QINETIQ

Service Definition Document

Security Assurance
Security Information Assurance Audit Security and Information Accreditation Support

Specialist Cloud Services

version 8.1

CESG Certified Service

Cyber Security Consultancy – Audit & Review

62740476CCSC

CESG Certified Service

Cyber Security Consultancy – Risk Assessment

62740476CCSC

Content

1. Introduction

QinetiQ has a large team of Information Assurance Consultants holding a variety of specialist skills, including those of the CESG Certified Professional (CCP) scheme, CISSP, CISM, 27001 Lead Auditors and Implementers.

Within most organisations information is an essential business asset critical to your success. As such, it is crucial that this information remains confidential, maintains its integrity and is available for the important business decisions to be made.

Your security can be breached in a number of ways; system failure, theft, inappropriate usage, unauthorised access or computer malware are to name a few. The consequences of such breaches can vary in severity, from the loss of sensitive or critically important information to reputational loss and/or even imprisonment.

QinetiQ's pedigree in the Information Security domain expertise can be traced back to the dawn of the Internet in the late 1970s when its predecessor, the Royal Signals and Radar Establishment (RSRE), based in Malvern, were involved in a research programme fundamental in the development and initiation of the Internet.

Having been there from the start, QinetiQ has established a reputable name as the first choice for many "blue-chip" companies, by boasting a team of industry experts, together with offering the latest technologies, capabilities and methodologies. This approach ensures consistency in advancing into the future of Cyber Security.

Because of our expertise, QinetiQ was selected to help define the security strategy for one of the largest systems integration projects currently being undertaken in the UK.

At the corporate level QinetiQ delivers expertise to develop and benchmark your overarching policy, strategy and supporting organisational structures and at the operational level to develop detailed security policy and strategy for individual business units or information systems.

For G-Cloud services QinetiQ can offer the following expertise that is aligned to the Service Offering Descriptions described in greater detail later in this document:

- security strategy
- security risk management
- security design
- cyber security consultancy
- security testing
- security incident management
- security audit services

Additional Cyber Security Services

- Cyber Security Threat Check.
- Military Cloud Services

QinetiQ is also vendor independent, so we are able to give you impartial advice to balance the best practice security protection against operational cost and need.

In addition to providing professionally qualified consultants, QinetiQ have been leading with CESG on the development of the CESG Certified Consultancy Scheme. This scheme aims to build on the experience of the CLAS scheme by certifying the services offered by consultancies to help customers' better match their requirements to services that consultancies offer. This approach will enable the delivery of a wider and more complex range of security services to government and other clients.

QinetiQ's expertise in this delivery has been independently and rigorously assessed by the NCSC under their Cyber Security Consulting Scheme (CSCS).

Each service offered is be led by a Head of Service Delivery who will have overall responsibility for that Service and has been interviewed by CESG to establish competence to deliver the Services stated.

We support a wide variety of HMG customers with a large number of services including; strategic research studies, vulnerability and threat assessments, IT Security Health Checks (ITSHC), Penetration Testing, security audits, security awareness training, accreditation support services such as risk assessments and technical controls audits and manpower to fill security relevant roles such as Security and Information Risk Advisor (SIRA), IT Security Officer (ITSO) or Security Assurance Coordinator (SAC).

Our team are delighted to discuss your requirements and how QinetiQ can help.

This offering to G-Cloud is based on elements from QinetiQ's Advanced Cyber Threat team. It contains Service Descriptions for the following services:

- Security Assurance Coordinator/IT Security Officer(ITSO);
- Security Information Assurance Audit Services
- Security and Information and Accreditation Support
- Security Information Assurance Consultancy Services
- Cyber Security Preparedness Review Consultancy Service
- Cyber Security Maturity Review Consultancy Service
- Cyber Security Remediation Consultancy Support Service
- Information Technology Security Health Check (ITSHC) - Network and/or Application Technical Assessment Service
- Cyber Threat Check Service
- ISO 27001 Information Security Management System Sample Audit Service
- Military Cloud services

2. Security Assurance Coordinator/ITSO Service

The IT Security Officer (ITSO) and Security Assurance Coordinator (SAC) provide impartial management of the Information Assurance (IA) of Information Systems (IS) in-line with security policy to deliver the Senior Information Risk Manager's (SIRO's) strategy.

