

Cyber Services Healthcare

Service Category: Security Services, Cloud Support Services

About Our Service

Frazer-Nash delivers comprehensive cyber services to empower health and social care organisations and MedTech to secure and manage their cloud-enabled services. We integrate people, processes and technology and apply our industry expertise with innovations to protect patient data, maintain compliance and strengthen resilience across healthcare supply chains.



Service Features

Cyber strategy and governance for cloud-enabled health care systems

Systems-based engineering approach to solve healthcare challenges

Model-based approach to enterprise and technical architecture

Enable transformation with secure MedTech e.g. AI diagnostics support

Socio-technical system analysis to understand threats, vulnerabilities and risks

Technology strategies and roadmaps to streamline migration plans

Network and information systems design and assurance of patient data

Installation security and accreditation of secure facilities

Data analytics and modelling to optimise decision-making and risk mitigation

Medical supply chain security analysis and assurance

Service Benefits

Accelerate digital health technology with confidence in security and resilience

Increase confidence in managing cyber risks and compliance obligations (DSPT)

Improve decision capacity with robust, transparent and actionable insights

Reduce expenditure through implementing models to solve complex challenges

Efficient design of services and business through architectural design

Improve understanding and mitigation of cyber-related threats to your business

Adopt an agile approach to information assurance for evolving needs

Improve confidence in healthcare systems and supply chain security

Empower your care workers with transferred skills and knowledge

Achieve Secure by Design principles across technology, facilities and processes

Detailed Service Definition

What is cyber?

Cyber refers to the virtual domain created by the connection of information systems, networks and services. Cyber encompasses human interaction with these systems, as well as machine-to-machine interactions and related digital and physical healthcare processes.

Detailed Service Definition (continued)

Our cyber offering

At Frazer-Nash we treat cyber as a global domain within the information environment where entities interact. As such, it may be considered to consist of the virtual environment formed from, or enabled by, information services (including cloud services), and the interdependent networks of information technology infrastructures on which these services run, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. This also includes the complex layers of networked medical devices and legacy technologies. We consider the demands of operating within cyberspace and healthcare holistically and in context, not just from technology perspective, but also considering people and processes and how those facets interact and form dependencies as well as other overriding imperatives like patient wellbeing and safety.

We recognise the need to understand our client's view of the different aspects of cyber and, with our extensive service offerings within this domain, can tailor our services to meet their individual, and often unique, requirements.

Detailed Service Definition (continued)

The range of services we can include in this domain is extensive and includes:

Cyber Strategic Advice – Providing advice across all levels of a healthcare organisation supporting strategy, vision and policies on the threats to data and assets and how to protect them from cyber-attacks. Our advice considers people, processes, information, technology and facilities in countering threats to clinical systems and patient data. Strategies are aligned to NHS Data Security and Protection Toolkit (DSPT) and DTAC (Digital Technology Assessment Criteria).

Cyber Systems Engineering – This is a robust approach to the design, creation and operation of information systems, including healthcare IT, OT, and IoT systems, electronic health records, diagnostic platforms, and connected medical devices. This consists of the identification and qualification of user needs and requirements, creation of alternative system design concepts, design trades, selection and implementation of the best design, verification that the design is properly built and integrated and post implementation assessment of how well the system meets (or met) the user needs. This also includes the principles of Secure by Design, DSPT and DTAC to ensure systems are built securely and sustainably for the expected life of the system and in accordance with the desire risk appetite across the integrated care system and supply chains.

Detailed Service Definition (continued)

Cyber Systems Architecture – This provides the knowledge and skills across the development and acquisition lifecycles to provide environments which require high levels of information security for healthcare systems. This covers the principles of information protection, and the role application technology has in meeting the goal of safeguarding patient data. We support the design and build of secure architectures for electronic health records (EHR), diagnostic platforms, and IoT-enabled medical devices, ensuring resilience against cyber threats and compliance with NHS DSPT, DTAC, and CAF frameworks. A key consideration is the devolution of capability to a services-based architecture of which the cloud is core component to enable innovation and new capabilities for integrated care systems. This can include the design or development of a wider-business Target Operating Model to that improves the resilience of healthcare systems, which alongside technology changes can identify wider-changes needed like user training, clinical safety training, develop and organisational restructuring and policy changes to achieve safe and effective patient care.

