NHS
South West London

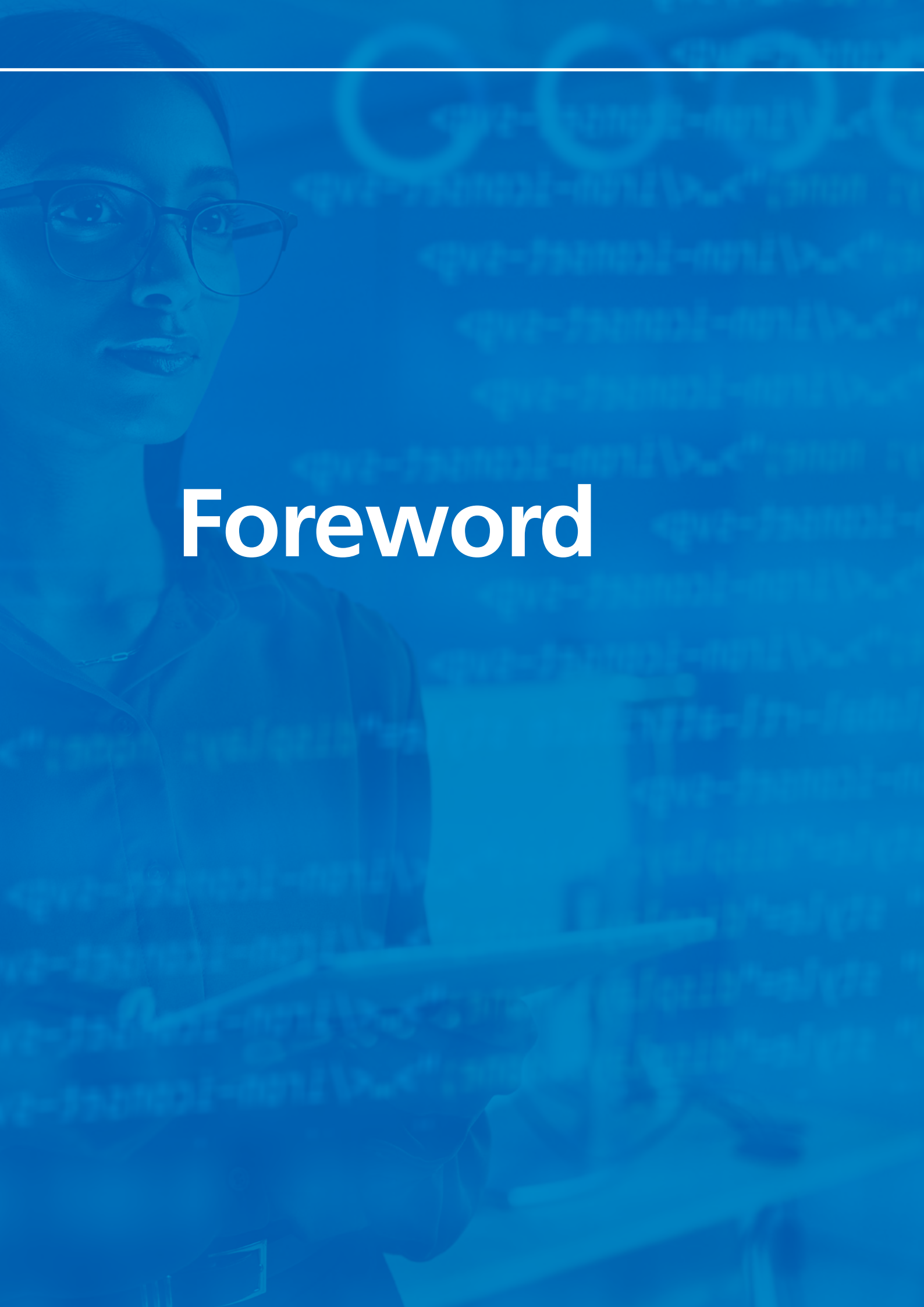
South West London ICB:

Cyber Security Strategy

2025 – 2030

February 2025

Contents



Foreword

Foreword

The SWL ICB Cyber Security Strategy outlines how strengthening cyber security over the next five years will enhance the quality of care for our service users. By driving cross-system collaboration, we aim to build a collective cyber protection that leverages economies of scale, ensuring a more resilient, efficient, and unified approach to safeguarding critical services. Through shared initiatives, resource optimisation, and strategic coordination, we will enhance cyber resilience while enabling the effective deployment of advanced technologies and expertise across the ICB.

"Cybersecurity is a fundamental part of patient safety and a cultural priority for SWL ICB. Protecting our digital infrastructure means protecting lives, and this requires a business-wide commitment across all levels of our ICB. This strategy ensures that cybersecurity is embedded into our operations, promoting a culture of shared responsibility and resilience, so we can continue delivering safe, high-quality care to those who depend on us."

Dr John Byrne
Chief Medical Officer
NHS SWL Integrated Care Board

"As we drive digital transformation across SWL ICB, security must be embedded in everything we do. This strategy ensures that our digital initiatives are built on a strong and consistent foundation of cybersecurity, safeguarding patient data, critical systems, and the trust our communities place in us. By working collaboratively, we will create a resilient and future-proof digital healthcare ecosystem."

Martin Ellis
Chief Digital Information Officer NHS SWL Integrated Care Board

Executive Summary

Overview (1/3)

The SWL ICB Cyber Security Strategy sets out a unified and collaborative approach to managing cyber risks across all NHS provider organisations within South West London. Recognising the critical importance of protecting essential healthcare services, the strategy provides a robust framework to ensure the confidentiality, integrity, and availability of systems, data, and patient services.

Aligned with the **Department of Health and Social Care (DHSC) Cyber Strategy to 2030,** the strategy addresses local challenges by encouraging collaboration, standardisation, and resilience. It underscores the shared responsibility across NHS provider organisations, emphasising the principle that **"we are only as strong as our weakest link."**

This strategy was developed through a collaborative process, engaging stakeholders across the ICB to address local priorities while adhering to national requirements. It aligns with the **revised Data Security and Protection Toolkit (DSPT)**, which is now based on the **National Cyber Security Centre's Cyber Assessment Framework (NCSC CAF)**, alongside other national guidelines. The strategy is mainly informed by:

Comprehensive cyber assessments of NHS provider organisations.

Feedback from existing governance arrangements.

Lessons learned from recent cyber incidents across the NHS, along with key takeaways from our inaugural ICB-wide cyber incident simulation exercise.

Overview (2/3)

The strategy outlines six key objectives designed to improve the ICB's overall cybersecurity posture and ensure a consistent, system-wide approach:

Our First objective, Strengthening Governance focuses on the cyber function of the Integrated Care Board (ICB) and the respective boards of NHS provider organisations by better aligning accountability, oversight, and coordination with knowledge and executive cyber awareness, and responsibilities.

The second objective, Managing Risk aims to develop a broader approach across SWL ICB to manage cyber risks. This is focused on creating greater transparency of the overall risk position and what is required to remediate it.

Objective three Understanding Critical Systems and Suppliers develops a significantly better knowledge of systems and suppliers that are critical to the delivery of essential services in SWL ICB. This also includes gaining better grasp on the impact and dependencies in the event of these systems and suppliers becoming unavailable for prolonged periods due to cyber incident.

For objective four, Prevention and Resilience is crucial to develop stronger control structures and systems to prevent cyber attacks and to implement processes that increase resilience across the ICB. It is inevitable that the ICB will succumb to some form of cyber attack, but it needs to be able to resist the complete shutdown and loss of its critical systems.

Objective five, Detecting and Responding to Threats and Incidents seeks to develop out the detection and response capabilities for the ICB. This aims to deliver a centralised approach to monitoring and detection of cyber threats and co-ordinating incident response across our critical systems and services, supported by NHS England centralised services and other partner services.

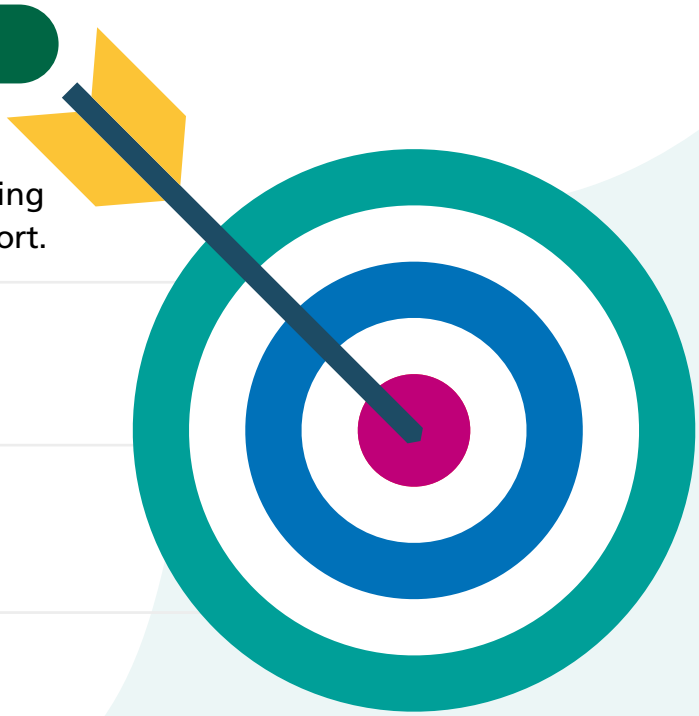
Finally, objective six, Embedding Cyber Awareness and Culture deals with obtaining and retaining cyber talents and ways to develop the cyber security workforce. This includes training on specific cyber security skills alongside the synchronised training and awareness of end users in the ICB around the risks of cyber attacks.

