Level 0 Applicant Guide

Introduction

The Defence Standard (Def Stan) 05-138 was introduced in 2015 as part of the UK government's national cyber security programme, responding to escalating cyber threats. Over the past decade, the defence standard has evolved, and its latest iteration, issue 4, marks a pivotal shift. This version expands the Defence Standard's scope beyond solely protecting MOD-identifiable information to enhancing the overall resilience of an organisation against threats.

The Ministry of Defence (MOD) recognises the importance of ensuring suppliers adhere to the Defence Standard. This document serves as a guide to help applicants prepare for an assessment against the Def Stan 05-138 i4.

By providing a structured and consistent approach to these assessments, MOD seeks to uphold the highest level of cyber security across its supply chain. The Defence Standard sets out the criteria for suppliers in its 148 controls, which are applied into four progressively stringent levels. MOD suppliers are expected to attain a level of security specified in their contracts with the MOD, which is referred to as the Cyber Risk Profile.

The overall aim of this certification scheme is to enhance the cyber resilience of the organisations applying for certification. Whilst some organisations may already meet the controls others may be deficient in some areas, as part of the application these areas will become apparent and (if possible) remediated prior to assessment.

Defence Cyber Certification/Cyber Risk Profile Levels

A Cyber Risk Profile level will be assigned to any new procurement/contract or requirement by the MOD awarding body; this level then defines which controls the supply chain is required to adhere to.

The Defence Cyber Certification scheme is used to assess whether the controls have been met. It is important to note that the Cyber Risk Profile and Defence Cyber Certification levels are the same.

Applicant organisations may, under the new DCC scheme, apply for assessment and then certification at any level. This allows them to demonstrate compliance with the chosen level by means of a certificate and will remove the need for future assessments on a contract-by-contract basis for levels less than or equal to their certification.

There are 148 controls in total, but no single level contains all the controls. This is due to some controls overlapping or being replaced by more comprehensive controls at a higher level.

The Defence Cyber Certification Levels are:

Level 0 (3 controls)

Level 0 is normally assigned where there is a very low level of assessed cyber risk to a supplier delivering an output. It requires supplier organisations to demonstrate basic cyber security practices and forms the foundation level for all future assessments higher than level 0.

Level 1 (101 controls)

Level 1 is normally assigned where there is a low to moderate level of assessed cyber risk to a supplier delivering an output. It requires supplier organisations to demonstrate a comprehensive cyber security programme with good practices.

Level 2 (139 controls)

Level 2 is normally assigned where there is a high level of assessed cyber risk to a supplier delivering a contracted output. It requires supplier organisations to demonstrate advanced cyber security oversight and planning which drives robust organisational and cyber practices.

Level 3 (144 controls)

Level 3 is normally assigned where there is a substantial level of assessed cyber risk from a supplier delivering a contracted output. It requires supplier organisations to demonstrate expert cyber security capabilities that fully take advantage of the 'defence in depth' methodology to appropriately protect the organisation against new and evolving threats.

The Level 3 assessment will be conducted as part of a pilot scheme, incorporating a hybrid approach that combines both Level 2 and Level 3 controls. Applicants will be required to provide responses and evidence for all Level 2 controls as well as all Level 3 controls, totalling 145 controls.

- This pilot scheme is currently the only pathway to achieve Level 3 certification. It offers flexibility for organisations pursuing Level 3 by allowing them to:
- Achieve Level 3 certification if the Level 3 pass mark is met.
- Achieve Level 2 certification if the Level 2 pass mark is met but Level 3 pass mark is not achieved.

Defence Cyber Certification Process

For the DCC process please see the **DCC Process Guide**.

The process varies according to the level, please ensure you follow the correct process for your level.

Third Party Assistance

Except for work allowed to attain Cyber Essentials (CE) and Cyber Essentials Plus (CE+), the only assistance the assessing Certification Body can provide is in an advisory role; they cannot make any changes or perform any actions.

