DCPP
Defence Cyber
Protection Partnership

Defence Cyber Protection Partnership

A joint MOD and industry initiative to improve the protection of the defence supply chain from cyber threats.

Introduction to the **Defence Cyber Protection Partnership**

The Defence Cyber Protection Partnership (DCPP) is a joint UK Ministry of Defence (MOD) and industry initiative put in place to improve the protection of the defence supply chain from cyber threats.

DCPP has developed a Cyber Security Model (CSM) that will be rolled out by the MOD to protect 'MOD Identifiable Data'. Applicable contracts will undergo a risk assessment to determine a cyber risk profile and the requirements for suppliers.

A new online service, **Supplier Cyber Protection**, will support both the MOD and suppliers to meet the requirements of DCPP.

What does DCPP involve?

The new Cyber Security Model includes requirements for the MOD and its suppliers. The key elements are highlighted below, and the end-to-end process is summarised on page 2.

- The Risk Assessment (RA); used to measure the level of cyber risk for a contract
- Requirements that suppliers must meet for the contract's assessed level of cyber risk
- The Supplier Assurance Questionnaire (SAQ), which a supplier must complete to demonstrate compliance
- Flow down of risk assessment, through the supply chain to sub-contractors

The CSM is applicable through **DEF STAN 05-138** and **DEFCON 658.**

DCPP Process Overview

The CSM process is outlined below, from the initial Risk Assessment of a new contract, through to sub-contract flow down. For more information about the requirements for suppliers at each level of cyber risk, see overleaf.

A **Risk Assessment (RA)** must be completed for all new requirements, on the **Supplier Cyber Protection service**.

The RA will assign one of five cyber risk profiles and issue a unique **Risk Assessment Reference (RAR)** for the contract.

The RAR will be shared with potential suppliers to enable them to respond on Supplier Cyber Protection.

Suppliers bidding for a contract must complete a **Supplier Assurance Questionnaire (SAQ)**, on the Supplier Cyber Protection service.

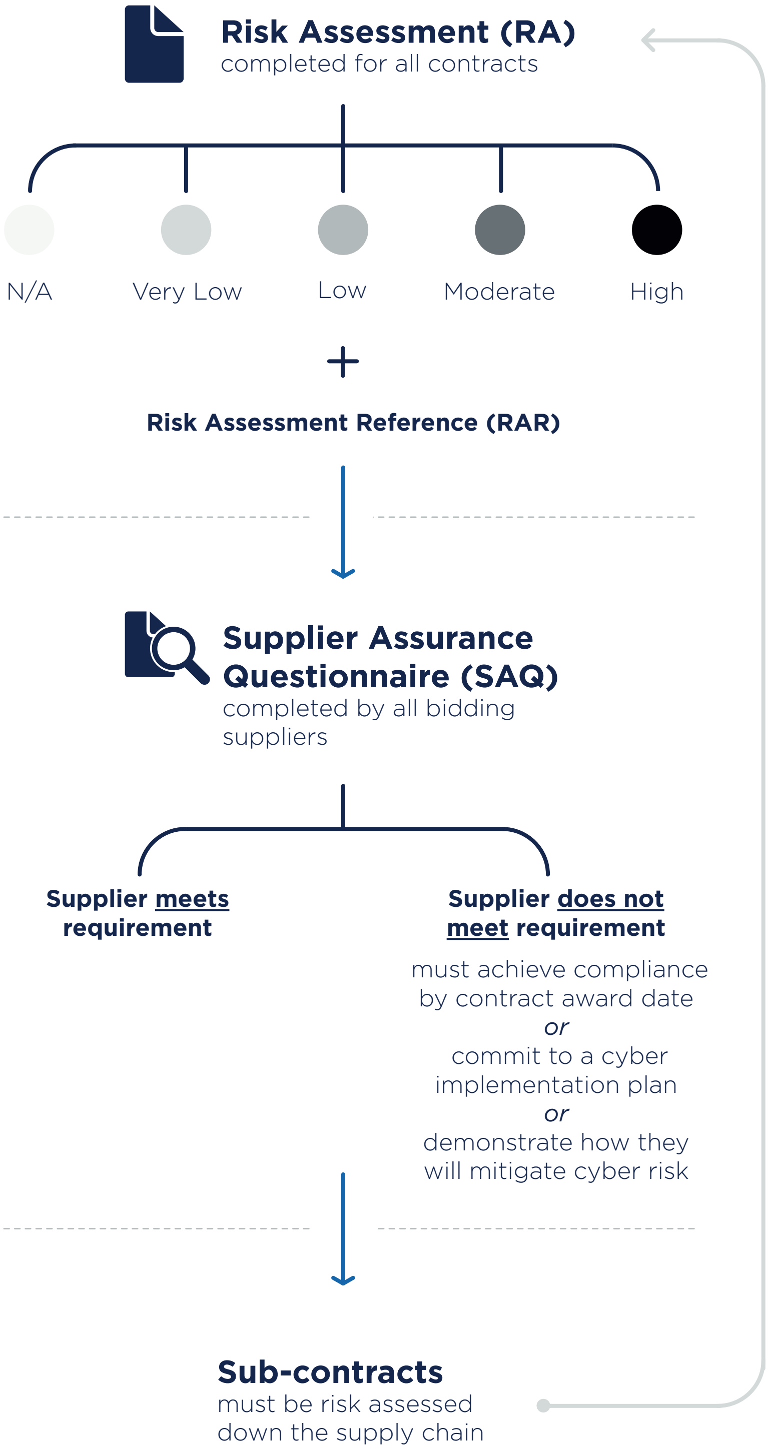
Suppliers should enter the contract RAR and will be required to respond to questions relevant to the contract's cyber risk level.