Overview (3/3)

This strategy envisions a SWL ICB where all NHS provider organisations work collaboratively to mitigate cyber risks, safeguard essential services, and respond effectively to incidents. Success will mean achieving:

- Clear accountability for cyber security across all levels of governance
- A centralised repository of critical systems and suppliers, enabling proactive risk management.
- A user base that is better aware of cyber risks, supported by a community of qualified cyber professionals.
- Consistent implementation of foundational cyber controls
- Unified threat detection and response capabilities, reducing the impact of cyber incidents.

Our aim is to achieve this mainly by:



1. Strengthening cooperation between NHS provider organisations and leveraging NHS England provided services and support.
2. Investing in skills, training, and shared resources to enhance our cybersecurity capabilities.
3. Using joint procurement and economies of scale to maximise resources and reduce costs.
4. Establish ongoing processes to track progress, ensure compliance, and adapt to emerging risks

Background

Background (1/3)

About Us

South West London Integrated Care Board and the NHS provider organisations is a collaborative partnership across the footprint of 6 Local Authorities, bringing together 6 NHS Trusts, 174 GP practices, and other key stakeholders to deliver better health and care outcomes for our residents.

Covering a diverse population of approximately **1.5 million people**, we focus on ensuring equitable access to high-quality healthcare services, reducing health disparities, and improving overall population health. Our structure reflects a collective approach to integrated care. Together, we work to enhance patient care pathways, ensure financial sustainability, **and leverage technology to improve operational efficiencies.** By **coordinating** efforts across these diverse providers, we ensure that health and care services are designed around the needs of our population, **promoting innovation and resilience** in the face of **emerging challenges, including cyber threats**. This strategy underscores our commitment to **securing the digital foundations upon which we deliver essential services.**

Our Providers

Local Authorities

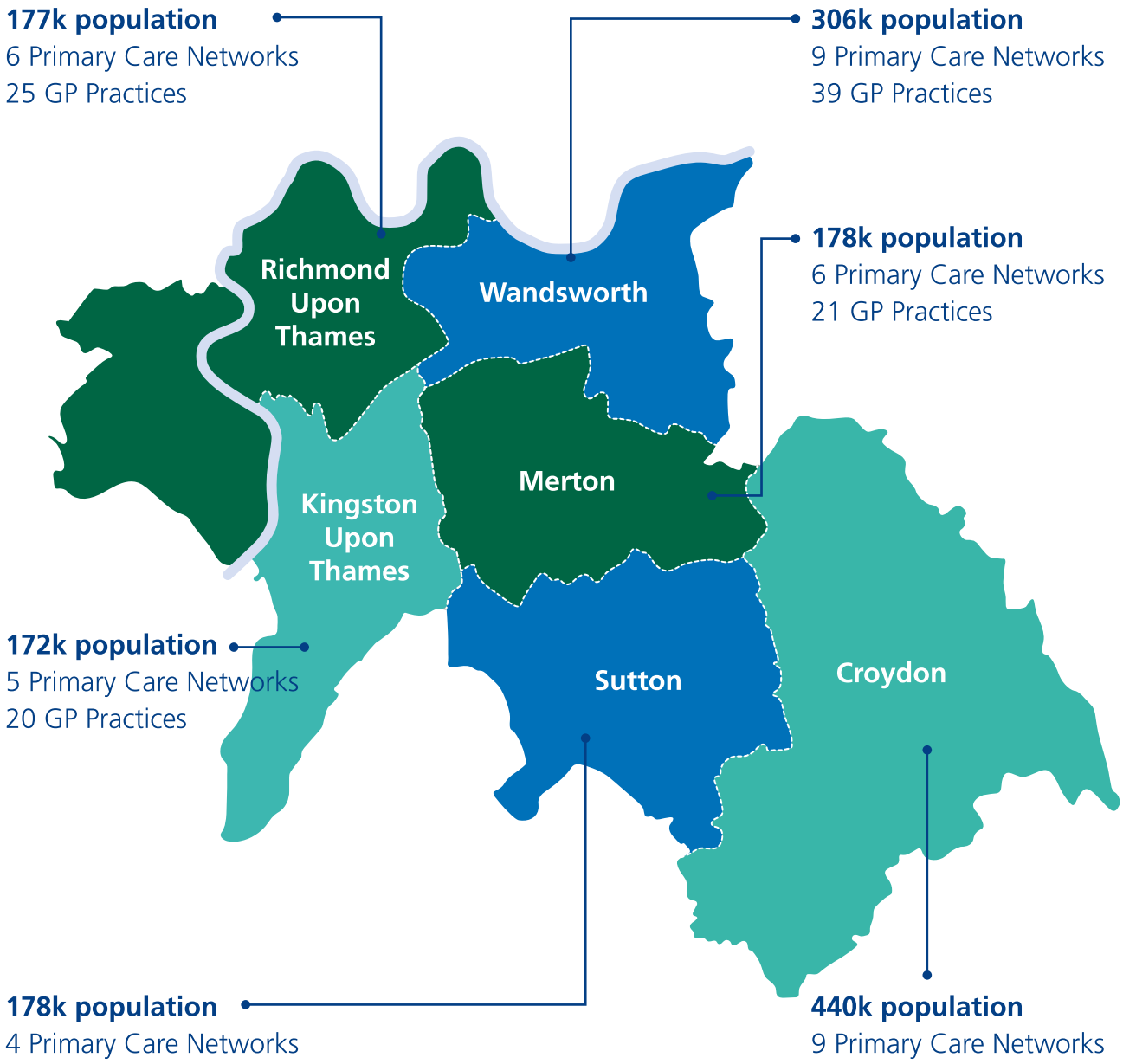
- Wandsworth council
- Sutton council
- Richmond council
- Merton council
- Kingston council
- Croydon council

NHS Provider Trusts

- Croydon Health Services NHS Trust
- Epsom and St Helier University Hospitals NHS Trust
- Kingston and Richmond NHS Foundation Trust
- Royal Marsden NHS Foundation Trust
- South West London and St George's Mental Health NHS Trust
- St George's University Hospitals NHS Foundation Trust

Community Providers

- Central London Community Healthcare NHS Trust
- Your Healthcare CiC


177k population
6 Primary Care Networks
25 GP Practices
306k population
9 Primary Care Networks
39 GP Practices
178k population
6 Primary Care Networks
21 GP Practices
Richmond Upon Thames
Wandsworth
Merton
Kingston Upon Thames
Sutton
Croydon
172k population
5 Primary Care Networks
20 GP Practices
178k population
4 Primary Care Networks
440k population
9 Primary Care Networks

Background (2/3)

Why we need this strategy

This strategy seeks to address the critical and evolving threats facing the NHS, ensuring that SWL ICB pursues a unified, proactive approach to safeguarding our systems, data, and patient services.

Recent cyber incidents, such as the Synnovis cyber attack, have demonstrated the devastating impact cyber threats can have on healthcare services. These events disrupt essential patient care, threaten sensitive data, and undermine trust in digital systems. This strategy acknowledges that protecting our collective services requires a cohesive, system-wide effort.

The strategy aims to:

- **Strengthen governance and accountability** by embedding cyber security into board-level priorities across SWL ICB.
- **Protect patient care and critical services** through a robust and unified cyber posture.
- **Enable faster recovery from cyber incidents** with clear roles, streamlined processes, and coordinated responses.
- **Enhance public trust** by ensuring data security and enabling the confident adoption of new digital technologies.

Through collaboration with our NHS provider organisations and partners, alignment with national direction, and proactive risk management, this strategy sets the foundation for a resilient and secure digital future across South West London ICB.

How was it created?

Strategy was developed in alignment with the responsibilities outlined in the DHSC Cyber Security Strategy to 2030, incorporating key frameworks such as the DSPT-aligned NCSC Cyber Assessment Framework (CAF), “What Good Looks Like” and other relevant frameworks. Also, locally commissioned assessments engaged stakeholders across the ICB, ensuring our strategy reflects collective needs and priorities while addressing national and regional requirements.

NHS England mandate requires every ICB to develop a cyber strategy aligned with the DHSC Cyber Strategy to 2030. **However, for South West London (SWL), this goes beyond compliance. We’ve recognised that building a resilient cyber future requires a proactive and cohesive approach.**

Background (3/3)

These priorities aim to protect the delivery of care across SWL ICB, ensuring a reasonable balance between security and clinical needs.

We are committed to supporting the safeguarding of digital assets used in the delivery and support of our essential services, and protecting sensitive data across our diverse networks. To achieve this, we will focus our efforts on:

1.

Aligning to the industry requirements, frameworks and standards

2.

Defining clear metrics to measure the success of the Strategy and its impact on our collective cyber security posture

3.

Maximising the value of leveraging national NHS tools and services

4.

Building an ICB-wide cyber security governance structure led by the ICB Board, with adequate resources to deliver on our objectives

5.

Promoting a risk-driven approach to mitigate the impact of cyber incidents, and improving cyber awareness and culture

These priorities were shaped through a blend of national guidance, local collaboration, and insights from locally commissioned cyber assessments. While the national direction provided a clear framework, we engaged extensively with our ICB providers through existing forums, such as the Cyber Assurance Group (CAG), Digital Infrastructure Steering Group (DISG), and the Digital Leadership Team (DLT).

