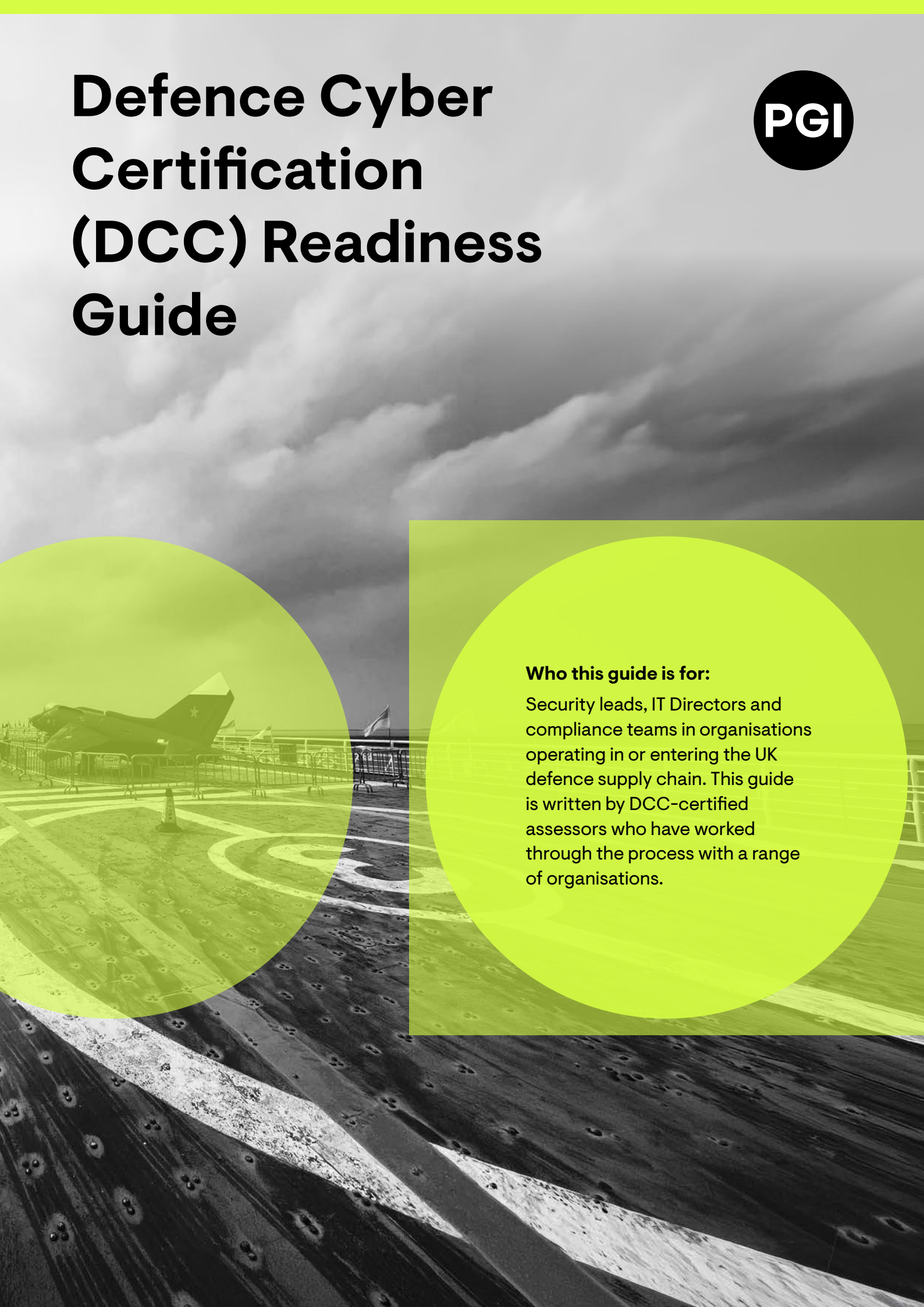
Defence Cyber Certification (DCC) Readiness Guide



Who this guide is for:

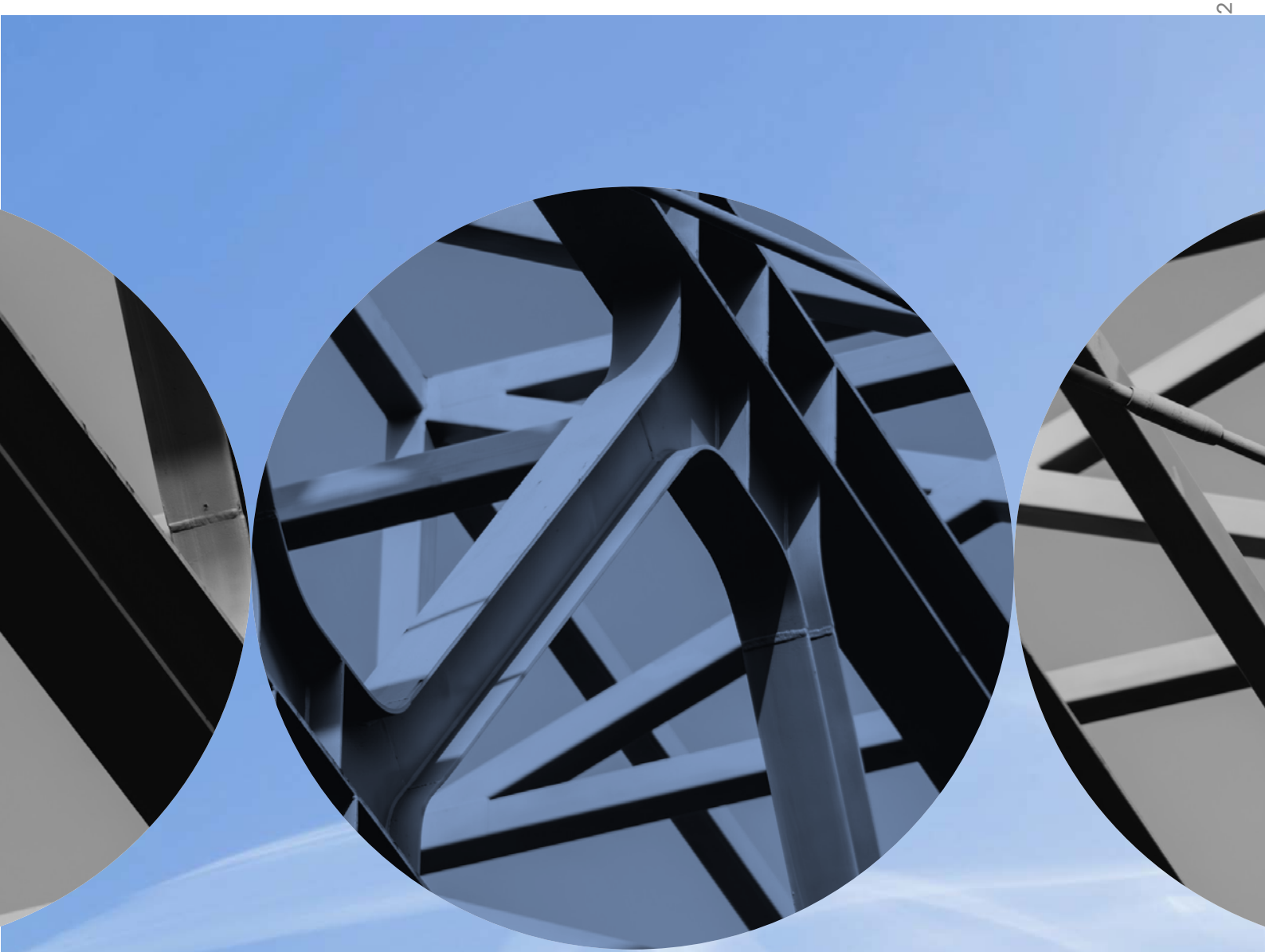
Security leads, IT Directors and compliance teams in organisations operating in or entering the UK defence supply chain. This guide is written by DCC-certified assessors who have worked through the process with a range of organisations.

What is the DCC scheme?

The UK Ministry of Defence (MoD) has introduced the new Defence Cyber Certification (DCC) scheme: A security framework for suppliers in the defence supply chain, designed to enhance overall resilience against cyber threat.

The DCC is an organisation-wide comprehensive certification. It provides assurance that your entire organisation has the right cyber security measures and controls in place — not just for one contract, but for all defence business opportunities.

Even if your organisation is small, the DCC scheme applies if you deliver services or products that touch the defence sector, even indirectly.



Visit: www.pgitl.com
Email: findoutmore@pgitl.com
Phone: +44 (0) 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT, UK
PGI - Protection Group International Ltd.
Registered in England & Wales. 07967865

Getting started

1 Identify your Cyber Risk Profile (CRP)

Start by confirming the CRP associated with your MoD contracts to help you determine the certification level you need to meet. The associated level determines the security controls you'll need to implement and evidence you'll need to provide. This will be made clear in the ASR and application guidance.

2 Understand the certification level and what's required

You need a clear understanding of what you're being assessed against. The CRP defines the level you need, but you need to ensure you understand the process and expectations involved in achieving it. It may drive changes in processes, documentation or technology in order to achieve the desired certification.

