Crown Commercial Service

RM1557.15

Security Architecture and Cyber Security Services

Lot 3 – Cloud Support Services

CACI

data + technology

Contents

For further information:

☎ **+44 (0)20 7602 6000**

✉ **digital.marketplace@caci.co.uk**

www.caci.co.uk

1. Description of Services

Our Security Architecture and Cyber Security Services build on our team's experience in delivery enterprise scale Critical National Infrastructure for the United Kingdom. With ever expanding threat landscape and increase in volume and sophistication of attacks ensuring systems are secure and can be delivered at pace with the required level of confidence and assurance required is a growing challenge.

Our services, based on Security Architecture standards and secure DevSecOps principles, address the end-to-end security requirements to securely develop or migrate workloads and services to cloud while automating compliance and assurance functions (compliance as code) of cloud workloads.

We have a proven track record of delivering and operating large scale enterprise cloud platforms including the award-winning Home Office EBSA platform, which securely operates over 30K containers a day across three departments serving over 50 development teams.

Our teams consist of Security Architects and IT professionals with many years' experience in successful implementation of cloud solutions. CACI is already in engaged in providing consultancy support services via G-Cloud, including working on transition of existing systems to new hosting and software cloud-based solutions.

We provide detailed, domain specific and delivery focussed support capabilities through our G-Cloud consultancy support services, delivered by a team with an enviable reputation and many years delivery experience.

Our different Security Architecture and Cyber Security Services offered over G-Cloud 15 are described in more detail in the following sections.

2. Governance, Risk and Compliance

Our highly skilled and experienced Governance, Risk and Compliance (GRC) consultants will develop and integrate a collection of capabilities that will enable your organisation to reliably achieve objectives, address uncertainty and act with integrity. Our commitment extends beyond compliance; we are dedicated to fostering a culture of excellence and integrity within your organization. By implementing robust risk management strategies and cultivating a proactive approach to governance. Our GRC consultancy services go beyond achieving short-term requirements; they are about laying the groundwork for enduring success, enabling your organization to thrive in an ever-evolving landscape while upholding the highest standards of governance, risk management, and compliance.

Top Features

- Security Strategy and Planning
- Cloud Security Strategy
- Security Architecture and Programme Design
- Supply Chain Risk Management
- Automated IT Cloud Security Compliance Management
- Information Security Assessment and Assurance
- Security Framework and Risk Assessments
- Security policy, compliance & audit management
- Information Governance
- GDPR compliance

Benefits

- A defined and documented security strategy
- Improved visibility into security posture of organisation
- Improved security culture and awareness
- Tailored to meet the needs and priorities of your organisation

3. Data Security

Our Data Security service and approach provide an end-to-end view of managing the security and privacy of data in your organisation. Assessing and delivering a robust data security assessment and programme involves several key steps. It begins with a thorough evaluation of the organisation's existing data security infrastructure, identifying vulnerabilities and compliance gaps. This assessment considers data flows, access controls, encryption methods, and regulatory requirements. Next, a tailored data security programme is developed, integrating technological solutions, policies, and procedures to mitigate risks and align with organisational objectives. Ongoing monitoring, testing, and training are essential to ensure the programme's effectiveness and adaptability to evolving threats. Collaboration across departments and a commitment to continuous improvement are crucial for successful implementation and maintenance of the programme.

Top Features

- Data Discovery and Classification
- Critical Data Protection
- Data Security Strategy and Architecture
- Data Loss Prevention and Encryption
- Data Security Assessment
- Data Privacy Services
- Information Governance
- GDPR compliance
- Key Management and Classification

Benefits

- Improves data governance
- Protects sensitive information
- Ensures compliance
- Reduces risk of data breaches
- Enhances business continuity

4. ITHC Management

Our highly skilled and experienced consultants will define your ITHC scope, search for an appropriate ITHC provider and manage a remedial action plan.

We can optionally provide remediation assurance using industry standard tools for vulnerability assessment and penetration testing, prior to formal retesting.

Top Features

- Highly experienced consultants delivering service.
- We will create an ITHC scope based principal security concerns
- Use pre-defined list of security concerns and threats
- Source ITHC provider to meet your budget, timescales
- Create and manage a remedial action plan
- Support technical implementation of recommendations from the ITHC.