Mission and Vision

Our Mission and Vision

As digital transformation accelerates across SWL ICB, ensuring a robust and resilient cyber security structures are critical to safeguarding patient services, protecting sensitive data, and maintaining public trust. This Strategy is built on a foundation of collaboration, strong leadership, and a shared responsibility for cyber resilience across all organisations.

Cyber security is not just a technology challenge, it is a cultural priority. Executive leadership plays a pivotal role in shaping a security-conscious environment, setting expectations, and embedding cyber resilience into everyday practices. By fostering a top-down commitment to security, this strategy ensures that every individual, from leadership to frontline staff, recognises their role in protecting our essential services from cyber attacks and incidents.

At the heart of this strategy are our mission and vision, guiding our approach to cyber security across the ICB.

Our Mission

To foster a collaborative and resilient cyber security culture across SWL ICB by implementing a unified governance approach, promoting secure operational practices, and embedding accountability at all levels. We are committed to safeguarding the confidentiality, integrity, and availability of critical systems, data, and patient services, while proactively mitigating risks, and preventing unauthorised access, ensuring that patient information remains safe and protected.

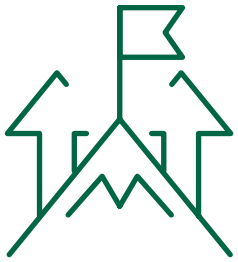
Start well

Live well

Age well

Our Vision

To establish a digitally secure and resilient ICB, where **leaders champion** cyber security, encouraging a culture of shared responsibility across NHS provider organisations, the ICB, and strategic partners. Through **strategic coordination and continuous engagement**, we aim to protect against cyber threats, enhance system reliability, and ensure the accessibility of our essential services.



While each organisation retains responsibility for its cyber risk, SWL ICB will drive alignment, best practices, and collective resilience through transparent leadership and cross-organisational collaboration.

Together, we will strengthen cyber governance, promote a proactive security culture, and empower every individual to play their part in securing the systems that support our essential services, building a resilient and secure future for our residents.

Establishing the Strategy

Cyber Security Strategy Development

Putting the Strategy Together: A collaborative Journey

To establish a **comprehensive and effective SWL ICB Cyber Strategy,** we began by gaining an understanding of the cyber security posture across our sub region. This journey started in 2023 with a **system-wide cyber assessment** using the **CIS Critical Security Controls (CSC) Level 2** for Critical National Infrastructure (CNI), recognising the NHS as a vital part of this designation.

Understanding the Baseline

The assessment included an evaluation of existing controls aligned with frameworks such as the Data Security and Protection Toolkit (DSPT), Cyber Essentials, NCSC's 10 Steps, and NHS guidance on "What Good Looks Like." Through workshops and targeted technical sessions with SWL ICB organisations, we explored gaps and alignment across people, processes, and technology, identifying strengths and areas for improvement.

Aligning with National Frameworks

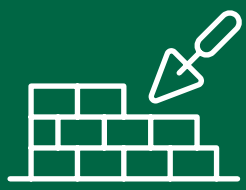
Following the national direction to align the DSPT with the NCSC Cyber Assessment Framework (CAF), we completed a CAF evaluation in 2024 of our NHS provider organisations. This step ensured that our strategy reflected national priorities and compliance requirements while maintaining relevance to local needs.

Collaborative Approach and Integration

In crafting the strategy, we reviewed local digital strategies from member organisations, integrating their priorities wherever feasible. Stakeholder collaboration through workshops, technical discussions, and inputs from existing oversight groups including SWL ICB DLT and CAG provided rich insights to meeting national requirements while supporting unique local needs.

Our thought process (1/2)

The SWL ICB Cyber Security Strategy is driven by the need to **address common systemic challenges**, build on our current progress, and **seize opportunities to strengthen resilience across** South West London. This strategy ensures a coordinated, system-wide approach to cyber security that transcends compliance, **fostering alignment between** our NHS provider **organisations** while recognising each organisation's independence.



1.

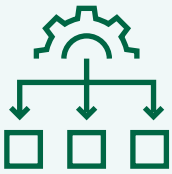
What We're Building On

2.

Key Challenges

3.

Unlocking Economies of Scale



4.

Existing Model

5.

Tight Financial Climate

6.

Strengthening Partnerships with NHS England

Our thought process (2/2)

Governance is siloed within IT/Digital teams, limiting its reach and effectiveness. This approach leaves gaps, as it fails to address the broader SWL ICB risks that span clinical, operational, and data management domains.

Recent cyber assessments including **CIS Critical Security Controls (CSC) level 2 and NCSC CAF** highlighted areas requiring focus for improvement including cyber governance, risk/asset management, supply chain security, data security, monitoring/incident response, recruitment/retention of skilled cyber professionals, etc

By **managing cyber security investments** and **coordinating resources** at the ICB level, we can achieve greater value while reducing duplication of effort. Leveraging our collective size enables more efficient procurement and streamlined implementation of security solutions.

Three key groups are central to driving cyber security across SWL ICB:

- SWL Digital Leadership Team – comprising CIOs and their equivalents across SWL's IT ecosystem.
- SWL Digital Infrastructure Steering Group (DISG) – comprising IT infrastructure/ operation leads.
- SWL Cyber Assurance Group (CAG) – Comprising all cyber leads across SWL ICB

Like other ICBs, **SWL faces funding constraints due to broader pressures across the NHS.** These limitations impact our ability to invest in improving cyber maturity, attract skilled professionals, and deliver consistent training.

A **crucial step** in achieving the SWL ICB cyber strategy is to **maximise the use of NHS England's tools** and services in strengthening our collective security capabilities while significantly reducing costs for the ICB and its member organisations.

Objectives

Cyber Security Objectives

Building on system-wide assessments and collaborative efforts, we have established six key cyber security objectives to enhance our overall cyber resilience. These objectives were shaped through stakeholder consultations, findings from assessments, and alignment with national direction and industry good practices. They are:

Strengthening Governance

To strengthen the cyber function of the Integrated Care Board (ICB) and the respective boards of NHS provider organisations by better aligning accountability, oversight, and coordination with knowledge and executive cyber awareness, and responsibilities.

Managing Cyber Risk

To develop a broader approach across SWL ICB to manage Cyber risk. This is focused on creating greater transparency of the overall risk position and what is required to remediate it.

Understanding Critical Systems and Suppliers

To develop a significantly better knowledge of systems and suppliers that are critical to the delivery of essential services in SWL ICB. This also includes gaining better grasp on the impact and dependencies in the event of these systems and suppliers becoming unavailable for prolonged periods due to cyber incident.

Prevention and Resilience

To develop stronger control structures and systems to prevent cyber attacks and to implement processes that increase resilience across the ICB. It is inevitable that the ICB will succumb to some form of cyber attack, but it needs to be able to resist the complete shutdown and loss of its critical systems.

Detecting and Responding to Threats and Incidents

To develop the detection and response capabilities for the ICB. This aims to deliver a centralised approach to monitoring and detection of cyber threats and co-ordinating incident response across our critical systems and services, supported by NHS England centralised services and other partner services.

Embedding Cyber Awareness and Culture

To develop out the detection and response capabilities for the ICB. This aims to deliver a centralised approach to monitoring and detection of cyber threats and incidents across our critical systems and services, supported by NHS England centralised services and other partner services.

1. Strengthening Governance

We will implement robust governance structures, policies, and standards to ensure that overall accountability for cyber security across SWL ICB rests with the ICB's **Board and the respective boards of NHS provider organisations**, with clearly defined expectations. Boards may delegate cyber responsibilities to subsidiary boards or strategic committees, ensuring strong business representation to oversee cyber security management and drive the strategy's objectives. This approach includes setting a clear risk appetite and empowering appropriately skilled individuals at all levels to make informed decisions. The detailed activities are reflected in a separate implementation plan document.

Our status at this point

Cyber security governance in SWL ICB is currently channelled through the **Digital Board**, to the **Digital Infrastructure Steering Group (DISG)**, which mainly consists of IT and technical leads, and then to the **Cyber Assurance Group (CAG)**, made up of cyber leads across the ICB. This approach primarily views cyber security as a component of IT and digital infrastructure, limiting its broader relevance as an organisation-wide priority.

What outcome are we striving for?

The new governance structure will elevate cyber security to a system-wide priority, with **overall accountability held by the ICB's board and respective boards of NHS provider organisations**. The ICB Digital Board, **with representation from all key business areas**, will provide delegated ICB board oversight, ensuring comprehensive **coverage beyond technical aspects**, while a new Cyber Assurance Committee with appropriate business representation will focus on providing independent assurance **to the ICB board through the Senior Management Team (SMT)**. The existing Cyber Assurance Group will be revised into a **Cyber Technical Group (CTG)** with advisory responsibilities.

How this might be achieved?

A system-wide alliance to deliver and maintain this strategy.	Agree an inclusive cyber governance structure, and Target Operating Model (TOM)	Confirm a reporting process up to the ICB board.

2. Managing Cyber Risk

We will aim to develop a framework across SWL ICB **based on a supportive culture** to effectively manage cyber risk with the potential to cause the greatest harms. This would foster greater transparency in understanding the overall risk landscape and identifying the necessary steps for remediation. A key component of this approach is the adoption of a more robust and integrated supplier risk management framework in line with national direction. The detailed activities are reflected in a separate implementation plan document.

Our status at this point

Cyber risk management across SWL ICB is fragmented, with NHS provider organisations independently managing risks through varied approaches. This inconsistency results in non-uniform risk assessment outputs and limits the ICB's visibility of risks that could potentially disrupt the delivery of healthcare services across our sub region.

What outcome are we striving for?

