AMR Cyber Security PART OF INFINUM

Cyber Security Model V4 and Defence Cyber Certification

WHITE PAPER

DATE: January 2026
VERSION: 1.0
AUTHOR: Tom Miller

TABLE OF CONTENTS

TABLE OF FIGURES

Introduction

On 26 November 2025, the Ministry of Defence (MOD) issued Industry Security Notice (ISN 2025/07), formally implementing the Cyber Security Model (CSM) v4 and retiring the interim measures that supported DEFCON 658 (ISN 2024/02).
From 3 December 2025, all MOD suppliers must comply with the following requirements:

- *"New Risk Assessments (RAs) and SAQs issued in response to such must be generated and submitted using the tooling made available on gov.uk.*
- *Existing RAs raised via the interim process but not yet advertised under an ongoing procurement must be withdrawn and a new RA raised.*
- *If an RA was raised via the interim process and advertised under an ongoing procurement before this announcement, the ongoing tender activity (including processing of remaining SAQ submissions) may be completed via the interim process, or restarted under a new RA, at MOD's determination."*

What is the CSM?

The Cyber Security Model (CSM) ensures that cyber security is considered throughout the defence supply chain. The CSM outlines a risk-based, proportionate approach for suppliers to manage cybersecurity risk and is contractually enforced via Defence Condition 685 (DEFCON 658). The CSM includes the following aspects:

- **Risk Assessments**: Authority (MOD) Delivery Teams will complete an initial risk assessment for the procurement, programme or engagement that will determine a Cyber Risk Profile (CRP).
- **Cyber Security Standard for Defence Suppliers**: The Authority have published a Defence Standard (DEFSTAN 05-138) which lists the cyber security controls required for each CRP.
- **Supplier Assurance Questionnaires (SAQ)**: Suppliers must self-assess against the CSM requirements, in the form of an SAQ on the Supplier Cyber Protection Service online portal.
- **Flow Down**: The CSM requires suppliers to complete their own Risk Assessments on their sub-contractors to confirm their new Cyber Risk Profile (CRP). The sub-contractor will then be required to complete an SAQ against these CRP requirements.
- **Cyber Improvement Plan (CIP)**: When a supplier cannot meet the requirements of the CSM, they must complete a CIP, which will detail why they are not currently compliant, actions to be taken and timeframes for achieving compliance.

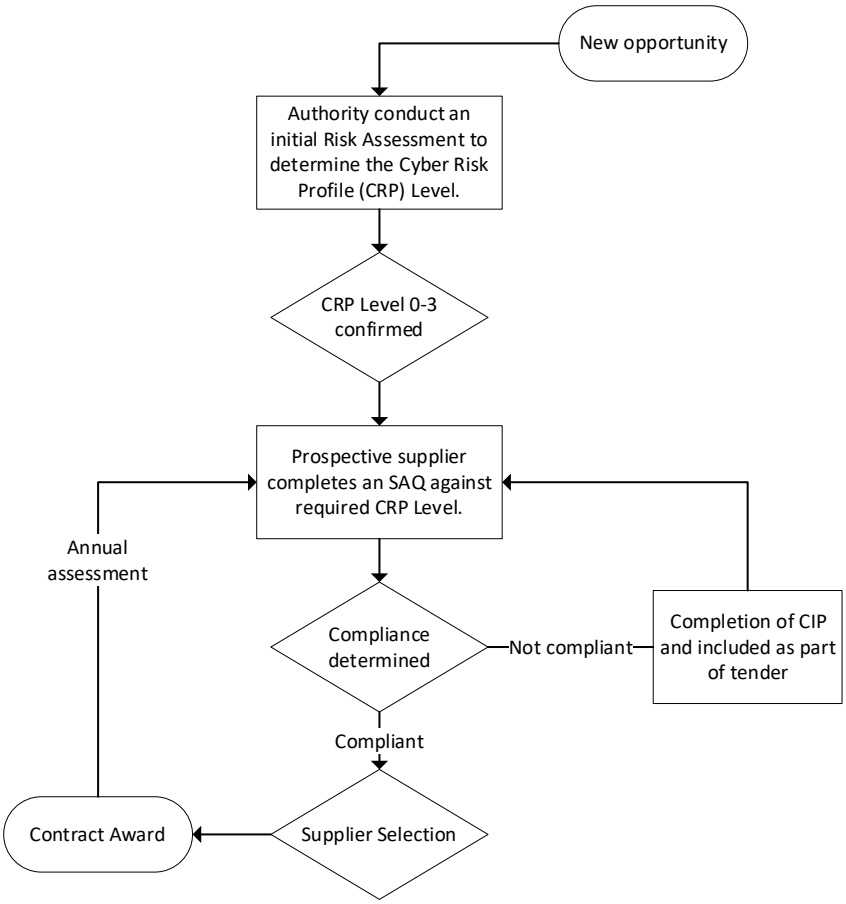

Figure 1 CSM V4 Flow

DEFSTAN 05-138

Defence Standard (DEFSTAN) 05-138 outlines the minimum cyber security control requirements applicable to the various CRP levels. These requirements are considered as a 'minimum', and the Authority may specify further requirements on a per-contract basis.

The CRP Levels are defined within DEFSTAN 05-158 as:

0. **Level 0 - Basic(3 controls):** The Level 0 'Basic' CRP 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.
1. **Level 1 - Foundational(101 controls):** The Level 1 'Foundational' CRP 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.
2. **Level 2 -Advanced (139 controls):** The Level 2 'Advanced' CRP 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.
3. **Level 3 - Expert (144 controls)** The Level 3 'Expert' CRP 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 protect the organisation against new and evolving threats appropriately.

These are the controls that will be assessed and reported by the supplier in the SAQ.

Defence Cyber Certification (DCC)

The Defence Cyber Certification (DCC) has been created by the MOD and IASME acting as the Certification Authority. The DCC will serve as a means of independently verifying compliance with the CSM.

Suppliers with a valid DCC certification are *not yet* exempt from completing elements of the SAQ; however, the intention is for DCC certification to be recognised within the Supplier Cyber Protection Service.

Suppliers with DCC will be required to conduct an annual check-in and recertification every three years via an approved DCC certification body, such as AMR CyberSecurity.

The DCC provides a point-in-time assessment against DEFSTAN 05-138 for Defence Suppliers. Suppliers can achieve DCC certification in four levels, aligned with the CRP Levels from the CSM.

How AMR CyberSecurity Can Help

AMR CyberSecurity supports many Prime Defence Suppliers and subcontractors within the Defence Supply Chain to assess, identify, and manage cyber security risks within their contracts.

AMR CyberSecurity has extensive experience in managing cyber security risk and has security-cleared consultants who can assist and support organisations with the CSM.

As a certified DCC Certification Body, AMR CyberSecurity can deliver both independent assessments or targeted consultancy to help organisations achieve and maintain compliance under the DCC scheme.