

DEFENCE SUPPLY CHAIN EXPLAINER

Secure by Design, and what actually reaches a supplier

The government policy, the contract conditions that carry it into a defence supply chain, what can be certified and what cannot. Current at September 2026.

THE POLICY ITSELF

An approach, and not a standard

Secure by Design aims to increase the government's cyber resilience by building cyber security into digital delivery from the start and throughout the life of a service. It is an approach with principles and activities behind it. It is not a standard, and there is nothing to be certified against.

Who it binds

It binds government. Departments and their delivery teams must follow it for digital services and technical infrastructure in scope of digital and technology spend controls, and that obligation comes through the Government Cyber Security Standard rather than from Secure by Design itself. Delivery teams evidence it by self-assessment.

It binds a supplier through nothing at all. The published guidance tells third party suppliers to speak to their security contacts to understand what applies to them. Obligations reach a supplier only when a department writes them into a contract.

The ten principles

Create responsibility for cyber security risk. Source secure technology products. Adopt a risk-driven approach. Design usable security controls. Build in detect and respond security. Design flexible architectures. Minimise the attack surface. Defend in depth. Embed continuous assurance. Make changes securely.

The Ministry of Defence has its own

An Industry Security Notice issued in 2023 introduced a Ministry of Defence Secure by Design covering the definition, acquisition, development, maintenance and disposal of information-based capabilities, which the notice takes to include networks, applications, services, information technology, operational technology, platforms and weapons systems. It runs on seven principles rather than the cross-government ten, and it names suppliers among the parties it reaches. A supplier delivering into defence should ask which of the two is being invoked, because they are not the same document.

A NAME THAT MEANS THREE THINGS

Make sure everyone is discussing the same one

Three separate things carry almost the same name, and they have nothing to do with each other. Contracts, tender questions and internal papers confuse them regularly.

- **Secure by Design, government cyber.** The approach described on the previous page, owned within UK government, about building cyber security into digital delivery.
- **Secured by Design, with a d.** Owned by the UK Police Service and run by Police Crime Prevention Initiatives Limited. About designing out crime through the physical security of buildings and developments, with a Police Preferred Specification for products certified by a body accredited by the United Kingdom Accreditation Service.
- **Secure by design, consumer products.** A separate programme sitting under the product security regime for consumer connectable products, in force since April 2024.

Searching gov.uk for the phrase lands on the consumer product collection rather than the government cyber approach, which is part of why the confusion persists.

How to tell which one you have been asked about

Look at who is asking and what they are buying. A department or a prime procuring a digital service means the government cyber approach, and will usually cite the Government Cyber Security Standard or an Industry Security Notice alongside it. A developer, an architect or a housing client means the police scheme, and will talk about a Police Preferred Specification and about doors, windows and layouts. A manufacturer of connected consumer products means the third one, and will be talking about statements of compliance under the product security regime.

Where a question sits in a tender with no citation at all, the honest answer usually starts by asking which is meant. A supplier that answers the wrong one looks careless in a way that is hard to recover from, and a supplier that asks looks like it knows the territory.

Worth settling early

Where a tender or a contract says Secure by Design without a reference, ask which one is meant, and whether the cross-government version or the Ministry of Defence version applies. The answer changes what is being asked of you. No supplier can be certified against any of them, which is covered later in this document.

The condition that carries cyber into the contract

DEFCON 658 lays out the contractual terms for the Cyber Security Model. It is incorporated into a Ministry of Defence contract where information attributable to or capable of identifying an existing or proposed defence capability, activity or personnel will be transferred to the supplier or created by it.

What it asks of the supplier

- Complete the Supplier Assurance Questionnaire, and repeat it annually.
- Comply with Defence Standard 05-138 at the Cyber Risk Profile assessed for the contract.
- Produce a Cyber Implementation Plan where full compliance has not yet been reached.
- Report cyber security incidents.

The flow-down, which is the part that catches people

The condition requires the contractor to include equivalent provisions in relevant sub-contracts, and the contractor itself carries out the risk assessment for each of those sub-contracts. The authority assesses the risk for the prime contract. Everything below that is the prime's to assess, to flow down, and to stand behind.

That obligation is where most of the practical difficulty sits. It is not a document exercise. It asks a supplier to make a judgement about each of its own suppliers, record it, act on it, and be able to show later that it did.

How the profile is set

The authority's delivery team runs a risk assessment producing a risk assessment reference and a Cyber Risk Profile. The supplier then self-assesses against that profile through the Supplier Assurance Questionnaire on the Supplier Cyber Protection Service.