SWL ICB will adopt a unified and standardised approach to cyber risk management, ensuring consistent practices across all organisations. This approach will prioritise identifying and addressing risks with the greatest potential to harm healthcare services, promoting greater system-wide visibility and resilience.

How this might be achieved?

Adopt a unified cyber risk management framework across the ICB	Create risk management artefacts including policies, and guidance for consistency across the ICB.	Create a risk reporting process into the ICB Cyber Security Office.

3. Understanding Critical Systems and Suppliers

Critical systems and suppliers are essential to delivering healthcare services across our ICB, yet their management is fragmented, with no centralised oversight. This lack of visibility hinders effective risk management, coordinated incident response, and cost efficiencies. By establishing a central repository of critical systems and suppliers, we can enhance resilience, improve cybersecurity, and optimise resources through better understanding and proactive management of these vital assets. The detailed activities are reflected in a separate implementation plan document.

Our status at this point

Localised Management: Currently, critical systems and suppliers are managed independently by each NHS provider organisation, resulting in fragmented records and no adequate ICB-wide visibility.

Limited Interdependency Mapping: The interdependencies between systems, services, and suppliers across the ICB are not fully understood, leading to inefficiencies and potential blind spots in risk management.

Reactive Engagement: Due to the lack of centralised visibility, the ICB struggles to proactively engage with suppliers or leverage economies of scale to manage risks or costs.

What outcome are we striving for?

Our goal is to establish comprehensive, centralised visibility of all critical systems and their suppliers, gaining a clear understanding of their role in supporting essential services and interdependencies across the ICB.

Additionally, we strive to adopt a proactive approach to managing these assets and supplier relationships, including joint procurement initiatives that leverage economies of scale while addressing the specific needs of local organisations.

How this might be achieved?

Create and maintain a centralised repository of critical systems and suppliers	Conduct an interdependency mapping exercise and Impact analysis	Develop a joined-up supplier management and engagement framework.

4. Prevention and Resilience

Cyber attacks continue to pose a significant threat to healthcare delivery, and within our ICB, our ability to prevent attacks and to **implement processes** that increase resilience varies across organisations. While some providers have robust control structures in place, others are less equipped, leaving critical gaps in our collective resilience. As the saying goes, **"we are only as strong as our weakest link."** Therefore, we aim to establish a minimum, consistent set of foundational cybersecurity controls across SWL ICB to prevent cyber attacks and minimise the impact of cyber incidents on our essential services. The detailed activities are reflected in a separate implementation plan document.

Our status at this point

Prevention and resilience capabilities vary across ICB organisations, with some providers having more advanced controls than others, creating vulnerabilities in our collective resilience.

While incident response and recovery plans exist, they lack consistency across the ICB.

What outcome are we striving for?

We aim to establish an ICB-wide baseline of prevention and resilience capabilities, ensuring all providers have effective and consistent foundational controls like endpoint protection, MFA, patch management, vulnerability management, disaster recovery and business continuity. Our goal is collective resilience, strengthened through improved collaboration, shared best practices, and reliable incident mitigation measures to safeguard our essential services.

How this might be achieved?

Define and Implement consistent minimum standards for foundational controls.	Agree a support model for risk mitigating and compensating controls.	Establish a plan for ongoing monitoring and assurance on agreed controls.

5. Detecting and Responding to Threats and Incidents

Detecting and responding to cyber threats is a critical component of our ICB cybersecurity strategy, distinct from prevention and resilience. While prevention focuses on reducing vulnerabilities, this objective aims to ensure we can identify and respond effectively to threats and incidents when they occur. By centralising detection capabilities and enhancing response planning, we aim to strengthen our ability to mitigate threats swiftly and collaboratively across SWL ICB, aligning with the DHSC's "Defend as One" objective. The detailed activities are reflected in a separate implementation plan document.

Our status at this point

Detection and response capabilities are currently fragmented and managed locally by individual NHS provider organisations, with varying levels of maturity and no centralised visibility across the ICS. This limits the ability to coordinate responses or identify patterns in threats that could impact multiple providers.

What outcome are we striving for?

Our goal is to establish a centralised, cost-effective system for monitoring, detecting and responding to cyber threats and incidents across the ICB. This will provide **consistent visibility, reporting, and coordination, while allowing NHS provider organisations to retain local risk ownership.** This improved capability will include robust incident response plans and playbooks, more frequent simulation exercises, and improved awareness to mitigate the impact of threats, including insider risks.

How this might be achieved?

Agree and implement SWL ICB centralised threat monitoring and response model.	Standardise and align incident response plans for effective coordination.	Confirm a plan for regular cyber simulation/tabletop exercises.

6. Embedding Cyber Awareness and Culture

Our ambition here focuses on empowering our users to effectively respond to evolving cyber threats while promoting an approach to attracting and retaining cyber talent and strengthening the cyber security workforce by knowledge sharing and close collaboration. This involves providing targeted training on specialised cyber security skills while also promoting cyber awareness and education for all ICB employees on the risks of cyber attacks, their role in mitigating those risks, and their responsibilities in responding to and recovering from potential cyber incidents. The detailed activities are reflected in a separate implementation plan document.

Our status at this point

Cyber training and awareness across SWL ICB is managed independently by each provider, resulting in varied programmes across organisations. This includes Annual Mandatory Data Security Training, routine end-user communications, inconsistent and irregular board assurance training, as well as annual phishing and incident simulation exercises. The lack of standardisation creates inefficiencies, such as users having to repeat mandatory training when transitioning between organisations within the ICB. However, challenges persist in attracting and retaining skilled cyber resources within the NHS due to uncompetitive financial benefits and lack of incentives when compared to other industries. This disparity limits the ICB's ability to sustain a skilled workforce, further exacerbating inconsistencies in cyber training and preparedness across organisations.

What outcome are we striving for

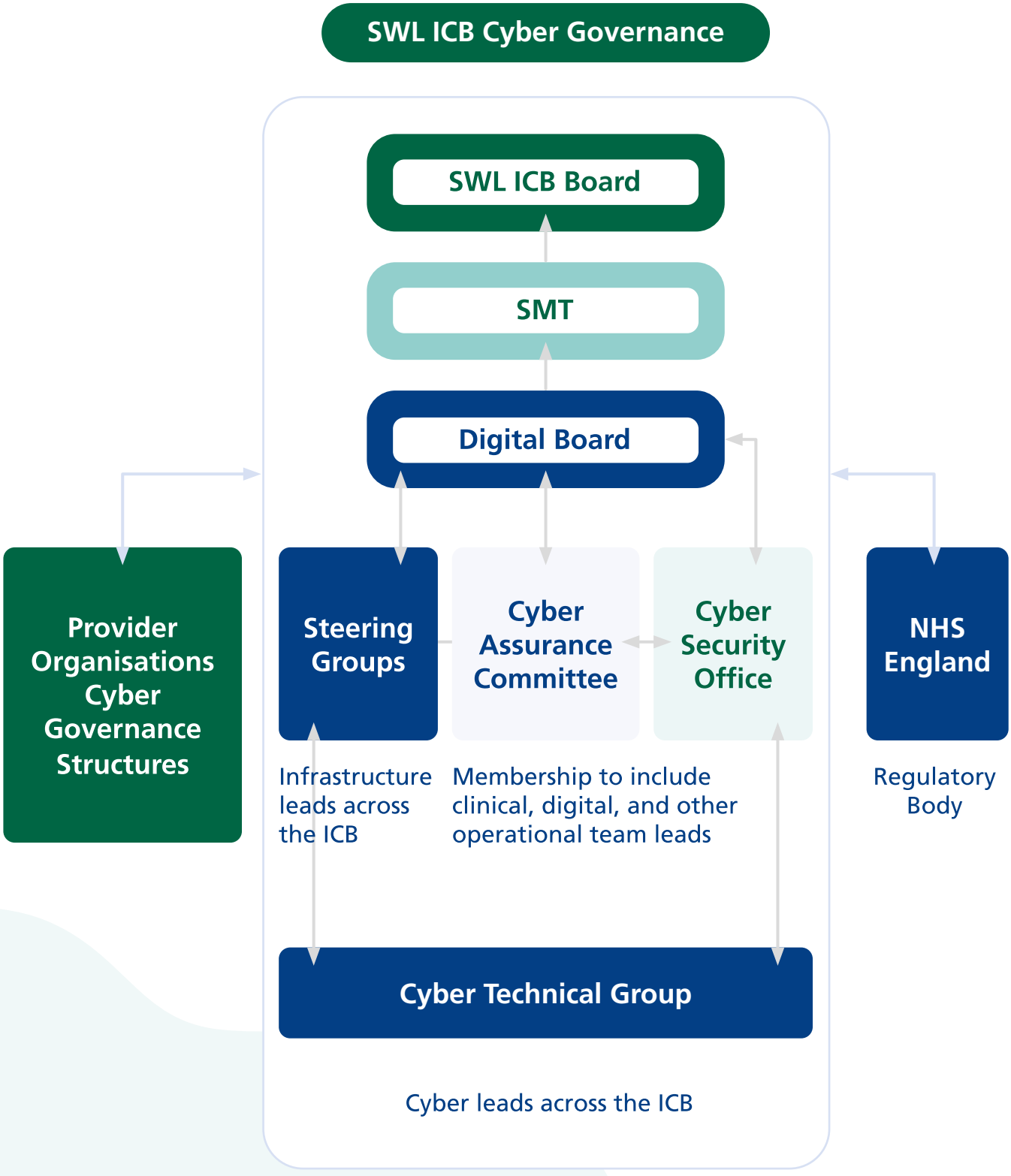
Cyber training and awareness to be standardised across SWL ICB, ensuring consistency in content and delivery while allowing individual organisations to retain responsibility for execution. By encouraging the adoption of NHS England's Training and Awareness services, we will establish a joined-up approach, enabling seamless transitions for staff moving between organisations and promoting a unified understanding of cyber risks and responsibilities across the ICB.

