CYBEXIS

WHITE PAPER | DEFENCE SUPPLY CHAIN

Defence Cyber Certification for Medium-Sized Organisations

Key challenges, priorities and practical hints for suppliers preparing for DCC under the MOD Cyber Security Model

October 2026

Clarity in complexity. Confidence in every decision.

At a glance

- The MOD has asked all Defence industry partners to achieve DCC Level 0 by 31 December 2026, including Cyber Essentials for applicable business-critical systems.
- DCC certifies the organisation, not a contract. Scope is organisation-wide and stays the same at every level; only the depth of controls changes (3 controls at Level 0 up to 144 at Level 3).
- Every level is independently assessed, including Level 0. Certificates last three years with annual attestation, and Cyber Essentials or Cyber Essentials Plus must be renewed every year.
- For medium-sized firms the hardest parts are usually scope, evidence from managed service and cloud providers, and fitting preparation around live bids. Starting early is the single biggest success factor.

Who this is for: Managing directors, IT and security leads, bid teams and contract managers in SMEs and mid-sized firms that supply UK Defence directly or through a prime contractor.

Information correct as of October 2026. Free to share with attribution to Cybexis.

1. Why defence suppliers are in the spotlight

Defence supply chains are attractive to capable adversaries because they offer a route to sensitive information and, increasingly, a way to disrupt delivery of military capability without attacking the MOD directly. The 2025 Strategic Defence Review stated plainly that UK Defence continues to carry intolerable levels of cyber risk, and the supply chain is a priority target [1]. High-profile incidents, including the 2024 compromise of a contractor-operated payroll system holding service personnel data, have shown how a breach at one supplier becomes a Defence problem.

The wider threat environment reinforces the point. The NCSC recorded 204 nationally significant incidents in the year to August 2025, more than double the previous year [2], and ransomware attacks on UK manufacturers in 2025 demonstrated that disruption of a single firm can halt production across hundreds of smaller suppliers. For a medium-sized engineering, software or services firm, the question is no longer whether cyber security will be tested in procurement, but how.

The MOD's answer is Defence Cyber Certification (DCC): independent, reusable assurance that a supplier meets the control level its contracts require.

2. How DCC fits together

DCC was developed by the MOD with IASME and launched in May 2025, with Level 0 opening in July and Levels 1 to 3 in August 2025 [3]. It sits within a wider set of mechanisms that are often confused:

Mechanism	Role
Cyber Security Model v4 (CSMv4)	The MOD's risk-based process for building cyber security into procurement. Each activity is given a Cyber Risk Profile from Level 0 to Level 3. Live since 3 December 2025 [3].
Def Stan 05-138 Issue 4	The control standard used by CSMv4. It sets the minimum controls for each Cyber Risk Profile and broadens scope from MOD data to the resilience of the supplier organisation itself [4].
DEFCON 658	The contract condition that applies CSM requirements and requires them to flow down through subcontracting tiers.
Supplier Assurance Questionnaire (SAQ)	The supplier's self-assessment, completed through the Supplier Cyber Protection Service. Still required alongside DCC for now [4].
Defence Cyber Certification (DCC)	Independent certification that the controls for a given level are in place. Under ISN 2026/02 (March 2026), buyers must accept a valid certificate as satisfying the corresponding Def Stan control requirement [5].

Table 1. The main components of Defence cyber assurance.

The four levels

DCC level	Typical assessed risk	Def Stan controls	Cyber Essentials prerequisite
Level 0: Basic	Very low	3	Cyber Essentials
Level 1: Foundational	Low to moderate	101	Cyber Essentials
Level 2: Advanced	High	139	Cyber Essentials Plus
Level 3: Expert	Substantial	144	Cyber Essentials Plus

Table 2. DCC levels and control counts (source [4]). A higher-level certificate satisfies all lower levels.

Organisations can apply directly for any level, and the level for a given contract is set by the MOD or prime contractor through the Cyber Risk Profile. Assessment is carried out by IASME-assured certification bodies in two phases: a theoretical phase, where the applicant explains and evidences how each control is met, and a practical phase, where the assessor verifies that controls operate as described. **No level is a self-**

assessment. Certification lasts three years, supported by an annual attestation and annual renewal of Cyber Essentials or Cyber Essentials Plus [4].

