CyberSmart

Defence Cyber Certification:

Your playbook for levels 0-1

Contents

Defence Cyber Certification (DCC) is an evolution, not a revolution

The Defence Cyber Certification marks a significant shift in how suppliers demonstrate their security credentials when working with the UK Ministry of Defence (MOD).

Where once self-assessment cybersecurity questionnaires were sufficient to prove your suitability, the DCC builds on existing standards to create a rigorous, independently verified certification framework.

While the scheme is still technically voluntary, suppliers can expect increasingly stringent cybersecurity requirements in the coming years. Early adoption puts you ahead of the curve, demonstrating your commitment to cyber resilience.

Key takeaways

What is DCC?

The Defence Cyber Certification is a comprehensive, organisation-wide cybersecurity framework. Developed by the MOD in partnership with IASME, it is an independently verified accreditation that proves a defence supplier meets the required cybersecurity standards to bid on government contracts.

Why does it matter?

DCC replaces inconsistent self-assessment with an independently verified certification framework. Suppliers should expect it to become a mandatory requirement for bidding on defence contracts in the years to come, in response to escalating cyber threats across the globe.

A single DCC certificate proves your organisation-wide security posture, and you can use it across multiple MOD contracts – provided they are assessed at or below your certification level. For example, if you achieve Level 1 certification, you can use this single certificate for any contracts requiring Level 0 or Level 1, eliminating the need for repeated contract-by-contract security assessments.

Beyond meeting contractual requirements, DCC demonstrates your commitment to protecting sensitive defence data and your ability to operate as a trusted partner in the defence supply chain. For many suppliers, certification isn't just about compliance – it's about future-proofing your business as cyber standards continue to evolve and ensuring you remain eligible for the full range of MOD opportunities.

When did it come into effect?

Level 0 launched in July 2025, followed by Levels 1, 2, and 3 in August 2025.

Tips for success

- ✓ Use a structured checklist to track compliance with relevant security controls
- ✓ Engage your whole team – cyber resilience isn't just an IT responsibility
- ✓ Conduct internal audits before the formal assessment
- ✓ Be factual and honest in your evidence and documentation
- ✓ Don't hesitate to ask your Defence Cyber Certification partner for clarification if you're unsure about any aspect of the process

What is Defence Cyber Certification?

Defence Cyber Certification provides a structured framework for assessing and assuring the cybersecurity posture of UK defence suppliers. Developed by the MOD in partnership with IASME (the scheme's Certification Authority), the DCC builds upon the long-established Defence Standard 05-138 (DefStan 05-138).

A single certification covers multiple contracts at or below your certified level. It lasts for three years – subject to annual attestations and maintaining a valid Cyber Essentials certification.

Certification levels

Designed to account for any type of MOD work, the DCC operates across four levels of security controls:

- LEVEL 0 – VERY LOW RISK
- LEVEL 1 – LOW-MODERATE RISK
- LEVEL 2 – HIGH RISK
- LEVEL 3 – SUBSTANTIAL RISK

The MOD determines your required certification level based on the nature and sensitivity of the contracted work – it's cyber risk profile (CRP).

LEVEL 0 – VERY LOW RISK

The entry-level certification for contracts with very low cyber risk. Beyond maintaining Cyber Essentials certification, Level 0 requires compliance with **two additional basic controls**.

This level is suitable for suppliers providing low-risk goods or services with minimal cyber exposure. For example, supplying non-technical goods like stationery, facilities management services, or catering where there's minimal interaction with MOD systems or sensitive data.

LEVEL 1 – LOW TO MODERATE RISK

Designed for organisations with low to moderate CRPs, Level 1 requires you to comply with **101 controls** covering:

- Robust governance
- Risk management
- Protective controls
- Incident response
- Staff training

Cyber Essentials remains the technical baseline. Most defence suppliers working on standard contracts require Level 1 certification. This typically includes organisations providing IT support services, standard software solutions, training and consultancy services, or logistics support where some access to MOD systems or official data is required.

LEVEL 2 – HIGH RISK

For contracts presenting high cyber risk, Level 2 demands advanced cybersecurity oversight and planning. With **139 controls**, Level 2 demands:

- Sophisticated governance
- Continuous monitoring
- Robust technical assurance
- Effective third-party supplier oversight

Cyber Essentials Plus certification becomes mandatory at this level, which requires independent external validation of your technical controls. Level 2 also stipulates a defence in depth methodology to mitigate evolving threats.

This level is aimed at suppliers who regularly handle sensitive MOD data, provide managed IT services for defence operations, or develop bespoke software systems that integrate with MOD infrastructure.