The questionnaire is repeated annually, so this is a standing obligation rather than a bid-time one. A supplier holding several contracts at different profiles works to the highest of them in practice, because the standard behind them is assessed across the organisation rather than contract by contract.

Where you cannot yet comply

The condition anticipates this. A Cyber Implementation Plan sets out what is missing, what will be done and by when, and is agreed rather than simply declared. That is a legitimate position to be in and it is better than an optimistic questionnaire, which is the failure mode most likely to be found out later. What matters is that the plan is real, that somebody owns it, and that the dates in it are the dates things actually happen.

The control set behind the condition

Defence Standard 05-138, Cyber Security Standard for Suppliers, issue 4 dated 14 May 2024, holds the controls that DEFCON 658 points at. Its scope is worth quoting in substance, because suppliers regularly read it too narrowly. It applies to the supplier's overarching corporate or enterprise environment, covering all the organisations, systems, processes, procedures and data necessary for effective protection, going beyond just the information provided in support of the contracted output.

The standard is therefore assessed at organisation level. It is not a per-contract control set, whatever the contract that triggered it.

Four levels, numbered

- **Level 0, Basic.** Three controls.
- **Level 1, Foundational.** A hundred and one controls.
- **Level 2, Advanced.** A hundred and thirty-nine controls.
- **Level 3, Expert.** A hundred and forty-four controls.

Version 4 of the Cyber Security Model introduced these numbered levels. The earlier labels Very Low, Low, Moderate and High belong to version 3 and are legacy. A contract or an internal document still using them is working from the old model, which is itself worth noticing.

What organisation level means in practice

A supplier that has carefully secured the one network segment used for a defence contract, and left the rest of the business alone, has misread the scope. The standard reaches the corporate environment, because an attacker reaching the business through its finance system does not stop at the boundary somebody drew on a diagram. Scoping conversations that begin with how little can be included tend to end badly.

Editions move

DEFCON 658 has circulated in several editions and the Cyber Security Model has moved through versions with transitional arrangements. Check the edition named in your own contract rather than assuming the current one. This document deliberately avoids quoting an edition number for that reason.

THE CERTIFICATIONS, AND THEIR EDGES

Four things that exist, and what each stops short of

Defence Cyber Certification

Launched in 2025 and operated by IASME on behalf of the Ministry of Defence through assured certification bodies, this gives independent third-party certification at levels matching the Defence Standard 05-138 control set. An Industry Security Notice issued in March 2026 confirms that a supplier holding current certification at a level equal to or greater than the requirement satisfies that control requirement under DEFCON 658.

This is a real change and a recent one. Any guidance written before 2026 that says defence cyber assurance is self-assessment only is now out of date. What it certifies is the control set. It says nothing about how the supplier conducts itself on a particular customer's contract.

Cyber Essentials and Cyber Essentials Plus

The National Cyber Security Centre scheme covering five technical controls, described as the minimum standard recommended by government and aimed at the most common internet-based threats. Cyber Essentials is a self-assessment marked by a certification body. Plus adds independent technical testing of the same five controls. Defence Standard 05-138 requires it as a control in its own right, so it bites at the levels that include those controls. Confirm which level applies to you from the standard rather than from a supplier's summary of it.

It is a point-in-time technical baseline over a declared scope boundary. It says nothing about governance, people, or how obligations are discharged on a contract.

ISO/IEC 27001

Certification against the 2022 edition covers an information security management system, granted against the organisation's own declared scope, its own Statement of Applicability and its own risk appetite. It does not examine performance on any named customer contract, and it does not test whether defence obligations such as flow-down, facility clearance conditions or Secure by Design participation are being discharged well.

Facility Security Clearance

The renaming of what used to be called List X, in place since the start of 2023. For Ministry of Defence contracts it is granted by the Industry Security Assurance Centre, and it applies where a supplier holds or processes assets classified SECRET or above, or international partners' assets at CONFIDENTIAL or above. It attaches to a specific facility, so a supplier with several sites may need several clearances. A supplier cannot apply for it. The requirement is sponsored by the contracting authority.

WHAT NONE OF THEM ANSWERS

Nobody assesses how you actually handle the work

There is no certification, accreditation or conformity assessment scheme against the Secure by Design principles. Not for a department and not for a supplier. The published guidance states plainly that Secure by Design is not an assurance process and that delivery teams evidence it by self-assessment.

So a supplier asked by a customer to support that customer's Secure by Design obligations has no route to show that it does so well. It can describe what it does. It cannot point at anyone who has checked.

