

# STRENGTHENING YOUR DEFENCE SUPPLY CHAIN WITH DEFENCE CYBER CERTIFICATION (DCC)

## WHAT IS DCC?

The Defence Cyber Certification (DCC) is the Ministry of Defence's new organisation-wide cybersecurity assurance framework for suppliers in the defence sector. Developed with IASME, it provides independent validation that an organisation meets the cyber requirements aligned to DEFSTAN 05 138 and applicable risk levels.

DCC replaces previous inconsistent self assurance methods with a structured, evidence based certification process covering four levels (0-3), all beginning with Cyber Essentials.

## WHY DCC CAME ABOUT?

From rising geopolitical tensions to the sheer scale of the supply chain (over 130,000 indirect jobs), inconsistent cyber maturity has become a serious risk. The MOD responded by strengthening expectations through Secure by Design principles and updates to DEFSTAN 05 138, leading to the creation of DCC.

The UK Defence supply chain is increasingly targeted by threat actors due to:

- Rising geopolitical tension, including conflict spill-over risks.
- Vast supply-chain exposure: over 130,000 indirect jobs support MOD operations, creating inconsistent cyber maturity across suppliers.
- Legacy reliance on self-assessed controls under Cyber Essentials Basic, providing limited assurance.

To address these gaps, HMG and the MOD strengthened expectations through Secure by Design principles and the updated DEFSTAN 05 138 Issue 4, culminating in DCC, a formal way to assess, validate, and uplift supplier cyber resilience.

## HOW THE DCC PROCESS WORKS

We've supported organisations across many different sectors and we bring that experience to every engagement.

The certification journey includes:

### 1. Gap analysis and readiness review

We break down DEFSTAN 05 138 and pinpoint exactly where your current posture meets (or misses) the mark. Expect clear, jargon free guidance you can act on.

### 2. Tailored remediation planning

Based on your risk profile and target DCC level, we build a practical, achievable uplift roadmap shaped around how your business operates.

### 3. Hands on expertise

Our defence grade consultants bring a unique blend of technical knowledge and real world experience in high assurance environments.

### 4. End to end guidance through Certification

From documentation and evidence collation to communicating with Certification Bodies, we remove friction, reduce delays, and help you proceed with confidence.

Level	No. of controls	What it means	Ideal for
Level 0 – Basic	3 controls	Entry-level assurance confirming the absolute minimum baseline posture. Often used for low-risk suppliers.	Organisations with minimal exposure or handling non-sensitive information.
Level 1 – Standard	101 controls	Demonstrates structured cybersecurity practices with formal security controls.	Suppliers with moderate MOD interaction or low-medium risk profiles.
Level 2 – Advanced	139 controls + Cyber Essentials Plus	Incorporates robust technical and organisational controls, independently tested.	Organisations handling sensitive systems or higher-value defence contracts.
Level 3 – Expert	144 controls + Cyber Essentials Plus	The highest assurance level, verifying maturity against the most demanding security expectations.	Suppliers supporting critical systems, high-threat environments, or classified projects.

## WHY DCC MATTERS TO DEFENCE SUPPLIERS?

Achieving DCC demonstrates:

- Credibility and trust with MOD buyers.
- Competitive advantage in tenders requiring validated cyber assurance.
- Reduced organisational risk, elevating resilience against emerging threats.
- Alignment with national standards, including NCSC, NIST and Secure by Design principles.

## WHAT LRQA CAN DO FOR YOU?

Drawing directly from our published insight, LRQA helps organisations navigate the entire DCC journey, from early discovery through to audit readiness and ongoing attestation.

We support you by delivering:

### 1. Gap analysis and readiness review

Our experts interpret DEFSTAN 05 138 requirements and pinpoint where your posture falls short. We translate technical controls into clear, actionable improvements.

### 2. Tailored remediation planning

We design practical uplift plans shaped around your risk profile, business operations, and required DCC level.

### 3. Hands on support from defence grade professionals

LRQA consultants carry deep experience across MOD, NATO, and Defence Primes. We blend technical expertise with real world understanding of high assurance environments.

### 4. Continuous guidance through Certification

From documentation preparation to liaising with Certification Bodies, LRQA ensures you meet every requirement with confidence, reducing friction, delays, and uncertainty during DCC assessment.

## WHY CHOOSE LRQA?

We know that you require a cycle of services that continuously affirms the scope of your environment to be tested and to understand your remediation requirements. Our approach to continuous assurance is designed to enable real-time risk management – which means faster resolution of issues, better risk mitigation and less business disruption.

Our Continuous Assurance service combines the precision and efficiency of automation with the expertise and critical thinking of human-led oversight. This blend enables us to deliver comprehensive, real-time cybersecurity management that adapts to evolving vulnerabilities, providing a more robust and reliable defence than traditional, point-in-time testing.

LRQA has a proven track record in delivering advanced cybersecurity solutions. Our global team of specialists brings deep expertise across various sectors, helping clients navigate the complex cybersecurity threat landscape.

As an LRQA Continuous Assurance client, you will receive...?