

Cyber Risk Assessment

Service Category: Security Services, Cloud Support Services

About Our Service

We help organisations improve their cyber resilience against evolving threats, including AI-driven attacks and supply chain risks. Our service is a socio-technical assessment investigating people, process and technological facets of your organisation, aligning with NIST principles to Identify, Protect, Detect, Respond and Recover and deliver actionable and prioritised insights.



Service Features

**Orientation and
cyber risk report
with prioritised
insights**

**Cloud security
posture and risk
analysis**

**Internet of Things /
operational
technology security
/ risk assessment**

**Maturity
assessment aligned
to NIST / Secure by
Design principles**

**Enterprise supply
chain risk analysis**

**Socio-technical
modelling
describing the
organisation /
system under
investigation**

**Recommendations
on areas for further
investigation to
mitigate cyber risk**

**Recommendations
for penetration
testing (pentest)**

**Recommendations
for GDPR
compliance or
information
assurance audit**

**Governance and
management
support to
implement security
changes**

Service Benefits

Improved resilience
against advanced
cyber threats,
including AI-driven
attacks

Improved
understanding of
your system
landscape and
exposure risks

Improved ability to
manage your
system exposure

Improved
prioritisation of
investment for
resilience to a
cyber-attack

Evidence-based
artefacts for cyber
insurance and
regulatory audit



Detailed Service Definition

Frazer-Nash will undertake a cyber risk assessment (or cyber vulnerability investigation) as an independent socio-technical analysis of your people, processes, information, technology and infrastructure (facilities) to determine likely areas of cyber-attack or exploitation, identify vulnerabilities and develop recommendations.

We will work with you to help you to understand the cyber-related vulnerabilities and risks you are exposed to across the target system or your whole business, as required. Within our team of experts, we will be able to communicate any concerns to you and your stakeholders in meaningful terms.

Detailed Service Definition (continued)

Our process

Frazer-Nash will conduct an in-depth cyber risk assessment following a mature framework and methodology. We can tailor the approach to best fit your system under investigation and to any specific requirements or organisational needs.

There are four main stages:

- **Orientate:** collect information about your specific systems.
- **Understand:** develop a system of systems model of your business / target system and confirm that this is a true representation.
- **Assess:** use the model to identify likely vulnerabilities by working through possible attack paths and using threat intelligence, ensuring that relevant stakeholders are engaged throughout.
- **Quantify:** our specialists will deliver stakeholder workshops to quantify risks and mitigations and then present the findings of the investigation in an output that is easily understood and prioritised to best enable prompt and effective decisions.

Detailed Service Definition (continued)

Our team

Frazer-Nash will bring a range of disciplines to conduct your investigation. A dedicated cyber technical lead will use a team of experts from our Information Assurance, Human Factors and Information Systems teams and can draw on our breadth of domain and technology specialists as required from across sectors. As the investigation evolves, and if your needs change, we will be responsive and flexible to assign the right resources to ensure the delivery meets your needs.

We will engage with your system lead and work with you and your staff, including other suppliers as necessary, as a blended-team to fully document the relevant system or business and processes. We will identify issues or concerns (cyber vulnerabilities and resulting risks) that need to be addressed. Our approach is scalable and so is suitable for any size business or system.

Detailed Service Definition (continued)

Outputs

Throughout the investigation we will share with you relevant information and formal outputs as a continuous communication. Feedback and discussion on these will ensure that we can tailor the overall investigation to best fit your needs and desired outcome. Some of these are mandated on some methods (e.g. cyber vulnerability investigations) and we will tailor the outputs and nature of those as part of our proposal and as part of the orientation phase of our work with you to ensure you receive relevant and timely input to your business operations through the process.

Indicative deliverable products are:

- Orientation/Cyber Risk Assessment Report. Confirmation that we have sufficient information to progress.
- Socio-Technical System Model. Visual representation of people, organisation and technical interfaces and dependencies.
- Cyber Security Maturity Assessment Report. Benchmarks against NIST, Secure by Design principles or other regulatory standards.
- Cloud and IoT / OT Security Exposure / Posture Report.
- Prioritised Risk List. Risk register of cyber risks identified and prioritised to guide decisions.

Detailed Service Definition (continued)

Outputs (continued)

- Cyber Essentials and Cyber Essentials Plus assessment
- Mitigation and Recommendation Roadmaps. Support sustainable organisational change.
- Governance and Management Models and Change Support. Support systemic improvements in the organisation to multiply benefit.
- Executive and Stakeholder Engagement and Briefing Pack. Bring stakeholders and decision makers on the journey to understand complex technical issues and risk and make informed decisions.

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

