ICS partner organisations	Short-Term	

STRATEGIC OBJECTIVES

6. People and Culture (2/3)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **People and Culture**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
People and Culture	6e	Develop an ICS-wide cyber training and awareness programme for all ICS partner organisations' staff. This should utilise a number of methods, from campaigns (e.g., Cyber Savvy), newsletters, phishing simulations, handouts, bite-size training opportunities throughout the year, and online training. Where possible, the training should focus on cyber impact on patient safety and use real-life examples from clinical settings to make the training meaningful. It should also cover the latest cyber trends, cyber threats and emerging issues.*	ICS Cyber Management Board	Medium-Term	
	6f	Embed cyber security training as part of the onboarding process across all ICS partner organisations, covering the most essential topics, outlining staff responsibilities	ICS partner organisations	Medium-Term	<u>6f</u>
	6g	Identify where specialist cyber security training may be required for certain groups, e.g., procurement teams, incident response teams, information asset owners, etc.	ICS partner organisations	Long-Term	<u>6b, 6c</u>
	6h	Where specialist cyber security training may be required for certain groups, develop and roll out the additional training across all ICS partner organisations.	ICS Cyber Management Board	Long-Term	<u>6g</u>
	6i	Define a blueprint for Digital Champions (e.g., the Bright Sparks programme in place in certain ICS partner organisations) that can be implemented across ICS partner organisations to uplift cyber culture, promote cyber knowledge and awareness	ICS Cyber Management Board	Long-Term	

* May require investment into technical solutions to deliver.

STRATEGIC OBJECTIVES

6. People and Culture (3/3)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **People and Culture**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
People and Culture	6j	Develop management information on the impact of training delivered. This should aim to track improvements in user awareness after training (e.g., percentage of staff failing phishing exercises) and identify who may require additional training. Consider gamification of training completion and simulation results across the ICS partner organisations	ICS Cyber Management Board	Long-Term	<u>6e, 6f, 6h</u>
	6k	Set up a centrally managed cyber apprenticeship programme to encourage cyber professionals to join the ICS cyber security team. To improve retention, provide those in senior positions with designated time to mentor trainees and contribute towards the success of the training programme. Where there is appetite, develop a scheme to place and rotate apprentices across ICS partner organisations to support local cyber security teams.	ICS Cyber Management Board	Long-Term	

STRATEGIC OBJECTIVES

7. Knowledge Sharing and Good Practice

The ways in which cyber security knowledge is shared can facilitate, or limit adherence to good practice within organisations. Mechanisms that allow users to easily search for and share cyber security information can significantly increase efficiency and improve consistency in cyber practices.

Where are we now?

Knowledge is currently shared across the ICS through the Cyber WhatsApp Group, Cyber Bulletins, the Cyber Associates Network, the wider Cyber Group meetings and the Cyber Teams channel. Calls for assistance are frequently answered, especially when support and ideas are needed and there are ongoing discussions on cyber security good practice. However:

- There is currently no formalised ICS-wide accessible platform or guidance for sharing, storing, managing or classifying cyber security knowledge, contact lists, resources, meeting notes and external materials.
- Although the Cyber Group members are receptive to asking for and offering feedback and ideas, there are fewer instances of celebrating successes, and those that contribute the most to the overall cyber security of the ICS are often not acknowledged.
- There are limited in-person event opportunities for cyber security related learning and knowledge sharing.
- While there is a dedicated C&M workspace focused on 'Future NHS', it is not widely used.



Where do we want to get to?

The ICS has built a **strong cyber security knowledge sharing culture**, where all are given the **opportunities** and **tools** to effectively share and **discuss cyber good practice**, knowledge, innovations in the industry and latest cyber activities. The ICS recognises the **contributions of individuals** in maintaining and enhancing their cyber culture by **celebrating their accomplishments**.

How do we get there?

➤ **Key activities to assist the C&M ICS with resolving the existing gaps and reach the desired state:**



Create an ICS-wide accessible knowledge sharing platform and corresponding guidance.



Organise and host regular ICS-wide cyber security events to facilitate knowledge sharing and celebration of success.



Identify and reward biggest contributors to knowledge sharing platforms.

STRATEGIC OBJECTIVES

7. Knowledge Sharing and Good Practice (1/2)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Knowledge Sharing and Good Practice**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
Knowledge Sharing and Good Practice	7a	Continue the use of the instant messaging platforms and other existing communication channels across all ICS partner organisations (i.e., the Cyber WhatsApp Group, Cyber Associates Network, Cyber Bulletins, Cyber Teams Channel and C&M Cyber Workspace on 'Future NHS') to promote knowledge-sharing resources and their usage, share cyber security news and intelligence, ask for help from partner organisations where required and continue the ongoing discussions on cyber security good practice.	ICS partner organisations	Immediate	
	7b	Build a centralised ICS-wide knowledge sharing platform* (such as Notion, Microsoft SharePoint or Confluence) to enable all ICS partner organisations to share, organise, store, easily browse and access the cyber security-related information and documentation. The platform should aim to include: <ul style="list-style-type: none"> • Templates for cyber policies, processes, standard operating procedures, response plans registers, as well as guidance and handbooks available for ICS partner organisations to use. • Security configurations good practice for commonly used applications and software. • Lessons learnt from implementation of tools, systems, services and incidents. • A contact list for key cyber resources across the ICS, e.g., internal and external SMEs, that can be contacted for specialist knowledge and questions. • Cyber security staff training good practice and certification-studying materials. • Where appropriate, records of cyber security meetings (e.g., minutes of Cyber Group) and notes on knowledge gained from industry conferences and events. • Links to external cyber good practice materials, such as reports on the latest cyber trends, cyber threats and emerging issues and details of the regulatory requirements. 	ICS Cyber Management Board	Medium-Term	<u>2f</u> , <u>2g</u> , <u>3c</u> , <u>5a</u> , <u>5c</u> , <u>5e</u> , <u>6d</u> , <u>8c</u>

STRATEGIC OBJECTIVES

7. Knowledge Sharing and Good Practice (2/2)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Knowledge Sharing and Good Practice**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
Knowledge Sharing and Good Practice	7c	Grant access to this platform to the key individuals across the ICS partner organisations and encourage the use of the platform to upload and access cyber-related documentation and best practice. As part of this, implement a protocol for an ICS assigned resource to review, classify, manage documentation and good practice and notify key contacts across the ICS partner organisations of key new additions.	ICS Cyber Management Board	Medium-Term	7b
	7d	Establish a mechanism to track the biggest contributors to the knowledge sharing platform, in terms of both value and volume (e.g., ICS partner organisations), to recognise and reward them for their efforts, to encourage all ICS partner organisations to share knowledge. This can be achieved by hosting an awards ceremony during internal cyber summits and conferences	ICS Cyber Management Board	Medium-Term	7b
	7e	Host regular cyber security learning sessions, Cyber Group meetings, cyber conferences and events, continuing with those practices that are already in place. These activities should be hosted both online and offline, and follow the principles of openness, encouraging interaction and provide positive incentives for ICS partner organisations to attend. These should include: <ul style="list-style-type: none"> • Sharing of knowledge and experience on current cyber security topics, trends and threats. • A mechanism to celebrate successes of cyber security professionals across the ICS partner organisations (e.g., awards ceremonies). • Presentations by external cyber security SMEs, academics and vendors to discuss the latest developments in cyber security industry. 	ICS Cyber Management Board	Long-Term	

STRATEGIC OBJECTIVES

8. Cyber Security Policies and Processes

Policies and processes are essential when setting a standard for cyber security activities across organisations. They should be clear, consistent, accessible and trackable to ensure that staff understand their individual roles and responsibilities within their organisation's wider collective cyber security posture.

