Scoping Guide

Introduction

Determining the correct scope is the first and most critical step of any certification. It serves as the cornerstone for the entire assessment process. Given its significance, it is highly recommended that the CEO/CISO (or an equivalent company official) is aware of the proposed scope, accuracy and relevance to the certification being sought.

This guide provides detailed instructions on how to determine which elements should be considered in scope, However, as the Applicant is most familiar with their own organisation, it is ultimately the Applicant's responsibility to:

a) Determine the scope of their assessment.
b) Present and document the scope in a clear, detailed and comprehensive manner.
c) Answer the scheme questions and provide the necessary supporting evidence.

It is important to note that failure to adequately and accurately define the scope (e.g. under scoping) will result in a failure to achieve certification, even if all required controls have been met.

Your scope must be clearly documented, as it will be reviewed and discussed with the Assessor. The Assessor may challenge aspects of your scope to ensure itis appropriate and sufficient. To ensure your scoping statement is clear and complete, you must provide the following:

- A list of systems, services, and functions that are both **in scope** and **out of scope** for the DCC scheme.
- A list of systems, services, and functions that are both **in scope** and **out of scope** for Cyber Essentials (CE) and Cyber Essentials Plus (CE+).
- Diagrams illustrating the above, including how the different scopes overlap.
- A list of sites and their functions (e.g. workshop, head office etc)

DefStan 05-138 issue 4

Organisations familiar with DefStan 05-138 i3 will be used to risk assessments based around Ministry of Defence Identifiable information (MODII).

DefStan 05-138 i4 is different in that it focuses on whole organisation security and resilience. Naturally, this means that the focus of the scope has changed and is likely to draw more of the organisation into scope than previously.

DefStan 05-138 i4 states the following:

"1.1 The scope of this standard is the Supplier's overarching corporate or enterprise environment. All Supplier organisations, systems, processes, procedures and data necessary for its effective protection of Data and/or Functions are within the scope of this standard, going beyond the protection of just the information provided to the Supplier in support of that contracted output.

1.2 This standard is, therefore, intentionally broad, ensuring that a Supplier organisation, irrespective of any controls required for a specific contracted output, has the appropriate minimum levels of controls in place for the level of risk to which that Supplier organisation is expected more generally.

2.6 Where the term 'Functions' is used in Clause 3, it is helpful to consider this term as referring to both general business activities essential for ongoing operations and any specific activities related to delivering contracted outputs.

2.7 Where the term 'Data' is used in Clause 3, it is helpful to consider this term as encompassing any information generated, stored or handled by the Supplier in support of its Functions."

The scope is not just about the data held. If the processes and systems are essential for the organisation to operate as a business, then it must be within the Defence Cyber Certification scope.

What should be in the Defence Cyber Certification Scope?

In short, the scope of the Defence Cyber Certification should be whole organisation. Specifically, the company or legal entity responsible for delivering the service to the MOD must be considered in scope. However, this does not mean that every part of the organisation is included. Only the essential services and functions necessary to maintain the organisation's operations are in scope. For example, systems such as HR, IT, and stock management are likely to be in scope, whereas non-essential areas like cafeterias or vending machines typically are not - unless, of course, your organisation depends on them to function effectively.

The scope must include all processes, systems and business parts that are required for the business to function and deliver in a secure and resilient manner.

When defining your scope, it's important to consider not only the devices and networks directly involved in fulfilling the MOD contract but also covers all other systems critical to the functioning of your business. These could include payroll systems, building entry systems, industrial control systems, operational technology (OT), order and stock management systems, as well as heating, ventilation, and environmental controls (HVAC) systems, among others. To assist in determining which systems and areas are essential, it is recommended to use a scoping method such as the Five Lens approach from GovAssure. While this method is not mandatory, it can be a helpful tool to ensure your scope is accurate and comprehensive. Ultimately, if any system, process, or function is required for your organisation to operate, then it must be included within the DCC scope.

Conversely, if a system is not essential for your organisation to function, it may be excluded from scope. If you are uncertain, consider the potential impact of a particular system or function being unavailable for a day, a week, a month, or longer. Ask yourself: What would the consequences be, and could the business continue to operate effectively without it?

The Applicant knows their organisation best. The Applicant is responsible for ensuring the scope covers everything it needs to.

There are five key elements to consider when defining the scoping boundaries:

1. **Tools and Technology**

This includes all technology used within the organisation, whether connected to the internet or not.

