FRAZER-NASH CONSULTANCY
A KBR COMPANY

Digital Enterprise Risk Management (ERM) - Healthcare

Service Category: Security Services, Cloud Support Services

About Our Service

Comprehensive digital risk assessments, cybersecurity aligned with NHS DSPT and ISO 27001, clinical safety compliance to DCB0129/DCB0160, business continuity planning under NHS EPRR, and real-time monitoring of critical health systems. Embeds governance, interoperability standards, and resilience measures to safeguard patient data, clinical workflows, and operational integrity across UK healthcare organisations.

Service Features

- Comprehensive digital risk assessments across clinical and corporate systems
- Cybersecurity aligned with NHS DSPT, ISO 27001, NCSC CAF
- Clinical safety compliance to DCB0129 and DCB0160 with CSO oversight
- Business continuity planning aligned to NHS EPRR and ISO 22301
- Real-time monitoring of critical health system risk indicators
- Interoperability assurance for FHIR, PRSB, SNOMED CT, medicines dictionary
- Supply chain and third-party assurance for healthcare technology vendors
- Architecture optimisation using TOGAF and open systems principles
- Data protection controls aligned to UK GDPR and DPA 2018
- Embedded governance with SIRO, Caldicott Guardian, and board reporting

Service Benefits

- Reduced clinical safety incidents through proactive risk management
- Improved cyber resilience across NHS and care organisations
- Strengthened data privacy and lawful processing under UK GDPR
- Enhanced continuity and recovery for critical digital health services
- Greater assurance of interoperability and consistent patient record standards
- Reduced supplier and third-party risk across ecosystems
- Clear governance, accountability and reporting for boards and committees
- Faster, safer delivery of digital change and transformation
- Optimised architectures reducing complexity, cost and operational risk
- Embedded risk culture improving decisions and everyday practices

Detailed Service Definition

Our digital enterprise risk management service helps NHS and wider health and social care organisations identify, assess, and mitigate digital risks across clinical and administrative systems, assuring resilience, regulatory compliance, and patient safety.

Scope

- Acute, community, mental health, ambulance, primary care, ICSs and ICBs, arms-length bodies, local authority social care and commissioned providers.
- People, process, information, technology and facilities across whole-system care pathways and shared care records.
- Clinical and corporate systems, infrastructure, cloud platforms, data flows, medical devices and digital therapeutics.

Detailed Service Definition (continued)

Key features

- Comprehensive risk assessments for digital transformation initiatives and operational services.
- Cybersecurity frameworks aligned with NHS Data Security and Protection Toolkit and ISO 27001.
- Business continuity and disaster recovery planning for critical health systems, aligned to NHS EPRR and ISO 22301.
- Real-time monitoring and reporting of digital risk indicators and operational resilience metrics.
- Clinical safety risk management and hazard logging aligned to DCB0129 and DCB0160.
- Interoperability risk management aligned to NHS FHIR, PRSB record standards, SNOMED CT and dm+d.
- Supply chain and third-party assurance aligned to DSPT, NCSC CAF and NHS supplier assurance expectations.
- Architecture and process optimisation based on TOGAF and open systems principles.
- Continuous improvement with routine and periodic risk processes embedded as business as usual.

Detailed Service Definition (continued)

UK policies, standards and conventions

Information governance and privacy:

- UK GDPR and Data Protection Act 2018.
- NHS Data Security and Protection Toolkit (DSPT) Standards Met.
- Caldicott Principles and local Caldicott Guardian oversight.
- NHS Records Management Code of Practice and retention schedules.
- Privacy and Electronic Communications Regulations for electronic communications.
- Information Sharing Agreements, Data Processing Agreements and DPIAs.

Detailed Service Definition (continued)

Cyber security and resilience:

- NCSC Cyber Assessment Framework (CAF) for Operators of Essential Services under NIS Regulations 2018.
- NCSC Cloud Security Principles and logging guidance.
- NCSC Cyber Essentials and Cyber Essentials Plus for baseline controls.
- NHS England Cyber Security guidance, including HSCN connectivity requirements and network security baselines.
- HMG Security Policy Framework where applicable to central bodies.

