

CYBERSECURITY ADVISORY & ASSURANCE SERVICES

Independent advisory support to
strengthen cybersecurity governance, risk
management and assurance across NHS
and public sector organisations.

Delivering Meaningful Impact
Across NHS Healthcare



Cybersecurity Advisory & Assurance Services



Introduction



Cybersecurity is a critical consideration for NHS and public sector organisations operating in increasingly complex digital environments. Effective cybersecurity requires clear governance, proportionate risk management and informed decision-making aligned to organisational objectives, regulatory expectations and operational realities.

Cybersecurity Advisory & Assurance Services provide independent, buyer-side consultancy support to help organisations understand their current cybersecurity posture, strengthen governance and assurance arrangements, and plan proportionate improvements. Services are advisory in nature and are designed to support informed decision-making without assuming responsibility for live security operations, incident response or managed security services.

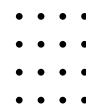
Why St. Vincent's Consulting



St. Vincent's Consulting supports NHS and wider public sector organisations at critical points of digital, clinical and organisational change, where cybersecurity decisions are complex, scrutiny is high, and the margin for error is small. Our role is to provide objective, independent advice that supports clarity, confidence and appropriate oversight.

We act in the buyer's interests, not those of technology vendors or managed service providers. Our approach combines practical experience of complex digital programmes with a strong understanding of public sector governance, clinical safety and information assurance, enabling organisations to strengthen cybersecurity arrangements while retaining ownership and accountability.





Why buyers typically use this service



- Seeking an independent assessment of cybersecurity posture and maturity
- Strengthening governance, assurance and risk management arrangements
- Undertaking major digital change, recovery or transformation activity
- Preparing for internal or external review, audit or regulatory scrutiny
- Requiring proportionate cybersecurity assurance without introducing managed services

Engagements typically support:

- Clearer understanding of current cybersecurity posture and priority risks
- Improved confidence in governance, assurance and decision-making
- Practical, proportionate improvement recommendations aligned to organisational context
- Strengthened internal capability and clarity on next steps

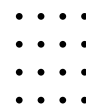
Service Overview

Cybersecurity Advisory & Assurance Services provide structured, modular advisory support focused on cybersecurity strategy, posture assessment, governance, assurance and capability development. Services may be commissioned individually or combined, depending on organisational requirements and risk profile.

All services are delivered on an advisory basis. Services exclude cybersecurity operations, monitoring, tooling deployment, vulnerability scanning as a managed service, incident response, recovery activity and managed security provision.

In practice, this means providing clear, proportionate advice that supports informed cybersecurity decisions without creating operational dependency.





Service Features & Capabilities



Cybersecurity Strategy & Posture Advisory

Organisations often require independent support to define a cybersecurity strategy and understand the current security posture in relation to organisational objectives and risk appetite.

Key features include:

- Review of cybersecurity strategy and alignment with organisational priorities
- Advisory input to posture and maturity assessment
- Identification of key risks, gaps and dependencies
- Support for prioritisation and roadmap development



Cyber Risk & Assurance Advisory

Effective cyber risk management depends on clear governance, proportionate controls and independent assurance.

Key features include:

- Advisory input to cyber risk identification and assessment
- Review of governance, controls and assurance frameworks
- Support for risk reporting and assurance documentation
- Alignment with organisational governance and escalation processes

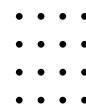
Architecture & Design Assurance (Cybersecurity)

Cybersecurity considerations must be embedded within digital and technical architectures to reduce risk and support sustainable delivery.

Key features include:

- Advisory review of security architecture principles and design approaches
- Identification of security risks and design considerations
- Support for informed decision-making within approval and assurance processes





Capability Development & Knowledge Transfer



Sustainable cybersecurity capability requires clear roles, skills development and embedded governance rather than reliance on external operations.