How this might be achieved?

Create a cyber training and awareness policy and plan	Conduct cyber training needs assessment to identify gaps in knowledge and resource.	Create a process to track and report cyber training compliance across the ICB.

Governance and Accountability

Proposed Governance and Accountability



SWL ICB Cyber Security Governance

What will each group do? (1/2)

SWL ICB Cyber Security Governance framework outlines the roles and responsibilities of key groups responsible for overseeing, guiding, and implementing cyber security across the ICB. This governance structure ensures accountability, strategic alignment, and operational effectiveness in managing cyber risks and safeguarding essential services. Each group plays a distinct role in driving the success of the ICB cyber security strategy, from high-level oversight to day-to-day implementation and assurance.

ICB Board

- Has overall accountability for the strategic direction and oversight of cyber security within the ICB.
- Approves the cyber security strategy and risk management framework.
- Receives high-level reports on the ICB cyber security performance and major incidents.

Digital Board

- Provides strategic direction for digital transformation and oversees the implementation of the cyber security strategy.
- Receives reports from the Cyber Assurance Group.
- Ensures alignment of cyber security considerations with digital transformation initiatives.

Cyber assurance Committee (CAC)

- Provides independent assurance on the effectiveness of cyber security controls and risk management processes.
- Reviews and approves cyber security policies and procedures.
- Maintain close engagements with the Cyber Security Office.
- Reports into the Digital Board.

Senior Management Team (SMT)

- Responsible for the key decisions and recommendations to the board on the cyber and digital transformation strategies
- Provide executive level oversight of all the programs happening across the ICB.

What will each group do? (2/2)

Cyber Technical Group

- Provide technical advisory on cyber security to CSO and DISG
- Provide collaboration platform for cyber leads across the ICB.

Steering Groups

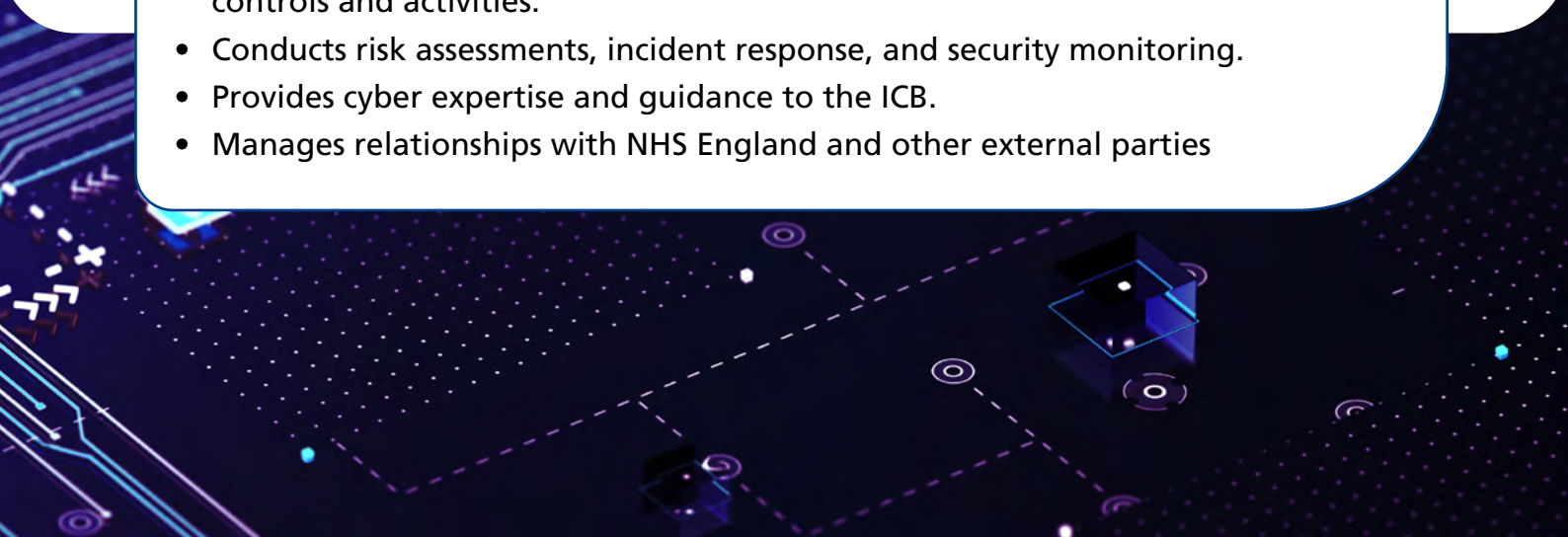
- Support efforts to improve cybersecurity within their respecting domains including digital infrastructure, data, clinical, etc.

NHS provider organisations

- Continue to own and manage their cyber risks just as they do now.
- Notify the ICB of local cyber risks with the potential to cause the greatest harms.
- Support and participate in all SWL cyber initiatives and activities.
- Provide assurance on the effectiveness of their security controls to the ICB.
- Adopt this strategy and demonstrate alignment of local initiatives and controls

Cyber Security Office (CSO)

- Responsible for the day-to-day implementation of cyber security strategy, controls and activities.
- Conducts risk assessments, incident response, and security monitoring.
- Provides cyber expertise and guidance to the ICB.
- Manages relationships with NHS England and other external parties



What will each role do? (3/3)

SIRO

- Ensures cyber security is integrated into the ICB/ICS overall risk management and governance framework.

Board Executive

- Champions cyber security at the ICB/ICS board, ensuring that appropriate investments to deliver this strategy are considered by the board.

CDIO

- Oversees ICB/ICS cyber security investment and budget.
- Ensures alignment of cyber security with ICB/ICS-wide business strategy and operations.
- Owns ICB/ICS-wide digital risks.

CCIO

- Leads the integration of ICB cyber security, into digital health initiatives to safeguard patient data and system integrity.
- Ensures security measures are seamlessly embedded in clinical workflows, balancing protection with operational efficiency.
- Advocates for a cybersecurity-conscious culture across all clinical strategic and operational teams.

CISO

- Leads/directs the delivery of the ICB cyber strategy, including the development of action plans, policies, standards, and guidelines.
- Oversees the Cyber Security Office and services provided to NHS provider organisation.
- Provides subject matter expertise and assurance to the board on the effectiveness of cyber security controls across the ICB.

Deputy SIRO

- Oversees data protection compliance across the ICB, collaborating with DPOs from NHS provider organisations.
- Ensures alignment of cyber security with ICB/ICS-wide business strategy and operations.
- Offers guidance on ICB-wide Data Protection Impact Assessments (DPIAs).

Chairs of Committees/Groups

- Oversees activities of respective committees/groups, ensuring initiatives align with cyber security requirements and best practices.
- Champions the adoption of cyber security best practices within their respective committees/groups.

Divisional Leads

- Oversees the management of risks (areas including cyber security risks) in their respective and provides assurance on local risk treatment measures.
- Champion the adoption of this strategy in their respective business areas and provides assurance on local controls.

Cyber Lead

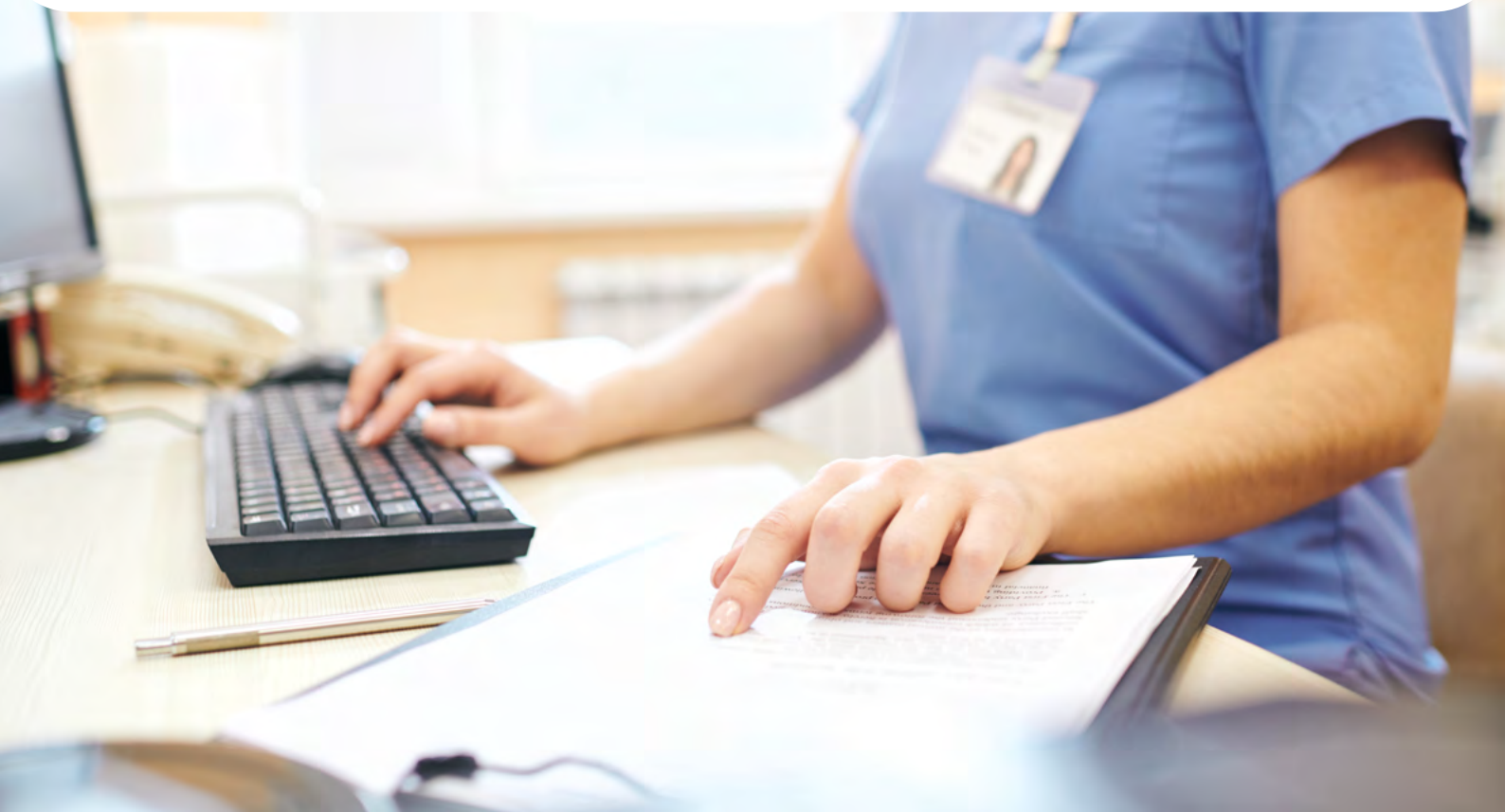
- Develops and implements the organisation's cybersecurity policies, risk assessments, and compliance frameworks.
- Acts as the primary liaison between the technical security team and senior leadership, providing updates on cyber threats and mitigation plans.