Where are we now?

The C&M ICS has developed templates for cyber security policies and standards based on ISO 27001 and made them available to all organisations to use as required. The ICS partner organisations have a local intranet site to store and communicate cyber security policies with their staff. However:

- Each ICS partner organisation has its own cyber security policies and there is little consistency across C&M ICS, with over twenty different versions of policies and processes covering the same topics.
- Although a set of cyber security policy and standards templates was created two years ago and made available to all organisations, uptake is uncertain and there is no central resource to maintain or update these templates for best practice.
- While the ICS partner organisations have a central location to store cyber security policies, processes and standards, and while some assurance mechanisms exist, there is currently no complete view of the usage of the policies, and understanding of staff knowledge of their responsibilities for security.



Where do we want to get to?

The C&M ICS has a **uniform approach** to managing cyber security across the patch in the form of **standardisation** and **continuous improvement** of cyber security policies and processes, alongside **consistent identification** of policy **non-compliance**.

How do we get there?

➤ **Key activities to assist the C&M ICS with resolving the existing gaps and reach the desired state:**



Review, update and share existing cyber security policy templates across the ICS.



Develop and publicise guidance for implementation of policy templates within ICS partner organisations.



Develop a mechanism for ICS partner organisations to track policy compliance and identify breaches

STRATEGIC OBJECTIVES

8. Cyber Security Policies and Processes (1/3)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Cyber Security Policies and Processes**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
Cyber Security Policies and Processes	8a	Review the suite of existing cyber security policy, processes and standards templates aligned to the ISO 27001 framework to identify whether any additional templates should be developed, e.g., a template for Risk Management Policy, Cyber Incident Management Policy, Information Backup Policy etc.	ICS Cyber Management Board	Short-Term	
	8b	Update the existing example policies, processes and standards, in line with latest relevant frameworks and standards guidance, e.g., ISO 27001 and NCSC CAF. These policies, processes and standards should be tailored to the intended audience where possible. For example, an Acceptable Use Policy designed to be understood by all staff should outline their responsibilities in simple English, whereas Access Management Standard or Data Security and Protection Policy, tailored towards IT professionals, should outline the requirements in sufficient detail.	ICS Cyber Management Board	Medium-Term	<u>8a</u>
	8c	Share the updated templates across all the ICS partner organisations to encourage consistency in approaches, e.g., as part of the developed knowledge sharing platform.	ICS Cyber Management Board	Medium-Term	<u>7b</u> , <u>8b</u>



STRATEGIC OBJECTIVES

8. Cyber Security Policies and Processes (2/3)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Cyber Security Policies and Processes**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
Cyber Security Policies and Processes	8d	<p>As part of sharing of the templates, develop additional guidance and share with ICS partner organisations. This guidance could include:</p> <ul style="list-style-type: none"> • Directions to updating the templates to accurately reflect the ICS partner organisation's arrangements, or guidance on implementing good practice outlined within the policy and processes templates. • Directions for sharing the policies and processes with respective ICS partner organisations' executive management for review and approval. • Suggestions for frequency of review of policies and processes to ensure they remain valid. • Directions for communicating policies and processes with organisations' staff, embedding staff's responsibilities as part of local training efforts, as well as developing a clear and engaging summary of key staff responsibilities from relevant cyber security policies and procedures for staff to comply with. 	ICS Cyber Management Board	Medium-Term	<u>8c</u>
	8e	<p>Consider whether it would be beneficial to develop standard operating procedures for common cyber activities and tools widely used by ICS partner organisations. Where there is appetite amongst the ICS partner organisations, develop standard operating procedures, sharing those with ICS partner organisations.</p>	ICS Cyber Management Board	Medium-Term	
	8f	<p>Establish a cadence for regular review and update of the cyber security policy and processes templates, as well as standard operating procedure, where appropriate, assigning a responsible individual.</p>	ICS Cyber Management Board	Long-Term	<u>8b</u>

STRATEGIC OBJECTIVES

8. Cyber Security Policies and Processes (3/3)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Cyber Security Policies and Processes**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
Cyber Security Policies and Processes	8g	Where changes are made to templates, communicate the changes with ICS partner organisations, with guidance on implementation of suggested changes within local policies.	ICS Cyber Management Board	Long-Term	<u>7b</u> , <u>8f</u>
	8h	Agree on a mechanism for ICS partner organisations to feed back to the ICS on the use of the templates and regularly share feedback on the templates.	ICS Cyber Management Board	Long-Term	<u>8c</u> , <u>8d</u>
	8i	Where appropriate, develop a mechanism for ICS partner organisations to track policy compliance and identify breaches. As part of this, develop and share guidance for responding to identified instances of non-compliance with cyber security policies and processes. This may be achieved via performance indicators, and would depend on the specific policy and process.	ICS partner organisations	Long-Term	<u>8b</u>



STRATEGIC OBJECTIVES

9. Cyber Baseline and Minimum Standards

Baselines and minimum standards for cyber security controls are an important component in laying strong foundations and uplifting the state of cyber security across an ecosystem of organisations to reduce the likelihood of compromise.

Where are we now?

All organisations across the C&M ICS follow the DSPT requirements as the minimum standard for the security of systems and data, which will shortly incorporate NCSC CAF requirements. Several ICS partner organisations have already achieved or are working towards Cyber Essentials Plus certification. However:

- The DSPT mandates that ICS partner organisations provide an annual, self-assessed ‘snapshot’ of data protection and cyber security arrangements. There is presently no reporting to acquire an overview of the state of cyber security throughout the entire ICS for the remainder of the year.
- There is no standard baseline across the ICS partner organisations for cyber security controls above that which is set by the DSPT requirements. While several organisations achieved Cyber Essentials Plus certification, this has not been possible for all.



Where do we want to get to?

The C&M ICS supports ICS partner organisations in upholding **robust cyber security and improving cyber resilience** by building smart foundations in a form of **minimum cyber security standards**, putting ‘**secure by design**’ principle at the heart of the approach.

How do we get there?

➤ **Key activities to assist the C&M ICS with resolving the existing gaps and reach the desired state:**



Identify whether the DSPT should be supplemented by another standard to set a baseline across the ICS.



