



Defence Cyber Certification Overview

The Defence Cyber Certification (DCC) is a comprehensive security framework, alongside a formal and independently assessed certification process, to ensure cyber security compliance within the UK's defence supply chain.

Developed by the Ministry of Defence (MoD) and IASME to align with industry best practice, as well as international standards (including NCSC CAF, NIST CSF and ISO27001), DCC aims to strengthen cyber resilience and enhance security within UK defence procurement.

DCC may eventually replace the current system, whereby suppliers have to complete a Supplier Assurance Questionnaire (SAQ) on a contract-by-contract basis, with a single and standardised, organisation-wide assessment. The new scheme removes the requirement for multiple assessments and simplifies assurance across the defence supply chain, with certification valid for three years conditional upon an annual attestation.

How it works

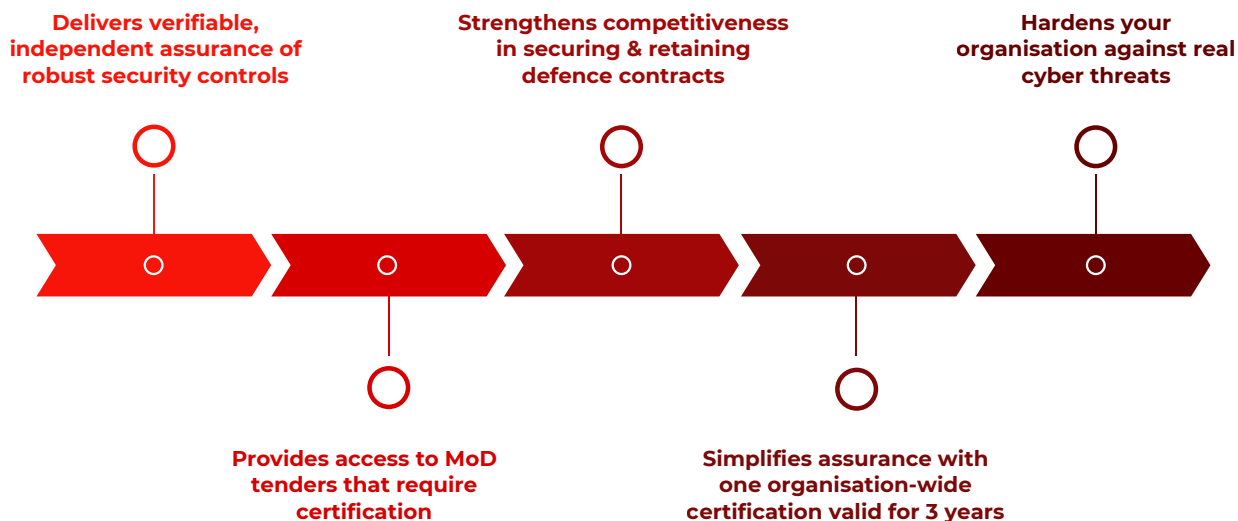
Based on Defence Standard 05-138 i4, every defence contract is assigned a cyber risk level from DCC Level 0 to Level 3, with each Level subject to a number of controls contained within the Standard.

DCC also requires current Cyber Essentials and/or Cyber Essentials Plus certification depending on the Level.

DCC Level	Number of Controls	CE Requirement
0	3 controls	Cyber Essentials
1	101 controls	Cyber Essentials
2	139 controls	Cyber Essentials Plus
3	144 controls	Cyber Essentials Plus

The certification process involves a single, point-in-time assessment to determine the applicant's cyber security posture. Organisations must verify their compliance with the applicable controls, describe the measures in place to achieve them, and provide supporting documentary evidence to their Assessor.

What are the benefits?



How Fortis Cyber® can support

As well as being a Certifying Body for DCC Level 0 and Level 1, Fortis Cyber® also provides a range of consultancy services to support you on your journey to Defence Cyber Certification:



Readiness Assessment and Gap Analysis

Assessing current security posture, identifying gaps against the framework and providing prioritised recommendations to meet compliance requirements. This is the theoretical scoring element.



Policy, process and documentation

Developing or refining cyber policies and processes to ensure clear and auditable documentation. This is part of the assist/consult and implement to prepare the applicant for DCC.



Technical Security Implementation

Hardening systems and networks to meet secure configuration requirements. Cyber Essentials and Cyber Essentials Plus certification (mandatory for all DCC Levels).



Security Testing & Assurance

Secure configuration reviews and CREST-accredited Vulnerability Scanning, Automated Pen Testing as a Service (PTaaS) and Penetration Testing.



Training and Awareness

Workshops in preparation for evidence collection and audits and staff cyber awareness training.



Information Security Officer as a Service

Ongoing support with governance, security strategy and continuous improvement, maintaining DCC compliance and managing annual attestations.

Whether you are preparing for your first DCC assessment or looking to harden existing controls, Fortis Cyber® will ensure cyber security is embedded across your organisation, so you are in a strong position to meet the requirements for Defence Cyber Certification.

Get in touch for more information or contact us via enquiries@fortiscyber.co.uk and let our experts support you with clear, actionable guidance on DCC compliance.