CSMv4: What Suppliers Need to Know

Guidance to suppliers for meeting Rolls-Royce standards

The UK Ministry of Defence (MOD) has introduced **Cyber Security Model Version 4** (CSMv4) to strengthen cyber resilience across the defence supply chain.

The updated model — replacing CSMv3 (previously referred to as DEFCON 658 and Def Stan 05-138 Issue 3) — reflects the increasing sophistication of cyber threats and places greater emphasis on protecting critical defence programmes and information.

What's changed?

CSMv4 moves beyond data protection and focuses on demonstrating resilience through effective cyber risk management.

Key changes include:

- **Greater focus on critical systems** — Suppliers must identify and protect systems that support MOD deliverables and understand how cyber risks could affect them.
- **Risk-based approach** — Cyber requirements are now more closely aligned to the level of cyber risk presented by the contract, system, or service.
- **Improved evidence requirements** — Organisations will need to provide stronger, objective evidence that security controls are implemented and operating effectively.
- **Enhanced governance and assurance** — Emphasis increases on senior leadership accountability, continuous monitoring, and ongoing improvement, moving beyond point-in-time assessments.
- **Supply chain resilience awareness** — Suppliers are expected to understand and manage cyber risks within their supply chains, ensuring that essential subcontractors are appropriately protected.
- **Continuous improvement** — CSMv4 encourages organisations to embed cyber security into everyday business operations through regular reviews, risk assessments, and remediation activities.

What does this mean for suppliers?

Suppliers should begin reviewing their existing cyber security requirements against CSMv4 requirements and identify any gaps. Early preparation will make future contract compliance significantly easier.

Priority actions include:

- Identifying critical systems supporting defence contracts.
- Reviewing CSMv4 cyber requirements.
- Reviewing cyber governance and risk management processes.
- Ensuring evidence is available to demonstrate compliance.
- Assessing cyber risks presented by subcontractors.
- Developing an improvement plan to address identified gaps.

FAQs

Why has CSMv3 been replaced?

CSMv4 has been introduced to address the evolving cyber threat landscape and provide a more robust, risk-based approach to protecting UK defence programmes. It strengthens resilience across the entire supply chain rather than focusing solely on protecting data as it flows through the supply chain.

Does CSMv4 apply to every supplier?

Not necessarily. The level of CSMv4 requirements depends on the cyber risk associated with the contract, service, or information being handled. Buyers will determine the appropriate cyber requirements during procurement.

Will suppliers need to complete a new assessment?

Existing suppliers will be asked to demonstrate compliance with CSMv4 requirements as contracts are renewed or varied, or when new procurements are undertaken. Under CSMv4, annual MOD Supplier Assurance Questionnaire (SAQ) reviews will be carried out.

What evidence will be required?

Suppliers should expect to provide evidence such as:

- Cyber security policies and procedures.
- Risk assessments.
- Asset and critical systems inventories.
- Vulnerability management records.
- Incident response plans.
- Security awareness training records.

- Audit reports and assurance activities.
- Supplier assurance evidence.

What are "critical systems"?

Critical systems are the people, technology, processes, and information essential to delivering contracted products or services. CSMv4 requires organisations to identify these systems and understand the impact if they were compromised.

Do subcontractors need to comply?

Where subcontractors have access to MOD information or provide products or services that support delivery of a MOD contract, appropriate cyber security requirements may need to be flowed down.

Is Cyber Essentials Plus enough?

Cyber Essentials or Cyber Essentials Plus remain important baselines, but they are not sufficient on their own to demonstrate compliance with CSMv4. Suppliers will need to show that cyber risks are effectively managed through governance, technical controls, and ongoing assurance.

Is a Cyber Improvement Plan (CIP) acceptable for contract award?

Yes, provided the prime contractor reviews and formally approves the CIP. Once accepted, the CIP becomes a contractually binding deliverable under DEFCON 658, and failure to hit agreed milestones can affect contract compliance status.

What should be done now?

We recommend that suppliers:

- Review the CSMv4 requirements.
- Identify any gaps against current practices.
- Understand which systems support MOD contracts.
- Engage senior management.
- Develop a prioritised CIP.

What happens if suppliers are not compliant?

Failure to demonstrate appropriate cyber security may delay contract award, impact contract performance, require corrective actions, or affect eligibility for future defence opportunities.

Where can suppliers get help?

ISASME can provide guidance on cyber requirements, implementation expectations, and support.

What is the Defence Cyber Certification (DCC) scheme, and how does it relate to CSMv4?

DCC is the official assurance framework recognized by the MOD to prove compliance with Def Stan 05-138 Issue 4 controls. Holding an active DCC certificate at or above a contract's Cyber Risk Profile level serves as pre-verified evidence of compliance, streamlining SAQ submission process from yearly to every three years.

Looking ahead

CSMv4 is designed to improve the resilience of the entire defence supply chain. Organisations that prepare early will not only meet MOD expectations more efficiently but will also strengthen their overall cyber security posture, reduce business risk, and increase customer and partner confidence.

Tip

Don't wait until the next contract review. Start identifying critical systems, gathering evidence, and engaging suppliers now. Early preparation will make CSMv4 implementation much smoother. In addition, review **"Find a Certification Body."**

SUPPLIER COMMUNICATION | Rolls-Royce's Global Supplier Portal is your first stop for information and documents. Go to suppliers.rolls-royce.com for more.