Frontline
IT Consultancy

Cyber Security Operations and Threat Response

Frontline Consultancy and Business Services Ltd offers a fully G-Cloud-compliant portfolio of Cyber Security Operations and Threat Response services, specifically designed to meet the rigorous standards and evolving needs of UK public sector organisations. Our G-Cloud 15 offering delivers a holistic, integrated approach to cyber security, ensuring that all services are aligned with government frameworks, industry best practices, and the compliance requirements set out by the G-Cloud procurement process.

Our suite of services includes:

Cyber Security & Resilience Bill Audit:
This independent, non-invasive audit is aligned with the UK Cyber Security & Resilience Bill, NCSC guidance, ISO/IEC 27001, and NIST CSF. It provides a clear, actionable assessment of your organisation's security posture, supporting compliance with statutory and regulatory obligations, and helping demonstrate due diligence to auditors and stakeholders.

Cyber Training and Monitoring:
Our automated, user-centric training platform is designed to meet G-Cloud's emphasis on user awareness and risk reduction. It delivers personalised security awareness modules, real-world phishing simulations, and robust reporting to ensure measurable improvement and compliance with standards such as GDPR, HIPAA, and ISO 27001.

Frontline Advanced Real-Time Monitoring:
Leveraging AI-driven network behavioural analysis, this service provides continuous, standards-aligned monitoring and reporting. It supports compliance by delivering transparent, auditable records of network activity and incident response, in line with G-Cloud's requirements for accountability and risk management.

Managed Cloud Event Monitoring:
Built on Microsoft Sentinel, this service offers centralised, real-time visibility and threat detection for cloud environments. It is fully integrated with Microsoft 365 and Azure, ensuring compliance with cloud security best practices and supporting the secure adoption of cloud services as encouraged by G-Cloud.

Managed Vulnerability Scanning:
Regular, automated scanning of internal and external assets ensures early identification and remediation of vulnerabilities. Detailed, standards-based reporting (CVE/CVSS) and compliance mapping help organisations meet G-Cloud's requirements for proactive risk management and regulatory alignment.

Secure Administrative Access:
This solution provides secure, auditable remote access to critical systems and privileged accounts, with centralised credential management and strong multi-factor authentication. It is designed to support compliance with ISO 27001 and other relevant standards, ensuring secure operations in hybrid and remote work environments.

All Frontline services are delivered in accordance with G-Cloud's principles of transparency, security, and value for money. Our solutions are underpinned by robust SLAs, clear reporting, and a commitment to continuous improvement—empowering public sector organisations to operate securely, demonstrate compliance, and respond confidently to the evolving cyber threat landscape.

Frontline
IT Consultancy

Advanced Real-Time Monitoring – Modern Network Security Made Simple

Why Frontline?

Frontline combines cutting-edge technology with expert security analysis to deliver proactive, reliable, and effective monitoring solutions that safeguard your business.

What is Advanced Real-Time Monitoring?

Frontline Advanced Real-Time Monitoring is a network visualisation and behavioural analysis service, powered by DarkTrace, that employs a combination of machine learning, Artificial Intelligence (AI) and security expertise. The service uses state-of-the-art technology to intelligently monitor traffic in and out of your network and learns the standard behaviour and processes that occur within your infrastructure daily. Alerts are triggered to show potential malicious activity when anything deviates from baselined, normal behaviour, allowing our security experts to analyse and advise on next steps so that your business can stay ahead of any potential cyber threats. Customers subscribed to the Advanced Real-Time Monitoring service are continuously monitored, and reported on each month, using standard processes, tools, and policies. A fundamental prerequisite of this service is that a DarkTrace appliance exists on the network to be monitored (this appliance is not included in the service charges).

Why Choose Advanced Real-Time Monitoring?

Increased Visibility of Network Traffic:
Unparalleled visibility into access and transfer of information in and around the network as well as into and out of the organisation.

Notification and Reporting:
Notification of high data transfer volume within, into and out of the network, and data breach identification.

Machine Learning and AI:
Allows a 'normal baseline' to be determined, making anomalies easier to identify.

Detection and Identification:
Early identification of malicious activity so that your business can stay ahead of any potential attacks.

