



Your Trusted Cyber Security Partner

G-Cloud 15 – Service Definition

Document

**Cyber Security, Security Architecture, Cloud
Consulting & Assurance Services**

v1.0

A decorative graphic at the bottom of the page consisting of a series of blue, glowing particles or dots that form a wavy, horizontal line across the width of the page.

Table of Contents

1. About Cyber Security Specialists	4
2. Security Consultancy	6
3. Security Architecture & Secure Design	7
4. Cloud Security Consultancy	8
5. Data Protection & GDPR	9
6. Penetration Testing	10
7. Our Certification Services	11
7.1 Cyber Essentials Plus Certification	11
7.2 ISO 27001 Certification	11
8. DevSecOps	12
9. AI Security Consultancy	13
9.1 AI Security Assessment	13
9.2 AI Secure Design Review	13
9.3 AI Regulatory Compliance	14
10. Additional Information	15
10.1 Pricing	15
10.2 Ordering & Invoicing	15
10.3 Termination Terms	15

10.4 Customer Responsibilities

15

1. About Cyber Security Specialists

We pride ourselves in providing expert, pragmatic and cost-effective Consultancy services to our Public Sector Clients, embedding our Consultants within Agile Project teams to ensure Security forms part of a Digital projects DNA.

Cyber Security Specialists have a wealth of experience in supporting the UK Public Sector and have worked with the majority of Central Government Departments over the past decade. We are proud to provide our Cyber Consultancy services via the Government's G-Cloud framework, Cyber Security Services framework and also Digital Outcomes & Specialists.

Our team of Cyber Security Specialists enables us to deliver a bespoke range of services including:

- CREST Penetration Testing
- Threat Led Penetration Testing & Red Teaming
- Cyber Security Maturity Audits
- Cloud Security Design
- Cloud Security Auditing
- Security Architecture & Secure by Design
- DevSecOps & Secure Engineering
- AI Security Consultancy
- Governance, Risk & Compliance
- Data Protection & GDPR Consultancy
- Cyber Essentials Plus certification
- ISO 27001 certification



Our Consultants have a wealth of experience supporting Local and Central Government Departments and hold key industry qualifications and certifications such as:

- NCSC Certified Professional (CCP)
- ISO 27001 Lead Auditor
- ISO 27001 Lead Implementer
- Certified GDPR Practitioner & Data Protection Officer
- Certified Information Systems Security Professional (CISSP)
- Information Systems Security Architecture Professional (CISSP-ISSAP)
- Comprehensive Certified Information Security Manager (CISM)
- SABSA Chartered Architect (SABSA)
- AWS Certified Solutions Architect
- AWS Certified DevOps Engineer
- Certified Ethical Hacker (CEH)
- CREST Registered Penetration Tester (CRT)
- Offensive Security Certified Professional (OCSF)

Our team all hold Security Clearance (SC) with many also holding Developed Vetting (DV) Clearance. In addition to holding the highest industry certifications, many of the team also hold NCSC (National Cyber Security Centre) certifications and were members of the now retired CLAS scheme (CESG Listed Advisor Scheme).

More information can be found by visiting <https://www.cybersecurityspecialists.co.uk>.

2.Security Consultancy

Cyber Security Specialists provide a range of services to measure, manage and control Cyber Risk within your organisation.

Our Cyber Security Consultancy services align to leading industry standards from both **NCSC (National Centre for Cyber Security)**, **NIST**, **CIS** and **SANS**, enabling us to identify the most appropriate Cyber Security Framework for your Organisation size and vertical.

We support Organisations in ensuring that Cyber Security is understood and implemented effectively, minimising the risk of being subject to a successful cyber-attack and improving resilience.

Our Security Consultancy service cover the following core areas:

- Performing Cyber Security Maturity Assessments
- Defining Cyber Security Strategies & Roadmaps
- Creating Cyber Security Policies and Processes
- Performing Asset Based or Control Based Risk Assessments
- Supporting the execution of Cyber Security Improvement Programs

3. Security Architecture & Secure Design

Cyber Security Specialists can work with your Organisation to ensure that your systems are adequately protected from today's cyber security threats. We can design your security controls from the ground up or review your existing systems and advise on security improvements, based on the current threat landscape.

Our Security Architects can support your Organisation ensuring that any technology in use is secure by design and built to industry best practice. We have deep experience in designing and securing Cloud workloads, Systems and Web Applications for some of the busiest online services in the Public Sector. This has included working independently or in conjunction with inhouse Authority Architects and Engineers.