Cyber Specialist

- Monitors, detects, and responds to cyber threats, ensuring the security of systems, networks, and data.
- Implements cybersecurity controls, tools, and frameworks to safeguard against evolving threats.

All Staff

- Takes personal responsibility for own security and the security of the organisation's assets under/within your management and control.
- Comply with policies, standards, and guidelines, and report risks, incidents, and breaches.
- Be a cyber champion for the organisation.

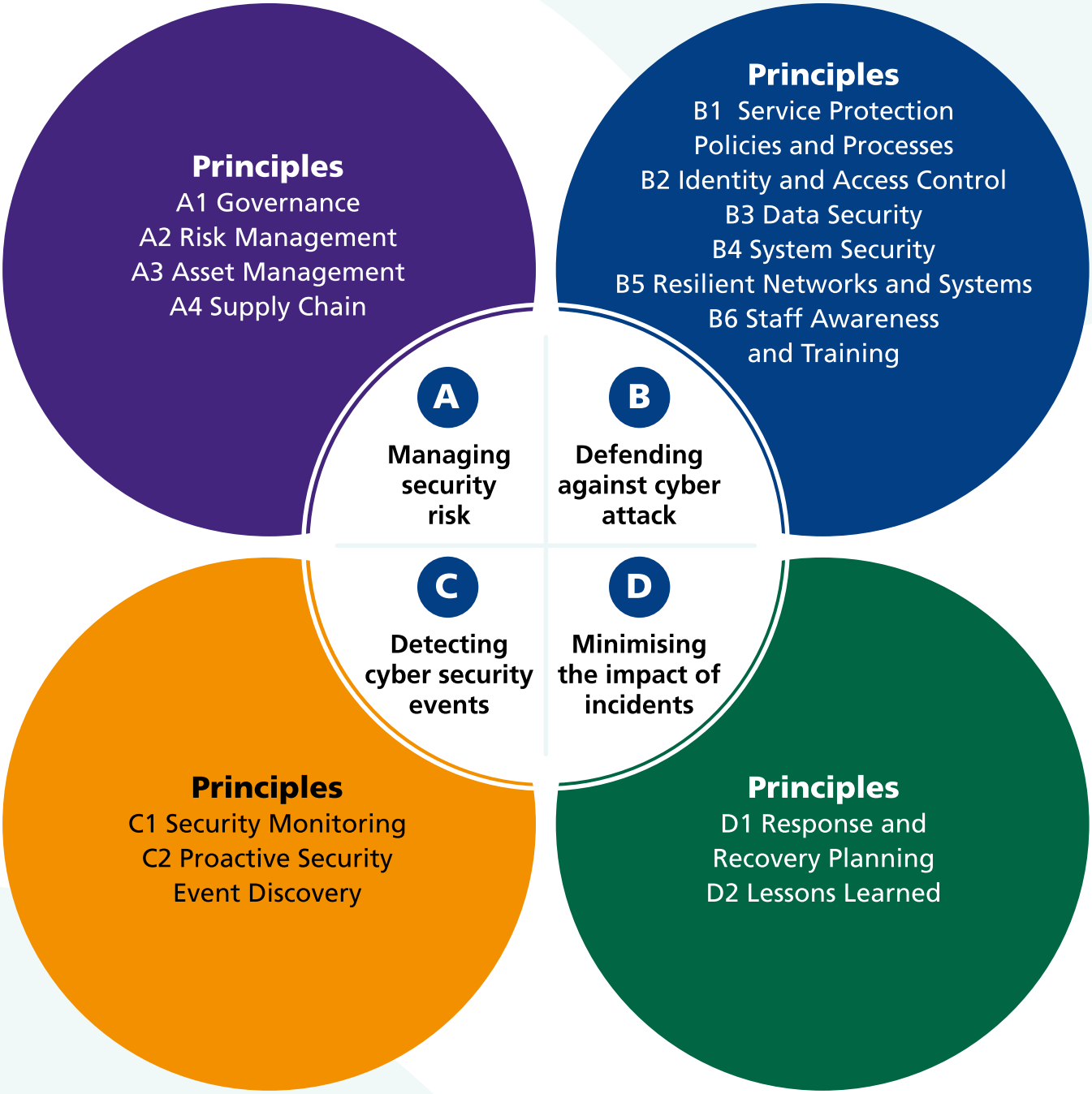


Aligning with National Direction

Alignment

Our goal is to strengthen the collective cyber security posture across SWL ICB while aligning with the DHSC Cyber Security Strategy, the overarching SWL ICB mission and vision, and the objectives of the ICB Digital Strategy.

Our strategic direction for cyber security aligns with national direction (DHSC) and the NCSC Cyber Assessment Framework



The Cyber Assessment Framework (CAF) identifies four overall security objectives that are supported by the above 14 principles.

Health & Social Care Cyber Security Strategy

The DHSC cyber strategy to 2030 sets out an approach to cyber resilience that will apply across health and social care systems, including adult social care, primary care, secondary care and the critical supply chain.

The aim is for all health and social care organisations to achieve cyber resilience no later than 2030. Below are its strategic pillars:

Health & Social Care Cyber Security Strategy

Five pillars, which have been developed collaboratively across the sector, will support every organisation in meeting this vision for a cyber-resilient health and social care sector, complementing one another in setting out the approach. They will enable a focus on the change's organisations and teams across health and social care can prioritise to improve cyber security over the long term.

Focus on the Greatest Risks and Harms

Mitigating the greatest risks in health systems by ensuring critical assets and services are protected. By 2030, the sector aims for enhanced risk understanding, improved threat visibility, proportionate mitigations, and robust use of NIS regulations. National, regional, and ICB teams.

Defend as One

Leveraging NHS scale and collaboration to enhance cyber resilience. By 2030, it aims for integrated sector-wide approaches, coordinated threat detection, clear risk accountability, and localised implementation of national strategies, supported by strong partnerships and shared resources.

People and Culture

Building a robust cyber security culture across health and social care. By 2030, it aims to establish cyber security as a vital profession, foster a 'just culture,' grow the workforce, and ensure all staff understand their role in cyber resilience.

Build Secure for the Future

Focus on embedding security into the health and social care system's design. By 2030, it aims for secure-by-design services, resilient supply chains, and clear, aligned standards. Collaboration, supplier engagement, and proactive governance are key.

Exemplary Response and Recovery

Focus on minimising the impact of inevitable cyber attacks through preparedness and rapid recovery. By 2030, it aims to ensure rehearsed response plans, robust incident management, and improved resilience across all levels of health and social care.

How we Align with DHSC Cyber Security Strategy

Each of the five pillars explains how we will achieve our goals. Some of these approaches fall under the responsibility of SWL ICB to lead and implement, forming an integral part of our SWL ICB Cyber Security Strategy and its associated actions.

Shared Understanding of Risks: SWL ICB will establish a unified approach to identifying and managing cyber risks across all NHS provider organisations, ensuring consistent awareness and response.

Increased Visibility of the Attack Surface: Comprehensive asset management and real-time monitoring will provide full visibility into vulnerabilities across SWL's digital estate.

Proportionate Cybersecurity Mitigations: Security measures will be prioritised and scaled based on risk assessments to protect critical systems without overextending resources.

Effective Use of NIS Regulations: SWL ICB will ensure clear understanding and proportionate application of NIS regulations to strengthen the resilience of essential health services.

Collaborative Cybersecurity Efforts: SWL ICB will strengthen partnerships among its NHS provider organisations to share data, resources, and best practices for enhanced collective cyber resilience.

Coordinated Threat Intelligence: SWL ICB will integrate with national threat intelligence networks to ensure rapid detection, response, and communication of cyber threats across the sector.