Frontline IT Consultancy

0333 323 2141

info@frontline-consultancy.co.uk

Pain Points vs Solutions

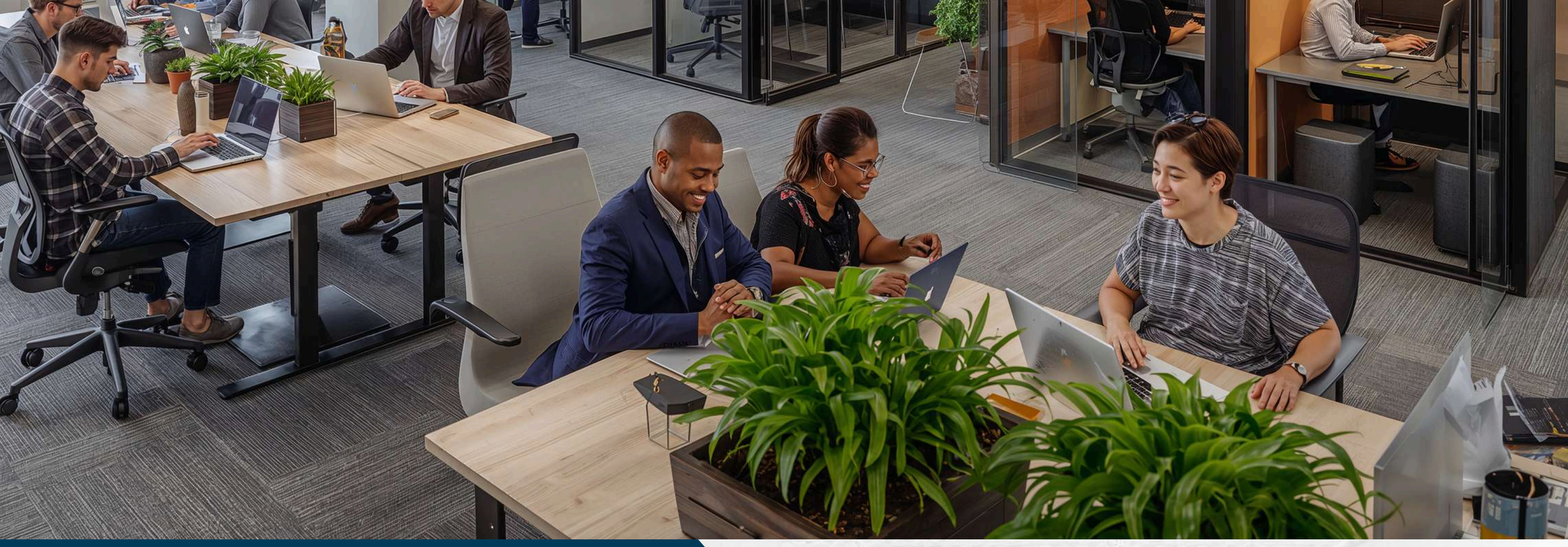
Pain Point	What Users Experience	How Managed Cloud Event Monitoring Solves It
Limited visibility into cloud security	Difficulty identifying threats across multiple services	Centralised monitoring with Microsoft Sentinel
Slow detection of breaches	Delayed response to security incidents	Real-time analysis and AI-driven threat detection
Compliance challenges	Risk of failing audits and regulatory requirements	Built-in compliance support and reporting

Optional Add-Ons-

Additional premium options available upon request.

£500.00 base charge per month.

Frontline Private Cloud only.



Managed Cloud Event Monitoring - Advanced Cloud Security Monitoring Made Simple

What is Managed Cloud Event Monitoring?

Frontline offers a robust security monitoring service leveraging Microsoft Sentinel to ensure your organization's cloud service environment is secure, compliant, and resilient against cyber threats. Our service integrates multiple data sources to provide a unified, real-time view of your cloud security posture. Our SIEM service uses industry standards to analyse event data in real time, enabling early detection of data breaches and targeted attacks.

Why Frontline?

Frontline combines industry-leading technology with expert security professionals to deliver a comprehensive cloud event monitoring solution. Our proactive approach ensures your business remains secure, compliant, and resilient against evolving cyber threats.

Why Choose Managed Cloud Event Monitoring?

Visibility:
Microsoft Sentinel provides a centralised platform for monitoring your key cloud services.

Proactive Threat Hunting:
Enables our security team to proactively search for and mitigate potential threats before they cause harm.