LEVEL 3 – SUBSTANTIAL RISK

The highest certification level addresses substantial cyber risk from suppliers delivering contracted outputs (the goods, services, or systems you provide). For example, mission-critical software, cloud infrastructure for sensitive operations, or advanced defence technology components.

Level 3 requires compliance with **144 controls** to demonstrate expert cyber security capabilities that fully leverage defence in depth principles.

Cyber Essentials Plus is required for Level 3, along with the most rigorous governance, technical, and operational security measures. This level is typically reserved for suppliers handling the most sensitive defence work, such as:

- Developing mission-critical command and control systems
- Providing cloud infrastructure for classified operations
- Designing weapons systems components
- Manufacturing advanced defence technology where compromise could have severe operational impact

Why was it created?

The UK government's defence supply chain faces increasingly sophisticated cyber threats. According to Thales' 2024 Data Threat Report, 93% of organisations in the critical national infrastructure sector have observed an increase in cyber-attacks in 2024.

Traditional self-assessment questionnaires varied significantly in quality and interpretation. Inevitably, this led to inconsistencies in how suppliers demonstrated compliance.

DCC addresses these challenges by providing:

- Independent, third-party verification of security controls
- Consistent assessment standards across suppliers
- Organisation-wide security assurance, rather than contract-by-contract checks
- Clear, graduated levels aligned to cyber risk profiles

The scheme supports the MOD's Cyber Resilience Strategy for Defence, shifting focus from protecting MOD identifiable information to enhancing overall organisational security and resilience.

When did DCC come into effect?

The MOD and IASME opted for a phased rollout for the Defence Cyber Certification, which took place over summer 2025.

- Level 0 went live in July 2025
- Level 1 became available in August 2025
- Levels 2 and 3 became open to applicants at the end of August 2025

When will DCC become mandatory?

Currently, DCC is technically a voluntary scheme, but you should expect it to become mandatory in the near future. The transition represents a shift from self-assessment questionnaires to independently verified certification as the standard method of demonstrating compliance with MOD cybersecurity requirements.

Under the Cyber Security Model (CSM), the MOD conducts risk assessments of procurements to determine the cyber risk profile level required. This CRP level determines which DCC certification level suppliers must hold to bid for that contract.

The timeline for mandatory implementation depends on the formal contractual invocation of CSM version 4, which the MOD will announce via Industry Security Notice. The CSM takes a risk-based, proportionate approach focusing on the organisation as a whole rather than specific products or services. All aspects of your operations are considered when assessing and managing cyber risks, which is why DCC requires organisation-wide compliance rather than project-specific certification.

What does this mean in practice?

Many prime contractors are already requesting DCC from their subcontractors ahead of any formal mandate, creating early adoption pressure across the supply chain. The MOD has made clear that suppliers should expect increasing requirements to hold valid Defence Cyber Certification for the duration of their contracts.

How does DCC align with other cybersecurity standards?

DCC builds upon and complements existing cybersecurity standards like Cyber Essentials and ISO 27001.

Cyber Essentials

All DCC levels require a valid Cyber Essentials certification, as this forms the technical foundation of the scheme. **Level 0 and Level 1 require standard Cyber Essentials, whilst Levels 2 and 3 require Cyber Essentials Plus.**

ISO 27001

DCC controls map closely to ISO 27001 Annex A controls. This covers:

- Information security policies
- Supplier security
- Physical security
- Incident management
- Access control

If you're ISO 27001-certified, or working towards it, you've probably laid most of the groundwork for DCC. That said, you'll still need to provide specific evidence for each control.

Cyber Assessment Framework (CAF)

The structure of DCC's controls mirrors the National Cyber Security Centre's (NCSC) Cyber Assessment Framework, which focuses on governance, protection, detection, and response.

NIS2 Directive

For managed service providers and organisations subject to NIS2 regulations, Defence Cyber Certification compliance complements the requirements you already adhere to. Both emphasise:

- Risk management
- Supply chain security
- Incident reporting
- Executive accountability

Which organisations are affected most by DCC?

Essentially, any organisation working on MOD contracts below the ‘Secret’ classification level should expect to be subject to DCC requirements going forward. Typically, this includes:

Defence contractors and subcontractors supplying goods or services to the MOD

Technology and software providers developing systems for defence applications

Professional services firms providing consulting, training, or support to defence organisations

Managed service providers supporting IT infrastructure for defence clients

Manufacturing and logistics companies in the defence supply chain

> *DCC compliance complements existing cybersecurity standards, which aim to raise cyber resilience through a set of similar, standard controls. MSPs and SMEs who get ahead with DCC will find themselves better prepared as regulatory requirements evolve.*
>
> – CyberSmart

Common challenges and pitfalls

Evidence preparation

Many suppliers already follow good security practices but lack documentation. DCC assessments are evidence-driven, requiring policies, logs, training records, and proof of implementation for each control.