Detailed Service Definition (continued)

Clinical safety:

- DCB0129 Clinical Risk Management for manufacturers and suppliers of health IT systems.
- DCB0160 Clinical Risk Management for deployment and use within care organisations.
- Clinical Safety Officer role and clinical hazard logs integrated with change, release and incident processes.
- IEC 62304, IEC 82304-1 and ISO 14971 for medical device and health software risk management where applicable.
- UK MDR 2002 and MHRA guidance for Software as a Medical Device and UKCA marking.

Business continuity and emergency preparedness:

- ISO 22301 Business Continuity Management Systems.
- NHS Emergency Preparedness, Resilience and Response (EPRR) Framework.
- Civil Contingencies Act 2004 duties for Category 1 and 2 responders and Local Resilience Forums.
- IT service continuity integrated with clinical service continuity, surge plans and fallback processes.

Detailed Service Definition (continued)

Technology and architecture:

- TOGAF for enterprise and systems architecture.
- Open systems architecture principles to enable agile, through-life risk response.
- ITIL 4 for service management, change enablement, incident, problem and configuration management.
- HSCN and NHS Spine conventions, identity and access management standards where relevant.
- NCSC architecture patterns for secure design and zero trust principles.

Interoperability and Data Standards:

- HL7 FHIR for APIs and information exchange.
- PRSB standards for structured records and care plans.
- SNOMED CT clinical terminology and dm+d for medicines.
- NHS Organisation Data Service codes and NHS number usage conventions.

Detailed Service Definition (continued)

Cloud and data hosting:

- Technology Code of Practice and Service Standard considerations for public sector digital services.
- UK data residency, sovereignty and lawful basis controls.
- Secure-by-design landing zones and Well-Architected principles for major cloud providers.

Supply chain and procurement:

- Supplier DSPT compliance and right-to-audit clauses.
- Contractual security schedules, SLAs and exit plans aligned to business continuity.
- Secure development lifecycle expectations and vulnerability disclosure.
- Assured connectivity, integration and support arrangements for HSCN and ICS-wide platforms.

Detailed Service Definition (continued)

Governance and roles:

- Senior Information Risk Owner (SIRO) for information risk oversight.
- Caldicott Guardian for patient confidentiality and data sharing controls.
- Clinical Safety Officer for health IT clinical risk management.
- Information Asset Owners and Administrators for local asset risks and controls.
- Board and Quality Committees for risk appetite, assurance and accountability.
- ICS and ICB governance forums for system-level risk coordination.

Detailed Service Definition (continued)

Approach

Frazer-Nash provides a balanced digital enterprise risk management approach, working with you to plan, organise and control business activities to minimise the impacts of risks on your finances and patient outcomes. We define, map and develop actionable plans covering financial, strategic and operational risks.

Whole system view

Our approach takes a whole system view of your organisation, spanning people, process, information, technology and facilities. We shift focus from siloed compliance regimes to outcomes-based risk reduction aligned to the NIS Regulations and NCSC CAF objectives.

Risk taxonomy

We use the Cabinet Office approach to four types of risk: internal, external, strategic and major project, adapted to healthcare contexts including clinical harm, data privacy, operational continuity and regulatory compliance.

Detailed Service Definition (continued)

Methods, tools and techniques

We use best-practice methods, tools and techniques to reduce enterprise risk and develop a common risk management language through building blocks, routine processes and periodic activities. We ensure risk management is embedded across the organisation, not confined to specialist practitioners.

Engagement model

We work with you through face-to-face meetings, workshops and appropriate engagement processes such as surveys to undertake the following:

- Define scope: Engage stakeholders to identify and prioritise threats to essential functions, critical systems, critical assets and critical processes, and determine associated risks. Incorporate local risk registers, incident data, clinical hazard logs and audit findings.
- Enterprise and system modelling: Use standard-based modelling approaches, such as TOGAF, to describe and document systems and identify key interfaces, data flows and dependencies across care pathways and shared care records.
- Map risks: Determine which threats could jeopardise business objectives or clinical safety, share information and set controls to offset risks. Align control objectives to DSPT, NCSC CAF, ISO 27001, DCB0129 and DCB0160.

