

Cyber Maturity Review Service

A QinetiQ Cyber Security Service

Key Benefits

- Analysis and assessment of the cyber maturity of the business organisation
- Suitable for organisations of all sizes and in all sectors
- Recommendations of standards suitable for the individual organisation
- Assessment can be undertaken against a wide range of industry relevant guidelines and standards
- Allows cost effective focus on specific areas needing improvement

Cyber Security guidance and standards can be complex and often difficult to navigate, informing a multitude of options and approaches to achieve compliance to good practice. Understanding the organisation's maturity allows a focussed approach to be taken, allowing the business to manage specific areas needing improvement. This targeted approach allows for a cost-effective methodology to be implemented, which will support cyber governance objectives; align to specific standards; or act as an enabler in achieving a formal certification against an industry standard.

The initial assessment is key to understanding the organisational maturity and can be benchmarked against relevant industry good practice. Subject to your requirements we can assess against the following exemplar approaches;

- ISO 27001 – Information technology – Security techniques – Information security management systems – Requirements

- National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF)

- Network and Information Systems Directive (NISD)

- NCSC Cyber Assessment Framework (CAF)

- Cybersecurity Capability Maturity Model (C2M2)

These assessments will be completed for the IT systems, the IT/OT interfaces, including the controls in place at the boundaries for those systems. It will be delivered by professionally qualified cyber security consultants.

The QinetiQ Approach

QinetiQ's Cyber Maturity Review is a base level maturity assessment that will deliver an understanding of your cyber maturity when assessed against specific standard(s) and good practice and identify remedial actions necessary to improve the maturity of your environment. It will include:

– A consultant-led Workshop attended by appropriate members of your team(s) allowing an in-depth review and maturity assessment of your cyber security plans to be complied

– In depth maturity assessment and report of your cyber security arrangements and the assigned roles/responsibilities

– In depth assessment and report of the maturity of your cyber security approach to identifying and protecting core assets critical to your business operations

– An assessment report of the maturity of your approach to managing cyber risks, including residual risks

– Comprehensive assessment and report of the maturity of threat and vulnerability management practices and approach

– Review of your methods regarding the ongoing cyber awareness and training of your personnel.

QINETIQ IN CONFIDENCE

On completion of the review, you will gain a more detailed understanding of your level of cyber maturity or compliance to the specific cyber standard(s), demonstrating how you compare against industry good practice, with a QinetiQ-provided roadmap to achieve improvements where necessary.

Our review is based on cyber good practice, enabling us to gain the necessary insight into your organisational cyber practices and culture. The approach will make use of a facilitated Workshop with your key cyber stakeholders, to undertake an initial fact-finding exercise against the chosen standard(s). This will identify of any areas requiring potential improvements.

This activity will provide an understanding of the independently assessed areas of shortfall in your organisational security posture and support the creation of a prioritised roadmap enabling you to complete a project plan for the closure of the identified gaps. QinetiQ's approach will allow for the maximum re-use of current policies and other business procedures for a cost-effective, targeted outcome.

The assessment approach assesses the cyber maturity of your organisation in relation to industry good practice and recognised standards. For reporting and assessment processes, we will use the following descriptors:

- Level 1 – Initial: your organisation adopts ad hoc processes only

- Level 2 – Established: your organisation is a developing system of repeatable processes to identify and manage cyber risk

- Level 3 – Business enabling: your organisation has formally defined steps or a performing system that has been established as part of your business processes

- Level 4 – Quantitatively managed: your organisation reviews results by metrics or sustaining system to pro-actively identify and manage cyber risk

- Level 5 – Optimised: your organisation has fully adopted cyber security risk management into your continuous improvement of the processes.

Basis of Maturity Review

Based on the Workshop and initial findings, it is likely that some business areas or systems would benefit from a more detailed assessment of the identified gap (shortfall). In that situation, we will work iteratively with stakeholders to refine the assessment to the point where the business area risks resulting from the gaps are captured and presented, and options for their effective remediation are clearly articulated through a remediation plan.

Input - you will provide available cyber information pertaining to your organisation, including the asset register (of the systems and components), network diagrams, and any current threat and risk assessments you may have (if completed). This information will be used to inform the Cyber Maturity Review.

If threat and risk assessments have not been undertaken, a separate activity will be required by you to provide these assessments, although we can offer completion of these for you as a separately priced activity.

Output – a detailed report indicating the current level of cyber maturity and providing recommendations for remedial actions to improve your cyber security maturity in line with good practice. The output report will comprise of the following elements:

- Executive Summary

- Scope of the Cyber Security Review

- Activities undertaken

- Findings achieved

- Current Cyber Maturity Status

- Gap Analysis against desired Cyber Maturity Status

- Remediation Plan, with prioritised recommendations

Other QinetiQ Cyber Services

This service forms part of a wider service portfolio, which seeks to help organisations mature their digital resilience and to help build 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 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 MATURITY REVIEW SERVICES

QINETIQ/20/01937

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