Develop a reporting dashboard to collate the current cyber security status of all ICS partner organisations.



Where possible, standardise the annual cyber security audit approach across the ICS partner organisations.

STRATEGIC OBJECTIVES

9. Cyber Baseline and Minimum Standards (1/2)

Below are the activities recommended to achieve ICS Cyber Security Strategy of **Cyber Security Baseline and Minimum Standards**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
Cyber Security Baseline and Minimum Standards	9a	Conduct an assessment to identify whether the DSPT needs to be supplemented by an additional cyber security framework or standard (e.g., Centre for Internet Security cyber security controls, Cyber Essentials Plus, or ISO 27001) to form a cyber security baseline and provide additional guidance on cyber security controls to ICS partner organisations.	ICS Cyber Management Board	Medium-Term	
	9b	If deemed necessary, identify which elements of the framework or standard should be prioritised or considered mandatory for implementation across the ICS partner organisations. This should be supplemented with guidance on what compliance with each aspect could good look like, as well as appropriate technical standards for network and information systems security (e.g., standard builds for end-points, firewall configurations, etc.).	ICS Cyber Management Board	Medium-Term	<u>9a</u>
	9c	If deemed unnecessary to supplement DSPT with an additional cyber framework or standard, collate and/or develop additional guidance, good practice and/or standardised technical standards for meeting the requirements of the DSPT to encourage consistency in approaches across the ICS partner organisations.	ICS Cyber Management Board	Medium-Term	<u>9a</u>
	9d	Communicate any requirements which are defined as part of activities 9a and 9b to the ICS partner organisations.	ICS Cyber Management Board	Medium-Term	<u>9a, 9b</u>
	9e	Develop a reporting tool, e.g., a dashboard, to collate the current cyber security status of all ICS partner organisations in one central place, creating the necessary data flows to collect the required information. This could be done by adding detail into the existing IT Health Assurance Dashboard, or considered as part of SOC reporting in the future.*	ICS Cyber Management Board	Long-Term	<u>9a, 9b, 9d</u>

STRATEGIC OBJECTIVES

9. Cyber Baseline and Minimum Standards (2/2)

Below are the activities recommended to achieve ICS Cyber Security Strategy objectives of **Cyber Security Baseline and Minimum Standards**:

Objective	ID	Activities	Accountable Lead	Priority for Implementation	Dependencies (activity reference)
Cyber Security Baseline and Minimum Standards	9f	Identify thresholds for the current cyber security status results (e.g., 'green', 'amber', 'red') and identify an appropriate escalation path for items breaching the thresholds.	ICS Cyber Management Board	Long-Term	<u>9e</u>
	9g	Using the information from the dashboard, collate a report on a monthly basis to be presented and discussed at the monthly Cyber Security Group meetings. Items rated as 'amber' and 'red' should be prioritised to identify requirements for additional support.	ICS Cyber Management Board	Long-Term	<u>9e</u> , <u>9f</u>
	9h	Identify which metrics and results should be reported to senior leadership, and ICS partner organisations' boards, supplementing with guidance for communicating results and potential implications.	ICS Cyber Management Board	Long-Term	<u>9g</u>
	9i	Identify whether there is a need for additional cyber security audit beyond the DSPT assertions compliance currently mandated by NHS England. If deemed necessary and where possible, standardise the cyber security audit approach across the ICS partner organisations. This should consider standardisation of auditing authority (e.g. conducted by NHS England or MIAA), scope of the audits etc., to enable a comparable picture across the organisations.	ICS Cyber Management Board	Long-Term	

STRATEGIC OBJECTIVES

Investing into cyber security

Under this Strategy, we have identified nine strategic objectives that would enable us to continue to develop and maintain a secure health and care system across C&M, level up our cyber security maturity, ensuring that our systems are cyber secure and resilient.

In order to **implement the activities under the strategic objectives** to reach our desired target state within the next five years, a certain level of **investment is required**. Majority of the identified activities would predominantly depend on **time and effort** from **dedicated resources as part of the ICS R-SOC and CCoE** (as outlined on pages 60-62). Some, however, would require investment into **technical solutions**.

Below is a summary of the activities that may require significant investment into technical solutions. While in some cases, the activities can be met by building upon the existing tools, in some cases, further investment into external solutions may be required:

Objective	Activity ID	Summary of Activity	Potential Technical Solution Required	Estimated Level of Investment Required
Cyber Incident Management	<u>3g</u>	Establish an ICS-wide SOC with cyber-surveillance and incident response capability.	Asset Manager, SIEM, Security Orchestration, Automation and Response (SOAR) tool, Threat Intelligence Platform (TIP), Extended Detect and Response (XDR), Penetration Testing tool*	High*
	<u>3h</u>	Establish centralised ICS monitoring systems that would enable the ICS to monitor for abnormal or malicious activity within the ICS systems and networks.		
Cyber Procurement	<u>4b</u>	Develop a centralised register of all cyber suppliers into the ICS.	Third-party register and/or risk management platform (e.g., RiskLedger)	None to Low**
Third-Party Risk Management	<u>5d</u>	Develop a platform for ICS partner organisations to share information about supplier performance and issues experienced across the ICS.		
Knowledge Sharing and Good Practice	<u>7b</u>	Build a centralised ICS-wide knowledge sharing platform to enable all ICS partner organisations to share, organise, store, easily browse and access the cyber security-related information and documentation.	Knowledge sharing platform (e.g., Notion, Microsoft SharePoint or Confluence)	Low to Medium**
Cyber Baseline and Minimum Standards	<u>9e</u>	Develop a reporting tool to collate the current cyber security status of all ICS partner organisations in one central place.	Cyber security state dashboard (e.g., IT Health Assurance Dashboard, risk management tool, SIEM)	Low to Medium**

* Depending on the R-SOC model selected (in-house, outsourced, hybrid).

