DCPP
Defence Cyber
Protection Partnership

Supplier Cyber Protection service

How it works (Concept of Operation)

January 2017 (Version 1)

DCPP
Defence Cyber
Protection Partnership

Introduction

The 'Concept of Operation' outlines the key processes which will implement the new Cyber Security Model (CSM)

This includes requirements for **suppliers**:

- Completing a Supplier Assurance Questionnaire
- Cyber Essentials certification
- Risk assessing sub-contracts

and requirements for **Ministry of Defence**:

- Risk assessing new requirements
- Evaluating supplier bids

All processes are supported by the online **Supplier Cyber Protection** service:
https://suppliercyberprotection.service.xgov.uk/

The service allows MOD and suppliers to meet their requirements, and manage their contracts online.

Contents

DCPP
Defence Cyber
Protection Partnership

1. Risk Assessment

The Ministry of Defence must complete a Risk Assessment (RA) for all new requirements

The RA will assign one of five contract **risk levels** from the Cyber Security Model:

- Not Applicable
- Very Low
- Low
- Moderate
- High

This requirement also applies to suppliers that sub-contract elements of work (see 5. Flow down to sub-contractors)

This information and a **Risk Assessment Reference** will be:

- Submitted by the Project Team to MOD Commercial
- Shared with potential suppliers in the contract notice / information

**The process does not replace any contract specific requirements addressed by the Security Aspects Letter*

View the Risk Assessment workflow for more information at **https://www.gov.uk/**

2. Supplier Assurance Questionnaire

Suppliers bidding for contracts must complete a Supplier Assurance Questionnaire (SAQ)

Contracts with a Very Low, Low, Moderate or High risk level require an SAQ to be completed.

This requirement also applies to sub-contracts (see 5. Flow down to sub-contractors)

Suppliers should sign in to Supplier Cyber Protection and:

- Enter the contract's Risk Assessment Reference (provided by contracting authority)
- Complete the SAQ, or re-use a previously completed SAQ

Suppliers can choose the scope of their SAQ response to cover:

- Just the system(s) required to deliver the contract
- Or, a wider network which can be re-used as a response for future SAQs

View the Supplier Assurance Questionnaire workflow for more information at **https://www.gov.uk/**

3. Cyber Essentials requirement

All contracts require suppliers to hold valid Cyber Essentials Certification

Cyber Essentials is the recognised baseline standard for cyber security, developed by HM Government. It provides a statement of five basic controls:

> Boundary firewalls and internet gateways; Secure configuration; Access control; Malware protection; and Patch management.

For **Very Low** risk contracts – suppliers must hold valid **Cyber Essentials** certification

For **Low, Moderate** and **High** risk contracts – suppliers must hold valid **Cyber Essentials PLUS** certification

The Supplier Assurance Questionnaire will prompt suppliers to **enter the certification body name and certificate number**

For more information on Cyber Essentials, see the **Cyber Essentials guide.**

4. SAQ review

The Supplier Assurance Questionnaire will determine whether a supplier meets the required compliance level for the contract

If a supplier **does not meet** the required compliance level:

- It must commit to achieving this level by the date of contract award
- **Or**, commit to a cyber implementation plan which demonstrates how and when they will achieve compliance

If full compliance is not possible, suppliers must demonstrate how they will mitigate cyber risk

For suppliers that are unable to comply with the requirements of the Cyber Security Model, please refer to '**DCPP Cyber Security – Industry Buyer and Supplier Guide**'

5. Flow down to sub-contractors

Successful suppliers must complete a Risk Assessment for all sub-contracted elements

Suppliers must complete a Risk Assessment for each sub-contract using the Supplier Cyber Protection service:

- A Risk Assessment Reference will be generated for the sub-contract
- This must be shared with competing sub-contractors, who must in turn complete a Supplier Assurance Questionnaire.
- This process is repeated, until sub-contract risk becomes N/A

The service will link sub-contract RAs and SAQs to the master contract.

If a supplier is sub-contracting multiple elements, they have the option to group together any contracts that share common attributes and complete a single RA

6. Data visibility

Contracting authorities will only have visibility of their Risk Assessments and Tier One Supplier Assurance Questionnaires directly linked to them

This applies to MOD users and sub-tier suppliers that complete a Risk Assessment for sub-contracted work

There are a small number of MOD employees with visibility of the whole supply chain:

- To provide Management Information when requested (e.g. No. of contracts, risk levels)
- To identify non-compliance (without a prescribed risk acceptance process)
- To identify suppliers that carry greater risk through aggregation of contracts, than suggested by individual Risk Assessments

7. Annual review

The MOD will be prompted on an annual basis to review its Risk Assessments, and suppliers will be prompted to re-complete their Supplier Assurance Questionnaires

Where a change in risk level is recorded:

- The tier one supplier is also required to review their Risk Assessment (RA) of any sub-contracted elements, and
- Where tier one records a change, the tier two supplier must review their RAs, and so on until there is no change in risk level
- The change in risk is subject to a contract change being agreed and a formal contract amendment
- Supplier(s) delivering the contract(s) will be expected to demonstrate compliance with the revised level of risk (or put in place appropriate mitigations)

The Cyber Security Model will be kept under a process of on-going review, under the auspices of the Measurements and Standards group