Advanced Threat Detection:
Utilises AI and machine learning to detect threats quickly and accurately.

Integration:
Seamlessly integrates with your existing M365 and Azure services.

Scalability:
Built on Azure, it can handle massive amounts of data and scale as needed.

Compliance Support:
Helps organisations meet regulatory requirements and improve their security posture.

Frontline IT Consultancy

0333 323 2141

info@frontline-consultancy.co.uk

Pain Points vs Solutions

Pain Point	What Users Experience	How Managed Cloud Event Monitoring Solves It
Limited visibility into cloud security	Difficulty identifying threats across multiple services	Centralised monitoring with Microsoft Sentinel
Slow detection of breaches	Delayed response to security incidents	Real-time analysis and AI-driven threat detection
Compliance challenges	Risk of failing audits and regulatory requirements	Built-in compliance support and reporting

Optional Add-Ons-

Additional premium options available upon request.

£103.00 base charge per month.

£8.00 per user charge per month.

12 months term.

Cyber Training and Monitoring – Modern Cyber Risk Reduction Made Simple.

What is Cyber Training and Monitoring?

Frontline's Cyber Training and Monitoring service establishes a baseline of security knowledge within your business, identifies knowledge gaps, and uses automated analysis to direct your team to the right training. The service covers phishing and online information security (InfoSec) training, with options for DarkWeb monitoring and tailored phishing content. Delivered through interactive modules and simulated phishing campaigns, it helps protect against online threats and demonstrates measurable improvement over time.

Why Frontline?

Frontline combines deep cyber expertise with a collaborative approach, ensuring compliance, resilience, and customer trust.

Why Choose Cyber Training and Monitoring?

- **Proactive cyber risk reduction:** Reduce the likelihood of successful cyber attacks through continuous education.
- **Personalised, automated training:** Training tailored to individual knowledge gaps for maximum impact.
- **Real-world phishing simulations:** Build lasting awareness with realistic phishing scenarios.
- **Measurable improvement and compliance:** Track progress and demonstrate compliance with robust reporting.
- **Multilingual support for diverse teams:** Ensure accessibility and engagement across global teams.
- **Comprehensive reporting and actionable insights:** Gain visibility into performance and areas for improvement.

Frontline IT Consultancy

0333 323 2141

info@frontline-consultancy.co.uk

Pain Points vs Cyber Training and Monitoring Solutions

Pain Point	What Users Experience	How Cyber Training and Monitoring Solves It
High risk of phishing attacks	Employees fall victim to phishing emails, exposing sensitive data.	Provides targeted training and phishing simulations to build awareness.
Knowledge gaps in cyber security	Staff lack understanding of key security practices.	Automated gap analysis and personalised training close knowledge gaps.
Difficulty proving compliance	Challenges in demonstrating adherence to standards.	Comprehensive reporting supports compliance with GDPR, HIPAA, ISO 27001.
Emerging threats on DarkWeb	Limited visibility into compromised data.	Optional DarkWeb monitoring alerts and mitigates risks promptly.

Optional Add-Ons:

Advanced DarkWeb Monitor for real-time breach alerts and targeted training.

Tailored Phishing builds real-world phishing simulations using suppliers and organisations your business uses, build lasting awareness.

£5.00 per user charge per month.

12 month term.

Darkweb monitoring: £260.00 charge per month.

12 month term.

Tailored phishing: £115.00

12 month term.

Frontline IT Consultancy

0333 323 2141

info@frontline-consultancy.co.uk

Secure Administrative Access – Modern Remote Access Made Simple

What is Secure Administrative Access?

This service provides a robust and secure solution for remote access to critical systems, applications, and privileged accounts. Designed to meet the needs of modern hybrid and remote work environments, it ensures that administrators, employees, and third-party contractors can securely access sensitive resources from any location while adhering to stringent security and compliance standards. The service combines centralised credential management, strong authentication, and flexible access options to deliver a seamless and secure user experience.

Why Frontline?

Frontline combines industry expertise with cutting-edge technology to deliver secure, reliable, and compliant remote access solutions. Our commitment to customer success ensures that your business remains protected and productive.

Why Choose Secure Administrative Access?

Robust Security:
Implements strong authentication and centralised credential management.