Key features include:

- Advisory input to cybersecurity capability and skills assessment
- Support for defining roles, responsibilities and governance arrangements
- Knowledge transfer and mentoring to support internal capability development

Cybersecurity Assurance Interventions (Advisory-Led)

In some circumstances, targeted advisory-led cybersecurity assurance interventions are required to inform governance and assurance activity while retaining organisational ownership and accountability.

Key features include:

- Advisory input to vulnerability assessment findings and remediation planning (based on third-party or internal assessments)
- Cyber Essentials and Cyber Essentials Plus preparation and assurance support
- Advisory input to penetration testing programmes and interpretation of findings
- Virtual Chief Information Security Officer (vCISO) advisory support

User Information, Guidance and Support

Buyers are provided with appropriate guidance, documentation and advisory outputs throughout engagements. This may include briefing materials, analysis outputs, assurance reports and recommendations to support auditability and internal ownership.

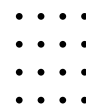
Onboarding and Offboarding

Onboarding activities confirm scope, objectives, governance arrangements and information requirements. Offboarding includes structured handover of advisory outputs and recommendations following engagement completion.

Availability and Delivery Model

Services are delivered in collaboration with buyer stakeholders and operate within established governance frameworks. Engagements may be delivered remotely, on-site or through blended delivery models, depending on programme requirements.





Pricing and Commercial Information



Pricing is provided on a time-and-materials or fixed-price basis, depending on engagement scope and duration. Pricing details are published on the Digital Marketplace.

The service does not include system implementation, live system operation or managed services.

Certifications and Standards

Where applicable, service delivery takes account of recognised public-sector standards, guidance and best practice relating to digital transformation, architecture, estates programmes and assurance. This may include alignment with NCSC guidance, DSP Toolkit requirements, ISO 27001 and Cyber Essentials, where relevant to buyer context.

Procurement Information

Cybersecurity Advisory & Assurance Services are available to NHS and wider public-sector organisations through the G-Cloud 15 framework, under Lot 3 (Cloud Support).

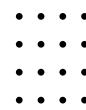
Services may be procured directly via the Digital Marketplace in accordance with the G-Cloud framework rules. Buyers may award Call-Off Contracts without further competition where the service meets their requirements.

Further information on service scope, pricing and engagement options is available via the Digital Marketplace.

Additional Information

Further information, including service features, pricing and engagement options, is available via the Digital Marketplace. Buyers may request additional information to support evaluation and Call-Off Contract award in accordance with the Framework Contract.





East and North Hertfordshire NHS Trust Cybersecurity Recovery and Advisory Support During EPR Go-Live

Context

East and North Hertfordshire NHS Trust experienced a significant ransomware cyber incident at a critical point during the go-live of its Electronic Patient Record (EPR) programme. The incident created heightened operational, clinical safety and organisational risk, requiring rapid recovery activity alongside continued delivery of a major digital change programme.

The Trust required independent, senior cybersecurity advisory support to help stabilise governance, maintain assurance and support informed executive decision-making during a highly constrained and high-pressure period.

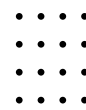
Advisory Support Included:

- Independent advisory leadership and coordination support during cybersecurity recovery activity
- Advisory input to programme replanning, risk management and assurance while operating in a constrained operational environment
- Support to executive reporting, governance forums and decision-making processes to maintain oversight during parallel cyber recovery and EPR activity

Impact:

- Maintained effective governance and assurance during a major cyber incident and live EPR go-live
- Supported programme stabilisation while preserving appropriate risk oversight and executive confidence
- Enabled informed, proportionate decision-making at Trust leadership level during one of the most challenging phases of delivery





Large NHS Trust Cybersecurity Posture Review and Assurance Advisory

A large NHS Trust required an independent assessment of its cybersecurity posture against recognised standards.

Advisory support included:

- Cybersecurity posture and maturity assessment
- Assessment against DSP Toolkit, ISO 27001, Cyber Essentials Plus and NCSC guidance
- Advisory input to governance, assurance and improvement planning, including vCISO support

Impact:

- Improved visibility of cybersecurity risks and maturity gaps
- Strengthened governance and assurance arrangements