Benefits

- Awareness and management of vulnerabilities.
- Compliance with industry or sector specific standards.
- Flexible service tailored to the needs and priorities of organisation.
- Experience managing remediation work across suppliers and service providers.

5. Cloud Compliance Assessment

Our highly skilled and experienced consultants will carry out compliance assessments for your solution or services against industry or sector specific standards, policy or guidance. Our consultants can optionally work with you to use the compliance assessment output to define a plan for certification (where relevant and applicable).

You will be provided with comprehensive advice, guidance and a report identifying where compliance can be asserted based on documentary evidence or observations provided by your organisation and any compliance gaps we have identified.

Top Features

- ISO 27001/27002
- NIST Special Publication 800-144
- Cyber Essentials Scheme (CES)
- IASME Information Security Standard
- Cloud Security Principles (CSP)
- Centre for Internet Security (CIS) Controls
- HMG Security Policy Framework
- Centre for Internet Security (CIS) Benchmarks
- Building Security In Maturity Model (BSIMM)
- AWS Well Architected Framework

Benefits

- Our service provides a cost-effective compliance assessment process.
- Compliance with industry or sector specific standards.
- Flexible service tailored to the needs and priorities of organisation.
- Identifies Compliance Gaps
- Reduces Legal and Regulatory Risks
- Enhances Data Protection
- Improves Security Posture
- Accelerates Cloud Adoption/Migration Programme

6. SOC Services

Our highly skilled and experienced consultants specialise in designing a dynamic cyber security monitoring capability tailored to meet the evolving needs of organisations transitioning to hybrid cloud architectures. This includes:

- Defining a flexible logging architecture for cyber security event logs that accommodates the unique requirements of hybrid cloud infrastructures while adhering to organisational and technical security standards.
- Documenting a baseline security monitoring policy detailing the events and attributes crucial for effective cyber security monitoring, forensics, and threat intelligence in hybrid cloud environments.
- Providing professional advice and guidance on adapting and integrating the documented baseline cyber security monitoring policy and logging architecture to seamlessly align with the complexities of hybrid cloud environments, ensuring cohesion with existing organisational structures, processes, and technologies.

Top Features

- Security Operations Consulting
- SIEM Design and Deploy
- Detection & Response consulting
- Documented policy and processes to support security monitoring
- Traceability of risks to event recording and alerting requirements
- Risk scenario workshops to test end-to-end capability
- User education and training

Benefits

- Traceability of monitoring requirements to risks
- Increased visibility and situational awareness
- Technology vendor agnostic capability
- Highly experienced security monitoring consultants delivering service

7. DevSecOps

Our highly skilled and experienced consultants will review and assess your organisation's DevSecOps maturity against principals found within industry maturity models and assist you in achieving the benefits of a mature DevSecOps adoption.

Adopting and transitioning to a true DevSecOps model is as much about culture and education as it is about the tools and the processes. In our experience many organisations focus on the later at the expense of the former. In addition, while adopting good DevSec practices have been the focus of many development teams, providing the SecOps to seamlessly integrate end to end service management with security is a more difficult journey.

Top Features

- Culture (relationship and collaboration between teams)
- Secure Development Training Services
- Cloud Platform Engineering
- Technology vendor agnostic assessment
- DevSecOps strategy, implementation and toolchain
- Patch and vulnerability management
- Depth of static and dynamic code analysis
- Secrets management
- Integration with wider service management
- Application Security Testing Services (AppSec)
- Secure Development Support Services

Benefits

- Documented maturity assessment and improvements roadmap
- Independent assessment against industry maturity models
- Provides useful input into risk assessments and technology roadmaps
- Identification of skills and technology gaps
- Flexible service tailored to meet the needs and priorities of your organisation

8. Identity and Access Management

Our consultants have the experience to help assess, design and rationalise the tools and process required to secure your enterprise.

Identity and Access Management is a key principle of a Zero Trust architecture: “Continuous verification, all the time, for all resources”.

The migration to cloud underscores the critical importance of Identity and Access Management in ensuring secure, efficient, and compliant access to resources and data wherever they may reside. Organisations must prioritize IAM initiatives to effectively address the unique challenges posed by cloud computing and leverage its benefits while maintaining robust security controls.