Flexible Access:
Supports secure access for administrators, employees, and third-party contractors.

Compliance Ready:
Meets stringent security and compliance standards for hybrid work environments.

Seamless Experience:
Provides a user-friendly interface for secure remote access.

Frontline IT Consultancy

0333 323 2141

info@frontline-consultancy.co.uk

Pain Points vs Solutions

Pain Point	What Users Experience	How Secure Administrative Access Solves It
Unsecure remote access	Risk of data breaches and unauthorised access	Provides strong authentication and centralised credential management
Compliance challenges	Difficulty meeting regulatory requirements	Ensures adherence to security and compliance standards
Complex access management	Manual processes and inefficiencies	Delivers streamlined, flexible access options

Optional Add-Ons:

Premium options available for enhanced security and compliance features.

£57.00 per user charge per month.

12 month term.

Cyber Security & Resilience Bill Audit – Modern Cyber Risk Assessment Made Simple.

Why Frontline?

Frontline combines deep cyber expertise with a collaborative approach, ensuring compliance, resilience, and customer trust.

What is Cyber Security & Resilience Bill Audit?

The Cyber Security & Resilience Bill Audit is an independent, non-invasive assessment designed to identify vulnerabilities in your IT systems before threat actors do. It provides clear, actionable insights to help you prioritise risk, strengthen your security posture, and support compliance with UK legislation and industry standards. This service is ideal for organisations seeking to enhance their cyber resilience and customer trust.

Why Choose Cyber Security & Resilience Bill Audit?

Clear, Actionable Risk Categorisation:
Risks are categorised using a straightforward Red/Amber/Green system, making it easy to understand and prioritise actions.

Non-Invasive, Collaborative Approach:
The audit is conducted with minimal disruption to your operations, working alongside your team to ensure a smooth process.

Supports Compliance and Assurance:
Aligns with the UK Cyber Security & Resilience Bill, NCSC guidance, ISO/IEC 27001, and NIST CSF pillars, supporting both compliance and customer assurance.

Independent, Expert Perspective:
Gain an unbiased view of your IT risk and security posture, delivered by experienced cyber security professionals.

Comprehensive Coverage:
All aspects of your IT systems and infrastructure are reviewed, ensuring no gaps in your security assessment.

