



Qi Consulting
www.qi-consulting.co.uk

G-Cloud 14 Cloud Support Services

Service 3: Cyber Security Risk Assessment & Management

- **Service Overview**

We provide Cyber Security risk assessment and risk management services to support your Cloud-based solutions, delivered by our consultants.

This service supports an organisation's in-house security team by providing an expert add-on to existing capabilities covering all aspects of information assurance including:

- Development and analysis of IT security policies and procedures
- IT and business risk analysis and business impact analysis
- BS/ISO 7799 health-checks, compliant policies, procedures and implementation
- Implementation of Government security standards
- Development of understandable risk appetite statements
- Risk Management and Accreditation Documentation Set (RMADS)
- Advice on the application of the NIST 800-39 Risk Management approach
- Information Security Reviews
- Mentoring and training

All our cyber security consultants have experience of operating at board level and tailoring the services we deliver to specific business need. We apply these skills to provide assurance to stakeholders in the soundness of information handling.

Our emphasis is on knowledge transfer, we provide mentoring and training, and work in joint teams to ensure the required information assurance skills and awareness are in place throughout the customer organisation.

We facilitate risk assessments in our client organisations. We can bring knowledge of generic threat sources, and specific threat sources in some areas. We share our knowledge of the process of carrying out risk assessments. We normally use a qualitative NIST 800-30 approach, but can also use IS1&2 if required.

We also provide advice, guidance and recommendations on how Information Assurance exposures, including cyber security risks, could be managed to help clients make risk decisions and develop strategies for risk management.

We will develop or strengthen the client's risk management framework which defines how assets are to be protected, systems monitored, recovery planned and practised and where risks are accepted.

We can provide advice on the application of the NIST 800-39 Risk Management Approach in the context of the SPF security outcomes and good commercial practice.

- **Service Management**

Our team of Service Managers focuses on providing a seamless service to our customers. They examine requests for resources, locate suitable candidates, draft tender bids and maintain contact with our consultants during their assignments.

Our Assignment Lead will agree with the customer at project initiation exactly what management reports will be required and in what format. We then commit to deliver these reports to the required timescales. Key performance indicators are developed and agreed with the customer to ensure the effective measurement of performance and the outcomes of all assignments.

During the course of the assignment continuous dialogue on progress takes place between the consultants and the customer and monthly 'Keep in Touch' progress meetings (KITs) are arranged to formally report on the progress of the project. In addition, where appropriate, a 'sign-off' meeting is held to present the final report, finalise the project and discuss post-contract completion support, if any is necessary.

- **Service Levels**

Customers are allocated dedicated Service Managers who will:

- Maintain contact with key buyers at mutually agreed intervals and undertake quarterly contract review meetings if desired.
- Be available to answer requests or queries during the hours agreed. This is typically 09.00 – 17.00 office hours, 07.00 – 21.00 via mobile phone.
- Work towards the following response times for the provision of services:

Start date	Target Response Time
Same Day	1 hour
Next Business Day	3 hours
1-2 Business Days	4 hours
3-6 Business Days	1 Business Day
7 or more Business Days	3 Business Days

We have an established set of processes and procedures to deal with any issues raised regarding the performance of both our consultants and account management team. This forms an integral part of our ISO9001:2015 accredited Quality Management System.

- **Sub-contractors**

Qi Consulting consists of a small central organisation with access to a pool of over 600 associate consultants, SMEs and selected specialist partners. We have a very broad base of experience amongst our associate consultants, however in order to deliver the best value to our clients we often use partners to enhance our delivery capability in specialist areas.

Because of our structure and delivery approach we have developed a robust approach to selecting and managing third party relationships, which is strictly on the basis that:

- Qi Consulting retains the contractual relationship and responsibility for the quality and timeliness of the work;
- The use of any third party is transparent to our client; and
- The work is managed in accordance with our ISO 9001:2015 certified QMS.

- **Training**

We aim to ensure that all the consultants providing our Cyber Consultancy Services under this framework are fully up to date with current thinking on the subject. We do this in three ways: through the professional development of our consultants; through formal and informal networks; and by maintaining knowledge repositories.