Top Features

- Identity Governance and Administration
- Identity and Access Strategy and Assessment
- Hybrid Cloud Identity Strategy
- Access Management Design and Deploy
- Multi-factor Authentication Design and Deploy
- Privilege Access Management policy and implementation
- Insider Threat Protection
- Consulting & Systems Integration

Benefits

- Centralised Management
- Improved Security
- Enhanced User Experience
- Scalability and Agility
- Compliance and Governance
- Cost Optimisation

7. Information Assurance and Security

CACI IS ISO27001, ISO9001 & CYBER ESSENTIALS+ ACCREDITED

- CACI is committed to ensuring its people, processes, information and technologies are secured in line with an industry best practice standard for security whilst adhering to our legal, regulatory and contractual obligations. CACI maintain an Information Security Policy and associated corporate policies to ensure its staff, processes, information and technologies manage the risk from threats.
- The Information Security Policy is certified to ISO/IEC 27001 best practice standard for information security. These policies are reviewed regularly by the CACI Information Security group and tested by both internal and external audits. The Business Continuity and Disaster Recovery Plan(s) are also integral to our ISO27001 accreditation. All changes in risk or interested parties' requirements are reflected in procedures across the business alongside a commitment to continual improvement and industry best practice.
- Information Intelligence Group (IIG) have secure facilities and have additional governmental controls on top of the standard CACI Security Policy.
- In addition, CACI have attained Cyber Essentials+ and ISO9001 accreditation. CACI has a very strict approach to data breaches. We are unambiguously committed to complying with GDPR with full sponsorship at Board Level.
- Staff are cleared up to Developed Vetting (DV).

8. Ordering and Invoicing Process

CACI PRIDES ITSELF IN BEING EASY TO DO BUSINESS WITH

With this in mind, we take an agile approach to all our engagements, working closely with customers and their stakeholders to design and deliver cloud services in an iterative manner. This enables us to meet specific requirements as well as delivering value and benefit for our customers as early as possible.

Prior to the delivery commencing, our Engagement Manager will work with the customer to agree the outcomes for the engagement, including:

- Defining the success criteria and ensuring the commercials align
- Agreeing specific deliverables for the engagement
- Agreeing the specific ways of working and governance for the engagement
- Understanding the security constraints and ensuring the relevant clearances are in place
- Defining and agreeing the team size/resourcing required
- Putting the commercials in place in line with the G-Cloud framework

We will then produce a proposal which contains a Services Supply Agreement, detailing the scope of work and the associated price. For details about our standard invoicing process, please refer to the Terms and Conditions document.

9. Testing and Quality Assurance

CACI TEST ENGINEERS BRING EXTENSIVE EXPERIENCE OF CLOUD-NATIVE TESTING WITH INDUSTRY RECOGNISED TOOLING

- CACI have an engineering mindset, delivering software and cloud solutions to exacting standards of performance and quality.
- Our ISTQB qualified Test Engineers have extensive experience, quality assuring and performance testing mission critical applications across the full testing lifecycle. They work in agile teams, either embedded in the customer's organisation or as part of a wider CACI team, and our Test Engineers bring a wealth of Cloud-Native Test Automation experience.
- Our testing model follows an automation by default approach and ensures continuous testing is undertaken throughout the lifecycle to help improve the quality and speed of software delivery. This includes the use of automation tooling and the implementation of Continuous Integration and Delivery (CI/CD) pipelines. Our test engineers have a DevSecOps mindset, which means they focus on quality, security and operational running when they are quality assuring a system.
- We work closely with our customers to define a Test Strategy and supporting approach to automation that is designed for services running in the cloud, be that public, private or hybrid. Our Test Engineers will work collaboratively with the business, technology and security teams to understand their requirements and associated business and technical risks. From that they define a risk-based test strategy and related test plans with automation at its heart. We can advise on the technology and tools that best meet the specific needs of each customer environment, integrating with existing systems as processes as appropriate.
- CACI Test Engineers bring extensive experience of performance testing using a range of industry recognised tooling, often processing extremely high volumes of data. We also have engineers who have experience of Data Migration and Performance Testing legacy application as they are migrated to the cloud.