2. **Operations and Logistics**

The process and systems that support the delivery of your organisation's services and products.

3. **Administrative Functions**

The systems and processes that support the organisation's internal management and operations.

4. **Operational Locations**

All physical locations from which your organisation conducts its activities.

5. **People with Access**

This includes staff, visitors and third parties who have access to your information, systems, or physical sites.

Secure by Design (SbD)

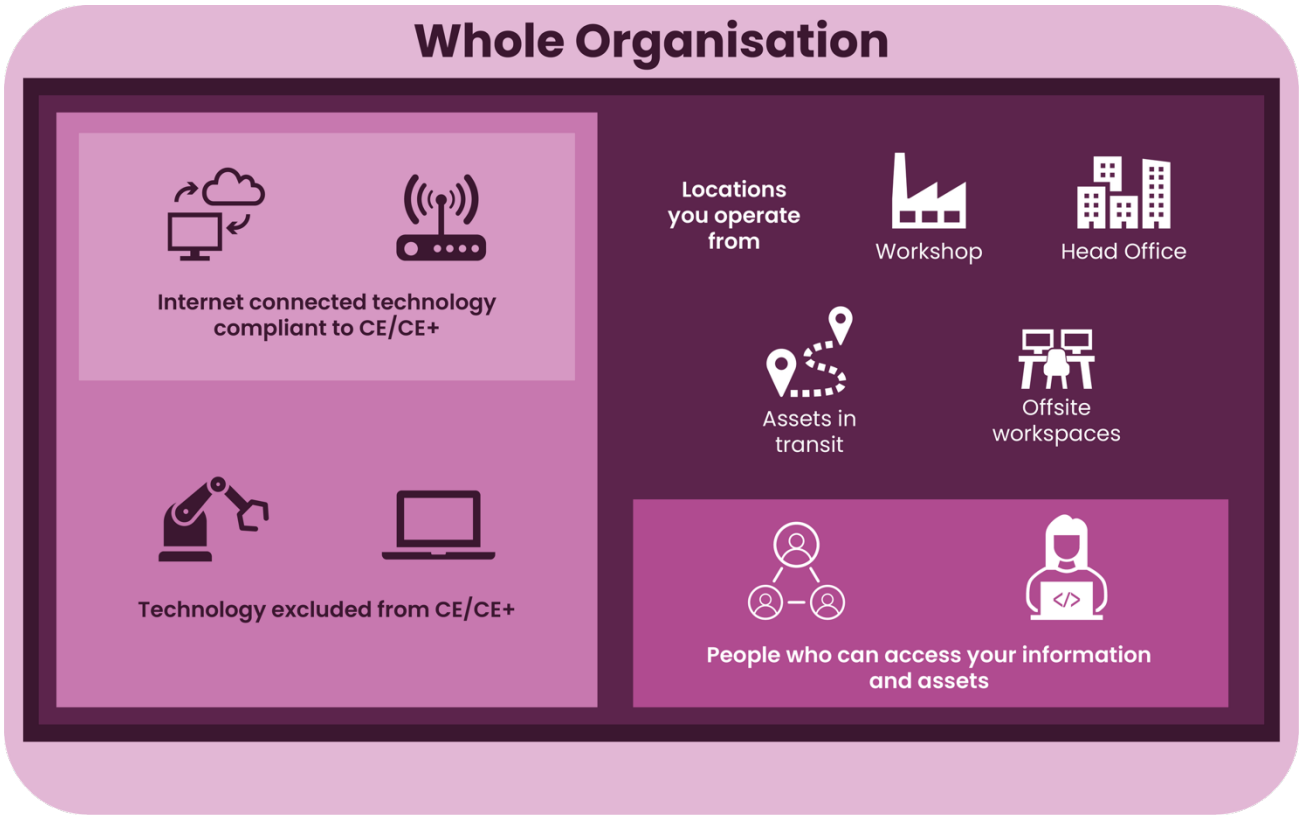
Secure by Design is potentially part of your overall security governance. This is an area awaiting further guidance which will be provided shortly.

Operational Technology

It is likely that not all OT systems, if any, need to be included in the scope. This will vary depending on the nature of your organisation. Every organisation is unique, performing different tasks in different ways using different tools. As a result, the systems and functions that fall within scope will differ from one organisation to another.

