Shared vision **Better together**

NHS Shared Business Services

Cyber Security Services

Reference: SBS/19/CW/ZMD/9348

When does the framework start?

12th May 2020 – 11th May 2022 (with option to extend to 2024)

Who can take advantage?

NHS, Local Authorities, Emergency Services, Education sector and all Public Sector Organisations located across the UK nations (England, Scotland, Wales, Northern Ireland)

Overview

This new framework offers external support services to help NHS and wider public sector organisations manage cyber risks and recover in the event of a cyber security incident.

Through design, delivery, testing, governance and assurance it enables service continuity in patient care by ensuring patient data is secured and critical services and systems remain available.

- **Lot 1** Emergency Cyber Incident Management
- **Lot 2** Cyber Security Consultancy Services
- **Lot 3** Security Personnel

Benefits of using the framework

NHS DIGITAL APPROVED

Supported and approved by NHS Digital with detailed input into specification and evaluation.

EMERGENCY RESPONSE & REGIONAL OPTIONS

Lot 1 provides highly specialised suppliers with ability to offer time-critical response 24/7/365 & enables customers to appoint providers on a regional basis as well as nationally.

END-TO-END CYBER RISK MANAGEMENT

Structured to guide you through your cyber risk management capability development: from emergency incident response, advisory on cyber security compliance, to on-going support from specialist security personnel.

CHOICE OF SUPPLIERS

Twenty-five suppliers to suit all requirements: from SME specialists, to global multi-national providers in a highly specialised marketplace

DIRECT AWARD

Ability to directly award a contract to approved suppliers on the framework.

MINI COMPETITION

Opportunity to run a mini competition to meet bespoke requirements as well as helping to drive further competitive pricing.

PRICE AND SAVINGS

Fixed public sector framework pricing offering competitive rates for consultancy and assurance services.

OJEU AVOIDANCE

A compliant procurement exercise has already been undertaken to offer a simplified procurement route in a complex and crowded market.

MANDATORY CERTIFICATIONS

All appointed suppliers have demonstrated Cyber Essentials Plus or equivalent (e.g. ISO27001)

Find out more
0113 307 1535

Sign up to access this framework: Frameworks Portfolio

Queries Email: NSBS.contractenquiries@nhs.net

Cyber Security Services

Reference: SBS/19/CW/ZMD/9348

Which suppliers are on the framework?

SUPPLIERS			
Accenture	CGI	Green Park Interim & Executive Search	NCC Group
Advent IM	Commissum	KPMG	PA Consulting
Airbus Defence & Space	DXC Technology	Leonardo	PWC
Auriga Consulting	Deloitte	Logicalis	QinetiQ
BSI Cybersecurity and Information Resilience	Ernst & Young	Mersey Internal Audit Agency	Softcat
Cancom Managed Services Ltd	Evodia	MTI Technology	Trustmarque (part of Capita)
CCL Forensics			

Scope of the framework: Lot Structure

LOTS
Lot 1 Emergency Cyber Incident Management Includes provision of urgent incident response capability for large-scale or local incidents, with the ability to quickly draw down expert skills and resource 24/7/365. Particularly useful to support incident control, containment, resolution and remediation in the event of a Cyber Security Incident.
Lot 2 Cyber Consultancy Services Delivers specialist support needed to enhance an organisation's cyber credentials, including Data Security On-Site Assessments, Security Testing, Technical Assurance, Forensics and Investigations, Policy Development, Awareness and Training. Particularly useful for any organisation that has a requirement to access ad-hoc or ongoing advisory support often strategic in nature with well-defined outcomes.
Lot 3 Security Personnel Includes supply of specialist personnel to support and augment existing in-house capability. Requirements are anticipated to be wide ranging and of a more routine nature. This lot will ultimately support organisations to reduce their exposure to threats, improve security defences and provide resource support to respond to cyber incidents.