Ministry of Defence

Cyber Security Model Version 3 Cyber Implementation Plan (CIP)

A guide to when a supplier / bidder has not met all the controls required on the Supplier Assurance Questionnaire (SAQ)

Guidance not applicable to Cyber Security Model Version 4.

Edition: 21st February 2024

The Defence Cyber Protection Partnership (DCPP) and the Cyber Security Model

To become a Defence supplier to MOD you need to meet the controls as set out in Def Stan 05-138 by the contract start date. This is done through the Supplier Assurance Questionnaire (SAQ).

Suppliers not meeting the controls at the bidding phase are still able to compete, but will be required to complete a Cyber Implementation Plan (CIP).

For example, if you completed a SAQ and do not have Cyber Essentials or Cyber Essential Plus, you can use the CIP to commit to having this certification in place by contract start date as well as submitting appropriate and accepted mitigation whilst you are awaiting accreditation.

Ministry of Defence

Cyber Implementation Plan

What?

What is the Cyber Implementation Plan?

The CIP allows a Supplier to propose mitigations where they have not demonstrated compliance with MOD's cyber security requirements as detailed within the Cyber Risk Profile. The CIP is a contractually binding document.

Is there a CIP Template?

Yes. This will be referenced at the end of this guide.

Remind me - What is the Cyber Security Model?

It's a risk-based proportionate approach, to protect MOD Identifiable Information (MODII) on supplier systems. Visit the DCPP web page.

Ministry of Defence

Cyber Implementation Plan

When?

When do I start the CIP?
After the SAQ has been submitted and a response returned indicating that not all the controls were met.

When do I submit the CIP?
Unless otherwise informed by the Delivery team, the CIP must be submitted with the tender.

The following slides explain how to complete a CIP and how it is evaluated.

Ministry
of Defence

Cyber Implementation Plan

What should I include?

The Cyber Implementation Plan should include risk mitigation actions related to only those controls not met within the Supplier Assurance Questionnaire.

Ministry of Defence

Contents

Ministry of Defence

What are my options with a CIP?

For any control that hasn't been met, there are five pre-defined options

1. The Supplier commits to meeting the controls by contract start date.

2. The Supplier commits to meeting the controls during the contract.

3. The Supplier demonstrates an alternative certification is sufficient.

4. The Supplier will be using another organisation's network.

5. [Least preferred]
This control will not be met.

Ministry of Defence

1. Committing to meet the controls by contract start date

CIP Options in detail

A supplier can commit to meeting the control(s) by the contract start date. They should state this intention, along with any projected dates, activities already taken, and any relevant certifications currently or previously held.

The Delivery Team should regularly monitor progress and add a milestone payment condition to the contract.

Additional: VL01 – Cyber Essentials

IASME's [free] Cyber Essentials Readiness Tool is a good way to demonstrate you have considered what is required to get Cyber Essentials certification (VL01). It is also a useful exercise for an organisation considering how to improve their cyber security.

Below are links to Cyber Resilience Centres who can give free advice and actively support Cyber Essentials and the NCSC Cyber Toolkit.

England and Wales

Scotland

Northern Ireland

Ministry of Defence

2. Committing to meet the controls during the contract

CIP Options in detail

A supplier can commit to meeting the control at a point during the contract.

This is similar to meeting the controls by contract start date but recognises that a control won't be ready when required.

This option is likely to be used if the contract start date is too close and there is sufficient duration.

The Delivery Team will need to consider if additional mitigations are required until the control is implemented. E.g. changing how information is exchanged.

The Delivery Team should regularly monitor progress and add a milestone payment condition to the contract.

Ministry of Defence

3. Demonstrate an alternative certification meets the requirements

CIP Options in detail

This option is only for:

- VL01 – Cyber Essentials
- L09 – Cyber Essentials Plus

It is not acceptable to say that Certificate 'X' is equivalent to Cyber Essentials (PPN 09/23, Q9). The supplier must demonstrate the controls required for Cyber Essentials have been implemented, whilst assuming the Delivery Team is unaware of the alternative certification.

The original guidance required a paragraph against each control. This has now been revised as follows:

Cyber Essentials:

Complete the CE Online Readiness tool and submit the output confirming the scope applies to the entire network. Add additional information on a separate page if clarification is needed.

Cyber Essentials Plus (beyond CE)

Confirm that a professional independent third party has carried out the checks as set out in the Cyber Essentials Plus Test Specification.

Ministry of Defence

4. The Supplier will be using another organisation's network

CIP Options in detail

This option allows a supplier to explain that they will be using another organisation's network. This network should have an appropriate level of accreditation. There also needs to be clarification of the scope, e.g. all MODII associated with the contract, or a specified sub set.

Example 1

The supplier will be issued with MODNET laptops which will be used for all MODII associated with that contract.

Example 2

The supplier will be using a sub-contractor's network that has UK MOD accreditation of at least SECRET. This will be for all work involving this level of classification. The flow down Risk Assessment Reference (RAR) and sub-contractor's SAQ reference are provided. The latter references the accredited system.

Example 3

The supplier will be using the prime's network which has been accredited to SECRET. This will be for all work involving this level of classification. The prime's SAQ is provided, referencing the accredited system.

This option acknowledges that the Supplier will not meet this control. A better CIP will give details about what is done, even though it might not meet the required standard. The intention is to provide the information necessary to give the project team options to manage the risk.

When evaluating a CIP the following should be considered by the assessor:

- Contract start date
- Contract end date / duration
- The MODII being provided to the supplier versus MODII generated by the supplier
- Worst case scenario if a hostile nation hacked into the supplier
- Alternative mitigations:
  - Can [higher risk] data be withheld (electronically) until security is implemented?
  - Can the supplier be provided with a MODNET or SCI laptop?
  - Can non-electronic copies be provided instead?
- The CIP is intended to be part of a conversation, not the final word.

Ministry of Defence

Evaluating a CIP

The table below summarises who can can agree the CIP. For MOD, it is assumed that guidance will be given by appropriate security personnel.

Cyber Risk Profile	Risk Acceptor	Informed of risk acceptance
Very Low	MOD Project SRO or higher tier supplier	Major business unit / front line command SIRO
Low	MOD Project SRO or higher tier supplier	Major business unit / front line command SIRO
Moderate	MOD Major Business Unit / Front Line Command SIRO	Major business unit / front line command SIRO
High	MOD Major Business Unit / Front Line Command SIRO	Major business unit / front line command SIRO

CIP Templates

- There are templates for all Cyber Risk Profiles:
  - Very Low
  - Low
  - Moderate
  - High

CIP forms should be sent to the MOD Delivery Team. Please note that the DCPP – Cyber Security Model team cannot approve / agree CIPs.