** Depending on solutions chosen (e.g., existing functionalities vs. new, bespoke tools).

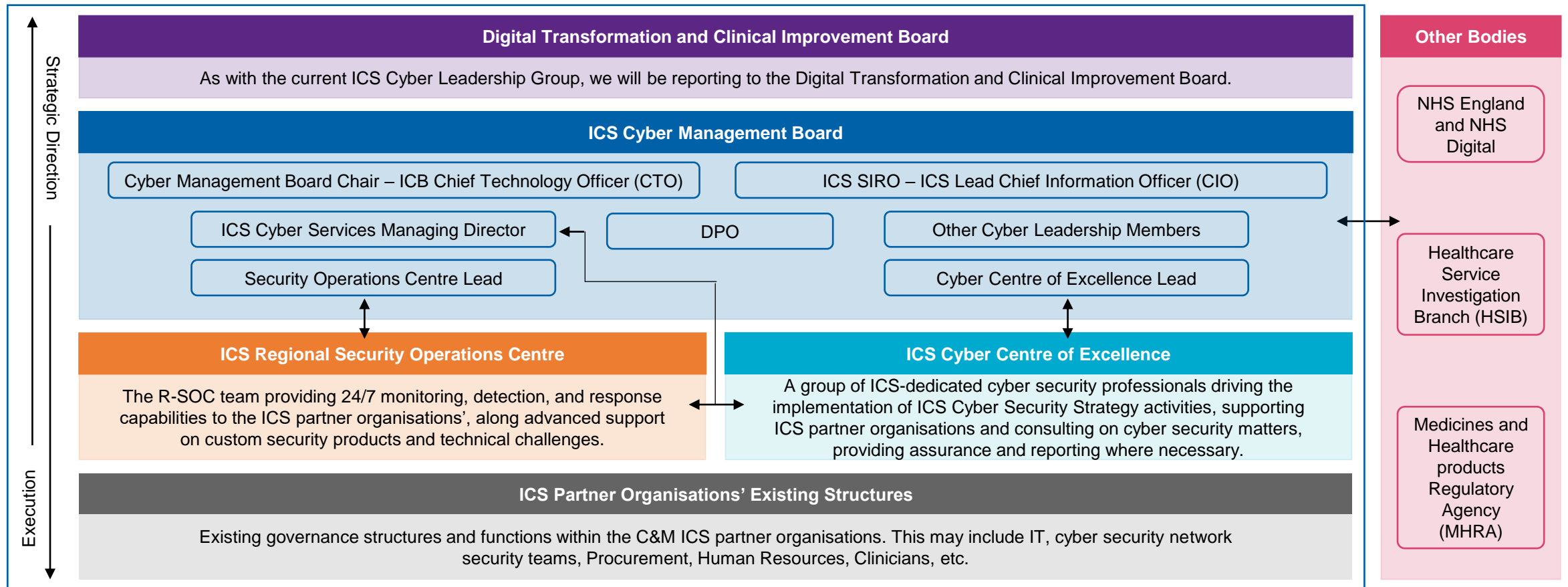
07 Governance and Accountability

PROPOSED ICS CYBER SECURITY GOVERNANCE

How do we work together as an ICS to achieve our objectives?

In order to move on as an ICS from a 'collaboration of the willing' to a **well-functioning, ICB-led unit** and **effectively implement this ICS Cyber Security Strategy**, we require a strong **foundation of effective cyber governance and accountability** model.

This model below demonstrates the **proposed governance structure** for cyber security across the ICS at high level, including the link between the local ICS partner organisations and other internal and external bodies. It is worth to note that while this proposed structure is built on the existing foundation, it is a change to our current operations, roles and responsibilities. Similarly, to effectively put this model into practice, we require **dedicated ICS resources** as part of the ICS Cyber Management Board, the **ICS R-SOC** and the **ICS CCoE to implement the strategic activities** outlined in the Strategy.



PROPOSED ICS CYBER SECURITY GOVERNANCE

What will each group do?

The cyber security governance groups will hold the following proposed key accountabilities and responsibilities:

ICS Cyber Management Board	ICS R-SOC	ICS CCoE	ICS Partner Organisations' Structures
<p>The C&M ICS Cyber Management Board will set the direction for cyber security activities for the ICS and its ICS partner organisations to drive improvements in cyber security.</p> <p>In this capacity, the Board will:</p> <ul style="list-style-type: none">• Oversee the investments into the ICS cyber security, including tools and services that would benefit ICS partner organisations.• Oversee and monitor ICS partner organisations' implementation of this Cyber Security Strategy and related action plans.• Define an approach to cyber risk identification and assessment across the ICS and monitor ICS risk exposure.	<p>The R-SOC will manage the detection, analysis, and response to cyber security threats across the ICS, including coordination of cyber incident response plans impacting more than one ICS partner organisation.</p> <p>The ICS R-SOC will also:</p> <ul style="list-style-type: none">• Support the CCoE in developing the ICS cyber incident management and response policies, procedures and playbooks.• Maintain contact with other national bodies, such as NHS England and NCSC on threat intelligence etc.• Report to the ICS Cyber Management Board on R-SOC findings, risks and incidents.	<p>The ICS CCoE will be responsible for the delivery of the underlying action plans within this Cyber Security Strategy, supporting ICS partner organisations in their responsibilities as required.</p> <p>As examples, the CCoE will:</p> <ul style="list-style-type: none">• Share cyber best practice amongst the ICS partner organisations, and discuss cyber security challenges.• Drive development of cyber security policy, processes and standards templates, working with the R-SOC where needed.• Report to the ICS Cyber Management Board on the status of ICS Cyber Security Strategy and its key activities implementation.	<p>The existing structures and IT/cyber security teams within C&M ICS partner organisations will be responsible for existing operational cyber security activities, while ensuring alignment with the ICS Cyber Security Strategy.</p> <p>Examples of activities would include:</p> <ul style="list-style-type: none">• Developing and maintaining local Business Continuity and Disaster Recovery Plans.• Conducting regular cyber security risk assessments and reporting top risks to the Cyber Management Board and CCoE.• Managing IT assets and monitoring security of key services, tools and networks. <p>ICS partner organisations will feed back and escalate cyber security challenges and issues facing to the ICS CCoE.</p>

PROPOSED ICS CYBER SECURITY GOVERNANCE



What would be the roles and responsibilities of ICS CSG members?

Cheshire and Merseyside

We propose a number of **new ICS Cyber Management Board roles** that would enable the Board to **fulfil its accountability to effectively implement this ICS Cyber Security Strategy**:

Role	High-Level Description of Accountabilities and Responsibilities
ICB CTO – Cyber Management Board Chair	<ul style="list-style-type: none"> • Chairs the ICS Cyber Management Board. • Accountable for implementation of the C&M ICS Cyber Security Strategy across the ICS, as well as meeting the ‘What Good Looks Like’ framework requirements.
ICS SIRO – ICS Lead CIO	<ul style="list-style-type: none"> • Oversees the ICS-level cyber security investment and budgeting. • Monitors the ICS partner organisations’ alignment with the cyber security obligations defined in the C&M ICS Cyber Security Strategy. • Oversees the highest cyber security risks across the ICS, and coordination of ICS-wide risk treatment measures as required.
ICS Cyber Services Managing Director	<ul style="list-style-type: none"> • Oversees the implementation of the ICS Cyber Security Strategy activities across the ICS, reporting on its progress to the Cyber Management Board. • Oversees the ICS-level cyber security services offered and delivered to the ICS partner organisations.
ICS DPO	<ul style="list-style-type: none"> • Monitors data protection compliance across the ICS, working with DPOs from individual partner organisations. • Provides advice on ICS-wide Data Protection Impact Assessments (DPIAs).
Cyber Centre of Excellence Lead	<ul style="list-style-type: none"> • Drives the implementation of the activities defined under the nine strategic objectives of the C&M ICS Cyber Security Strategy, working with the ICS Cyber Services Managing Director to identify any additional support required for the ICS partner organisations to meet their cyber security obligations under this Strategy.
Security Operations Centre Lead	<ul style="list-style-type: none"> • Oversees the implementation of the C&M ICS SOC, its prevention, monitoring and detection systems. • Support the CIO in identifying, collating and overseeing the highest cyber security risks across the ICS identified by the SOC. • Where necessary, coordinates cyber incident response across C&M ICS, including communications and threat intelligence to and from NHS England.
Other Cyber Leadership Members	<ul style="list-style-type: none"> • Support the Security Operations Centre Lead, Cyber Centre of Excellence Lead, ICS Cyber Services Managing Director, CIO and CTO in driving and overseeing the implementation of the C&M ICS Cyber Security Strategy and its strategic activities. • Collate and raise cyber security challenges and escalated issues from the ICS partner organisations to the Cyber Management Board as required.