Detailed Service Definition (continued)

- Action planning: Develop risk treatment plans to address unacceptable risks and risk gaps, prioritising quick wins and structural improvements. Integrate with ITIL change, release and problem processes and clinical safety sign-off.
- Systems architecture: Identify improvements to technical architecture to reduce complexity and associated risks. Apply open systems architecture principles to enable through-life, agile responses to future threats and risks, including zero trust and secure-by-design.
- Processing and automation: Identify suitable processes, technologies and platforms to improve and where possible automate inefficient manual processes. Include evaluation of cloud technologies to support risk reporting, risk assessment and governance, with attention to lawful basis, data residency and role-based access.
- Monitor and measure: Establish metrics to identify, monitor and maintain key risk and opportunity areas. Embed dashboards and routine reviews so enterprise risk management becomes business as usual.

Detailed Service Definition (continued)

Risk indicators and reporting

- Leading indicators: change volume, architectural deviation, clinical hazard backlog, supplier patch latency, privileged access growth, interoperability defects.
- Lagging indicators: major incident rate, clinical safety incident rate, data breach count, recovery time performance, audit non-conformities.
- Thresholds and triggers aligned to risk appetite and tolerances set by Board and ICS governance.
- Regular reporting to SIRO, Caldicott Guardian, CSO and relevant committees.

Detailed Service Definition (continued)

Deliverables

- Enterprise risk management framework tailored to UK healthcare policies and standards.
- Strategic and operational risk registers with clinical hazard logs linked to DCB0129 and DCB0160.
- Control library mapped to DSPT, ISO 27001, NCSC CAF and NHS EPRR.
- Architecture risk assessments and remediation roadmaps.
- Business continuity and disaster recovery plans aligned to ISO 22301 and NHS EPRR.
- Supplier assurance assessments and contractual control schedules.
- Dashboards for real-time digital risk indicators and performance trends.
- Training and awareness materials for clinicians, managers and digital teams.
- Playbooks for incident response, tabletop exercises and after-action reviews.

Detailed Service Definition (continued)

Integration with ICS and devolved contexts

- Alignment with ICS, ICB and provider collaboratives for system-level risk coordination and escalation.
- Consideration of devolved policies for NHS Scotland, NHS Wales and HSC Northern Ireland, while maintaining core UK-wide compliance to UK GDPR, NIS Regulations and NCSC guidance.
- Local Resilience Forum engagement for multi-agency planning and exercising.

Example risks and controls

- Clinical safety: apply DCB0129 and DCB0160 with CSO sign-off, maintain hazard logs, perform safety case updates on change, and integrate with ITIL governance.
- Cyber threats: align controls to NCSC CAF, implement multi-factor authentication, least privilege, secure configuration, patch management and continuous monitoring.
- Data protection: conduct DPIAs, enforce role-based access control, encryption in transit and at rest, audit logging and appropriate data sharing agreements.

Detailed Service Definition (continued)

- Interoperability: validate FHIR, SNOMED CT and PRSB conformance, maintain API inventories, versioning policies and contract testing.
- Continuity: define recovery time objectives and recovery point objectives, test failover, maintain runbooks and clinical fallback procedures.
- Supplier risk: ensure DSPT compliance, vulnerability disclosure, secure development lifecycle, right to audit and exit plans.

Benefits

- Reduced likelihood and impact of clinical safety incidents and data breaches.
- Improved operational resilience and recovery performance for critical health systems.
- Clear, consistent risk language and decision-making across the organisation.
- Assured compliance with UK healthcare regulations, standards and conventions.
- Better value from digital investments through risk-informed prioritisation.

Detailed Service Definition (continued)

Assumptions and dependencies

- Executive sponsorship, defined risk appetite and governance forums.
- Up-to-date inventories of systems, data flows, suppliers and medical devices.
- Access to incident, audit and clinical safety data for risk triangulation.
- Collaboration across clinical, operational, informatics and IT service teams.

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**.