Detailed Service Definition (continued)

Post-Quantum Cryptography Consultancy - Frazer-Nash is an NCSC-assured consultancy committed to helping NHS Trusts and other healthcare organisations prepare for the quantum era through discovery, migration and advice services. Our service includes cryptographic asset discovery, quantum risk assessment, and migration planning to quantum-safe algorithms – with the aim to improving the security of patient data systems. We develop adaptive crypto strategies that safeguard patient data and healthcare systems, providing future-proof resilience, compliance with emerging guidance, agility in a changing technology landscape and secure integration across legacy clinical systems and cloud environments.

Artificial Intelligence Cyber Security (incl. AI Diagnostics) - Frazer-Nash empowers organisations in designing and implementing secure AI systems that support health care diagnostics and delivery and are resilient to evolving threats, including adversarial AI attacks and vulnerabilities within medical system supply chains. We provide strategic guidance, rigour risk assessments, and secure development guidance aligned with NCSC, DSIT, ETSI, and NIST standards as well as NHS Standard and DSPT. Our service supports the creation of robust AI security strategies and governance frameworks, which further trust and understanding of AI tools to enable businesses to thrive. Security principles must be embedded throughout the AI lifecycle from model design and deployment through to maintenance, data management and secure disposal. By combining AI-informed strategy and governance with technical assurance with compliance alignment, we enable trusted and sustainable AI adoption across critical and commercial environments. This ensures resilience, accountability, and confidence in AI-driven innovation that can enhance patient care, protect patient safety and maintain compliance.

Detailed Service Definition (continued)

Cyber Risks Assessment and Vulnerability Investigation/Analysis - This provides a detailed understanding of a healthcare organisation's cyber domain, reducing the likelihood and impact of potential threats. This may include undertaking an audit for an organisation against a defined threat such as cryptolocker ransomware targeting patient data and medical devices. We aim to increase a healthcare organisation's cyber awareness, providing cyber security advice and advising on potential strategies and architectures, including hosting capability in the cloud. This could lead to a detailed assessment where Human Factors, Facilities, Information Security (INFOSEC), Penetration (PEN) Testing, and wider subject matter expert (SME) support is required to ensure compliance with standards is maintained.

Communications / Network Design - We plan and design secure, high-performance information and communications networks for healthcare environments, supporting the exchange of sensitive patient data across NHS Trusts, integrated care systems, and MedTech platforms. Our designs accommodate clinical workflows, traffic intensity, and interoperability requirements with legacy devices while enabling the secure and compliant devolution of capability to cloud-based services for electronic health records(EHR) and diagnostics platforms securely. We ensure resilience, compliance with NHS DSPT and CAF frameworks, and robust protection against cyber threats to maintain safe and reliable care delivery.

Detailed Service Definition (continued)

Data Analytics/Modelling - Data analytics is the science of examining raw data with the purpose of drawing conclusions about that information. In healthcare this can use patient records and diagnostics data to enable patient care delivery and inform organisational decisions. Data modelling allows the overall analysis to be presented in a format that is meaningful to everybody. Using both aspects across all areas of the business can enhanced decision-making and rapidly provide insight to inform patient care and organisational decisions. We proactively implement cyber security controls to stay within risk appetite, maintain compliance with standards and DSPT and identify emerging trends or issues.

Facilities / Communications Installation Security / IAM - We provide consultancy for the protection of data and assets within buildings or rooms and associated support infrastructure. We understand and advise on installation, Electro-Magnetic Capability(EMC), Information & Communications Technology (ICT), power and electronic security, Wi-Fi, Bluetooth Low Energy (BLE) and control structure and procedures. We draw on Site Coordinating Installation Authority (SCIDA) and TEMPEST Control Officer (TCO)expertise.

Detailed Service Definition (continued)

Information Security / Assurance - Our information security (INFOSEC) consultants deliver good practice advice and documentation to assure resilient healthcare systems and protection of patient data. We provide mitigations for compromises in confidentiality, integrity, and availability across all healthcare system, including electronic health records (EHR), diagnostic platforms, medical devices, clinical workflows and conventional IT. Our services extend to comprehensive supply chain audits and assessments, ensuring MedTech vendors and integrated care partners meet NHS DSPT, DTAC, and CAF standards and guidance. By addressing cyber security risks across the entire healthcare ecosystem, we strengthen resilience, maintain compliance, and safeguard patient care.

Why Frazer-Nash Consultancy?