Features

- Contributing to development of Risk Assessments to agreed national standards
- Contributing to development of SyOPs for new IT systems
- Providing advice on compliance with IT security policy
- Reviewing effectiveness of IT security controls
- Assisting investigations into IT security incidents
- Governance of Information Assurance
- Liaison with Accreditors and other Stakeholders

Benefits

- Ensuring IT security policy is updated as security threats evolve
- Defining target end state for security controls in IT systems
- Reporting the effectiveness of IT security controls to the DSO
- Advising on compliance with IT security policy and controls
- Contributing to IT service level definitions
- Promoting a security aware culture
- Initiating investigations into IT security incidents
- Consistency of approach to Accreditation risk management and governance

Service documents

- pdf document: Pricing
- pdf document: SFIA rate card
- pdf document: Service definition
- pdf document: Terms and conditions

Contact

QinetiQ Ltd

QinetiQ Framework Contract Management Office

01684 543800

OST@qinetiq.com

Pricing

The Pricing is on a resource day rate basis in accordance with the SFIA rate card.

All pricing is exclusive of VAT.

Ordering and Invoicing

On receipt of a request, QinetiQ can provide a proposal for the required resources to deliver the service.

Billing for the service is monthly in arrears. Payment can be via Purchase Order.

Termination Costs

There are no termination costs for this Service.

Consumer Responsibilities

As agreed on a case by case basis and stipulated in individual contracts and to provide where necessary, information relevant to specific analysis being conducted.

3. Security Information Assurance Audit Service

This service delivers confidence that risks to information systems are properly managed with a robust Information Assurance (IA) regime, and that formal assessment of an information system against its IA requirements is known and agreed prior to any accreditation.

Features

- Information Assurance Consultancy
- CESG Certified Cyber Security Consultancy
- CESG Certified Professionals (CCP)
- CCP staff at Practitioner, Senior and Lead for Audit discipline
- CISSP
- ISO/IEC 27002
- ISO/IEC 27001
- Leading audits assessing compliance with IA policies
- Providing supervision and guidance to IA auditors
- Developing audit plans

Benefits

- Providing independent opinion on IA control objectives
- Identifying systemic trends and weaknesses in security

- Recommending responses to audit findings
- Requirements analysis
- Provision of advice on management of security and information risk
- Company-wide assessment of consultancy services approved by CESG
- Assessed services led by Head of Delivery to provide governance and ensure consistency

Service documents

- pdf document: Pricing
- pdf document: SFIA rate card
- pdf document: Service definition
- pdf document: Terms and conditions

Contact

QinetiQ Ltd

QinetiQ Framework Contract Management Office

01684 543800

OST@qinetiq.com

Pricing

The Pricing is on a resource day rate basis in accordance with the SFIA rate card.

All pricing is exclusive of VAT.

Ordering and Invoicing

On receipt of a request, QinetiQ can provide a proposal for the required resources to deliver the service.

Billing for the service is monthly in arrears. Payment can be via Purchase Order.

Termination Costs

There are no termination costs for this Service.

Consumer Responsibilities

As agreed on a case by case basis and stipulated in individual contracts and to provide where necessary, information relevant to specific analysis being conducted.

4. Security and Information Accreditation Support Service

Security and information risk advice provides a firm understanding of the security risk environment. It identifies the potential threats and vulnerabilities and evaluates them in terms of likelihood and impact, to determine how the resulting risks may be reduced.