Management buy-in

Achieving certification requires sponsorship, policy approval, resource allocation, and organisational commitment. Without leadership support, progress often stalls.

Resource constraints

Smaller organisations may struggle to allocate sufficient time and expertise to implement controls, gather evidence, and prepare for assessment whilst maintaining normal business operations.

Maintaining compliance

Achieving certification is one thing; maintaining it is another. It requires annual attestations and continuous compliance audits which can be difficult to coordinate if you haven't set clear roles and responsibilities or embedded cybersecurity best practices into your everyday operations.

> ***"Getting management buy-in early on is essential. DCC compliance isn't just an IT project – it impacts policies, processes, and budgets across your business."***
>
> – CyberSmart

DCC misconceptions

As with any certification scheme, several misconceptions have emerged that muddy the waters.

1. Cyber Essentials certification is enough for DCC Level 0-1

Cyber Essentials is mandatory for all DCC levels, but it's just the foundation. Level 0 requires compliance with two additional controls, while Level 1 requires compliance with 101 controls total.

2. DCC is a checkbox exercise

Far from it. Assessors will review your documentation, interview staff, request demonstrations of controls in action, and verify that you've implemented the relevant security measures. Simply having policy documents without operational evidence won't suffice; you need hard proof to back it up.

3. Once certified, you're set for three years

Although your certification is valid for three years, you must complete annual attestations to confirm ongoing compliance with DCC and Cyber Essentials. You'll need to keep evidence up to date, maintain security controls, and demonstrate ongoing adherence.

4. Certification allows you to handle classified information

An active certification isn't a demonstration of your ability to handle or process classified information. Classification requirements are outlined in separate Defence Conditions (DEFCONs). For example, DEFCON 660 for OFFICIAL-SENSITIVE and DEFCON 659A for SECRET information.

If your work involves classified material, you'll need specific clearances and demonstrate compliance with relevant DEFCONs.

How to prepare for DCC: A step-by-step checklist

Preparing for Defence Cyber Certification requires systematic planning and execution. Follow these nine steps to make your experience a smooth one.

STEP 1

CHECK YOUR REQUIRED LEVEL

Confirm whether your MOD contract needs Level 0, 1, 2, or 3 certification.

If you don't yet have an MOD contract but are preparing to bid for one, consider which level aligns with the type of work you'll be doing. You can apply for certification at any level, even without a current contract.

STEP 2

GET CYBER ESSENTIALS CERTIFIED

Cyber Essentials is the baseline for all levels of DCC. It covers the five essential security controls that protect businesses against common cyber threats:

- Firewalls and internet gateways
- Secure configuration (devices and software)
- User access control and admin privileges
- Malware protection
- Security update management (patching)

If you're not sure where to start, consider working with a Cyber Essentials certification partner.

> *"You can't certify only the parts of your organisation that handle MOD data or sensitive projects directly – the scheme is designed to elevate security across your organisation."*
> – CyberSmart

STEP 3

DEFINE WHAT'S IN SCOPE

Decide which systems, data, locations, and sites your certification needs to cover. Unlike some certification schemes that allow limited scope, DCC adopts a whole-organisation approach.

It's not enough to certify the project team that deal with the MOD directly. To achieve certification, every system and department must meet the security standards outlined in the scheme. This includes:

- Critical IT systems and networks
- Cloud services and infrastructure
- Staff with access to operational systems

Document your efforts clearly in a Statement of Scope to provide written proof during audits.

STEP 4

CONDUCT A GAP CHECK

Compare the security measures you currently have in place against the required DCC controls for your level. Level 1 features 101 controls, so a systematic approach is essential to ensure nothing falls through the cracks. Identify where you have:

- Full controls in place with supporting evidence
- Partial or in progress measures
- Gaps that require new policies, processes, or technical measures

Create a simple tracker (using a spreadsheet or project management tool) listing each control, its status, supporting evidence, and outstanding actions.

STEP 5

ADDRESS GAPS

Address any partial or incomplete controls identified during your gap analysis.

This may involve:

- Developing or updating security policies (acceptable use, incident response, access control, data backup, etc.)
- Implementing technical measures (logging, vulnerability scanning, multi-factor authentication, etc.)
- Establishing new processes (risk assessments, access level reviews, security training, supplier vetting)
- Assigning clear roles and responsibilities for administering security measures

STEP 6

COLLECT EVIDENCE

Collect and organise everything your assessor will need to determine that you've implemented each control correctly and they work as intended.

