

PROTECTING GOVERNMENT INFORMATION · GUIDE 6 OF 6

Bringing it together

Running physical, personnel, cyber and information security as one set of arrangements, and showing a customer that they hold together.

WHERE THE AREAS MEET

The gaps sit at the joins

Guides 2 to 5 took each area in turn. In practice, many of the problems a supplier meets arise where one area hands over to another, and each join needs someone to own it.

Join	What can be missed	What holds it together
Personnel and physical	A leaver still knows the cabinet combination or holds a building pass	A leaver checklist that recovers passes and changes combinations
Personnel and information	A screened person was never told which material is sensitive on this contract	A briefing drawn from the Security Aspects Letter or schedule, given before access
Cyber and information	A well-managed laptop is used to forward files to a personal account	Rules on where information may go, backed by technical controls that block the rest
Physical and cyber	An encrypted device is left in a car with its sign-in token	Device handling rules in the briefing, and a report route for the loss
All four and the supply chain	A subcontractor receives the drawings with no conditions attached	Assessment before engagement, and the conditions written into the subcontract

Every one of these gaps can exist in an organisation that holds good certificates for the separate areas. Most can be closed with a checklist or a line in a briefing once somebody is responsible for looking.

WHAT JOINS THE AREAS

Five things that turn four areas into one set of arrangements

- 1 One accountable person**
A named director, or someone with equivalent authority, accountable for security risk across all government work. Everyone should know who it is, and the role should be visible in how decisions are made.
- 2 One written procedure**
A single security procedure saying how contract requirements are identified and how the four areas are applied on each job. In a small firm it can be a few pages. It needs to be current and in use.
- 3 A risk assessment for each engagement**
Before each piece of work starts, a short assessment of what the customer requires and which controls apply to the information and sites involved. A general health and safety risk assessment does not do this job.
- 4 One route for incidents**
A single way for anyone to report a loss, a mistake, a cyber event or an approach, with no penalty for reporting in good faith, and a clear path on to the customer and, for MOD work, the Defence Industry WARP.
- 5 Control of the supply chain**
Subcontractors assessed before they start and held to the same conditions as your own staff while they work.

Proportionate for a small business

For a sole director practice, the accountable person and the procedure may be the same person and one short document. What matters is that the arrangements are written down and followed on each job.

SHOWING A CUSTOMER

Describe what you have, and no more

Government customers and prime contractors ask suppliers to evidence their security at tender and throughout a contract. The strongest answer is an accurate one, backed by records.

What each piece of evidence proves

Evidence	What it proves
Cyber Essentials or Cyber Essentials Plus	Five technical control themes, within the stated scope
Defence Cyber Certification	Defence Standard 05-138 controls at the certified level
ISO/IEC 27001 certification	A certified information security management system. A general standard, it does not examine the particular conditions of a government contract
Baseline Personnel Security Standard records	That the four checks were done for each named person
Signed Security Aspects Letter acknowledgement	That MOD requirements were accepted before work began

Statements to avoid

- "Our devices are approved for OFFICIAL-SENSITIVE." No such approval exists.
- "Compliant with Defence Standard 05-138" without the level. Compliance is always at a stated level.
- "Our staff are cleared" where they hold baseline checks. A baseline check is not a clearance.
- "Secure by Design certified." There is no certification against the government Secure by Design approach.

THE WESTMARK DEFENCE SUPPLIER MARK

One assessment across all four areas

The Westmark Defence Supplier Mark is for companies that supply defence and government. It examines the four areas together, with the governance, risk assessment, incident reporting and supply chain control that join them, against a published standard and control set.

What is examined	Covered in this series
Governance and accountability	Guide 6
Risk management and project implementation	Guide 6
Contractual, statutory and personnel security	Guides 1 and 3
Information and asset handling	Guides 2 and 5
Cyber and technical security	Guide 4
Incident management and continuous assurance	Guides 5 and 6
Supply chain	Guide 6

How it works

- **Scope.** Operational scope covers site-based work and Cyber scope covers digital and technical services. An organisation doing both is assessed at Combined scope.
- **Evidence from real work.** The assessor chooses a sample of three to six engagements, looks for records made during delivery and tests them with the people who did the work.
- **Proportionate.** Requirements state outcomes, and the organisation chooses the means. Simple arrangements in a small firm score the same as elaborate ones in a large firm.
- **Outcomes.** Westmark Defence Supplier Mark, or Westmark Defence Supplier Conditional with improvement actions to complete. An outcome is valid for 24 months, with a declaration at twelve months.
- **Disqualifying conditions.** A small number of serious failings prevent a positive outcome whatever the score, such as giving someone access without screening or failing to report a loss.

CLEAR ABOUT WHAT IT IS

What the Mark confirms, and what stays separate

An outcome is an independent judgement by Westmark Assurance that an organisation's delivery is consistent with the government's Secure by Design principles and with the security obligations placed on suppliers to the MOD and government.

The Mark confirms

That the four areas and the arrangements joining them were examined together, on real engagements, against published criteria, with a confidence level recorded.

Held separately

Government or MOD certification or approval, Cyber Essentials, Defence Cyber Certification, the Supplier Assurance Questionnaire, Facility Security Clearance and national security vetting. The Mark replaces none of them, and a holder may not claim that it does.

Where an existing certificate helps

Where a certificate you already hold evidences a requirement, the assessment takes account of it. A supplier with Cyber Essentials Plus or ISO/IEC 27001 is not starting again.

Checking a holder

Every Westmark Defence Supplier Mark and Conditional outcome is recorded on a public register showing the organisation, scope, outcome, confidence level, assessment date and expiry. A customer can check a claim without contacting the holder. Holders may describe their outcome only in the wording the scheme sets out, and may never publish their score.

Reading the criteria

The Defence Supplier Mark Assurance Standard and its control set are published in full at westmarkassurance.co.uk, so any organisation can see exactly what is examined before deciding anything.

LOOKING ACROSS ALL FOUR

The Westmark Defence Supplier Mark is built to look at all four areas and the joins between them, on your own engagements, against criteria anyone can read before deciding to be assessed.

WESTMARK ASSURANCE

Where the Defence Supplier Mark fits

Westmark Assurance provides independent security assurance, assessing organisations, premises and security arrangements against defined standards and frameworks.

The Westmark Defence Supplier Mark is for companies that supply defence and government. It assesses how an organisation identifies, controls and evidences security risk across the work it delivers, against a published standard and control set. The criteria are published in full at westmarkassurance.co.uk, so you can read exactly what is examined before you decide anything.

If you would like help putting these arrangements in place, we can introduce you to a Licensed Partner. Their preparation work is kept separate from our assessment, so an organisation they have supported is always assessed by someone independent of them.

Talk to us

For a conversation about the Defence Supplier Mark, or an introduction to a Licensed Partner:

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

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

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 or the Ministry of Defence.

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.