

Cyber Security Compliance Review Service part of Cyber Security Advisory

A QinetiQ Cyber Security Service

Key Benefits

- Assessment approach allows targeted interventions against specific legal, regulatory, and end customer requirements
- Will support formal certification against a chosen standard, or allows the business to be compliant with industry good practice
- Suitable for all businesses in all sectors allowing targeted improvements

Understanding the cyber security compliance requirements for your organisation can be a complex and time-consuming challenge, whether you aspire to achieve formal external certification, or to be compliant with recognised industry good practice.

The initial assessment is key to your understanding and can be undertaken to benchmark against relevant industry good practice and, subject to your requirements may be assessed against the following standards;

- 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)

These assessments should be completed for the IT systems and the IT/OT interfaces, including the controls in place at the boundaries for those systems.

Our Cyber Security Compliance Review is delivered by qualified and experienced cyber professionals, using a proven methodology and a clearly defined process. This process utilises a common tool that is implemented by a QinetiQ consultant with the customer in the following way:

- An engagement phase is conducted by a QinetiQ facilitator to confirm the cyber security standards within the scope of the compliance review and agree a date for a Review Workshop.
- A QinetiQ facilitator requests a list of stakeholders from the organisation for attendance and appropriate delegates attend the Workshop from the different areas of the customer business.
- During the Workshop, which takes up to a day to complete, the facilitator seeks evidence of the customer's current compliance status against the applicable standards.
- Following the Workshop, the QinetiQ facilitator works to identify areas of conformity and of non-conformity with the standard(s) and produces a report to document the shortfall ('gap') between the current compliance state, and the future desired position.
- The Report includes a prioritised action plan with a roadmap to address the identified gaps.
- A follow-up meeting is arranged with the stakeholders to discuss the output and provide an opportunity for clarification.

QINETIQ IN CONFIDENCE

- A final report is produced, capturing any observations from the follow-up meeting which is provided to the stakeholders.

QINETIQ

The QinetiQ Approach

On completion of the review you will gain a more detailed understanding of your status against the specific cyber security standard(s) considered, showing how you either meet, or need improvements in specific areas of the required compliance level. We will provide a prioritised roadmap to close any identified gaps and achieve improvements.

Our compliance review is based on assessing the quality and completeness of your organisation's evidence against each of the required cyber good practice elements expressed in the standards document(s). To enable us to gain the necessary insight into your organisational cyber practices and culture, it is recommended that we hold a workshop with your key cyber stakeholders to undertake an initial fact finding and gap analysis against the chosen standard(s).

Completion of this will workshop will support the creation of a report showing the current level of compliance and areas where there are gaps, for which remedial action will be required. The report will contain a prioritised roadmap allowing you to complete a project plan for gap closure that allows for maximum re-use of current policies and other company procedures.

As an in-depth assessment, the approach assesses the compliance status of your organisation using the following descriptors scale:

- Level 1 – Initial: your organisation adopts ad hoc processes only;
- Level 2 – Established: your organisation is developing a 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 art 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 the Security Compliance Review

Based on the workshop and subsequent gap analysis, some business areas or systems may require the deployment of additional measures (e.g. further cyber security controls, or evidence that existing controls are active). In that situation, we will work iteratively with stakeholders to refine the prioritised roadmap to the point where the specific measures to address identified areas of shortfall, and options for their remediation will be clearly articulated and can be effectively addressed through a Remediation

Input - You will provide available cyber compliance information pertaining to your organisation, including relevant Scope descriptions, Statements of Applicability, Information Security Management System (ISMS) details, and evidence of meeting the requirements detailed in the applicable standard(s). This can be exemplified through the implementation of applicable controls.

This information will be used to inform the Cyber Security Compliance Review. If this information is not available, a separate activity will be required by you to provide it. However, we can offer completion of these on your behalf as a separately priced activity.

Output – a detailed report indicating the current compliance status against the standard(s) within the scope of assessment and identifying any areas of shortfall (gaps). This will be supported by a prioritised action plan to remediate the gaps and attain compliance. The output report will comprise of the following elements:

- Executive summary
- Scope of the cyber security compliance review
- Activities undertaken
- Findings made
- Current cyber maturity status
- Gap analysis against desired compliance status
- Prioritised remediation plan

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

For further information, please contact Malvern Technology Centre
St Andrews Road, Malvern
Worcestershire, WR14 3PS

+44 (0)1252 392000
cyberenquiries@QinetiQ.com

Copyright QinetiQ Ltd 2026 | CYBER REVIEW SERVICES