Evidence may include:

- Written policies and procedures (signed and dated)
- Training records and attendance logs
- System configuration screenshots
- Patch management reports
- Access control lists and review records
- Incident logs and response documentation
- Backup logs and restoration test results
- Risk register and risk assessment records
- Supplier security questionnaires or agreements

STEP 7

BUILD YOUR RISK REGISTER

Defence Cyber Certification requires systematic risk management with periodic reviews to ensure ongoing compliance. As such, you'll need to maintain a risk register documenting your:

- Information assets
- Threats
- Vulnerabilities
- Existing controls
- Risk treatment decisions

Organise evidence clearly and cross-reference it against specific controls so it's easy for assessors to verify compliance.

STEP 8

RUN AN INTERNAL REVIEW

Before engaging a certification body to review your work, conduct an internal audit or dry run. Have someone who isn't involved in the process directly (ideally from another team or an external consultant) review your:

- Scope definition
- Cyber Essentials compliance
- Staff awareness and understanding
- Documentation completeness and clarity
- Evidence sufficiency and quality

An internal review helps you identify weak spots, so you can address them before formal assessment.

STEP 9

BOOK YOUR ASSESSMENT

Once you've finished your preparations and feel confident in your measures, engage an IASME-accredited certification body to conduct your assessment. If your Cyber Essentials certification partner is DCC-accredited, they should be able to do the honours. Alternatively, you can contact IASME for a list of approved certification bodies.

The certification body will:

- Explain the assessment process for your level
- Provide a quote based on your organisation's size and complexity
- Review your submission documentation
- Schedule and run your assessment
- Conduct interviews or demonstrations to verify controls
- Issue a certificate upon successful assessment (or a report detailing gaps if unsuccessful)

5 tips for DCC success

1. Use a checklist to manage your security controls

Download the Applicant Guide and Assessment Submission Record from IASME for your target level and convert it into a working checklist. Track each control's status, assigned owner, evidence location, and completion date.

2. Map existing security controls against DCC requirements

If you're accredited to another security standard, like the Cyber Assessment Framework or ISO 27001, map their requirements against DCC. This helps you avoid duplication of effort.

For example, if you have an ISO 27001 Annex A.5.19 policy covering supplier relationships and security requirements, this directly addresses DCC supplier security controls. You simply need to present it appropriately and provide DCC-specific evidence showing how you've implemented it.

3. Engage with staff

Cyber resilience is everyone's responsibility, not just IT's. Build a security-aware culture across your business where:

- All staff receive regular security awareness training
- Employees know how to report security concerns
- Security is embedded in daily operations
- Teams understand their role in protecting business assets

When staff engage with security best practices, behavioural controls (training, incident response, secure working practices) become much easier to satisfy during assessment. Consider working with a cybersecurity awareness training provider if you don't have the time or resources to handle it in-house.

4. Don’t be afraid to ask for help

If you unclear about any aspect of DCC, contact your certification partner or IASME for clarification. They can explain exactly what’s required and even provide examples to help you navigate potential stumbling blocks. It’s far better to seek guidance than guess incorrectly and fail a control.

5. Be factual and honest

Resist the temptation to exaggerate your strengths or downplay your weaknesses during the documentation and assessment phase. Honesty and clarity are always the best policies. In practice, this means:

- If something isn’t applicable to your situation, explain why
- Be upfront about controls you haven’t implemented fully and the reasons why
- Don’t try to mislead or overstate compliance
- Keep answers concise and focused – assessors appreciate directness

> ***“Many suppliers already do the right things – they just don’t document it. DCC expects evidence. Without it, you may find yourself repeating work you’ve already done or missing something crucial.”***
>
> – CyberSmart

What does the certification process look like?

Once you've prepared your evidence and controls, the formal assessment phase begins.

It's easy to underestimate how long the process takes or miss critical obligations that could invalidate your certificate. For example, letting your Cyber Essentials certification lapse during the assessment process will result in automatic failure – even if everything else is on-point.

Timelines

Unfortunately, there's no defined timescale for DCC implementation. Ultimately, it depends on your preparedness, whether you need to remediate gaps before applying, and certification body availability.

Starting early is crucial. Rushing preparation can result in gaps and insufficient evidence, requiring you to reapply and pay again.