All our consultants that will be providing the service are CCP Certified and are members of professional and industry bodies including: BCS, IISP, Cyber Security Clusters and OWASP.

Each has a CPD plan which will include identifying ongoing activities to maintain the currency of their knowledge of cyber threats and their mitigation. As part of their professional development, our consultants attend conferences on Information Technology, systems engineering, data quality and other related matters. Through professional membership they have access to libraries such as CLASKB, IEEE, ACM and BCS.

All of our consultants are familiar with the policy issues and operational challenges facing the public sector, and therefore understand how cyber security fits into the overall picture.

Our knowledge repository provides a first point of reference for any investigation. This consists of information collected from internal and external sources including desk-based research, points of view, papers from professional bodies, information from suppliers, and informal peer networks.

- **Quality Management and Customer Satisfaction**

Qi Consulting uses its ISO 9001:2015 certified Quality Management System to manage, track and report on all assignments from bids to closure. Our QMS contains documented procedures and standards for, amongst other things: customer requirements handling; service realisation; document and data control; internal quality audit; management review; performance measurement and improvement; corrective and preventive action; and customer satisfaction.

These quality standards are mandatory for all services we deliver. They are monitored on a day-to-day basis by our directors and Quality Assurance Manager, and through an annual external audit by BSI.

Wherever possible we seek a formal post-assignment review, which includes feedback on the success of an assignment as a whole; its management; the performance of our team; and of the Qi Consulting Service Manager. It also seeks the customer's assessment of whether the assignment met or exceeded their expectation and their view of the overall value-for-money achieved.

We will seek customer feedback, both positive and negative, relating to an individual consultant's performance. Any negative feedback is followed up with the consultant involved, and we make every attempt to provide support to an individual to ensure that any issues can be avoided in the future.

- **Information Security**

Qi Consulting has an ISO/IEC 27001:2013 certified Security Management System, audited by BSI. As part of this we have implemented appropriate policies, procedures and technologies to protect Qi Consulting against cyber threats, using the same knowledge and cyber services we provide to our customers. We are also Cyber Essentials certified.

We have ISMS policies to protect our and our customers' confidential information. These cover: access control and password policy; anti-piracy; backup and restore; Data Protection; network systems monitoring; remote access and mobile computing; virus protection; information classification and labelling. We also implement a security incident management process.

We have a fully documented Business Continuity Plan, which is tested on an annual basis. Our server is backed up each day and a copy held off-site. A back-up server is maintained at an off-site location 30 miles from the main site. Disk restores are tested on a weekly basis. A full restore procedure is performed at least annually. Qi Consulting staff are able to work remotely and continue to operate the company's business even in the event of a disaster or emergency situation, and our consultants will continue to be able to provide services to our customers.

- **Ordering and Invoicing**

Customers can order services using the standard CCS pro forma or issue their own Purchase Orders.

Our invoicing processes are fully integrated with:

- Individual customers' Purchase to Pay (P2P) paperless systems (typically by registering with a secure web-based P2P system); and
- Supply chain/subcontractor paperless systems - all invoices, effort returns, expense claims and scanned evidence (e.g. receipts) are routed to a nominated email account; all payments are made by BACS, with remittance advices by email.

Depending on customer requirements, invoices can be:

- Monthly or weekly;
- Consolidated personnel invoices; and
- Consolidated single invoices of all consultants in a team.

Our secure system ensures verification and accuracy through checking at each stage in the process:

- Excel templates are used with built-in calculations to ensure accurate totaling of effort, rates, expenses and VAT; and
- Independent audit ensures that the contracted terms detailed in our management information system, including thresholds for discounts, are applied accurately.

Invoicing is undertaken monthly in arrears or based on agreed project milestones.

- **Pricing**

We can offer a variety of pricing models including fixed price and time and materials. Please see the document "Qi Consulting SFIA Definitions and Rate Card" for our day rates for this service.

- **Terms and Termination**

Please refer to the document "Qi Consulting Terms and Conditions".

The contract may be terminated by either party at 30 days' notice (by Qi Consulting if the service is being removed from the G-Cloud framework).

- **Further Information**

For more information please contact servicemanager@qi-consulting.co.uk or visit our website at <http://www.qi-consulting.co.uk/our-services/>