Our Secure Design service cover the following core areas:

- Enterprise Security Architecture
- Cloud architectures (SaaS, PaaS, IaaS)
- Zero Trust architectures
- On premise network Infrastructures
- Remote access solutions
- Identity & Access Management
- AI integration and adoption
- Secure Endpoints (Corporate and/or BYOD Programs)
- Data Security & Encryption
- Secure Configuration
- Vulnerability Management and Malware Protection
- Security Information and Event Management (SIEM) & Protective Monitoring
- Secure Coding and the SDLC
- CI/CD Pipelines and DevSecOps

4. Cloud Security Consultancy

Public Sector organisations are undergoing major transformation as they move their information from on-premise systems to Cloud Services such as **Office 365, AWS, GCP** and **Microsoft Azure** to increase mobile workforce productivity, improve operational agility, and lower costs.

As information moves from on-premise networks and into the Cloud, it can raise concerns about security, privacy and compliance. Our Cloud Security Specialists can ease this transition to the Cloud by ensuring that the appropriate security and privacy measures are in place, leaving you to take advantage of everything the Public Cloud has to offer, with the peace of mind that your services and data remain secure.

We have deep experience in designing and securing Cloud workloads for some of the busiest online services in the Public Sector. This has included working independently or in conjunction with inhouse Authority Architects and Engineers.

Our Cloud Security service cover the following core areas:

- Creation of 'green field' Public/Private Cloud Architectures
- Performing Secure Design reviews of existing Cloud Infrastructure & Workloads
- Design and implementation of proportionate and effective security controls
- Adoption of Cloud native security services
- Performing independent technical Cloud Security Audits
- Conducting Security Assurance Reviews & Risk Assessments
- Being the Cloud security SME on Client Governance Boards and Design Authorities

5.Data Protection & GDPR

Cyber Security Specialists and our team of experienced Data Protection and GDPR professionals can help your organisation, from assessing your GDPR compliance position and developing a remediation roadmap through to implementing a best-fit data compliance framework.

Whether you are an NHS Body, Charity, CNI or Public Sector organisation, we can tailor our Data Protection consultancy services to your individual business and compliance needs.

Our Cyber Security Specialists can support your Business in ensuring that Data Protection and GDPR Compliance is understood and implemented effectively to minimise the risk of being subject to a successful data breach.

Our Data Protection and GDPR Consultancy service cover the following core areas:

- **Gap Analysis** – a full audit of the Organisation against the key requirements of the GDPR.
- **Data Mapping Exercise** – identifying what personal data you hold, where it is stored and who you share it with.
- **Privacy Impact Assessment** – an assessment of the Privacy risks to the individuals whose personal data you hold.
- **Policies and Procedures** – all the documents you will need to ensure that you are able to fully meet the requirements of GDPR e.g. Data Protection Policy, Subject Access Request procedure, Data Retention Policies, Data Classification Policy.
- **Privacy By Design** – We can help to implement a Privacy by Design culture and ensure privacy is embedded into the daily working practices of your Organisation.

6. Penetration Testing

The Cyber Security Specialists Penetration Testing service is CREST-accredited. Holding this title is a great privilege and demonstrates that Cyber Security Specialists:

- is an entrusted partner for delivering high-quality Penetration Testing services
- has reliable methodologies and processes
- provides comprehensive reporting
- has highly skilled Cyber Security professionals

We have over a decade of experience in scoping and providing Penetration Testing to Clients of all different shapes and sizes from start-ups and Digital Agencies to multinationals and Public Sector Organisations. All of our testing is conducted in accordance with industry recognised standards such as CREST, OWASP and PCI-DSS requirements.

Our Penetration testing service cover the following core areas:

- Web Application Testing
- Mobile App Testing (IOS and Android)
- AI Solutions
- Source Code Security Review
- External Network Penetration Testing
- Internal Infrastructure Testing
- Firewall Ruleset Reviews
- Server Build Review
- Configuration Review
- Cloud Security Review
- VoIP & WebRTC Penetration Testing
- Red Team Exercises
- Threat Led Penetration Testing

7. Our Certification Services

7.1 Cyber Essentials Plus Certification

Cyber Essentials Plus is an NCSC backed and industry supported scheme assisting businesses in protecting themselves against the ever-growing threat of cyber-attacks and provides your organisation with formal certification demonstrating to your business partners, customers and regulators that you take cyber security seriously.

Cyber Essentials Plus requires an independent assessment of your security controls, to verify that they are in place and working.

Cyber Security Specialists are an accredited Cyber Essentials Certification Body for both Cyber Essentials & Cyber Essentials Plus, and our experienced team of Cyber Security Analysts can help to guide you through the process and successfully gain certification.

7.2 ISO 27001 Certification

ISO 27001 (ISO/IEC 27001:2022) is the international standard that provides the specification for an information security management system (ISMS).

The Standard is designed to help organisations manage their information security processes in line with international best practice while optimising costs. It is technology and vendor neutral and is applicable to all organisations – irrespective of their size, type or nature.