Clear Accountability for Cyber Risks: SWL ICB leadership and boards will adhere to nationally defined accountability standards, understanding their responsibility for managing local cyber risks and sector-wide impacts.

Optimal Use of Cybersecurity Services: SWL leaders and boards will actively leverage available national and regional cybersecurity services to mitigate the most significant risks to essential services.

Recognition of Cybersecurity as a Vital Profession: SWL ICB will promote cybersecurity as a critical and valued profession within the health and social care sector.

Attracting and Retaining a Diverse Workforce: SWL ICB will implement inclusive recruitment and retention strategies to build a skilled and diverse cybersecurity workforce.

Championing a Just Culture: SWL ICB will foster a 'just culture' that encourages transparency, learning, and accountability in cyber incident reporting and response.

Universal Cybersecurity Responsibility: SWL ICB will ensure all staff understand their individual roles in maintaining strong cybersecurity practices and actively contribute to safeguarding systems and data.

Understanding Emerging Risks: SWL ICB will proactively identify and manage emerging cyber risks through continuous monitoring and adaptive risk management strategies.

Managing Critical Supply Chain Risk: SWL ICB will strengthen supply chain security by implementing rigorous risk assessments and resilience measures across critical health and social care suppliers.

Secure by Design Services: All new services and technologies within SWL ICB will be developed and implemented with security embedded from the outset.

Clear and Aligned Standards: SWL ICB will adopt clear, well-understood security standards aligned with the Cyber Assessment Framework (CAF) to ensure effective cyber resilience.

Coordinated Incident Response: SWL ICB will align with national and regional cyber response frameworks to ensure rapid, unified action during cyber incidents.

Protected Patient Care Services: Critical healthcare systems will be prioritised and safeguarded to maintain uninterrupted patient and service user care during cyber disruptions.

Robust Recovery Plans: SWL ICB will implement tested disaster recovery and business continuity plans to quickly restore services after a cyber attack.

Continuous Communication: Clear communication channels will be established across all levels to provide timely updates and guidance during cyber incidents, reducing confusion and service disruption.

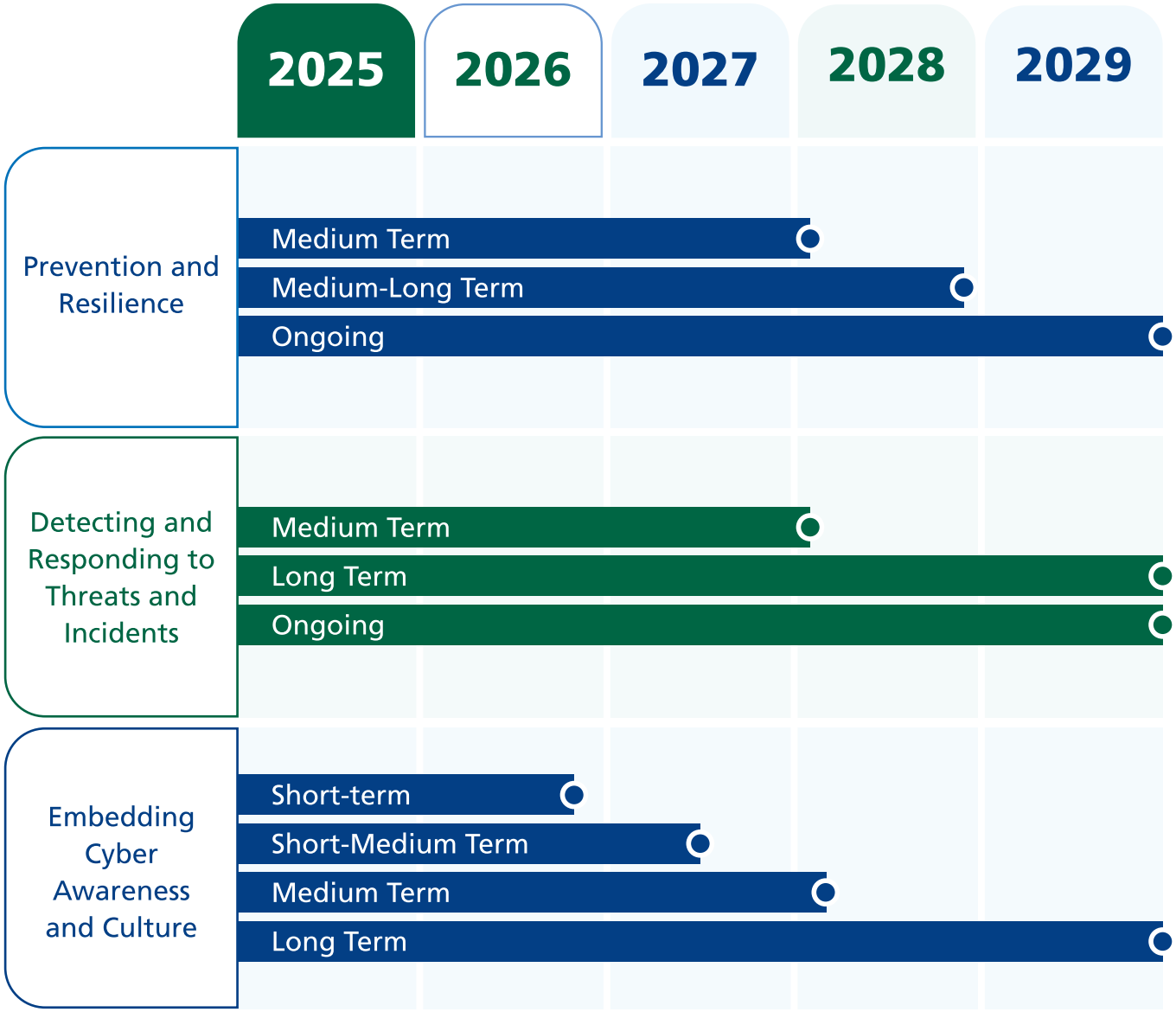
Cyber Security Frameworks Alignment

SWL ICB Strategy Objective	DSPT-CAF Objective/ Principle	DHSC Cyber Security Strategy Pillar	NIST CSF Function	What Good Looks Like
Strengthening Governance	A – Managing Risk	Focus on the Greatest Risks and Harms	Govern	Well Led
Managing Cyber Risk	A – Managing Risk	Defend As One Focus on the Greatest Risks and Harms	Identify	Safe Practice Improve Care
Understanding Critical Systems and Suppliers	A – Managing Risk	Focus on the Greatest Risks and Harms	Identify Protect	Safe Practice
Embedding Cyber Awareness and Culture	B – Preventing Against Cyber-Attack and Data Breaches	People and Culture	Protect	Support People
Prevention and Resilience	B – Preventing Against Cyber-Attack and Data Breaches D – Minimising the impact of Cyber Incidents	Build Secure for the Future	Protect Recover	Ensure Smart Foundations
Detecting and Responding to Threats and Incidents	C – Detecting Cyber Incidents D – Minimising the impact of Cyber Incidents	Defend as One Exemplary Response and Recovery	Detect Respond Recover	Safe Practice

Roadmap to Implementation

SWL Cyber Roadmap 2025-2030 (1/2)

SWL Cyber Roadmap 2025-2030 (2/2)



How We Measure Success

Objectives	Parameters	Our Ambition	Tracking Cycle
Strengthening Governance	Percentage of governance group meetings attended by key representatives.	90%/year	Quarterly
	Percentage of actions arising from governance meetings completed within agreed timelines.	80% YR1, 90% onwards	Quarterly
	Percentage of ICB board members and key governance group members completing cybersecurity training.	100%	Annually
Managing Cyber Risk	Percentage of organisations conducting cyber risk assessments aligned with ICB guidelines.	100%	Annually
	Percentage reduction in high-severity vulnerabilities identified through monitoring tools.	50% YR1, 75% onwards	Annually
	Percentage of critical suppliers assessed for cybersecurity risks.	100%	Annually
Embedding Cyber Awareness and Culture	Percentage of staff across all organisations completing mandatory cybersecurity training.	95%	Annually
	Percentage of positive feedback from staff surveys on cybersecurity confidence and awareness.	80% YR2, 90% onwards	Quarterly
	Percentage gaps in cyber skills, competencies and knowledge identified across the IT and/or cyber professionals across the ICB.	30%	Annually
	Number of cyber awareness campaigns launched across SWL ICB NHS provider organisations.	3 per Org per year	Annually
Understanding Critical Systems and Suppliers	Percentage of organisations contributing to the centralised inventory of critical systems and suppliers.	100% YR1, Quarterly Updates thereafter	Quarterly
	Percentage of critical systems and suppliers with interdependencies identified and documented across the ICB.	80% mapped YR1, 100% thereafter	Annually
	Percentage of critical suppliers engaged through an ICB-wide risk management and engagement framework.	100% by YR5	Annually
	Percentage of third-party suppliers with security ratings classed as high risk.	20% YR1, 10% YR2, 5% YR3, 1% thereafter	Quarterly
	Number of third-party suppliers which have had security incidents identified through formal and agreed notification processes.	To gain visibility and assurance on mitigation	Quarterly
	Number of third-party suppliers which have had security incidents identified through ICB assurance activities.	To gain visibility and assurance on mitigation	Annually
Prevention and Resilience	Percentage of organisations meeting baseline security controls (e.g MFA, patch management, secure endpoints).	90% YR1, 100% thereafter	Quarterly
	Number of ICB-wide tabletop or simulation exercises conducted annually.	1 per year, with 80% provider participation	Annually
	Percentage of organisations completing resilience benchmarking assessments annually.	100%	Annually
Detecting and Responding to Threats and Incidents	Percentage of organisations integrated into a centralised threat detection system over the strategy lifecycle.	20% YR2, 50% YR4, 80% YR5	Annually
	Number of cyber security alerts issued by NHS ‘Respond to an NHS Cyber Alert’ not responded to within the agreed timeframe.	0	Quarterly
	Percentage of organisations adopting the standardised ICB incident response framework.	100%	Annually

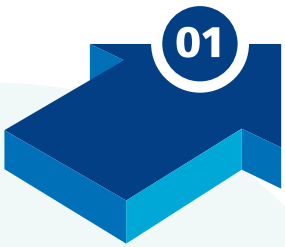
SWL Cyber Roadmap 2025-2030 (1/2)

Now that we have a clear direction for the next five years to improve collaboration among our NHS provider organisations and centralise cyber security controls and capabilities across the ICB, the following actions outline our next steps to turn these ambitions into reality and secure the necessary support to move forward.

