

Defence Cyber Certification readiness

For suppliers in the MOD supply chain who need to know which Defence Cyber Certification level their contracts require, what the gap is, and how long it takes to close. MOD asked industry partners in July 2026 to achieve DCC Level 0 by 31 December 2026.

SCOPE · 1 TO 2 WEEKS Requirement and scope review Which level your contracts require, to which part of the business, and the route to it. £1,950 from, plus VAT	LEVEL 0 · 2 TO 4 DAYS Level 0 readiness diagnostic Closing the gap to DEFSTAN 05-138 expectations at Level 0. Scoped on the diagnostic	LEVEL 1 · 4 TO 8 DAYS Level 1 readiness diagnostic Gap assessment across the Level 1 control set with a remediation roadmap. £4,500 from, plus VAT
--	---	---

What you receive

- ▶ Cyber Risk Profile interpretation and the DCC level it points to
- ▶ Gap assessment against DEFSTAN 05-138 Issue 4 at the applicable level
- ▶ Evidence register mapping each control to its supporting artefact
- ▶ Supplier Assurance Questionnaire alignment review
- ▶ Scope definition covering which entities, sites and systems are in
- ▶ Cyber Essentials position and what is required to close it
- ▶ Prioritised remediation plan with owners, effort and sequence
- ▶ Written readiness verdict and a realistic date for submission

The levels, and where Goldline works

LEVEL	REQUIREMENT	GOLDLINE
Level 0 · Basic	3 controls plus Cyber Essentials	Supported
Level 1 · Foundational	101 controls plus Cyber Essentials	Supported
Level 2 · Advanced	139 controls plus Cyber Essentials Plus. Must be led by a UK Cyber Security Council Principal	Not offered
Level 3 · Expert	144 controls plus Cyber Essentials Plus. Must be led by a Chartered professional at an NCSC Assured Consultancy	Not offered

Scope boundaries

- Goldline prepares suppliers. Assessment and certification are carried out by an assessor working for an IASME Certification Body or Assured Service Provider. Goldline does not hold DCC assessor status.
- DCC does not remove the Supplier Assurance Questionnaire. Risk assessments and SAQs remain live through the Supplier Cyber Protection Service, with annual review on contract anniversary.
- MOD has publicly asked industry partners to reach Level 0 by 31 December 2026. The specific contractual requirement is determined by the contract, DEFCON 658 invocation, Cyber Risk Profile and flow-down.
- Cyber Essentials certification is arranged with a certification body and its fee is paid directly by the client.

Why the scope review exists as a separate step. The most expensive error in this process is certifying the wrong scope, or to the wrong level. Establishing which contracts invoke DEFCON 658 and what Cyber Risk Profile applies costs less than remediating against a standard that was never required.