Our dedicated ISO 27001 consultants are highly qualified and experienced and can support you on every step of the way to gaining formal ISO 27001 certification for your Organisation. As well as implementation, we can also support with ISO 27001 training and internal audits.

8.DevSecOps

Cyber Security Specialists provide tailored DevSecOps consultancy across a wide range of Cloud Platforms including AWS and Microsoft Azure.

We utilise our experience in Cloud, DevOps and Cyber Security to streamline business transformation and Cloud migration to build robust and secure Cloud infrastructures.

DevSecOps services integrate security, development, and operations into a cohesive framework, embedding automated security controls (SAST, DAST, SCA) directly into the CI/CD pipeline. By fostering a shared responsibility culture, these services accelerate secure software delivery, reduce compliance risks, and identify vulnerabilities early in the development lifecycle.

Our DevSecOps service covers the following core areas:

- **CI/CD Pipeline Security** - Implementing automated security testing for every code change, enabling rapid, safe deployments.
- **Security-as-Code** - Embedding security configurations and policies into infrastructure as code (IaC) to ensure consistent compliance.
- **Continuous Monitoring** - Providing real-time, ongoing assessment of cloud and application infrastructure security.
- **Managed Security Services** - Offering expert-led, 24/7 monitoring, penetration testing, and vulnerability management.
- **Cultural Transformation** - Breaking down silos to ensure development, security, and operations teams collaborate on shared security goals.

9. AI Security Consultancy

AI applications and services have the power to enhance your services and customer support in many ways. Our team understands how beneficial AI integration can be and can support your business's transition into a modern, efficient operation by supporting your use of more reliable and proactive services through AI technology.

Cyber Security Specialists AI consultancy services can support Government Organisations in protecting their artificial intelligence systems and machine learning algorithms from cyber threats, adversarial attacks, and data breaches while ensuring robust data protection throughout the AI development life cycle.

9.1 AI Security Assessment

An AI security assessment is a systematic process for identifying, evaluating, and mitigating threats and vulnerabilities unique to AI systems, such as adversarial attacks, data privacy issues, and algorithmic bias, to ensure safe and reliable AI deployment.

Our team will perform a comprehensive evaluation of your AI systems and usage against the NIST AI Risk Management Framework and provide a formal documented report detailing an analysis of risks based on likelihood and impact, with clear categorisation across areas such as confidentiality, integrity, availability, safety, and compliance.

9.2 AI Secure Design Review

An AI Secure Design Review is a structured evaluation of an AI system's design to ensure that security, safety, and trustworthiness considerations are built in from the start before development or deployment.

We can help design secure AI frameworks and examine data handling practices, model robustness, access controls, and integration points to identify potential vulnerabilities such as adversarial attacks, data leakage, or misuse.

The review also considers compliance, monitoring, and ethical principles like fairness and accountability. Its outcome is a set of prioritised recommendations that guide teams in building AI systems that are secure, resilient, and aligned with regulatory and organizational requirements

9.3 AI Regulatory Compliance

AI Regulatory Compliance is the practice of ensuring that artificial intelligence systems meet all applicable legal, ethical, and technical requirements. It involves aligning with regulations such as the EU AI Act, GDPR, and sector-specific laws, while also addressing principles of fairness, transparency, accountability, and human oversight. Compliance requires strong data governance, bias prevention, security controls, and clear documentation to demonstrate that AI systems are safe, trustworthy, and lawful throughout their lifecycle.

Our team can help to ensure your AI applications meet industry standards including compliance or full certification to **ISO/IEC 42001 (the international standard for Artificial Intelligence Management System)**.

ISO 42001 is an international Standard dedicated to the management of AI systems. It provides a comprehensive framework that helps organisations develop, implement, and maintain AI technologies responsibly. The management system is designed to fit the specific risks and needs your business faces with the use of AI. This means you get a tailored approach that's right for your business.

10. Additional Information

10.1 Pricing

The pricing for all projects and services will be based on the individual SFIA rate card which lists the applicable prices for those services. The rate card gives the 'day rate' for resources at each skill category and responsibility level.

For any particular project we would aim to agree in advance with the customer what level of supporting resource is required. Using the blend of resource and the SFIA rates this would then enable us to determine the overall charge.

10.2 Ordering & Invoicing

The ordering and invoicing procedure will follow that defined for the Digital Marketplace.

10.3 Termination Terms

There are no additional Termination conditions. Terms are in accordance with the Framework Agreement and the Call-Off Contract.

10.4 Customer Responsibilities

We will discuss and agree any dependencies on the customer that are associated with any call-off requirement prior to work commencing. These responsibilities will differ depending on each specific call-off requirement. Any such dependencies would form part of the Call-Off Contract.