Features

- Bespoke Threat and Vulnerability Assessment creation and analysis
- Risk Assessment
- Security controls development
- Development of Risk Management Accreditation Document Sets (RMADS)
- HMG IA Standards
- Requirements analysis
- IAS1
- IAS2
- Domain Based Security (DBSy®)
- Acuity STREAM to capture security requirements and measure progress
- Information Assurance Consultancy
- Accreditation support services
- Security and Information Risk Advisor service

Benefits

- Selection of appropriate risk assessment techniques
- Identification of systemic information risks
- Recommending implementation of new IA controls
- Development of new IA controls and policies
- Ensuring compliance with applicable security and IA standards
- Ensuring effective management of security incidents
- Management of Senior Security and Information Risk Advisors
- Robust tracking and reporting for Governance Risk and Compliance

Service documents

- pdf document: Pricing
- pdf document: SFIA rate card
- pdf document: Service definition
- pdf document: Terms and conditions

Contact

QinetiQ Ltd

QinetiQ Framework Contract Management Office

01684 543800

OST@qinetiq.com

Pricing

The Pricing is on a resource day rate basis in accordance with the SFIA rate card.

All pricing is exclusive of VAT.

Ordering and Invoicing

On receipt of a request, QinetiQ can provide a proposal for the required resources to deliver the service.

Billing for the service is monthly in arrears. Payment can be via Purchase Order.

Termination Costs

There are no termination costs for this Service.

Consumer Responsibilities

As agreed on a case by case basis and stipulated in individual contracts and to provide where necessary, information relevant to specific analysis being conducted.

5. Security Information Assurance Consultancy Service

This offering to G-Cloud is based on elements from QinetiQ's Advanced Cyber Threat team. It contains Service Descriptions for the following three services:

- Security Assurance Coordinator/IT Security Officer(ITSO)
- Security Information Assurance Audit Services
- Security and Information Accreditation Support

Features

- Information Assurance Consultancy
- CESG Certified Cyber Security Consultancy
- CESG Certified Professionals (CCP)
- CCP staff at Practitioner, Senior and Lead for SIRA and Audit disciplines

- CISSP
- CISM
- ISO 27001 Lead Auditors
- Strategic research studies
- Vulnerability assessments
- IT Security Health Check (ITSHC)
- Penetration Testing
- Accreditation support services
- Security audits
- Technical controls audits

Benefits

- Providing advice on compliance with IT security policy
- Reviewing the effectiveness of IT security controls
- Assessing threats, and recommending effective measures
- Developing architectures attuned to the customers' specific requirements
- Delivering security strategy and policy based on industry best practice
- Promoting security awareness and skills through training people
- Helping customers attain and maintain accreditation for their systems

Service documents

- pdf document: Pricing
- pdf document: SFIA rate card
- pdf document: Service definition
- pdf document: Terms and conditions

Contact

QinetiQ Ltd

QinetiQ Framework Contract Management Office

01684 543800

OST@qinetiq.com

Pricing

The Pricing is on a resource day rate basis in accordance with the SFIA rate card.

All pricing is exclusive of VAT.

Ordering and Invoicing

On receipt of a request, QinetiQ can provide a proposal for the required resources to deliver the service.

Billing for the service is monthly in arrears. Payment can be via Purchase Order.

Termination Costs

There are no termination costs for this Service.

Consumer Responsibilities

As agreed on a case by case basis and stipulated in individual contracts and to provide where necessary, information relevant to specific analysis being conducted.

6. Cyber Security Preparedness Review Consultancy Service

This review is to give an understanding of potential gaps and remediation activities the client should be undertaking prior to a more in-depth review, or formal audit by a third party. This is a basic level compliance based review, as opposed to any technical testing, conducted at the operational Headquarters of the client.

Features

- Review of cyber security plans
- Review of arrangements and the assigned roles/responsibilities for cyber.
- Review of the approach in relation to risk assessment
- Review of the approach to risk management
- Review of how residual risk is documented
- Review of the approach regarding training of personnel.

Benefits

- provides an overview of current cyber preparedness;
- compares to present industry standards, guidance and good practice;

Service documents

- pdf document: Pricing
- pdf document: SFIA rate card
- pdf document: Service definition
- pdf document: Terms and conditions

Contact

QinetiQ Ltd

QinetiQ Framework Contract Management Office

01684 543800

OST@qinetiq.com

Pricing

The Pricing is on a resource day rate basis in accordance with the SFIA rate card.