Reporting obligations

DCC isn't a one-and-done accreditation – you need to demonstrate ongoing compliance throughout the three-year validity period. Once certified, you must:

- Complete annual attestations confirming ongoing compliance
- Renew Cyber Essentials (or Cyber Essentials Plus for Levels 2-3) annually
- Undergo full recertification every three years

Evidence requirements

You'll need to prove that you've implemented the necessary controls to the required standard through the assessment process. You must provide:

- An Assessment Submission Record detailing your answers to each control question (for Levels 1-3; not required for Level 0)
- Evidence demonstrating how you've implemented each control and that it works as intended
- Supporting documentation proving compliance under real-world conditions

Typically, you'll need to present evidence over screen-share sessions for lower levels, or during on-site visits for higher levels. You won't need to send documentation to certification bodies in advance – it remains within your systems and is presented upon the assessor's request.

You are responsible for securely storing evidence within their system for 3.5 years after certification. This evidence must be left unmodified. Failure to keep it stored or if it is seen to be modified can lead to revocation of the cert.

The benefits of working with a certification partner

Preparing for DCC can be daunting – particularly if you don't have a dedicated, in-house cybersecurity team to take the reins. Working with an experienced certification partner can simplify the process and give you the best chance of succeeding.

If you're not sure what to look for in a partner, narrow your search to those offering:

- Guidance at every stage of the certification process
- Scoping support
- Policy and documentation advice
- Technical implementation
- Training and awareness courses

Guidance at every stage of the certification process

A good partner explains certification requirements clearly, translating technical jargon into actionable steps. They help you understand what good looks like for each control and the type of evidence you'll need to satisfy assessors.

Scoping support

Look for a partner who can help you define appropriate scope, avoiding the common pitfall of scoping too narrowly or excluding critical areas.

Policy and documentation advice

Many organisations struggle with creating security policies from scratch. The best partners provide templates and examples to make your life easier.

Technical implementation*

Beyond policies, you may need help implementing technical controls like vulnerability scanning, logging, or access management. Choose a partner who can recommend appropriate tools and configurations appropriate to your environment and budget.

Training and awareness courses

Cyber awareness is a critical DCC requirement. Partners that offer structured training programmes help you instil cybersecurity best practices into your teams, so it becomes second nature.

* Your assessing certification body can explain requirements, verify your assessment scope, clarify questions, and provide blank templates - but cannot implement policies, modify systems, or create evidence they will later assess. For hands-on implementation support, you must engage a separate, independent partner. A certification body cannot assess its own work.

FAQs

Can I get Defence Cyber Certification if I don't have an active MOD contract?

Yes, you can apply for DCC at any level whether you hold an MOD contract or not. Proactive certification demonstrates preparedness and puts you in a strong position when bidding for future opportunities.

How long does DCC last?

Certification is valid for three years, subject to annual attestations and maintaining a valid Cyber Essentials certification (renewed annually). At the three-year mark, you'll need to undergo full recertification.

What happens if I fail the DCC assessment?

You'll receive a detailed report outlining the areas where you didn't meet requirements. You can address these gaps and reapply for assessment (with associated costs). Failed assessment are confidential and aren't shared with the MOD or other organisations.

Do I need separate certifications for each MOD contract?

No – that's one of DCC's key advantages. A single organisation-level certification covers multiple contracts at or below your certified level.

How does DCC differ from ISO 27001?

Although both accreditations cover information security management, Defence Cyber Certification is tailored to MOD requirements and DefStan 05-138 controls. ISO 27001 has a broader remit.

That said, the certifications complement each other. Many of the controls overlap, so pursuing both simultaneously is efficient. Just remember that DCC requires specific evidence formats.

How much does Defence Cyber Certification cost?

DCC costs vary based on your organisation's size, complexity, and the level of accreditation you're seeking.

Additional costs to bear in mind include:

- Cyber Essentials certification (if you're not already accredited)
- Security tools
- Infrastructure upgrades
- Staff preparation and training

Next steps

Defence Cyber Certification isn't about ticking boxes to win contracts. At its core, DCC is about building organisational resilience in the face of increasingly sophisticated cyber threats.

The controls required for DCC Levels 0-1 represent recognised best practices that protect your business, data, customers, and reputation. Every policy you write, every training session you deliver, and every vulnerability you patch makes your organisation more secure and better prepared to deal with whatever comes your way.

With the right preparation and support, Defence Cyber Certification is achievable for any business. To give yourself the best chance of success, start early, be systematic in your approach, engage with your people, and don't be afraid to ask for help when you need it.

Ready to start your DCC journey?

Explore our Defence Cyber Certification services and comprehensive support packages.

Talk to us

For support with accreditations, 24/7 threat detection, cyber insurance, and more, get in touch – we're happy to help.

☎ 0207 9936 990 🌐 cybersmart.co.uk ✉ hello@cybersmart.co.uk

CyberSmart