The assessing Certification Body may:

- Help the applicant prepare for, and attain CE/CE+
- Explain the DCC scheme and its levels
- Explain the DCC controls and how to meet them
- Clarify the question and identify the key components needed to provide a complete and accurate response
- Describe the necessary evidence needed to demonstrate that a control has been met
- Verify scope
- Supply blank template documents

The Certification Body may not:

- Implement any policy
- Implement any changes
- Answer any questions on behalf of the Applicant or dictate the answers
- Complete any documentation or prepare any answers or evidence that they will later assess

If you need additional support beyond the advisory role of the Certification Body, you have the option to engage a separate technology provider.

Determine Scope

For DCC scoping please see the **DCC Scoping Guide**.

Defence Cyber Certification Questions

DCC Core Questions/Controls Labelling

Below is an example of a question ID and control number you will encounter in completing this submission.

The levels indicated in brackets following the MOD question ID represent the corresponding DCC scheme levels to which this question or control applies.

IASME has retained these values from Def Stan and the MOD supply chain as follows;

EXAMPLE

0001.1 - (MOD 000011) - (L0-L3)

0001.1	MOD 000011	L0-L3
The question ID	The MOD supply chain portal Unique Question ID	The level covered

The questions have been taken from the MOD SAQ where possible, however there may be slight changes to the wording or new questions created if not available from the MOD at the time of writing. Where no question is available from the MOD it will have the identifier MOD 000XXX.

---LIVE QUESTIONS NOW FOLLOW---

0001 - Cyber Essentials

Terms

Cyber Essentials is a UK Government-backed certification scheme. It is aligned to five technical controls designed to prevent the most common internet-based cyber security threats.

Control Requirement

The Applicant shall have Cyber Essentials certification that covers the scope required for all aspects of the assessment and commit to maintaining this for the duration of the Defence Cyber Certification.

Jargon Buster

The Applicant must have Cyber Essentials certification that applies to all areas of the DCC certification scope that is applicable to Cyber Essentials within Cyber Essentials guidelines. The Applicant must keep this Cyber Essentials certification for as long as the Defence Cyber Certification lasts.

The Cyber Essentials scope of the Applicant organisation must align with the proposed scope of this Defence Cyber Certification assessment. It must be noted (as discussed during scoping) that Cyber Essentials scope is only internet-connected devices whereas DCC scope includes internet-connected and non-internet-connected devices. For clarification on Cyber Essentials please see the Cyber Essentials Knowledge Hub and for DCC scope, please see the separate DCC Scoping Guidance.

Your Assessor will verify that the Cyber Essentials and DCC scopes align as much as possible, but this will rarely be an exact match. A small organisation may be able to exactly align, but as DCC includes non-internet connected devices, there will usually be some differences between scopes. As such, it is important to add context to your answer so the Assessor can understand your Cyber Essentials scope and why it may vary from the DCC scope.

You should discuss your scope(s) with your chosen Certification Body as one of your first steps when answering the questions. If the Cyber Essentials scope does not adequately align, then it is an automatic failure.

Supplying a diagram showing which parts of the organisation/network fall within CE and how they relate to the DCC scope is recommended for all organisations.

0001.1 - (MOD 000011) - (L0-L3)

Does the organisation hold Cyber Essentials certification(s) that cover(s) the required scope for this activity?

Cyber Essentials has it's own guidelines for the devices that cannot be within scope, within those guidelines the Cyber Essentials scope must cover all of the applicable internet-connected devices/networks within the DCC scope.

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, my Cyber Essentials certificate covers all of my internet-connected networks/devices but does not include my non-internet-connected operational technology (ICS/SCADA).
Expected Evidence: Your certificate number, Cyber Essentials self-assessment questionnaire/report, diagram showing CE scope in relation to DCC scope

0001.2 - (MOD 000625) - (L0-L3)

Does the organisation commit to maintaining Cyber Essentials certification for the duration of any function related to this activity or DCC certification?

You must consider the Cyber Essentials certification covering contracts for their duration.

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes

Expected Evidence: An attestation or history demonstrating regular renewal.

Objective A - Managing security risk

Managing security risk. The Applicant has appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to its network, and information systems, including all network and information systems that protect all data.