> **The 31 December 2026 deadline**
>
> In July 2026 the MOD's Director of Cyber Defence and Risk asked all Defence industry partners to achieve DCC Level 0 by 31 December 2026, including Cyber Essentials for all applicable business-critical systems within scope [4][6]. IASME's public guidance still notes that DCC is not yet a universal contractual requirement, but suppliers should treat the date as the operational baseline and expect tenders to specify DCC increasingly.
>
> Level 0 is the floor, not the ceiling. Many medium-sized suppliers handling technical data, engineering services or connected products will be assigned Level 1 or Level 2 profiles.

3. Key challenges for medium-sized organisations

Medium-sized firms tend to sit in an awkward position: large enough to have complex IT, several sites and a mix of Defence and commercial work, but rarely with a dedicated security team. The same challenges recur.

Scope cannot be carved out

DCC is designed around the functions and services essential to the organisation operating securely and resiliently, whether they support MOD work or not. The scope stays the same at every level, and assessors can challenge exclusions that leave essential services outside the boundary [4]. Firms used to ring-fencing a "Defence enclave" for Cyber Essentials often find that identity, email, file storage, finance systems and remote access must all be brought in.

Evidence held by someone else

Most mid-sized suppliers rely on a managed service provider (MSP), Microsoft 365 or another cloud platform, and sometimes a parent company for core IT. The applicant remains accountable for showing that each relevant control is met, which means obtaining configuration exports, patching records, monitoring outputs and incident procedures from providers who may not be contractually obliged to supply them.

Operating evidence, not policy

Def Stan 05-138 requires controls to be documented, implemented and supported by auditable evidence. Policies are necessary but not sufficient. Assessors look for asset inventories, access reviews, vulnerability and patch data, logs, exercise records and supplier oversight that are current and attributable to the defined scope.

Cyber Essentials coverage gaps

The Cyber Essentials scope must cover the internet-connected devices, networks and cloud services within the DCC scope. Common gaps include personal devices used for email, unmanaged laptops on the shop floor, legacy servers kept for one application, and cloud services adopted outside IT. The Cyber Essentials v3.3 requirements, which took effect in April 2026, tightened expectations on device management and authentication [7].

Operational technology and test equipment

Manufacturing and engineering firms often have CNC machines, test rigs and lab networks that cannot run standard endpoint controls. Where these are essential to the business they must be considered, with appropriate compensating measures such as segmentation and controlled access, agreed with the certification body.

Timing against live procurements

Scoping, remediation, evidence gathering and assessment rarely fit inside a tender window. Suppliers that wait for a contract condition often have to submit a Cyber Improvement Plan instead, which is acceptable under CSMv4 but places them at a disadvantage against certified competitors.

Flowing requirements to your own suppliers

DEFCON 658 obligations flow down. A medium-sized prime or tier-two supplier must assign Cyber Risk Profiles to its own subcontracts and check that its subcontractors can meet them, adding a supplier assurance workload many firms have not resourced.

4. Priorities: a practical sequence

1. **Decide your target level from your pipeline, not your current contract.** Review live and anticipated Defence work with the bid team and primes. Certifying once at the highest likely level is usually cheaper than certifying twice.
2. **Define the legal entity and certification boundary.** List the essential functions and the systems, people, sites and third parties they depend on. Validate this boundary with your chosen certification body before doing anything else.
3. **Align Cyber Essentials (Plus) scope to the DCC scope.** Close device and cloud gaps first, because Cyber Essentials is the prerequisite and the most common reason for delay.
4. **Map controls to evidence.** Build a simple matrix of each applicable Def Stan 05-138 control, its owner, how it is met, and the evidence that proves it operates. Reuse ISO/IEC 27001 and Cyber Essentials Plus evidence wherever possible.
5. **Secure evidence from providers.** Write to your MSP and key cloud providers early, specifying the reports and access you need. Add evidence and audit support clauses at the next contract renewal.
6. **Remediate the gaps that matter most.** Typically: phishing-resistant MFA, privileged access management, centralised logging with defined retention, tested backups, documented incident response, and supplier security management.
7. **Run a readiness review, then book the assessment.** An independent mock assessment against the practical phase is the most reliable way to find weak evidence before the assessor does.
8. **Embed it as business as usual.** Calendar the annual attestation, Cyber Essentials renewal and three-yearly recertification, and review scope whenever the business changes significantly.