08 Cyber Security Strategy Execution

CYBER SECURITY KPIS

How will we measure the success of the ICS Cyber Security Strategy? (1/5)

We will use a set of **Key Performance Indicators (KPIs)** to track the **implementation of the C&M ICS Cyber Security Strategy** and **measure its ongoing success** in uplifting our cyber security state and strengthening our resilience. Detailed on pages 64-68 are examples and options of KPIs that we will select from to track Strategy implementation. Each of the example KPIs is defined along with a recommended reporting timeframe and implementation window, corresponding to **one or two strategic objectives defined within the Strategy**.

Strategic Objective	Metric	Metric Description	Priority for Implementation	Reporting Timeframe
Cyber Governance	Percentage of ICS Cyber Security Strategy activities in progress or completed.	Once the Strategy implementation and underlying strategic activities has begun under <u>activity 1b</u> , track the percentage of strategic activities in progress or completed, versus those that have not yet started.	Short-Term	Quarterly
	Percentage of ICS Cyber Security Strategy activities implemented within an agreed timeline.	As implementation of the Strategy and underlying strategic activities progresses under <u>activity 1b</u> , track the percentage of strategic activities being completed within the timeframe allocated during each implementation window.	Short-Term	Quarterly
	Number of non-compliances against defined partner organisation requirements identified (measured for each ICS partner organisation).	Once cyber security requirements for ICS partner organisations to comply with are agreed under <u>activity 1i</u> , track deviations from the set requirements per ICS partner organisation.	Long-Term	Quarterly
Cyber Risk Management	Percentage of cyber security risks on risk registers without an appropriate response strategy (e.g. without mitigating actions or controls, risk acceptance etc. (measured for each ICS partner organisation).	Once a cyber risk management methodology has been established under <u>activity 2c</u> and an ICS-wide centralised cyber risk repository developed under <u>activity 2i</u> , track the percentage of cyber security risks without an appropriate response strategy per ICS partner organisations.	Long-Term	Quarterly
	Percentage of IT assets in the asset repository without an impact assessment rating from the last year (measured for each ICS partner organisation).	Once an approach to identify and prioritise IT assets has been developed and distributed under <u>activity 2g</u> , track the percentage of IT assets in the asset repository without a current impact assessment rating per ICS partner organisation.	Short-Term	Quarterly
Cyber Incident Management	Number of critical and high cyber security incidents identified across the ICS in the last six months.	Once an ICS-level incident management policy has been developed and cyber incident severity ratings agreed under <u>activity 3a</u> , track the number of critical and high cyber security incidents identified across the ICS partner organisations.	Short-Term	Quarterly

CYBER SECURITY KPIS

How will we measure the success of the ICS Cyber Security Strategy? (2/5)

Strategic Objective	Metric	Metric Description	Priority for Implementation	Reporting Timeframe
Cyber Incident Management	Number of open 'critical' and 'high' rated vulnerabilities per ICS partner organisation logged in IT Health Assurance Dashboard.	Track the number of open 'critical' and 'high' rated vulnerabilities per ICS partner organisation logged in IT Health Assurance Dashboard.	Long-Term	Quarterly
	Number of cyber security incident alerts issued by NHS 'Respond to an NHS Cyber Alert' not responded to within the agreed timeframe.	Once key incident response roles and responsibilities and incident response plans and procedures have been established under activities 3a and 3b , track the number of cyber security incident alerts issued by NHS 'Respond to an NHS Cyber Alert' not responded to within the agreed timeframe.	Medium-Term	Quarterly
	Percentage of RTO and RPO missed during recovery testing for critical assets across ICS partner organisations.	Once guidance on data backup and restoration has been created under activity 3c , track the percentage of RTO and RPO missed during recovery testing for critical assets across ICS partner organisations.	Medium-Term	Ad Hoc
IT Procurement	Percentage of IT tools and services purchased outside of the existing services catalogue (measured for each ICS partner organisation).	Once a centralised register of all suppliers into the ICS has been developed under activity 4b and a framework for procurement of new services and tools established under activity 4f , track the percentage of IT tools and services purchased outside of the existing services catalogue per ICS partner organisation.	Medium-Term	Quarterly
	Number of cyber security tools across the ICS partner organisations that cannot interface with the ICS SIEM.	Once a the ICS-wide SIEM tool is implemented under activities 3g and 3h , identify the number of tools that cannot interface with the ICS SIEM for central monitoring.	Long-Term	Annually
	Monetary savings (in GBP) identified through ICS collective purchasing efforts of IT and cybersecurity tools and services.	Once a centralised register of all suppliers into the ICS has been developed under activity 4b and a framework for procurement of new services and tools established under activity 4f , track the savings made on an annual basis from collective procurement activities.	Medium-Term	Annually

CYBER SECURITY KPIS

How will we measure the success of the ICS Cyber Security Strategy? (3/5)

Strategic Objective	Metric	Metric Description	Priority for Implementation	Reporting Timeframe
Third-Party Risk Management	Percentage of third-party suppliers with Bitsight ratings classed as high risk.	Once the platform for ICS partner organisations to share information about supplier performance and issues experienced across the ICS is developed under activity 5d , track the percentage of third-party suppliers into the ICS with Bitsight ratings classed as high risk.	Long-Term	Quarterly
	Percentage of third party IT service providers into the ICS and its partner organisations that have not completed a risk assessment in the agreed time frames.	Once a TRPM framework that details guidance ensuring that third parties perform up to contractual expectations has been implemented under activity 5a , identify the percentage of third party IT service providers into the ICS and its partner organisations that have not completed a risk assessment in the agreed time frames.	Short-Term	Quarterly
	Percentage of third party IT service providers into the ICS and its partner organisations that have not engaged with mandated assurance activities in the agreed timeframe.	Once a TRPM framework that details guidance ensuring that third parties perform up to contractual expectations has been implemented under activity 5a , identify the percentage of third party IT service providers into the ICS that have not engaged with mandated assurance activities in the agreed timeframe.	Short-Term	Quarterly
	Number of third-party suppliers which have had security incidents identified through formal and agreed notification processes.	Once a TRPM framework that details guidance ensuring that third parties perform up to contractual expectations has been implemented under activity 5a , track the number of third-party suppliers which have experienced security incidents identified through formal and agreed notification processes.	Short-Term	Quarterly
	Number of third-party suppliers which have had security incidents identified through ICS assurance activities.	Once the TRPM framework that details third party assurance activities has been developed and implemented under activity 5a , track the number of third-party suppliers which have had security incidents identified through ICS assurance activities.	Short-Term	Quarterly