2314 - Ensure UK GDPR compliance

Control Requirement

The Applicant shall align with the processing of personal data is conducted in compliance with the UK Data Protection Act 2018 (UK DPA).

This control wants you to show how you comply with UK Data Protection Act 2018. It is recommended to follow the guidance of the Information Commissioner's Office. The Defence Cyber Certification scheme assessment is limited in scope and does not guarantee compliance with GDPR.

A GDPR policy must adhere to core principles, regardless of business size. These principles include lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability.

2314.1 - (MOD 000447) - (L0-L3)

Does the organisation have documented policies and procedures which ensure compliance with obligations under the UK General Data Protection Regulation (GDPR)?

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, this can be found in...
Expected Evidence: The policies or procedures documenting how you are complying with UK General Data Protection Regulation. This may be a dedicated policy or incorporated within other company documentation, such as a risk

register detailing the risks to the data subject. The size and nature of the organisation will determine the exact evidence available as smaller organisations may have simpler documentation compared to larger, more complex organisations.

2314.2 - (MOD 000446) - (L0-L3)

Does the organisation conduct Data Protection Impact Assessments (DPIAs) against data types it stores or processes?

Data Protection Impact Assessments (DPIAs) may include identifying data processing activities, assessing data types, identifying risks and impacts, mitigating risks and documenting them.

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes, we rigorously conduct assessment by...
Expected Evidence: To show that you're thoroughly conducting Data Protection Impact Assessments, you could provide: the procedure you use outlining how you conduct Data Protection Impact Assessments, the template or tool used to complete an assessment, or a report showing the output from assessments.

2500 - Resilient networks and systems

Control Requirement

The Applicant shall build resilience against cyber-attack and system failure into their design, implementation, operation and management of systems that support the operation of business Functions and protection of Data.

Jargon Buster

Although this control contains just two yes/no questions, it's important not to underestimate its significance. Resilience is a vast and vital concept that should be woven into the very fabric of your organisation, fortifying it as a whole.

We want you to demonstrate that.

When answering these questions, the control is looking for a few key elements. Let's break down the requirement:

Firstly “build resilience against cyber-attack and system failure”. The best way to start understanding the requirement is to focus on the word resilience. Resilience is “the quality of being able to return quickly to a previous good condition after a problem”.

Consider the ways in which you have strengthened the systems that support your organisation’s operations and protect its data. Beyond prevention, this requirement emphasises resilience and recovery.

This should encompass the entire lifecycle of those systems, from design and implementation to operation and ongoing management. Specifically:

- Design: When you are planning systems.
- Implementation: When you begin acting on those plans.
- Operation: When systems are actively used as part of your organisation’s main business functions.
- Management: The ongoing oversight, maintenance, and governance of the systems.

2500.1 - (MOD 000452) - (L0-L3)

Has the organisation assessed the degree to which its systems must be resilient to cyber-attack and system failure?

Jargon Buster

Focus your answer on the steps you took to evaluate how robust and secure your systems would need to be to withstand cyber-attacks.

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. We conducted a risk assessment and...
Expected Evidence: The evidence will vary according to organisation size and complexity. A micro sized company may only have a brief document showing the risks, whereas a large organisation will have multiple documents (including a risk register) to show the risks. The evidence must be tailored to the company size, service provided, and risks faced. You must show what systems are essential (which may be your scope) and the risks.

2500.2 - (MOD 000453) - (L0-L3)

Has the organisation built resilience into its systems to meet its resilience needs?

Jargon Buster

Focus your answer on the implementation of resilience into your systems.

Available answers (choose one):

- ☐ Yes
- ☐ No

Example: Yes. We have redundant network and endpoints...
Expected Evidence: The evidence should demonstrate tangible, practical actions taken to build resilience into your systems. The evidence should clearly show how these directly address the resilience needs identified in your earlier assessment. Avoid referencing policy documents or high-level plans. Focus instead on the

concrete actions and tools that ensure your systems can withstand and recover from disruptions, for example, implementing automated backups or uninterruptible power supplies.