Phase	Indicative duration*	Key outputs
Mobilise and scope	2–4 weeks	Target level agreed; boundary and essential functions defined; certification body engaged
Baseline and gap analysis	3–6 weeks	Cyber Essentials alignment; control-to-evidence matrix; prioritised remediation plan
Remediate and evidence	1–6 months	Control improvements; provider evidence secured; policies and records in place
Readiness and assessment	4–8 weeks	Mock assessment; evidence pack; certification body theoretical and practical phases

*Table 3. Indicative DCC journey for a medium-sized organisation. *Durations vary widely with level, starting maturity and provider dependencies. Level 0 can be much quicker if Cyber Essentials coverage is already sound.*

5. Hints and tips from the field

- **Don’t confuse the paperwork.** You will probably still need to complete the SAQ through the Supplier Cyber Protection Service even with a DCC certificate. Keep the two consistent.
- **Write a one-page scope statement.** A clear description of the entity, sites, users, systems and providers in scope saves hours of discussion with the assessor and keeps everyone aligned.

- **Use your Microsoft 365 or Google tenant well.** Many controls on identity, device compliance, logging and data protection can be met and evidenced through configuration you already pay for. Export baselines regularly as evidence.
- **Name an owner for every control.** Evidence goes stale when no one is accountable for it. Small firms can combine roles, but each control needs a name.
- **Collect evidence continuously.** Set a monthly routine to capture patch reports, access reviews and backup tests. It turns the annual attestation into a formality.
- **Make the Cyber Improvement Plan credible.** If you must bid before certification, a plan with named owners, realistic dates and funding is taken far more seriously than a list of intentions.
- **Ask your primes what they need.** Many primes are assigning profiles to subcontracts now and may share templates, expectations or timelines that help you prioritise.
- **Avoid over-engineering.** Level 0 is three controls plus Cyber Essentials. Build for the level you need with a clear path to the next, rather than an enterprise programme you cannot sustain.

DCC is a significant change for the Defence supply base, but for well-prepared medium-sized firms it is also an opportunity. A single, reusable certificate replaces repeated questionnaires, demonstrates resilience to primes and customers, and builds the operational discipline that protects the business whether or not Defence is its largest customer.

About Cybexis

Cybexis is an independent UK cyber security advisory, assurance and risk management practice based in Reading. Its insights series shares practitioner perspectives on the frameworks, regulation and threats facing regulated and high-risk organisations. www.cybexis.co.uk | hello@cybexis.co.uk

This paper is for general information only and does not constitute legal or regulatory advice. Requirements, deadlines and threat activity change; always confirm current obligations with your regulator, contracting authority or certification body.

Sources and further reading

[1] CyberSmart, CSMv4 is live: what defence suppliers need to know about DCC requirements (Feb 2026). https://cybersmart.co.uk/2026/02/csmv4-is-live-what-defence-suppliers-need-to-know-about-dcc-requirements/

[2] NCSC, Annual Review 2025: Incident management. https://www.ncsc.gov.uk/collection/ncsc-annual-review-2025/chapter-01-cyber-threat-to-the-uk/incident-management

[3] MOD Digital and Data, One year of Defence Cyber Certification (May 2026). https://defencedigital.blog.gov.uk/2026/05/08/one-year-of-defence-cyber-certification-building-stronger-cyber-resilience-together/

[4] Logiq, Defence Cyber Certification: requirements, levels and how to prepare (Aug 2026). https://www.logiq.co.uk/insights/what-is-defence-cyber-certification-dcc/

[5] MOD, ISN 2026/02: Use of DCC as assurance of control requirements under DEFCON 658. https://assets.publishing.service.gov.uk/media/69cba72ba60a12ca3913c610/ISN_2026-02_Use_of_Defence_Cyber_Certification__DCC__as_assurance_of_control_requirements_under_DEFCON_658.pdf

[6] MOD Digital and Data, Building cyber resilience in the UK one step at a time (July 2026). https://defencedigital.blog.gov.uk/2026/07/13/building-cyber-resilience-in-the-uk-one-step-at-a-time/

[7] Industrial News, Cyber Essentials raises bar on cyber basics (v3.3, April 2026). https://industrialnews.co.uk/?p=434196

[8] GOV.UK, Defence Standard 05-138 Issue 4. https://www.gov.uk/government/publications/cyber-security-for-defence-suppliers-def-stan-05-138-issue-4

[9] IASME, Defence Cyber Certification: frequently asked questions. https://iasme.co.uk/defence-cyber-certification/frequently-asked-questions/