CYBER SECURITY KPIS

How will we measure the success of the ICS Cyber Security Strategy? (4/5)

Strategic Objective	Metric	Metric Description	Priority for Implementation	Reporting Timeframe
People and Culture	Number of Digital Champions per ICS partner organisation.	Once a blueprint for Digital Champions has been developed across ICS partner organisations under activity 6i , track the number of Digital Champions per ICS partner organisation.	Long-Term	Annually
	Number of vacant cyber security roles across the ICS.	Once a list of the current cyber security roles/positions across the ICS under activity 6a has been collated, identify the number of vacancies and gaps.	Medium-Term	Quarterly
	Number of gaps in cyber skills, competencies and knowledge identified across the IT and/or cyber professionals across the ICS.	Once an assessment of skills, competencies and essential cyber qualifications currently possessed by ICS cyber security practitioners has been conducted and gaps identified under activity 6b , track the number of gaps in skills, competencies and knowledge across the ICS.	Medium-Term	Annually
	Number of cyber awareness campaigns launched across the ICS partner organisations.	Once an ICS-wide cyber training and awareness programme for all ICS partner organisation staff has been developed under activity 6c , track the number of cyber awareness campaigns launched across the ICS partner organisations.	Medium-Term	Annually
Knowledge Sharing and Good Practice	Percentage of users accessing the knowledge sharing library (measured for each ICS partner organisation).	Once a centralised ICS-wide knowledge sharing platform has been built and access has been granted to key individuals across the ICS partner organisations under activities 7b and 7c , track the percentage of users accessing the knowledge sharing library per ICS partner organisation.	Medium-Term	Quarterly
	Number of cyber security documents on the knowledge sharing library.	Once a centralised ICS-wide knowledge sharing platform has been developed under activity 7b , track the number of cyber security documents on the knowledge sharing library shared by ICS partner organisations.	Medium-Term	Quarterly

CYBER SECURITY KPIS

How will we measure the success of the ICS Cyber Security Strategy? (5/5)

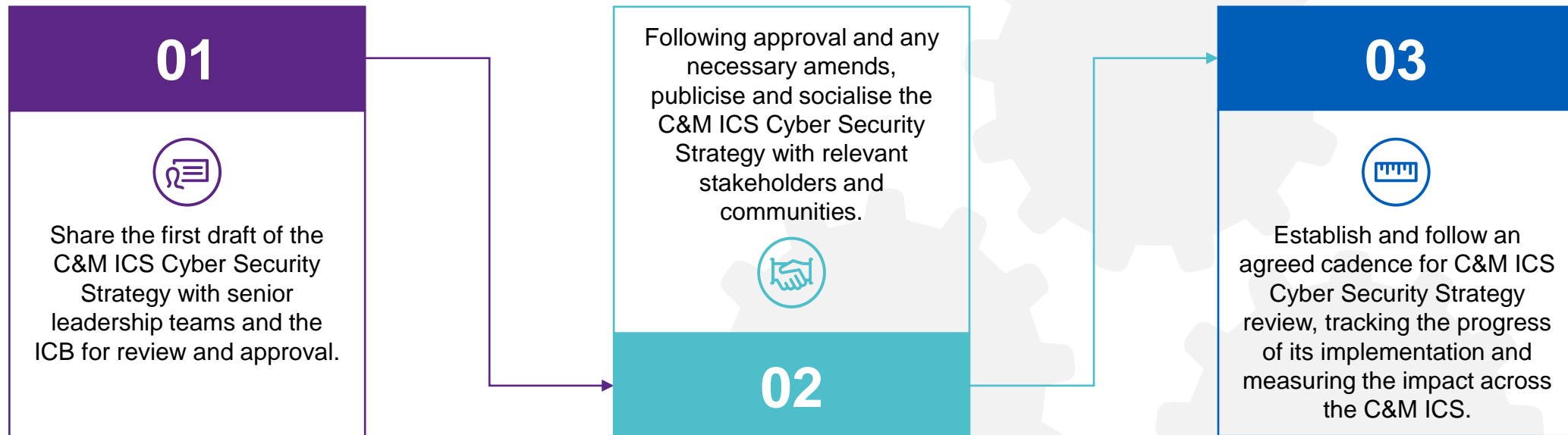
Strategic Objective	Metric	Metric Description	Priority for Implementation	Reporting Timeframe
Cyber Security Policies and Processes	Percentage of ICS partner organisations utilising the ICS cyber security policy and process templates.	Once the existing example policies and processes have been updated in line with the latest relevant frameworks and standards guidance (and shared across the ICS partner organisations under activity 8b , track the percentage of ICS partner organisations utilising ICS cyber security policy and process templates.	Medium-Term	Quarterly
	Percentage of cyber security policy and process templates undergoing annual review.	Once a cadence for regular review and update of the cyber security policy and process templates has been established under activity 8f , track the percentage of templates undergoing annual review and update.	Long-Term	Annually
Cyber Baseline and Minimum Standards	Percentage of unpatched or out of support devices on each ICS partner organisation's network.	Once a reporting dashboard has been established to collate the current cyber security status of all ICS partner organisations in one central place under activity 9e , track the percentage of devices remaining unpatched or out of support on each ICS partner organisation's network.	Long-Term	Quarterly
	Number of critical and high (CVSS scores) findings arising from annual penetration test (measured for each ICS partner organisation).	Once a reporting dashboard has been established to collate the current cyber security status of all ICS partner organisations in one central place under activity 9e , track the number of critical and high findings (as rated using CVSS scores) emerging from yearly penetration testing for each ICS partner organisation.	Long-Term	Annually
	Number of cyber security audit findings identified across the ICS partner organisations.	Once the annual cyber security audit approach has been standardised across ICS partner organisations under activity 9i , track the number of cyber security audit findings discovered across the ICS partner organisations.	Long-Term	Quarterly

NEXT STEPS

Implementing the Cyber Security Strategy and achieving our goals

This Strategy will help C&M ICS to **cement our position as cyber leaders** amongst our ICS peers, while **contributing towards developing and maintaining a sustainable health and care system** across C&M. To ensure our success, and achieve the strategic objectives we have set, we need to **socialise, refine and agree** this Strategy, validate that it meets the requirements of our ICS partner organisations and **gain endorsement** from management boards and leadership teams.

