Overview Document

What is Defence Cyber Certification?

The Defence Cyber Certification (DCC) is a comprehensive, cyber security certification framework for UK defence suppliers. Developed by the UK Ministry of Defence (MOD) and IASME, the certification is part of the broader initiative to enhance the cyber resilience of the UK's defence sector supply chain.

In contrast to the previous per-contract assessment approach, the DCC certification emphasises the overall security and resilience of the organisation. It shifts the focus from protecting 'MOD identifiable information' to providing a single, organisation-level, assurance which can be presented in support of UK Defence Procurements (subject to annual check-in and recertification every 3 years).

How does it work?

The DCC certification process involves a point-in-time assessment against an uplifted UK Defence Standard for cyber resilience in organisations.

Compliance (with this uplifted standard) is a requirement for all Defence procurement and contract activities.

Each Defence project undergoes a cyber risk assessment, which defines the necessary security measures for organisations delivering that project. Contractors will need to demonstrate compliance to the relevant security controls outlined in the Defence standard.

DCC Certification aligns with the tiered assurance levels (0-3) of the uplifted standard. It serves as a clear, proactive demonstration and assurance of an organisation's commitment to cyber resilience and

provides a visible ‘badge’ to assure other buyers that your company prioritises cyber security.

The DCC controls align to international cyber security standards, including relevant elements of the **Cyber Assurance Framework (CAF)** developed by the UK's National Cyber Security Centre (NCSC). The scheme aligns with the UK's broader cyber strategy, emphasising a 'whole of society' effort towards enhancing national cyber resilience, and reinforces the requirement for appropriate adoption of Cyber Essentials at its core.

The DCC certification scheme has the potential to ensure that all suppliers in the defence supply chain are independently assessed and certified with the appropriate levels of security.

What this means for Defence contractors

Successfully achieving and maintaining DCC certification demonstrates an organisation’s commitment to cyber resilience and robust security practices, providing assurance to stakeholders and unlocking opportunities within the UK defence sector.

All levels (0-3) start with Cyber Essentials certification, with Levels Two and Three requiring Cyber Essentials Plus. Applicants receive supporting documents to help them understand the controls and questions for the level they aim to achieve.

Applicants are responsible for demonstrating compliance with the controls, describing how they meet them, and providing evidence of meeting those controls via a remote or on-site assessment. The number of controls and the Assessor's level of expertise increases with the risk level.

IASME, the MOD's official cyber certification partner, manages the implementation of the DCC through its extensive network of assured Certification Bodies.

For more information about the Defence Cyber Certification or to begin the certification process, please contact IASME: info@iasme.co.uk

Key Features of the Defence Cyber Certification (DCC):

- A comprehensive, organisation-wide certification tailored for suppliers in the defence sector
- Fully aligned with international standards to address the evolving cyber threat landscape
- Designed to enhance the cyber resilience and security of the UK defence sector's supply chain
- Streamlined certification process, replacing the per-contract approach with a single certification covering multiple contracts