The SAQ will determine whether a supplier meets the requirements for the contract.

If a supplier does not meet the requirements of the contract's cyber risk profile, it must commit to achieving compliance by the date of contract award, OR; commit to a cyber implementation plan which demonstrates how and when compliance will be achieved. If full compliance is not possible, suppliers must demonstrate how they will mitigate cyber risk.

Successful suppliers must complete a Risk Assessment for **sub-contracts** and share the RAR with its potential sub-contractors, which will in turn complete an SAQ.

This process continues down the supply chain until no MOD Identifiable Information is transferred, stored or accessed electronically.



Risk Assessment (RA)
completed for all contracts

N/A

Very Low

Low

Moderate

High

+

Risk Assessment Reference (RAR)

Supplier Assurance Questionnaire (SAQ)
completed by all bidding suppliers

Supplier meets requirement

Supplier does not meet requirement
must achieve compliance by contract award date
or
commit to a cyber implementation plan
or
demonstrate how they will mitigate cyber risk

Sub-contracts
must be risk assessed down the supply chain

Cyber Risk Profiles

The cyber risk profile of a contract – 'Not Applicable' (N/A), 'Very Low' (VL), 'Low' (L), 'Moderate' (M) or 'High' (H) – determines the number of applicable requirements for suppliers.

Each requirement is made up of a series of individual controls that suppliers need to implement to demonstrate compliance. The number of requirements for each risk profile is outlined below.

Requirements are progressive as you move up the risk profiles, so the lower levels are the foundation of the higher levels and each level builds on the ones before.

N/A	Very Low	Low	Moderate	High
No action required	**1 very low control:** Cyber Essentials	**16 low controls** including Cyber Essentials Plus	**16 low controls** including Cyber Essentials Plus **+16 moderate controls**	**+16 low controls** including Cyber Essentials Plus **+16 moderate controls** **+12 high controls**
	CYBER ESSENTIALS	CYBER ESSENTIALS PLUS	CYBER ESSENTIALS PLUS	CYBER ESSENTIALS PLUS

Cyber Essentials certification

Cyber Essentials certification is a minimum requirement for contracts where MOD Identifiable Information is transferred, stored or accessed electronically.

Cyber Essentials is the government-backed and industry-supported scheme to guide businesses in protecting themselves against cyber threats. The Scheme defines a set of controls which, when properly implemented, will provide organisations with basic protection from the most prevalent forms of threats coming from the Internet.

Both Cyber Essentials and Cyber Essentials Plus involve an independently reviewed, self-assessment. However, Cyber Essentials Plus also tests a suppliers systems using a range of tools and techniques.

For further information about gaining Cyber Essentials, visit cyberaware.gov.uk