If your organisation relies on OT as an essential part of its operations – such as running CNC machines 24/7 as a core service - then those systems should be included in scope. However, if the CNC machine is only used occasionally for non-essential tasks, it may be excluded. The key factor in determining whether a system should be in scope is its importance to your organisation's ability to function. If a system is critical to your business operations, it should be included in your DCC scope.

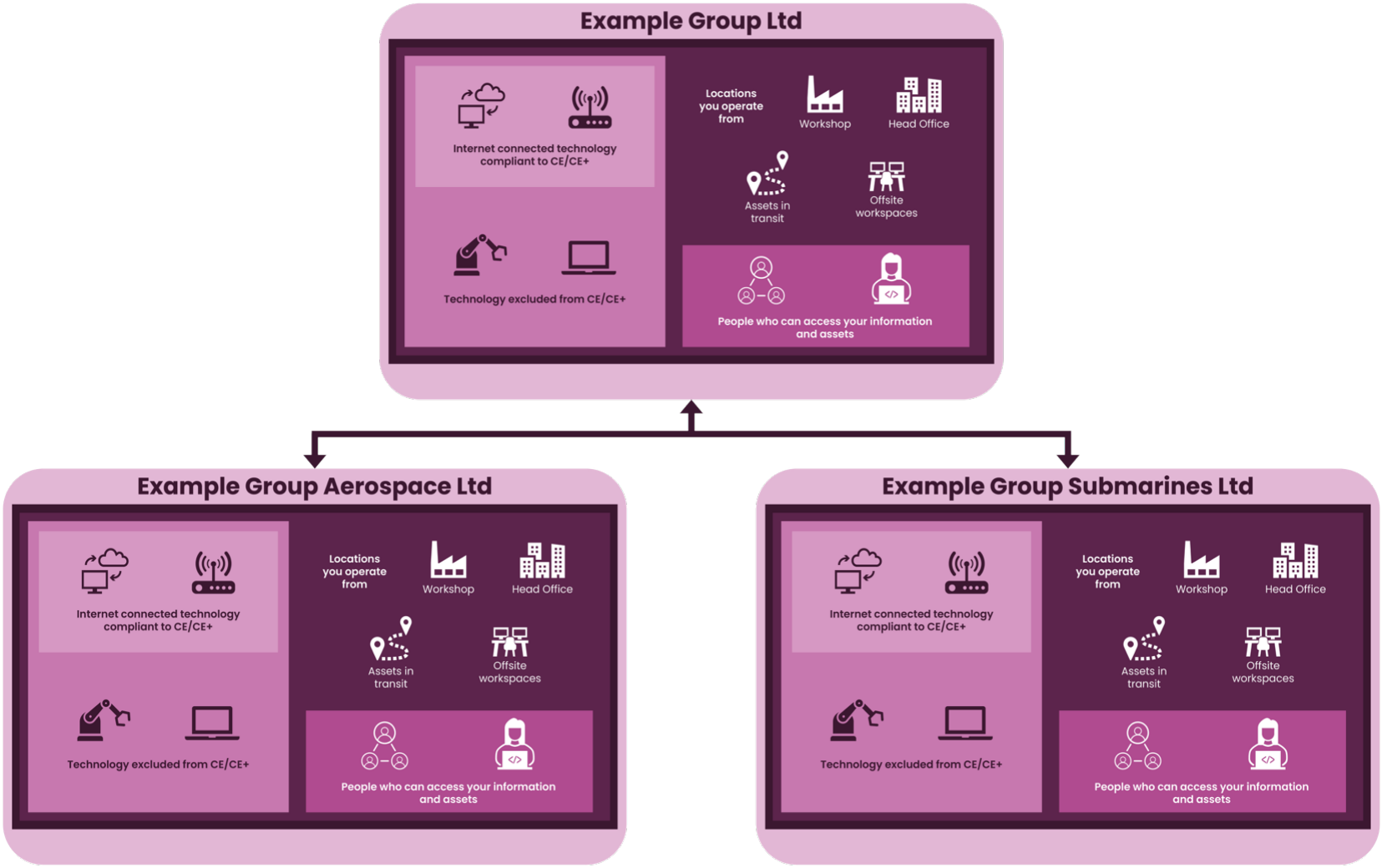
If OT is included in your scope, it's important to note that not all controls may be applicable. While you should aim to apply all controls wherever possible, there may be technical limitations that prevent certain controls from being implemented. For example, if anti-malware software cannot be installed on a CNC machine due to technical constraints, this limitation can be taken into account by the Assessor. In such cases, your assessment answers will need to demonstrate why the control cannot be applied and show evidence of alternative measures taken to mitigate the associated risks (e.g., Secure by Design (SbD) principles or other compensating controls).