All pricing is exclusive of VAT.

Ordering and Invoicing

On receipt of a request, QinetiQ can provide a proposal for the required resources to deliver the service.

Billing for the service is monthly in arrears. Payment can be via Purchase Order.

Termination Costs

There are no termination costs for this Service.

Consumer Responsibilities

As agreed on a case by case basis and stipulated in individual contracts and to provide where necessary, information relevant to specific analysis being conducted.

7. Cyber Security Maturity Review Consultancy Service

An in-depth assessment from an organisational perspective which looks at the 'cyber maturity' of the client. Clients benefit by receiving a thorough understanding of the risks and threats that they face in terms of compliance, technical cyber attack, and potential reputational damage. Clients also benefit by understanding any gaps in their posture and possible measures to address these.

Features

- In depth review and maturity assessment of cyber security plans
- In depth maturity assessment and report of arrangements and the assigned roles/responsibilities for cyber.
- In depth assessment and report of the maturity of approach to risk assessment of core assets critical to the business
- In depth assessment and report of the maturity of the approach to risk management
- In depth review of how residual risk is documented
- In depth assessment and report of threat and vulnerability management
- In depth maturity assessment and report

- A consultant-led Workshop attended by appropriate members of the client's team
- A detailed questionnaire generated for the client prior to the Workshop enables the client to gather the requisite information
- Review of the approach regarding training of personnel

Benefits

- Comparison with present industry standards, guidance and good practice;
- An in depth assessment of maturity against formal security requirements i.e. ISO27001, NIST etc
    - Level 1: the organisation has ad hoc processes, also described as 'Initial'.
    - Level 2: the organisation has a developing system of repeatable processes, termed 'Established'.
    - Level 3: the organisation has formally defined steps or a 'Performing' system termed 'Business Enabling'.
    - Level 4: the organisation has managing results by metrics or 'Sustaining' termed 'Quantitatively Managed'.
    - Level 5: the organisation has active optimisation or continuous improvement of the processes termed 'Optimised'

An in depth assessment of current cyber maturity enabling a remediation plan to address shortfalls;

Service documents

- pdf document: Pricing
- pdf document: SFIA rate card
- pdf document: Service definition
- pdf document: Terms and conditions

Contact

QinetiQ Ltd

QinetiQ Framework Contract Management Office

01684 543800

OST@qinetiq.com

Pricing

The Pricing is on a resource day rate basis in accordance with the SFIA rate card.

All pricing is exclusive of VAT.

Ordering and Invoicing

On receipt of a request, QinetiQ can provide a proposal for the required resources to deliver the service.

Billing for the service is monthly in arrears. Payment can be via Purchase Order.

Termination Costs

There are no termination costs for this Service.

Consumer Responsibilities

As agreed on a case by case basis and stipulated in individual contracts and to provide where necessary, information relevant to specific analysis being conducted.

8. Cyber Security Remediation Consultancy Support Service

Remediation support to improve the maturity of cyber security following a Maturity Review, by providing policies and templates and by guiding clients through the risk assessment process. This supports clients in achieving compliance to industry guidelines and good practice, including ISO27001, NIST requirements etc. The areas where remediation is needed may come from one of our other assessments, or from the client's own analysis of their needs.

Features

- We supply a set of policies and templates for the management, governance, and operational delivery of cyber security
- Templates supplied are tailored to suit the operational model within which the client operates
- Provisioned as a remote service to reduce cost and time constraints
- Supported by an Information Assurance professional to guide the client through the essential policies and procedural elements.

Benefits

- Tailored remediation activity specific to client need
- The nature and length of the engagement is determined by the identified gaps, and how much support the client requires.
- Output is client driven to achieve desired maturity level

Service documents

- pdf document: Pricing
- pdf document: SFIA rate card
- pdf document: Service definition
- pdf document: Terms and conditions

Contact

QinetiQ Ltd

QinetiQ Framework Contract Management Office

01684 543800

OST@qinetiq.com

Pricing

The Pricing is on a resource day rate basis in accordance with the SFIA rate card.

