CYBERSECURITY
SPECIALISTS

G-Cloud 14 - Service Definition

Cyber Security, Cloud Consulting & Assurance Services

v1.0

Table of Contents

1. About Cyber Security Specialists

Cyber Security Specialists provide cost effective Cyber Security services across a wide range of UK Government Departments and Private sector Organisations to support their digital transformation.

We pride ourselves in providing expert, pragmatic and cost-effective Security Consultancy services. Some of our Company accreditations and certifications are summarised below:

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)
- 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 (OCSP)

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

2. Our Consultancy Services

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 Government (HMG) 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 and also Digital Outcomes & Specialists.

We are experts in the secure design and assurance of Government Services within the OFFICIAL tier, and have supported the design, build and assurance of dozens of high-profile Government Services within Private, Hybrid and Public Cloud platforms such as AWS & Microsoft Azure.

Our Cyber Security Specialists 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).

2.1 Cyber Security

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.

Our Cyber Security Specialists can support your Business in ensuring that Cyber Security is understood and implemented effectively minimising the risk of being subject to a successful cyber-attack.

We help our clients in areas such as:

- Performing Cyber Security Maturity Assessments
- Defining Cyber Security Strategies
- Creating Cyber Security Policies and Processes
- Building Cyber Resilience through Process & Technology
- Supporting the execution of Cyber Security Improvement Programs
- Gaining formal Cyber Security Certification

2.2 Cloud Security

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

However as information moves out of your hands and into the Cloud, it raises 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 helped many of our Clients secure their Cloud workloads in areas such as:

- Secure design creation of 'green field' Public/Private Cloud Architectures
- Design review of existing Cloud Infrastructure & Workloads
- Design and implementation of proportionate and effective security controls
- Performing independent technical Cloud Security Audits
- Conducting Security Assurance Reviews to the NCSC Cloud Security Principles
- Producing Cloud focused Risk Assessments

2.3 Secure Design

Cyber Security Specialists can work with your Business to ensure that your systems are adequately protected from today's cyber security threats. You can engage with us to design your security from the ground up or to review your existing systems and advise on security improvements.

Our Security Architects can support your Business ensuring that any technology in use is secure by design and built to industry best practice in areas such as:

- Enterprise Security Architectures
- Cloud architectures (SaaS, PaaS, Iaas)
- Network Infrastructures
- Endpoints (Corporate and/or BYOD Programs)
- Data Security, Secure Configuration & Encryption
- Vulnerability Management and Malware Protection
- Security Information and Event Management (SIEM) & Protective Monitoring
- Secure Coding and the SDLC
- CI/CD Pipelines and DevSecOps

2.4 Data Protection & GDPR

Cyber Security Specialists and our team of experienced Data Protection and GDPR experts 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 SME, multinational, charity or public sector organisation, we can tailor our GDPR services to your individual 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 GDPR Consultancy services include:

- **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

2.5 DevOps

Cyber Security Specialists provide tailored DevOps 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.

We provide our clients with consultancy to advise and guide at every step of their journey to the Cloud supporting major decisions that organisations will face, from choosing the right Cloud type (e.g. public versus private) to the right Cloud service provider (e.g. Amazon Web Services versus Microsoft Azure).

We are advocates of Open Source and automation, and design and build appropriate CI/CD automation pipelines using industry best practice DevOps tools such as Gitlab, Jenkins, Terraform, Powershell, Ansible, Chef, Puppet, Docker and Kubernetes.

Whether you're taking your first steps towards the Cloud, or have a particular project in mind, let us support you on your journey.

2.6 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 services include:

- Web Application Testing
- Mobile App Testing (IOS and Android)
- 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

3. Our Certification Services

3.1 Cyber Essentials & Cyber Essentials Plus Certification

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

Cyber Essentials provides 5 core controls that when implemented correctly can prevent around 80% of cyber-attacks. These are:

- Malware Protection
- Boundary Firewall
- Patch Management
- User Access
- Secure Configuration

Cyber Essentials Plus has exactly the same requirements of Cyber Essentials (where you must show you have met the requirements of the 5 technical security controls). However, the critical difference is that Cyber Essentials Plus requires an independent assessment of your security controls, to verify that they are in place and working. Cyber Essentials Plus provides a higher level of security assurance and requires your Organisation to pass an internal & external Vulnerability Scan and a thorough Malware Protection Assessment performed by Cyber Security Specialists.

Cyber Security Specialists are an accredited Cyber Essentials Certification Body for both Cyber Essentials & Cyber Essentials Plus.

3.2 IASME Cyber Assurance Certification

Although ISO27001 is the globally recognised benchmark for Information Governance, smaller organisations find it challenging to get certified due to the cost and effort involved.

Many Organisations therefore choose the IASME standard as a more cost-effective certification and a steppingstone to achieving the ISO27001 at a later stage if required.

IASME Cyber Assurance enables you to demonstrate your Organisation's overall maturity level for good security and data privacy practices and that you are taking proper steps to protect customer information.

The standard covers 13 themes across 5 areas of control:

- Identify & Classify
- Protect
- Detect and Deter
- Respond and Recover

Cyber Security Specialists are an accredited IASME Cyber Assurance Certification Body.

3.3 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 latest version was published in October 2022.

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. They will be there to support you every step of the way to gaining formal ISO 27001 certification for your organisation, including:

- Gaining a competitive advantage your organisation
- A platform for your organisation to proactively manage information security risks
- Independent assurance to internal and external stakeholders of the information security management practices within your organisation
- Maximising the security, integrity and privacy of your organisation's information assets
- Understand the value of the different types of information your organisation holds
- Minimising the likelihood of regulatory and/or legislative breaches.

As well as implementation, we can also support with ISO 27001 training and internal audits.

4. Additional Information

4.1 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.

4.2 Ordering & Invoicing

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

4.3 Termination Terms

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

4.4 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.