Frontline IT Consultancy

0333 323 2141

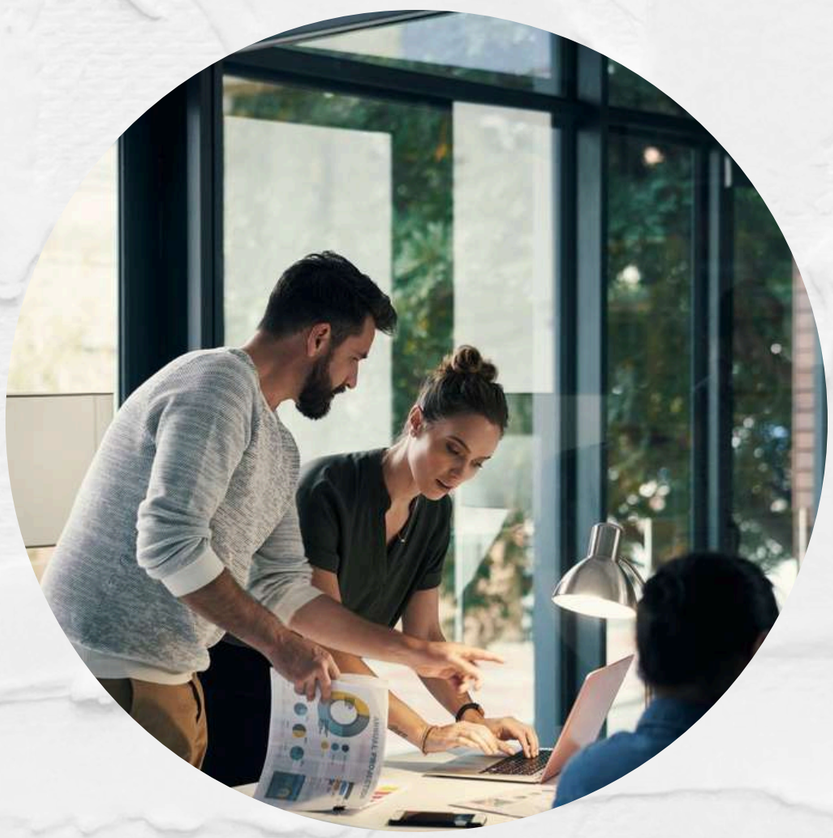
info@frontline-consultancy.co.uk

Pain Points vs Cyber Security & Resilience Bill Audit Solutions

Pain Point	What Users Experience	How Cyber Security & Resilience Bill Audit Solves It
Unclear risk exposure	Difficulty identifying and prioritising vulnerabilities	Provides clear, actionable insights and risk categorisation
Compliance uncertainty	Concerns about meeting regulatory and industry standards	Supports compliance with UK legislation and recognised frameworks
Operational disruption	Worries about audits impacting business continuity	Non-invasive approach minimises disruption
Lack of independent review	Internal assessments may miss critical issues	Delivers an unbiased, expert perspective

Optional Add-Ons:

Additional remediation services can be arranged separately if required.



£2,999 one off cost.

Frontline IT Consultancy

0333 323 2141

info@frontline-consultancy.co.uk

Managed Vulnerability Scanning- Proactive Risk Detection and Security Assurance

Why Frontline?

Frontline combines industry expertise with advanced tools to deliver a managed service that reduces risk, improves compliance, and ensures your business stays secure in an evolving threat landscape.

What is Managed Vulnerability Scanning?

Managed Vulnerability Scanning is a service focused on information security and data protection. It identifies risks, threats, and potential points of compromise across your IT systems. By scanning internal and external assets, the service helps protect confidentiality, availability, and integrity of data.

Why Choose Managed Vulnerability Scanning?

- Early identification of vulnerabilities to reduce risk.
- Comprehensive internal and external scanning for servers and applications.
- Categorisation of vulnerabilities using CVE and CVSS for informed decision-making.
- Monthly reporting with actionable recommendations.
- Alignment with ISO 27001 and Cyber Essentials standards.

Frontline IT Consultancy

0333 323 2141

info@frontline-consultancy.co.uk

Pain Points and Solutions

Pain Point	What Users Experience	How Managed Vulnerability Scanning Solves It
Unidentified vulnerabilities	Systems exposed to threats	Regular scans and reports highlight risks for remediation
Compliance challenges	Difficulty meeting security standards	Provides compliance reporting aligned to ISO and Cyber Essentials
Reactive security posture	Delayed response to threats	Proactive detection and early notification of issues

Optional Add-Ons:

Additional Frontline services can be purchased to complement vulnerability scanning.

£39.00 Base charge per month.

12 month term.

Support Cost Calculation Approach

Our support pricing model is designed to be transparent, fair, and aligned with the specific needs of the procuring entity. The total cost of support will be calculated based on the projected time required, which is determined through a collaborative assessment during the onboarding or procurement phase.
This projection will consider the following key factors:

Benefits of This Approach

Transparency:
Customers have full visibility into how costs are derived.

Flexibility:
Pricing scales with actual support requirements, avoiding unnecessary overhead.

Compliance:
Aligns with G-Cloud principles and SFIA framework standards.

Complexity of the Delivered Solution
The level of technical complexity, including:
Integration with existing systems
Custom configurations or bespoke development
Security and compliance requirements
Higher complexity typically requires more specialised resources and extended support coverage.

Hours of Operation:
Support costs will reflect the agreed service window:
Standard Business Hours (e.g., 09:00–17:00, Monday–Friday)
Extended Hours or 24/7 coverage, if required
This ensures flexibility for customers who need critical support outside normal operating hours.

Commercial Model:
All pricing will be based on the submitted SFIA rate card, ensuring:
Full compliance with G-Cloud pricing transparency requirements
Clear linkage between resource roles, skill levels, and associated costs
Rates are applied to the projected time for each role involved in delivering support.

Methodology for Cost Estimation:
Initial Assessment
We work with the customer to understand the solution architecture, operational requirements, and anticipated support needs.

Time Projection:
Using the complexity and operational factors,
we estimate the number of hours required for each SFIA role.

Cost Calculation:
The projected hours are multiplied by the corresponding SFIA rate,
producing a clear and auditable cost breakdown.

Frontline

IT Consultancy

0333 323 2141

info@frontline-consultancy.co.uk