Below is a brief outline of the initial steps we need to take:



09 Appendices

FRAMEWORKS AND REQUIREMENTS MAPPING

Covering all the bases (1/2)

In developing the C&M ICS Cyber Security Strategy, identifying the strategic objectives and underlying activities, we **considered and embedded the requirements of key external frameworks and standards**, such as: the security assertions outlined within the DSPT, 'What Good Looks Like' framework, NIS CAF, NIST CSF, as well as Cyber Essentials and a suite of ISO standards (e.g., ISO 27001). We have also developed this Strategy with wider government, NHS and ICS strategies in mind, such as the DHSC cyber security strategy to 2030. Below is a mapping of our **nine strategic objectives** and how the **underlying activities** relate to **four key frameworks**, and the **DHSC cyber security strategy pillars**:

Strategic Objective	Data Security and Protection Toolkit Standards	What Good Looks Like	NIS Cyber Assessment Framework	NIST Cyber Security Framework	DHSC Cyber Security Strategy
Cyber Governance	<ul style="list-style-type: none"> 'Personal confidential data' 	<ul style="list-style-type: none"> 'Well led' principle 'Ensure smart foundations' principle 'Safe practice' principle 'Empower citizens' principle 	<ul style="list-style-type: none"> A1 Governance 	<ul style="list-style-type: none"> Business Environment (ID.BE) Governance (ID.GV) 	<ul style="list-style-type: none"> 'Defend as one'
Cyber Risk Management	<ul style="list-style-type: none"> 'Personal confidential data' 'Process reviews' 'Continuity planning' 'Unsupported systems' 'IT protection' 	<ul style="list-style-type: none"> 'Ensure smart foundations' principle 'Safe practice' principle 'Improve care' principle 	<ul style="list-style-type: none"> A2 Risk Management A3 Asset Management B3 Data Security B4 System Security 	<ul style="list-style-type: none"> Asset Management (ID.AM) Risk Assessment (ID.RA) Risk Management Strategy (ID.RM) Data Security (PR.DS) Maintenance (PR.MA) 	<ul style="list-style-type: none"> 'Focus on greatest risks and harms' 'Defend as one' 'Build secure for the future'
Cyber Incident Management	<ul style="list-style-type: none"> 'Responding to incidents' 'Continuity planning' 'Unsupported systems' 	<ul style="list-style-type: none"> 'Safe practice' principle 	<ul style="list-style-type: none"> B5 Resilient Networks and Systems C1 Security Monitoring C2 Proactive Security Event Discovery D1 Response and Recovery Planning D2 Lessons learned 	<ul style="list-style-type: none"> Information Protection Processes and Procedures (PR.IP) Protective Technology (PR.PT) Anomalies and Events (DE.AE) Security Continuous Monitoring (DE.CM) Detection Processes (DE.DP) Response Planning (RS.RP) Communications (RS.CO & RC.CO) Analysis (RS.AN) Mitigation (RS.MI) Improvements (RS.IM) Recovery Planning (RC.RP) Improvements (RC.IM) 	<ul style="list-style-type: none"> 'Defend as one' 'Exemplary response and recovery'

FRAMEWORKS AND REQUIREMENTS MAPPING



Cheshire and Merseyside

Covering all the bases (2/2)

Strategic Objective	Data Security and Protection Toolkit Standards	What Good Looks Like	NIS Cyber Assessment Framework	NIST Cyber Security Framework	DHSC Cyber Security Strategy
IT Procurement	<ul style="list-style-type: none"> 'Accountable suppliers' 	<ul style="list-style-type: none"> 'Safe practice' principle 'Empower citizens' principle 	<ul style="list-style-type: none"> A3 Asset Management A4 Supply Chain 	<ul style="list-style-type: none"> Asset Management (ID.AM) Supply Chain Risk Management (ID.SC) 	<ul style="list-style-type: none"> 'Build secure for the future' 'Defend as one'
Third Party Risk Management	<ul style="list-style-type: none"> 'Accountable suppliers' 		<ul style="list-style-type: none"> A4 Supply Chain 	<ul style="list-style-type: none"> Supply Chain Risk Management (ID.SC) 	<ul style="list-style-type: none"> 'Focus on greatest risks and harms' 'Build secure for the future'
People and Culture	<ul style="list-style-type: none"> 'Staff responsibilities' 'Training' 	<ul style="list-style-type: none"> 'Support people' principle 	<ul style="list-style-type: none"> B6 Staff Awareness and Training 	<ul style="list-style-type: none"> Awareness and Training (PR.AT) 	<ul style="list-style-type: none"> 'People and culture'
Knowledge Sharing and Good Practice		<ul style="list-style-type: none"> 'Support people' principle 'Empower citizens' principle 'Improve care' principle 	<ul style="list-style-type: none"> B6 Staff Awareness and Training 		<ul style="list-style-type: none"> 'Defend as one' 'People and culture'
Cyber Security Policies and Processes	<ul style="list-style-type: none"> 'Personal confidential data' 'Managing data access' 'IT protection' 		<ul style="list-style-type: none"> B1 Service Protection Policies and Processes B2 Identity and Access Management B3 Data Security 	<ul style="list-style-type: none"> Identity Management, Authentication and Access Control (PR.AC) Data Security (PR.DS) Information Protection Processes and Procedures (PR.IP) 	<ul style="list-style-type: none"> 'Defend as one'
Cyber Baseline and Minimum Standards	<ul style="list-style-type: none"> 'Managing data access' 'Unsupported systems' 'IT protection' 	<ul style="list-style-type: none"> 'Safe practice' principle 	<ul style="list-style-type: none"> B2 Identity and Access Management B3 Data Security B4 System Security 	<ul style="list-style-type: none"> Asset Management (ID.AM) Identity Management, Authentication and Access Control (PR.AC) Data Security (PR.DS) Protective Technology (PR.PT) 	<ul style="list-style-type: none"> 'Focus on greatest risks and harms' 'Build secure for the future' 'Defend as one'

GLOSSARY OF TERMS

Understanding terms and acronyms (1/3)

In order to make the Strategy as accessible as possible, we have tried to make sure all **abbreviated terms**, **sector-specific language** and **jargon** are fully explained where unavoidable. We have provided a glossary of **frequently used terms and abbreviations** used on the Strategy below:

Abbreviation	Name	Definition
HCP	Health and Care Partnership	HCP is a collection of NHS, local authority, voluntary, community, faith and social enterprise organisations from across the nine local authority areas that make up Cheshire and Merseyside.
ICS	Integrated Care System	An ICS brings together the NHS organisations, councils and wider partners in a defined geographical area to deliver more joined-up approaches to improving health and care outcomes. There are 42 ICSs in England, including Cheshire and Merseyside, one of the country's largest. Each ICS has an Integrated Care Board and an Integrated Care Partnership.
ICB	Integrated Care Board	The ICB was established in July 2022 as the new statutory organisation to lead integration within the NHS. The C&M ICB have a unitary board and minimum requirements for board memberships in legislation. The ICB is responsible for the day-to-day running of the NHS in Cheshire and Merseyside, including planning and buying healthcare services.
ICP	Integrated Care Partnership	The ICP provides a forum for NHS leaders and local authorities to unite as equal partners alongside important stakeholders across C&M. Together, the ICP generates an integrated care strategy to improve health and care outcomes and experiences for the people in Cheshire and Merseyside.
	ICS partner organisations	Clinical commissioning groups, local authorities and NHS provider organisations from across the nine local authority areas of Cheshire and Merseyside, all collaborating under the umbrella of the C&M ICS.
CAN	Cyber Associates Network	The CAN, established by NHS Digital and NHS England, is a group of professionals with responsibility for, or a professional interest in, cyber security, which provides people with opportunities to shape and influence the cyber security landscape.
MIAA	Mersey Internal Audit Agency	Specialist provider of assurance and solutions services to the NHS and local authorities.
HSIB	Healthcare Safety Investigation Branch	The HSIB investigates and focuses on systems and processes in healthcare, identifying the factors that could have led, or could potentially lead, to harm patients.
MHRA	Medicines and Healthcare products Regulatory Agency	The MHRA is an executive agency of the Department of Health and Social Care in the UK, responsible for ensuring that medicines and medical devices work and are acceptably safe.
	Respond to an NHS Cyber Alert service	'Respond to an NHS Cyber Alert' service, which replaced CareCERT in 2020, provides NHS organisations a secure and effective way to respond to high severity cyber alerts.
LTP	NHS Long Term Plan	The NHS LTP was published in 2019, and sets out key ambitions for the NHS services over the next ten years.

GLOSSARY OF TERMS

Understanding terms and acronyms (2/3)



Cheshire and Merseyside

Abbreviation	Name	Definition
WGLL	What Good Looks Like	The 'What Good Looks Like' framework is built on established good practices to provide ICSs clear guidance to digitise, connect and transform services safely and securely, thus improving the experience and safety of the citizens.
DSPT	Data Security and Protection Toolkit	The DSPT is an online self-assessment tool that allows ICSs to measure their performance against the National Data Guardian (NDG)'s 10 Data Security Standards.
DPIA	Data Protection Impact Assessments	The DPIA is a process to help organisations identify and minimise the data protection risks of a project, especially for processing likely to result in a high risk to individual organisations.
DPO	Data Protection Officer	The DPO is an independent, adequately resourced expert in data protection and reports to the highest management level. DPOs assist in monitoring internal compliance and inform and advise on data protection obligations. The 'What Good Looks Like' framework mandates that all ICSs have a DPO.
CSO	Clinical Safety Officer	The CSO oversees the assurance of safety-related health IT software, ensuring suppliers and ICS partner organisations meet the required safety standards. CSOs also ensure that all safety-related risks associated with a health IT system are actively managed, and that appropriate mitigations are applied. The 'What Good Looks Like' framework mandates that all ICSs have a CSO.
SIRO	Senior Information Risk Officer	A SIRO is responsible for implementing and managing information risks within an ICS partner organisation. The SIRO oversees information risks within the organisation and will inform and advise the board on how to mitigate the risk according to the organisation's risk appetite. The 'What Good Looks Like' framework mandates that all ICSs have a SIRO.
CLG	Cyber Leadership Group	The CLG consist of individuals from across the community established in the aftermath of the WannaCry incident. The Group is currently responsible for setting the cyber security agenda, defining and delivering workstreams and coordinating activities.
	Cyber Group	The Cyber Group is open to all ICS partner organisations. Under the CLG's direction, it shares best practices, provides a sounding board for cyber developments, and creates the knowledge bridge between the ICB and local organisations to drive resilience through commonality, and consolidated spending, strategies, and contracts.
TOM	Target Operating Model	A TOM is a breakdown of the capabilities required and a corresponding estimate of the full-time equivalent (FTE) resources required to discharge those capabilities. An effective TOM enables the ICSs to defend against cyber security threats and manage residual risk effectively in collaboration with other departments (e.g., HR) on cyber security matters.
	Digital Champion	A digital champion is an employee within an ICS partner organisation chosen to help lead change, promote digitalisation, and influence colleagues to support the smooth onboarding of technologies. They can also act as cyber champions to educate on, promote and maintain good cyber hygiene practices across ICS staff.

GLOSSARY OF TERMS

Understanding terms and acronyms (3/3)

Abbreviation	Name	Definition
SIEM	Security Information and Event Management	SIEM is a security solution that helps ICS partner organisations recognise potential security threats and vulnerabilities before they have a chance to disrupt business operations. The underlying principle of a SIEM system is to aggregate relevant data from multiple sources, identify deviations from the norm and take appropriate action.
R-SOC	Regional Security Operations Centre	A R-SOC is a centralised function within an ICS partner organisation employing people, processes and technology to continuously monitor and improve the organisation's security posture while preventing, detecting, analysing and responding to cyber incidents.
	IT Health Dashboard	The IT Health Assurance Dashboard is a solution used by a number of ICS partner organisations that collates insights on the status and health of internal networks. Continuous, agentless network scanning (e.g., Nessus vulnerability scanner) and intuitive, tailor-made, near-real-time reports make risks easier to visualise, remediate and report on.
BIA	Business Impact Analysis	An analysis of an information system's requirements, functions, and interdependencies used to characterise system contingency requirements and priorities in the event of a significant disruption.
	Minimum Baseline	Minimum baselines are the agreed minimum cyber security controls required for safeguarding IT ecosystems based on their identified needs for confidentiality, integrity or availability protection. Minimum baselines for cyber security controls are essential in laying solid foundations and uplifting the state of cyber security across the ICS ecosystem to reduce the likelihood of compromise.
TPRM	Third-Party Risk Management	Working with third parties can introduce vulnerabilities and cyber security risks into the ICS ecosystem. As such, a standardised third-party risk management approach to assessing and managing third party goods and services is crucial.
KPI	Key Performance Indicator	A KPI is a quantifiable performance measure over time for a specific objective. KPIs provide targets for teams to shoot for, milestones to gauge progress, and insights that help people across the organisation make better decisions.
	Strategic Objectives	Strategic objectives are broad and clearly defined statements of 'end goals' that the ICS aspires to achieve within the next five years. Nine cyber security objectives have been identified to direct the C&M ICS efforts in enhancing its cyber security state through discussions with key stakeholders on the ICS's current and desired state, documentation review, and external factors, such as industry frameworks and good practices.
CE+	Cyber Essentials Plus	CE+ is a government-backed scheme that helps protect an organisation, whatever its size, against a whole range of the most common cyberattacks. Suppose you would like to bid for central government contracts that involve handling sensitive and personal information or providing certain technical products and services. In that case, you will require CE+ certification.
ISO 27001	International Organisation for Standardisation 27001	ISO 27001 helps organisations manage and protect their information assets to remain safe and secure. ICS partner organisations must document the relevant issues as part of their information security objectives and results of the risk assessment and maintain records of the competence of their staff.