Frazer-Nash Consultancy is an independent engineering and technology consultancy with over 35 years' experience delivering high-quality digital and cloud-enabled solutions. We support organisations operating in complex and regulated environments through our collaborative approach and deep expertise in digital engineering, software development and systems integration.

We are **solution and technology-agnostic**. We assess our clients' requirements and provide impartial advice and design solutions based solely on their needs. This independence enables us to select the most appropriate cloud technologies and architectures to deliver secure, resilient and value-for-money outcomes.

Our cloud solutions are informed by experience gained across multiple platforms, sectors and use cases. We combine proven engineering discipline with a strong understanding of integration and whole-system design to support and enable cloud adoption while managing risk and ensuring long-term sustainability.

Our Commitment to Quality

Frazer-Nash is committed to delivering consistently high-quality services and outputs that **often exceed customer expectations**. Quality is embedded throughout our ways of working, from engagement and communication through to delivery and assurance.

We actively monitor progress using our robust, proportionate controls, ensuring key decisions are subject to appropriate challenge. Each project is allocated a dedicated Project Manager, a Project Supervisor who independently reviews and approves monthly reports, and a Project Auditor for ongoing quality assurance.

We ensure accuracy and suitability for purpose of all deliverables, with independent verification by two reviewers. Our Quality Management System is certified to **ISO 9001 and TickITplus** (for software development), providing customers with confidence that our quality standards are externally assured and continuously maintained.

Our Security

Frazer-Nash operates robust security processes and controls suitable for handling sensitive and classified information **above OFFICIAL** up to and including **Top Secret**. Security is embedded across our people, processes and systems, ensuring information is protected throughout delivery.

We support sensitive and critical programmes across government and national infrastructure by applying strict information-segregation controls, including team separation to address security, or conflict-of-interest considerations

All 1500 staff hold **BPSS clearance as a minimum**, with the majority cleared to **SC** and over 225 consultants holding **DV clearance**.

Our IT systems are certified to **ISO 27001** and **Cyber Essentials Plus**, providing assurance that information security risks are proactively managed in line with recognised industry standards.

Our Approach to Subcontracting

Frazer-Nash primarily delivers services through our large base of permanent staff, supplementing this capability where required with trusted partner organisations to provide additional flexibility, specialist expertise and scale while retaining full delivery control.

We are experienced in engaging and managing subcontractors across the full project lifecycle, ranging from sole traders to large multinational organisations. Our structured approach ensures the right supplier is selected for each requirement and integrated effectively into the delivery team.

Our subcontracting processes focus on robust supplier identification and assessment, clear definition of scope, appropriate flow-down of contractual terms and conditions, and proactive risk management. All subcontractors are subject to proportionate commercial and technical due diligence to ensure they meet our standards for security, quality and delivery, enabling us to deliver outcomes on time, within budget and to the required quality.



Resourcing

Frazer-Nash employs over **1,500 technical specialists** across all grades, from **Follow to Set Strategy**, providing depth, continuity and scalability across a wide range of disciplines, backgrounds and experience levels.

To support agile and flexible delivery, our people are organised into defined **technical delivery areas** (including Information Systems, Cyber, Modelling and Software), which are deployed across multiple sectors such as central and local government, policing, health and energy. This structure, combined with strong portfolio, programme and project management (P3M), enables us to actively monitor demand and adapt resourcing throughout the project lifecycle.

We deliver complex requirements efficiently, consistently and at pace by forming tailored, multi-disciplinary teams led by a single accountable Project Manager.

Our consultants regularly work across different sectors, enabling us to cross-pollinate ideas, tools and best practice between domains. Drawing on in-house expertise, such as information security and human factors, we ensure effective and responsive delivery for every client.



Our Commercial Approach

Frazer-Nash adopts a flexible and transparent commercial approach to ensure best value and a model that aligns to each client's specific requirements. We collaborate with customers to clearly define the scope of services and agree a commercial structure that is predictable, proportionate and aligned to your required outcomes and effective delivery.

Depending on the requirement, this may include a **fixed-price model for clearly defined scopes**, or **time and materials using agreed day rates** where flexibility is required to accommodate evolving needs.

For longer-term or ongoing service requirements, and where we have control over resource flexibility, we can also offer a **single blended day rate** covering a range of grades. This provides simplicity, transparency and ease of management while maintaining access to the appropriate skills at the right time.

Next Steps

To discuss your requirements in more detail or request an order for services, please contact ccs@fnc.co.uk