The pattern across all four

- **Defence Cyber Certification** certifies a control set, at organisation level.
- **Cyber Essentials** certifies five technical controls, over a declared boundary.
- **ISO/IEC 27001** certifies a management system, against a scope the organisation chose.
- **Facility Security Clearance** clears a site to hold classified material.

Every one of them describes the frame around the work. None of them looks at the work. None asks whether flow-down to sub-contractors is being done with judgement or with a copied paragraph, whether the people attending a customer's site are actually cleared to the level claimed, whether a Security Aspects Letter changed anything on the ground, or whether the organisation behaves differently when the customer is not watching.

The position the buyer is left in

A prime contractor or a contracting authority carrying a flow-down obligation has to form a view about a supplier. Certificates tell it that the supplier holds certificates. The questionnaire tells it what the supplier says about itself. Neither tells it whether this supplier will handle a Security Aspects Letter properly, brief the right people, or raise a problem early rather than hoping it passes.

This is the gap the Defence Supplier Mark exists for

A buyer carrying a flow-down obligation has to satisfy itself about a supplier one way or another. Today that means doing the work itself at its own cost, or taking a self-declaration on trust. Those are the two options, and both are unsatisfactory for the party relying on the answer.

AND WHAT IT DOES NOT CLAIM

Assessed against a framework of our own

Westmark does not assess against Secure by Design, against DEFCON 658, or against Defence Standard 05-138. It assesses against the Westmark Defence Supplier control set, which is written to represent what those obligations ask for in working delivery, in terms that can be examined, scored and defended.

That distinction is deliberate and it is stated on every outcome we issue. A framework of our own can be published in full, applied the same way to every organisation, corroborated against evidence, reviewed by a second person and appealed. A claim to assess compliance with a government policy could do none of those things honestly, because the policy binds the department rather than the supplier and carries no conformity assessment scheme at all.

Why a framework rather than the obligations themselves

The obligations do not sit still. Defence Conditions are reissued, the Cyber Security Model has moved through versions with transitional arrangements, and the policy that started all of it binds the customer rather than the supplier. A scheme claiming to assess against those moving parts would be wrong within a year and could never be applied the same way twice.

A framework that Westmark owns can be published in full before anyone commits to anything, applied identically to a sole director and to a thousand-person business, corroborated against evidence rather than assertion, reviewed by a second authorised person before issue, and appealed by an organisation that thinks it was judged wrongly. None of those is available to a scheme that claims to certify compliance with somebody else's policy.

The control set is built to represent what the obligations ask for where the work happens. When the obligations move, the control set is revised, the version is recorded, and every outcome states the version it was assessed against. That is a maintenance job we carry rather than a claim we make.

What an outcome says

That an independent assessor examined defined arrangements across engagements the assessor selected, against a published control set, on a sample, on a date, and that a second authorised person confirmed the record before it was issued. Delivery personnel were interviewed without a manager present. A requirement reached full marks only where the evidence came from more than one independent source.

THE LIMITS, STATED PLAINLY

What an outcome does not say

It is not certification, accreditation or approval by government, the Ministry of Defence or anyone else. It does not establish compliance with the Secure by Design policy, with DEFCON 658, or with Defence Standard 05-138. It is not Cyber Essentials, it is not ISO/IEC 27001, and it is not a Facility Security Clearance. Holding it discharges no obligation a buyer owes to anybody.

What it gives a buyer is somebody independent having looked, with the scope printed on the outcome so they can see exactly what was examined and what was not.

This document has a shelf life

It is current at September 2026. Defence Conditions are reissued, the Cyber Security Model has moved through versions, and Defence Cyber Certification is recent enough that guidance written before 2026 is already wrong about it. Check the date on the cover against the date you are reading it, and check your own contract for the editions it names.

Talk to us

Tell us what you deliver, who you deliver it to, and what you are being asked for. We will tell you what an assessment covers and what it costs.

hello@westmarkassurance.co.uk · 033 33 356 873

1st Floor, 2 West Regent Street, Glasgow, G2 1RW

Verify any outcome at hub.westmarkassurance.co.uk/verify

Westmark Assurance is not an accredited certification body and does not offer UKAS-style certification. An outcome is a judgement by Westmark Assurance and carries no certification, accreditation or approval by government, the Ministry of Defence, the Security Industry Authority or the Home Office.

Westmark Assurance is a trading name of Ross Macdonald Consultancy Ltd, registered in Scotland, number SC848204. Registered office 1st Floor, 2 West Regent Street, Glasgow, G2 1RW.