Example scoping diagram for certifying whole organisation

DCC
Defence Cyber Certification

iasme



The above example shows a typical corporate structure encompassing multiple legal entities operating under a parent company. Each would require separate certification as separate entities. Where an entity makes use of elements of another (e.g. Aerospace uses the Group mail system), that element is treated as being provided by a 3rd party, with the same assurance/evidence requirements applying.

Large organisations with multiple stand-alone divisions will be required to seek certification for each distinct entity, ensuring that the scope covers all essential activities.

The Defence Cyber Certification scope should be the same for all levels of certification.

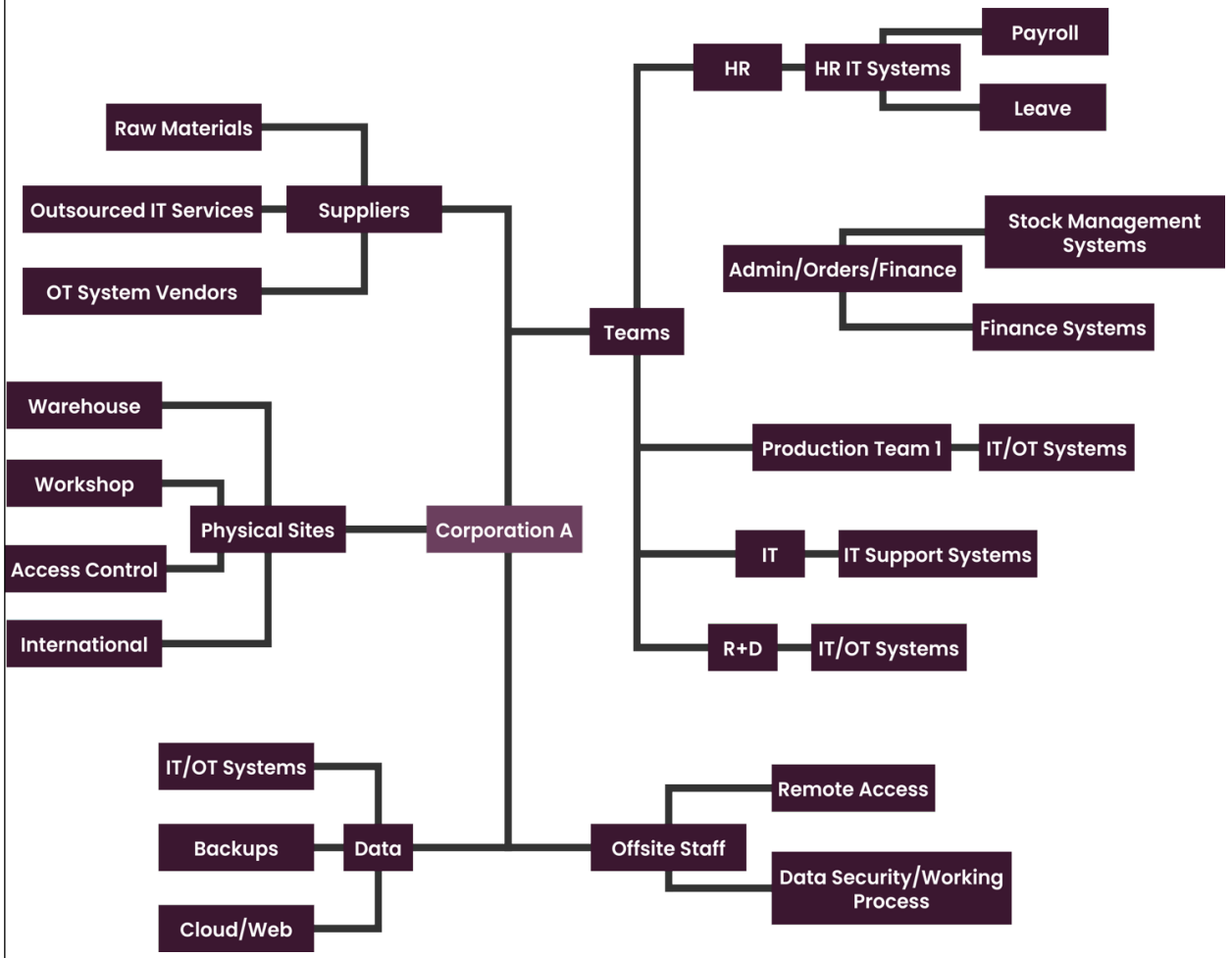
It is imperative that the Defence Cyber Certification scope is the same, as it will be reviewed during renewal or if certification levels change. If the Defence Cyber Certification scope does need to change - such as in the case of organisational restructuring or other valid reasons – these changes must be clearly communicated and justified. In summary, the scope defined in Level 0 should align with the scope for Levels 1–3 to ensure consistency and compliance.

