

Cyber Security Risk Assessment Services

A QinetiQ Cyber Security Service

Key Benefits

- Enables the business to clearly identify, and evaluate the business cyber risks allowing a clear focus on priority risks
- Modelling methodology allows risks to be identified in a business context, and articulated in business language for the benefit of senior decision makers
- Approach clearly identifies mitigating controls and via the workshop methodology allows options to be discussed to manage residual risks

Risk assessment is the identification, evaluation, and prioritisation of risks (defined as the potential that a threat will exploit a vulnerability in a business asset causing harm to the organisation) as a basis for subsequent risk management.

Risk management is the process of coordinating activities to direct and control an organisation in managing information risk so as to preserve the Confidentiality, Integrity and Availability of business information objectives, processes and assets. This also protects the reputation of the business. It encompasses the application of resources to minimise, monitor, and control the identified risks.

The QinetiQ Approach

QinetiQ's Security Risk Assessment Framework (SRAF) has been designed to tackle real-world risk assessment assignments expediently and pragmatically. The methodology is hierarchically applied to decompose complex systems, producing detail only in key areas, as required. It produces concise dashboard visualisations and actionable output which is easily consumed and rapidly assimilated at senior levels.

QinetiQ's ability to automate the labour-intensive parts of the risk assessment process enables our consultants to undertake pragmatic and realistic assessments of your complex real-world 'systems of systems' and to generate 'what-if' scenarios. This allows investment decisions to be made informed by risk-based evidence. Our consultants add value by focusing on the 'so what?' of the risk assessment assisting the client to determine, understand, and prioritise suitable remedial actions to manage risk.

Our team will rapidly capture and develop a rich model of business domains and information flows and develop it to detail relevant infrastructure artefacts, enabling our security experts to agree the scope of the system of interest and subsequently:

– Enumerate threats and risks (top down).

– Enumerate the compromise paths and evaluate the risks (bottom up).

QINETIQ IN CONFIDENCE

QINETIQ

Cyber Security Risk Assessment Approach

Using our highly visual Cyber ADVANTAGE™ (CyAD™) methodology, we are able to rapidly capture and develop a rich model of business domains and information flows and develop this model to detail relevant infrastructure, assets and artefacts. We supplement these entities to capture pertinent Threat Actors, associated levels of trust and identified risks.

Our Security Architects and Cyber Consultants work with you to undertake risk assessment at any of the three phases of system development: Requirements; Design; and Implementation. Each phase has a specific risk profile which may be tracked across the system lifecycle.

The CyAD™ model is based around the concept of a security domain, which represents a logical place where people work with information using a computer system, and which has connections with other security domains which are necessary to support business activity. Consequently, the focus is on the information that needs protection, the people that work with it, and the people with whom they exchange information.

The CyAD™ model can also describe the physical environments where people work, and the system boundaries where major system security measures are placed.

A systematic method is then applied to the model to identify and describe the risks to which valuable information assets are exposed, and to specify security measures that are effective in managing the risks cost effectively.

Basis of Service

We recommend that an initial Workshop is held with relevant stakeholders and SMEs to undertake the initial information gathering, capture the high-level CyAD™ model, and co-develop the rich systems level model.

This work provides a common basis of understanding and will enable QinetiQ to enumerate the threats, compromise paths and risks to produce the first level risk assessment.

Based on the initial Workshop and initial risk assessment, it is likely that some business areas or systems would benefit from a more detailed analysis and granular risk assessment.

In that situation, QinetiQ will work iteratively with the relevant stakeholders and SMEs to refine this deeper-level risk assessment to the point where the specific impact of those risks and options for their remediation are clearly articulated.

Input – we will ask your organisation to make suitable stakeholders and SMEs available. Access to relevant corporate documentation including risk management processes, network diagrams, processes and procedures will also be required to complete this work.

Output – a report indicating the current level of risk and its impact will be provided, together with prioritised recommendations for remedial actions to reduce risk.

The output report will comprise the following elements:

- Executive Summary including the risk and impact dashboard.

- The CyAD™ model.

- The risk assessment methodology.

- Impact statements with Confidentiality, Integrity and Availability risk analysis.

- Glossary and Definition of terms.

Other QinetiQ Cyber Services

This service forms part of a wider service portfolio, which helps organisations mature their digital resilience and to build and evidence confidence in their ability to deal with cyber-attacks through a holistic approach.

This service is a sub-service of Cyber Security Advisory.

Why QinetiQ Cyber

- Unmatched team of security vetted, expert cyber consultants, architects, engineers and human performance scientists
- Unique experience and patented intellectual property in securing the world's most complex, safety critical environments
- UKCSC registered cyber professionals, NCSC Assured Services

Copyright QinetiQ Ltd 2026 | CYBER SECURITY RISK ASSESSMENT SERVICES QINETIQ/20/01806

For further information please contact:

Malvern Technology Centre St
Andrews Road, Malvern
Worcestershire, WR14 3PS
United Kingdom
+44 (0)1252 392000
cyberenquiries@QinetiQ.com
www.QinetiQ.com