There are four DCC levels determined by the MoD, based on the contract risk:

- Level 0: Low-risk contracts
- Level 1–3: Increasing levels of risk

Aim for the level of certification aligned with the types of contracts you wish to pursue.

3 Define your organisation's scope

A confusing scoping statement can add unnecessary time to the process. From the outset, it's important to clearly define which areas of your organisation fall within the requirements. Scope must cover all processes, systems, people and third parties involved in fulfilling MOD contracts, including all essential services and functions necessary to maintaining business operations, including:

i. List of sites and their functions
ii. Brief list of IT networks and systems
iii. Brief list of OT network and systems
iv. Brief description of devices/assets
v. Data/document storage, electronic and other format
vi. Scoping diagram(s) showing systems inside and outside of DCC scope, and CE/CE+ coverage

For full details of scoping expectations requirements refer to the IASME scoping guidance which can be found here: https://iasme.co.uk/defence-cyber-certification/DCC-Scoping-Guidance.pdf

The scoping document must include the minimum detail as provided in the guidance. It's important that the scope is clear and concise.

Common scoping failures:
Organisations that define scope too narrowly, exclude third parties handling MoD data or produce diagrams that don't match their live environment.

Visit: www.pgitl.com
Email: findoutmore@pgitl.com
Phone: +44 (0) 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT, UK
PGI - Protection Group International Ltd.
Registered in England & Wales. 07967865

4 Map DCC requirements to existing standards

If you already operate an Information Security Management System (ISMS) for ISO 27001:2022, map the controls to your current Statement of Applicability and incorporate into the business.

Important note: While it's important to leverage the existing tools available to you, ISO 27001 maturity does not guarantee DCC compliance, particularly around technical controls and evidence recurrence.

5 Conduct a gap analysis

Review your current controls, policies, and processes. Do they meet the requirements for your assigned DCC level? Are they followed and effective?

i. **Review existing controls and Policies**
When completing to the ASR, you will need to reference policies and which exact section meets the requirement.

ii. **Assess technology and tooling**
The control is the requirement which you must meet. If the tooling, such as software, doesn't allow for you to meet the control, it doesn't mean the control is not applicable, it means the tooling might not be suitable for DCC. This is where you might need to make changes to meet those requirements.

iii. **Assess resource requirements**
Compliance isn't necessarily the responsibility of one person or team. Identify all employees who are involved in business operations that support DCC. You will need to document owners, asset owners, time and budget.

Where organisations fail:
Discovering tooling failures after the assessment process has begun, leading to delays and unexpected costs.

6 Gather evidence

DCC is evidence-based. You must be able to fully demonstrate how each control is met through clear, auditable evidence. Evidence gathering should not be treated as a one-off activity for assessment; it should be embedded into business-as-usual (BAU) operations.

Recurring tasks must genuinely recur and consistently produce evidence. Evidence should show when the activity happened, what was done and what outputs were produced.

Use calendar reminders, procedures, logs, reports, tickets or screenshots to demonstrate that the activity was completed on time and as required. Evidence must be created and maintained as part of BAU, not retrospectively.

Where organisations fail: Evidencing policies that are in place, but not having evidence of recurrence. Screenshots taken the day before will likely not pass muster.

Also consider configuration builds. Ideally, you should maintain documented configuration baselines for all systems, defining how each system is built and configured. This may include screenshots to evidence that required settings are applied.

Configuration builds are useful during annual reviews to verify that systems remain compliant with your policies and provide a reference for how systems should be configured. During assessment, the assessor will validate the live system to confirm the configuration aligns with the documented controls.

7 Train your people

Your employees play a critical role in maintaining compliance. They must understand their responsibilities, be familiar with relevant policies and processes and adhere to them in their day-to-day activities.

Untrained staff can inadvertently introduce internal risk, undermining your compliance posture. Regular, role-appropriate training helps ensure controls are understood and consistently followed as part of BAU.

8 Review your suppliers

If you work with third parties, you'll need to show evidence that you have oversight of their security practices and that they have the appropriate controls in place. This means conducting supplier due diligence and keeping records.

- Create an onboarding checklist to assess if a third party has the right security controls in place.
- Use a third-party questionnaire to ensure they meet your requirements and explore their security practices in more detail.
- Create written agreements to define your expectations and hold third parties accountable.
- Review your suppliers regularly after onboarding to ensure they continue to meet your required standards.
- Having a process if the supplier fails to meet requirements.

9 Don't leave it too late

Even if certification isn't mandatory for your current contracts, it is likely to become so in the near future. Starting early gives you time to address gaps proactively and avoid the cost and disruption of last-minute compliance. Non-compliance findings may require resources and budget you haven't planned for — build in time to respond.