All pricing is exclusive of VAT.

Ordering and Invoicing

On receipt of a request, QinetiQ can provide a proposal for the required resources to deliver the service.

Billing for the service is monthly in arrears. Payment can be via Purchase Order.

Termination Costs

There are no termination costs for this Service.

Consumer Responsibilities

As agreed on a case by case basis and stipulated in individual contracts and to provide where necessary, information relevant to specific analysis being conducted.

9. Information Technology Security Health Check (ITSHC) – Network and/or Application Technical Assessment Service

An on-site IT Security Health Checks (sometimes referred to as Penetration Testing) assessing security vulnerabilities in computer systems, from the perspective of an attacker with direct access to the network under test. Experts undertake testing which aims to simulate attacks against a target application or network using the same tools and techniques as the most highly skilled adversary.

Features

- All tests undertaken by QinetiQ are scoped by the professionally certified Security Health Check team
- Scope is highly accurate and offers the best value whilst addressing any specific concerns

- Every engagement is effectively bespoke/tailored to specific requirements, taking into account the risk profiles both of the system to be tested and of the customer.
- Testing can be conducted to deliver results for:
    - Infrastructure - testing of servers, security devices and network components to ensure they are built and secured in line with best practice
    - Applications - assessing the threat from both authenticated and unauthenticated attackers to published applications
    - Wireless/'Bluetooth' - networks based on both 802.11 and Bluetooth.
    - VoIP - concentrates on phone systems to determine how vulnerable it is to either deliberate Denial of Service or more subtle attacks such as eavesdropping or call redirection
    - On-host - a point-in-time assessment of the security posture of a particular host, whether this is a standard build desktop, server or infrastructure component
    - Product Assessments - bespoke assessments into both existing and new hardware/software solutions;
    - Social Engineering - a view of how easily its internal processes and staff can be manipulated to divulge sensitive information or to perform actions which might make further attacks possible;
    - 'Red Teaming' - the ultimate, practical, real world, assessment of an organisation's security position

Benefits

- Tailored activity specific to client need;
- Allows client understanding of their 'defence in depth' security by revealing the vulnerabilities that would be visible to a malicious insider.
- A full report and optional presentation describing activities and outcomes;
- reports prioritise areas of technical risk and present them in an easily understandable and actionable format

Service documents

- pdf document: Pricing
- pdf document: SFIA rate card
- pdf document: Service definition
- pdf document: Terms and conditions

Contact

QinetiQ Ltd

QinetiQ Framework Contract Management Office

01684 543800

OST@qinetiq.com

Pricing

The Pricing is on a resource day rate basis in accordance with the SFIA rate card.

All pricing is exclusive of VAT.

Ordering and Invoicing

On receipt of a request, QinetiQ can provide a proposal for the required resources to deliver the service.

Billing for the service is monthly in arrears. Payment can be via Purchase Order.

Termination Costs

There are no termination costs for this Service.

Consumer Responsibilities

As agreed on a case by case basis and stipulated in individual contracts and to provide where necessary, information relevant to specific analysis being conducted.

10. Cyber Threat Check Service

Cyber Threat Check capability provides a snapshot of threats to your enterprise and actionable intelligence by combining tactical information with a wider threat intelligence picture from a variety of sources. Combines data gathered from client systems with information from our own monitoring systems and services, along with Open Source intelligence, to form a snapshot of the threat landscape for a client organisation

Features

- Real attack information collected from systems and networks.
- Threat intelligence data, showing trends in campaigns, attacks and vulnerability exploitations.
- Technical threat information.
- Analysis based on a library of network attack signatures working with an advanced behaviour anomaly detection engine including rules tailored to specific enterprise threat analysis.
- A targeted view of campaigns and attacks tailored to particular business sectors.
- Open Source Threat Intelligence harvested from a wide variety of web and social media sites

- Collectors can be distributed throughout an Enterprise or combined in a single appliance, depending on the size of the network.
- Data collected from switch SPAN ports, up to 10Gbps line speeds for packet capture.
- Collectors can run in virtualised (cloud) environments as well as physical networks.
- Using advanced behaviour anomaly detection and Big Data technology for large-scale storage and analysis.