DCC
Defence Cyber Certification

iasme

This diagram illustrates an example of a small company and the key elements that make up its structure. As a starting point, it's important to evaluate each function or service and assess its criticality to your organisation. Once identified, each function or service should be further analysed to determine the resources and support required to sustain it. For instance, Research and Development (R&D) might not be a critical function for your organisation and could be excluded from the scope. On the other hand, your Production Team might be essential, which could bring Operational Technology (OT) into scope.

You should be able to clearly explain and objectively demonstrate that your scope encompasses all essential services and functions. Any decisions regarding what is included or excluded from the scope should be carefully considered, as these will be reviewed and discussed with the Assessor.



Cyber Essentials Scope vs Defence Cyber Certification Scope

All of the Defence Cyber Certification levels require either Cyber Essentials or Cyber Essentials Plus as the first requirement.

Achieving a whole-organisation scope is not always achievable. In such cases, the scope can be narrowed to focus on essential services/functions and the systems required to support them, while excluding certain elements that do not meet the requirements for CE/CE+.

It's important to note that any internet connected components within the DCC scope are automatically included in the CE scope (within CE guidelines).

Discussing the scopes of two different certification schemes – Defence Cyber Certification and Cyber Essentials – can quickly become complex. To clarify, it's essential to understand that these are two distinct schemes with separate objectives. To make this distinction easier, we have colour coded the two different scopes for this section.

The **Defence Cyber Certification scope** **must** either encompass or overlap with the scope defined for Cyber Essentials (or Cyber Essentials Plus (CE+). If your organisation holds multiple Cyber Essentials certificates, they can be considered collectively when aligning with the Defence Cyber Certification. If the **Defence Cyber Certification scope** is not sufficiently aligned with the **Cyber Essentials (or Cyber Essentials Plus (CE+) scope,** this will result in a failure. In the very rare instances where the **Defence Cyber Certification scope** and **Cyber Essentials (or CE+) scope** do not overlap, this must be clearly demonstrated to the Assessor. Neglecting to provide adequate justification will also result in an overall failure. It must be noted that Cyber Essentials is a separate certification scheme that focuses specifically on the internet-connected IT infrastructure used to support your business operations. Unlike DCC, Cyber Essentials does not extend to other types of infrastructure, such as air-gapped devices, entry control systems or heating, ventilation and air conditioning (HVAC)systems. However, the **Cyber Essentials scope** must fall within or overlap with the broader **Defence Cyber**

Certification scope. Cyber Essentials should be conducted using the latest Cyber Essentials guidance regarding which devices and networks may be excluded. It should also be emphasised that Defence Cyber Certification guidance does not supersede or overrule Cyber Essentials (or CE+) guidance. The **Cyber Essentials scope** is not limited solely to assets that directly process MOD Identifiable Information related to the product or service being provided. Any internet-connected device that provides an essential service to the business must be included in the **Cyber Essentials (or CE+) scope** (within Cyber Essentials guidelines).