Visit: www.pgitl.com
Email: findoutmore@pgitl.com
Phone: +44 (0) 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT, UK
PGI - Protection Group International Ltd.
Registered in England & Wales. 07967865

Interpreting the requirements

Controls mean what they say and apply to all systems within scope — an answer is only compliant if it's met by all systems in scope.

Make the most of the application guidance published by IASME for each ASR question, including a Jargon Buster to help with interpretation. Clear, well-evidenced answers reduce clarification rounds and keep your assessment on track.

Visit: www.pgitl.com
Email: findoutmore@pgitl.com
Phone: +44 (0) 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT, UK
PGI - Protection Group International Ltd.
Registered in England & Wales. 07967865

How the DCC assessment works

The assessment is completed by an independent Certified Assessor recognised by IASME. For first-time applicants starting from scratch, allow a 6–12-month window to prepare. A lot of this time is for your organisation to review the scoping guidance, understand the ASR and applicant guidance and prepare in-house. When reviewing your own scope and gaps, you may identify required changes for your polices, software or technology to meet the requirements. You need to ensure you give yourself enough time to budget, plan and implement any changes.

These phases are designed to ensure that your organisation can effectively demonstrate real, organisation-wide compliance to the DCC framework.

Phases

1

Readiness

The first stage focuses on preparation. We work with clients to ensure they have all the necessary documents and understand the DCC framework, the assessment process and the prerequisites. Scoping your business correctly is critical and we can help you define which functions, systems and processes need to be included.

This phase is also the time to be transparent about your organisation's overall readiness for DCC, as this can prevent significant cost later.

2

Assessment Record Submission (ASR)

Once readiness is confirmed, you will start by completing the Assessment Record Submission (ASR). This is similar to the Cyber Essentials process in structure, but requires input from across your organisation. Applicants must provide detailed answers, policies and evidence to demonstrate compliance.

This phase cannot be outsourced; it is an internal project requiring resourcing and cross-functional collaboration. At this stage, we can provide support to ensure your team understands the questions and expectations, but work like updating policies, implementing procedures and configuring systems will be your responsibility.

3 & 4

Review and clarification

Phase 3 involves theoretical marking, where your consultant reviews your submitted evidence and responses.

Phase 4 is a series of clarification rounds, if answers are unclear or incomplete. The number of rounds depends on the quality and completeness of the submission. Supplying clear, well-documented evidence from the start can reduce delays and additional consultancy hours required to understand and review documents, incomplete responses or unclear evidence.

5

Practical assessment

Compliance is demonstrated in real time, either remotely or onsite, depending on scope, complexity and DCC level. Practical assessment typically focuses on a representative sample of your environment – that means larger or more complex organisations may require additional time. This is where your policies, procedures and technical controls are validated against the standard.

6

Certification

Once all phases are successfully completed, certification is issued.

DCC is not a fixed-fee or fixed-duration assessment; it takes as long as necessary for your organisation to evidence that the standard has been met. Costs are aligned to the time and resources required.

Visit: www.pgitl.com
Email: findoutmore@pgitl.com
Phone: +44 (0) 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT, UK
PGI - Protection Group International Ltd.
Registered in England & Wales. 07967865

Benefits of the DCC Scheme

Stand out from competitors

DCC certification provides recognised, independently validated assurance of your cyber security posture. As a relatively new and specialised scheme, early adopters can stand apart when bidding for defence contracts.

Defence sector-specific security controls

The scheme provides defined, practical controls tailored to the defence sector, helping organisations understand exactly what needs to be implemented to align with MoD security standards.

Eliminates the need for repeated SAQs

DCC is the only accepted alternative to the Supplier Assurance Questionnaire (SAQ), removing the need to complete time-consuming questionnaires for each individual contract.

Independent, third-party validation

Certification provides external validation that your organisation has implemented the necessary controls and meets the security requirements of the defence sector, increasing trust with customers and partners.

Future-proof your organisation

Achieving DCC certification positions your organisation ahead of current defence supply chain requirements. As the certification becomes an increasingly required standard for suppliers, it reduces the need for reactive compliance efforts.

Strengthen supply chain security

DCC demonstrates that your organisation has mature security practices and is a reliable link in the defence supply chain. This is increasingly critical for winning and retaining contracts.

Long certification validity

Certification is valid for three years – one assessment across all defence contracts.

Ready to get started?

Whether you need help defining scope, running a gap analysis or understanding what assessment involves, speak to our team about a readiness review.

Visit: www.pgitl.com
Email: findoutmore@pgitl.com
Phone: +44 (0) 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT, UK
PGI - Protection Group International Ltd.
Registered in England & Wales. 07967865