Commence implementation and continually review.

Establish and follow an agreed cadence for the review of the strategy, tracking the progress of its implementation and measuring the impact across SWL ICB.

Following approval and any necessary amends, publicise and socialise the Cyber Security Strategy with relevant stakeholders and communities.



Share the draft SWL ICB Cyber Security Strategy with senior leadership teams and the ICB Board for review and approval.

Partnerships and Collaboration

Partnerships and Collaboration

Partnerships and Collaboration is critical for strengthening SWL ICB cyber security posture. Collaboration across our NHS provider organisations, arm-length bodies, third-party vendors, and national bodies will help drive resilience, innovation, and efficiency in our collective cyber defence.

Workforce and Community Collaboration

Staff and Leadership Engagement:

- **We will encourage collaboration between all teams including** IT/Digital, clinical, and other business operational teams to build the strong cyber-aware culture we seek.
- **Develop joint training programmes** with NHS provider organisations and professional bodies like BCS, The Chartered Institute for Cyber Security, etc.

Partnerships with National and Regional Bodies

- **We work closely with relevant government Institutions** on many fronts including coordinating cyber responses, funding, and in the development of this cyber strategy.
- **We utilise NHS England's funded tools** and resources to improve technical defences (e.g., NHS Secure Boundary and Cyber Alerts), and hope to improve uptake of these services in future.

Engagement with Third-Party Vendors

- **We will continue to engage with responsible vendors who share our values and objectives** to deliver on this cyber strategy. **This will be governed by robust policies for third-party suppliers** in line with NHS guidelines.
- **We continue to assess vendor compliance** with security standards such as, NCSC CAF, and NHS Data Security and Protection Toolkit (DSPT).

Funding Approach and Resourcing

Proposed Funding Approach

The successful implementation of our Cyber Strategy will rely on a coordinated and sustainable funding model that leverages existing resources while ensuring alignment with the objectives of this strategy.

NHS provider organisation Funding

Each NHS provider organisation will continue to fund its cyber security initiatives through current budget allocations. Providers will retain control over their local cyber security investments but will be required to demonstrate how these align with the overarching SWL ICB Cyber Strategy.

Integrated Care Board (ICB) Support

The ICB Board commits to contributing to the realisation of this strategy by allocating its statutory funding to support system-wide cyber security improvements, particularly resources required to effectively coordinate implementation of this strategy.

NHS England Funding

Funding provided by NHS England, earmarked for enhancing security across the ICB, will be centrally managed by the ICB. Decisions regarding the allocation and investment of these funds will be made collaboratively with NHS provider organisations. The ICB will establish mechanisms to ensure that these investments are consistent with the priorities and objectives outlined in the SWL ICB Cyber Strategy.

Economies of Scale and Collaborative Investments

The ICB, in collaboration with NHS provider organisations, will explore opportunities to optimise spending through shared investments. By leveraging economies of scale, SWL ICB can procure shared services, technologies, and solutions that deliver enhanced value and efficiency across all participating organisations.

Accountability and Transparency

A transparent process will be established to monitor and evaluate funding allocation, utilisation, and impact. This will ensure accountability and maximise the value of every investment toward achieving a robust and resilient cyber security posture.

Resource Considerations (1/2)

Capacity

The success of this strategy relies heavily on ensuring sufficient cybersecurity expertise across both NHS provider organisations and the ICB to drive its delivery. SWL ICB will prioritise resourcing and empowering the proposed SWL ICB Cyber Security Office to effectively coordinate and oversee the strategy's implementation. Similarly, NHS provider organisations are expected to allocate the necessary resources to fulfill their roles in achieving the strategy's objectives. As the strategy evolves and capacity needs grow, both the ICB and NHS provider organisations will explore opportunities to allocate investments strategically, prioritising funding to address risks capable of causing the greatest harms.

Personnel

The ICB will ensure that all necessary roles, including SIRO, CDIO, CCIO,CISO, DPO, Cyber Lead, Cyber Specialist and other relevant positions listed in the roles and responsibilities, are in place. This will drive the effective delivery of the Cyber Strategy, ensuring strategic alignment and robust operational execution across the ICB while enhancing cyber security controls and providing assurance to the ICB Board and NHS England.

Talent Exchange

To leverage skills within the ICB, a volunteer scheme will be encouraged, allowing NHS provider organisations to contribute resources and time to the ICB Cyber Security Office. This approach will foster autonomy and support the delivery of the strategy. Supported by an ICB training fund, individuals seeking professional growth will have the opportunity to develop their skills in exchange for dedicating a portion of their time to the central function.

Resource Considerations (2/2)

External factors

The National Security Risk Assessment identifies hostile cyber-attacks on UK cyberspace as a Tier 1 risk, highlighting the critical importance of proactive preparation. Additionally, supply chain and supplier attacks continue to pose a significant threat to operational continuity and service delivery.

Certain external factors influencing cyber risks within the ICB remain beyond our direct control. This strategy ensures that the ICB remains resource prepared to adapt and respond effectively to such external influences, supporting dynamic risk management and resilience across the system.

These factors, categorised under the PESTLE framework, highlight areas where external shifts could impact our ability to safeguard essential services:

Political

Changes in political priorities, policies, or manifestos may alter the focus on certain activities and services, requiring agility to adapt to new directives.

Legal

Evolving legislation, regulations, and compliance requirements necessitate ongoing adjustments to maintain adherence to standards and obligations.

Economic

Funding constraints and broader economic challenges may impact resource allocation for cyber security programmes.

Social

Changes in population behaviour, demographics, and expectations can influence healthcare delivery and, in turn, the cyber risks associated with supporting systems.

Environmental

Factors such as climate change, physical infrastructure risks, and environmental policies may indirectly influence cyber preparedness and resilience.

Appendices

Acronyms

SWL:	Southwest London
NCSC:	National Cyber Security Centre
CAF:	Cyber Assessment Framework
DHSC:	Department of Health and Social Care
DISG:	Digital Infrastructure Steering Group
DLT:	Digital Leadership Team
ICS:	Integrated Care System
IG:	information Governance
NCSC:	National Cyber Security Centre
ICB:	Integrated Care Board
NHS:	National Health Service
TOM:	Target Operating Model
PESTLE:	Political, Economic, Social, Technological, Legal and Environmental
DNS:	Domain Name System
SIEM:	Security Information and Event Management
SIRO:	Senior Information Risk Owner
e.g:	Example
CISO:	Chief Information Security Officer
BCS:	British Computer Society
CAG:	Cyber Assurance Group
CIS:	Center for Internet Security
IT:	Information Technology
CSC:	Critical Security Controls
CNI:	Critical National Infrastructure
MFA:	Multi-Factor Authentication
CCIO:	chief Clinical Information Officer
TOM:	Target Operating Model
DSPT:	Data Security and Protection Toolkit
CTG:	Cyber Technical Group
CSO:	Cyber Security Office
CAC:	Cyber Assurance Committee
CDIO:	Chief Digital Information Officer
DPO:	Data Protection Officer

Glossary of Key Terms

Individuals: The recipients of Health and Care services in SWL.

Critical Systems: IT /Digital systems essential to delivering healthcare services (e.g., Electronic Patient Records, Medical Devices, etc).

Cyber Resilience: The ability to prepare for, respond to, and recover from cyber incidents while maintaining operations.

Third party suppliers: This means any organisation providing goods or services to SWL ICB.

Health and social care leaders: This means those with oversight responsibilities of health and social care organisations, from local leadership teams to boards and their directors. Health and social care leaders are responsible for the cyber risk held by their organisation and will be held accountable in line with national performance frameworks.

Foundational Controls: These represent the essential baseline cyber defenses that all SWL ICB organisations will adopt. They include:

Identity and Access Management – (e.g Privileged Access Management, Password and MFA protections, Effective Account Lifecycle Management, etc

Malware Protection – (e,g Antivirus, Extended Detection and Response (EDR), etc)

Perimeter/Gateway Protections – Layered defence approach - (e,g Firewalls, Email/Web, DNS, etc)

Security Event Logging – (e.g SIEM, etc.)

Vulnerability Management – (e.g. updates/patching, etc)

Network protections – (e.g segmentation, port and protocol controls, etc)

Data Recovery Capabilities – (e.g Immutable Backup)

Data Protection – (e.g. Secure encryption, integrity protections, loss prevention, least privileged/need-to-know, etc.)

Secure Configuration of IT/Digital Assets

Assurance Exercises: (e.g Penetration tests, simulations, etc.)