For example, if your HR or order payments processing team is

1) critical to your business, and

2) using devices or networks connected to the internet,

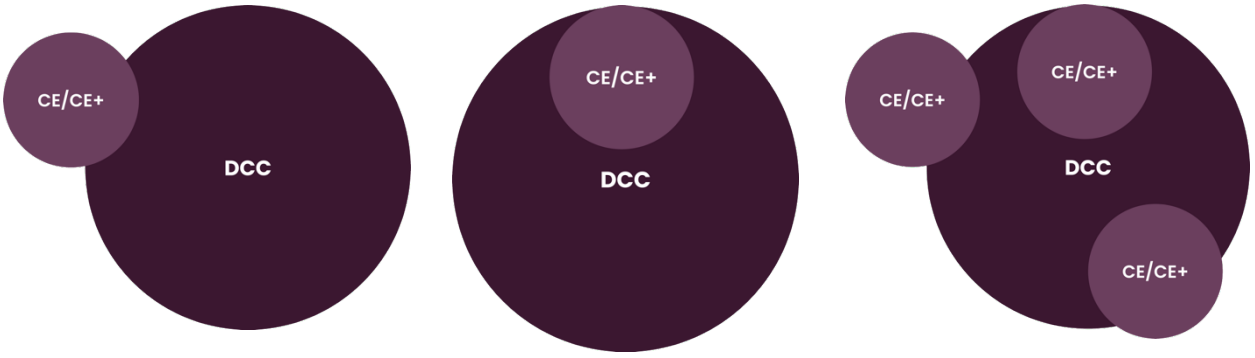
then those devices and networks must be considered part of your **Cyber Essentials (or CE+) scope.**

It is important to note that whilst best practice is to have your whole organisation within your **Cyber Essentials (or CE+) scope,** this is not always possible. If certain internet-connected devices (e.g., penetration testing devices) must be excluded from the **Cyber Essentials (or CE+) scope,** they may still need to be considered as part of the **Defence Cyber Certification scope.** The role of the Defence Cyber Certification Assessor is not to re-evaluate or re-score your Cyber Essentials (or CE+) submission. Instead, their responsibility is to assess whether the CE (or CE+) scope adequately meets the requirements of the organisation as part of the Defence Cyber Certification assessment. The Assessor must verify that the **Cyber Essentials (or CE+) scope** is appropriate and aligns with the **Defence Cyber Certification scope.**

To facilitate the Defence Cyber Certification assessment, it is important for the Applicant to clearly identify which networks and devices are internet-connected and fall within the **Cyber Essentials (or CE+) scope**. Non-internet-connected networks and devices should also be documented, as the Assessor will need to evaluate how the **Cyber Essentials (or CE+) scope** aligns with the **Defence Cyber**

Certification scope. Any differences between the two scopes, along with the rationale for those differences, must be clearly explained.

Overlapping scope	Fully aligned scope	Multiple CE certificates



Applicants are not required to complete their Cyber Essentials (or CE+) certification at the same time as pursuing Defence Cyber Certification. However, it is strongly recommended to consider the **Defence Cyber Certification scope** when applying for Cyber Essentials (or CE+). Wherever possible, Applicants should consult with the Certification Body (CB) responsible for assessing the **Defence Cyber Certification scope** to ensure alignment and reduce the risk of inadequate scoping.

Data Classification

DCC is not intended to address classified data, individual products, or specific projects. Suppliers may receive a Security Aspects Letter (SAL) outlining additional requirements that extend beyond the scope of DCC. The primary focus of DCC is to ensure that the organisation is resilient enough to continue functioning effectively in the event of a cyber incident. If a highly classified system falls within the DCC scope, the Assessor will not evaluate the classified data itself. Instead, they will expect to see evidence of proportionate controls and how the network supporting that system is managed and secured.

Scoping Attestation

Once you have determined your scope, you must document it in an attestation. This will help your Assessor understand your organisation and allow them to verify that your scope is appropriate and sufficient. Your attestation must include, at a minimum, the following information:

Defence Cyber Certification (DCC) Scope Attestation

I, [Full name and job title] , am authorised to make this statement on behalf of [full name of organisation]hereby attest that the statements and details provided in the Defence Cyber Certification Level [.] assessment for [full name of Organisation] dated [.] are accurate, complete, , and that no material facts have been omitted or misrepresented.

I confirm that all essential services and functions required for my organisation to operate normal business activities, and deliver contracted output, are within my DCC scope. This is comprised of:

(a) List of sites and their functions
(b) Brief list of IT networks and systems
(c) Brief list of OT network and systems
(d) Brief description of devices/assets
(e) Data/document storage, electronic and other format
(f) Scoping diagram(s) showing systems inside and outside of DCC scope, and CE/CE+ coverage

For the purposes of this attestation, a material fact is defined as any information that could influence the acceptance, validity, or assessment of the certification.

I understand that if any statements or details are later found to be misleading, inaccurate or incomplete, this may result in the invalidation and revocation of the certification.

By signing I make the above declaration on behalf of [full name of Organisation].