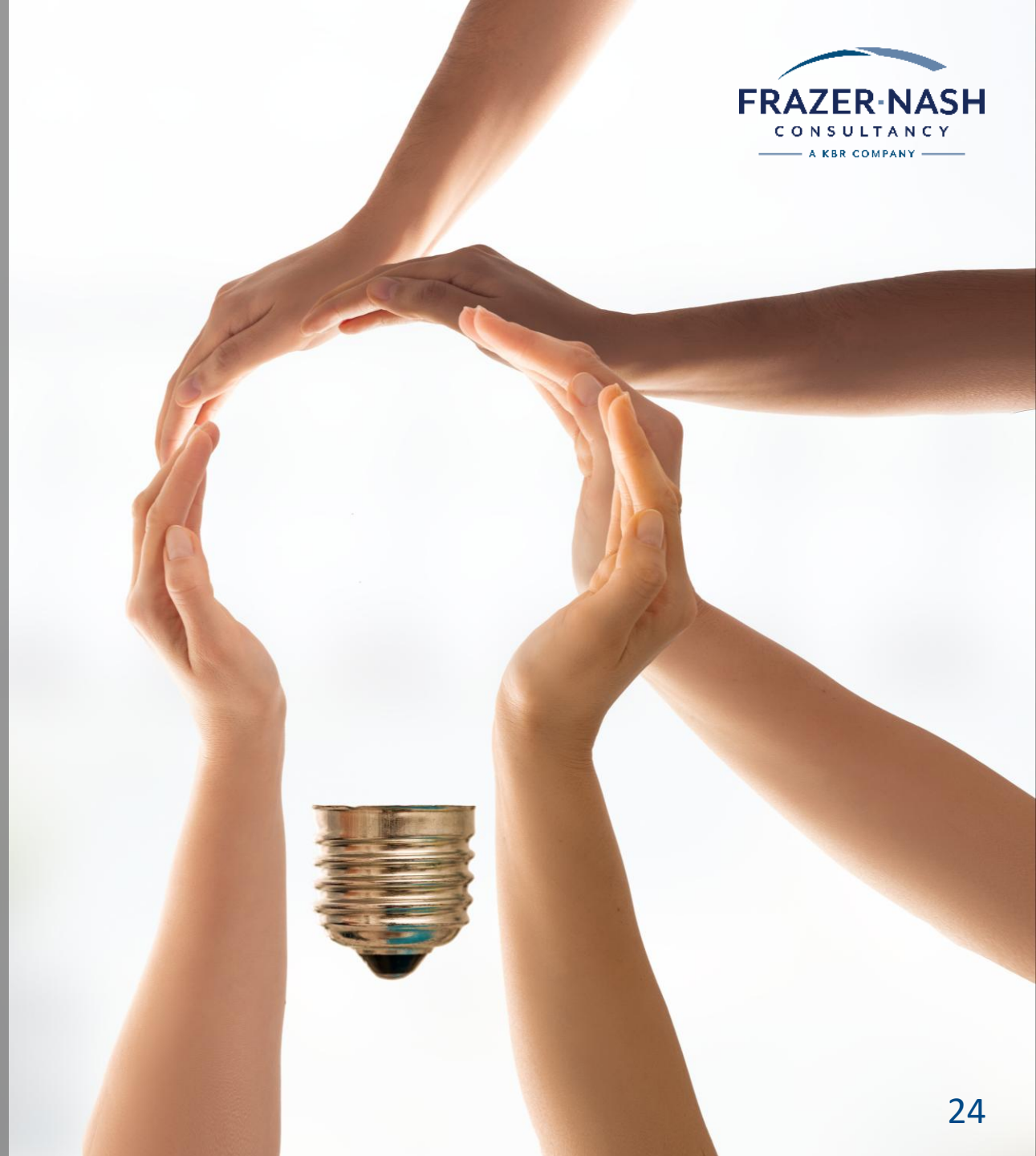
Our IT systems are certified to **ISO 27001 and Cyber Essentials Plus**, providing assurance that information security risks are proactively managed in line with recognised industry standards.

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**