10. After Sales Support and Service Levels

ITIL STYLE SERVICE OR DEVOPS STYLE SUPPORT

We provide service management and operational support for software provided by CACI and deployed in the cloud. We provide ITIL style service management capabilities alongside integrated DevOps style support. Details of the support offered are below:

- Office and extended office hours support as standard
- 24x7x365 for customers providing critical services (by agreement and additional cost)
- 1st, 2nd and 3rd line support provided as required
- Systems are in place to liaise with other support partners
- Contact via e-mail, phone and / or JIRA-based service desk ticketing system
- Custom SLAs agreed with customers to optimise the cost of service management depending on the level of support required and mission/business criticality of service
- Regular service reviews
- Focus on communications and reporting both across incident lifecycles and scheduled maintenance
- Support levels are agreed on a customer-by-customer basis to ensure the right fit to each customer's specific needs.

11. Business Continuity and Disaster Recovery Plan

OUR BUSINESS CRITICAL INFORMATION AND SYSTEMS ARE BACKED UP DAILY

- Our well established and regularly audited Business Continuity and Disaster Recovery Plans mitigates against all possible risks. The CACI Business Continuity Plan is a living and continuously updated solution which exceeds the requirements of ISO27001 accreditation. It is reviewed formally on an annual basis by external auditors as part of our ISO27001 audit and is accessible to all staff. It covers the response of the business in the case of a major incident or emergency.
- Our regular checks ensure we update our Business Continuity Plan to keep in line with emerging risks. As such it has evolved over time as we have grown as a business and taken on a broader variety of work with a range of customer requirements. The Business Continuity Plan reflects the nature of the work we do and how we would be able continue delivering the work promised to our customers in the event of an emergency or major incident. The Business Continuity Plan also considers the ever-changing threats and current political climate to ensure that our response is up to date with the threats and pressures we maybe under as a business working in the Defence and Intelligence Industries.
- The Senior Leadership Team regularly review the plan to ensure that we are aware of any changing business factors for this to remain a compliant and realistic document.
- CACI's secure connections and encrypted back-up devices are checked monthly as part of our IT Security and Encryption Procedure. In addition, the encrypted back-ups are tested and sent off site at the end of each working day to a specialist storage contractor. CACI's office in Bristol requires several systems to be operational in order to deliver the services it provide to its customers; these are tested daily by a member of the CACI Bristol Technical Team and more rigorously tested monthly by the CACI IT team as part of their Security Incident Policy and Response Procedure. The Business Continuity Plan requires these systems to be operational and effective for staff to work remotely in case of an emergency or major incident. Agreements are also in place with partner organisation, so that staff working on secure projects have back-up locations to work from.

12. Pricing Overview

WE OFFER FLEXIBLE PRICING MODELS TO ENSURE VALUE FOR MONEY

- After actively engaging with our customers to make sure our solution is the right fit, we offer a flexible commercial solution to ensure value for money. We have three typical models, namely Time & Materials, Fixed Price or Managed Service based. The following table provides more detail.
- The pricing approach for this consultancy service is set out in our Pricing Document and Lot 3 – Cloud Support Rate Card.

Model	Detail
Time and Materials (T&M)	T&M is appropriate where the requirements need further elaboration and are subject to change, or where customer consumption of certain elements, such as Architect or DevOps resource is variable. T&M is typically calculated on day rate using the Lot 3 – Cloud Support Rate Card.
Fixed Price (FP)	Fixed pricing can be offered when the statement of work requirements are clearly defined and agreed by both parties. This necessitates the availability of mature and accurate input documents so that the amount of effort to achieve the project deliverables can be calculated. In addition, any project risks, issues, assumptions or dependencies need to be stated and measured. Pricing is available on request and is based upon the day rates shown in the Lot 3 – Cloud Support Rate Card.
Managed Service (MS)	Managed Services are typically delivered via CACI's 24x7, 3-tier technical support working within our ITIL aligned Service Management system. Pricing is tailored to meet the customer's Service Level Requirements and is based upon the day rates shown in the Lot 3 – Cloud Support Rate Card.

Thank you

CACI

This report contains information and data supplied by CACI Limited that may (a) be created in whole or part using forecasting or predictive models and/or third party data and are not guaranteed to be error free by CACI, (b) contain data based on estimates derived from samples, and/or (c) be subject to the limits of statistical errors/rounding up or down. Except for title warranties all other implied warranties are excluded. CACI Limited shall not be liable for any loss howsoever arising from or in connection with your interpretation of this report.