Benefits

- A tailored snapshot of targeted threats and potential attacks to the client.
- Recommended actions including emergency action, triage, or further observation.
- Observed trends over a thirty-day period of cyber threat trends and intelligence.

Service documents

- pdf document: Pricing
- pdf document: SFIA rate card
- pdf document: Service definition
- pdf document: Terms and conditions

Contact

QinetiQ Ltd

QinetiQ Framework Contract Management Office

01684 543800

OST@qinetiq.com

Pricing

The Pricing is on a resource day rate basis in accordance with the SFIA rate card.

All pricing is exclusive of VAT.

Ordering and Invoicing

On receipt of a request, QinetiQ can provide a proposal for the required resources to deliver the service.

Billing for the service is monthly in arrears. Payment can be via Purchase Order.

Termination Costs

There are no termination costs for this Service.

Consumer Responsibilities

As agreed on a case by case basis and stipulated in individual contracts and to provide where necessary, information relevant to specific analysis being conducted.

11. ISO 27001 Information Security Management System - Sample Audit Service

Where Information Security Management System (ISMS) documentation exists in line with ISO27001, QinetiQ can perform a compliance audit to check that the client's documented processes and procedures are being implemented at the operational level, and adhered to, as directed by the policies.

Features

- Delivered by trained and experienced British Standard Institute (BSI) ISO 27001 Lead Auditors to undertake the audit activity.
- Scope and duration of the audit is agreed with the client prior to the assessment
- Sample based compliance audit can include corporate HQ, satellite locations or both, according to the needs of the client.

Benefits

- A full report of the findings of the sample audit.
- The sample approach is standard auditing practice and therefore usable as evidence.
- Recommended actions including emergency action, triage, or further observation.
- Bounded activity for the specific client environment

Service documents

- pdf document: Pricing
- pdf document: SFIA rate card
- pdf document: Service definition
- pdf document: Terms and conditions

Contact

QinetiQ Ltd

QinetiQ Framework Contract Management Office

01684 543800

OST@qinetiq.com

Pricing

The Pricing is on a resource day rate basis in accordance with the SFIA rate card.

All pricing is exclusive of VAT.

Ordering and Invoicing

On receipt of a request, QinetiQ can provide a proposal for the required resources to deliver the service.

Billing for the service is monthly in arrears. Payment can be via Purchase Order.

Termination Costs

There are no termination costs for this Service.

Consumer Responsibilities

As agreed on a case by case basis and stipulated in individual contracts and to provide where necessary, information relevant to specific analysis being conducted.

12. Military Cloud Services

This service delivers consultants with expertise in all aspects of Cloud hosting, software and support. The team work very closely with the Government agencies and are specialists in MoD systems and their security.

Features

Cloud support – focused on military systems, that can include

- planning
- setup and migration
- training
- security services
- quality assurance and performance testing
- ongoing support

Benefits

- Specialists in government requirements
- Security paramount to all services
- Assessed services led by Head of Delivery to provide governance and ensure consistency

Service documents

- pdf document: Pricing

- pdf document: SFIA rate card
- pdf document: Service definition
- pdf document: Terms and conditions

Contact

QinetiQ Ltd

QinetiQ Framework Contract Management Office

01684 543800

OST@qinetiq.com

Pricing

The Pricing is on a resource day rate basis in accordance with the SFIA rate card.

All pricing is exclusive of VAT.

Ordering and Invoicing

On receipt of a request, QinetiQ can provide a proposal for the required resources to deliver the service.

Billing for the service is monthly in arrears. Payment can be via Purchase Order.

Termination Costs

There are no termination costs for this Service.

Consumer Responsibilities

As agreed on a case by case basis and stipulated in individual contracts and to provide where necessary, information relevant to specific analysis being conducted.