

PROTECTING GOVERNMENT INFORMATION · COMPANION FRAMEWORK

Secure Endpoint Framework for Government Suppliers

Handling OFFICIAL and OFFICIAL-SENSITIVE information on company desktops, laptops, tablets and phones, for businesses supplying central government and the Ministry of Defence.

DOCUMENT CONTROL

About this framework

Document	Secure Endpoint Framework for Government Suppliers
Version	1.0, September 2026
Published by	Westmark Assurance
Series	Companion to the Protecting Government Information guides, and to Guide 5 on information security in particular
Review	At least once a year, and whenever a referenced policy, Defence Condition, Defence Standard or Industry Security Notice changes

Contents

1	The question this framework answers
2	How OFFICIAL-SENSITIVE works
3	The authority chain
4	Framework structure, Parts A to G
5	Putting it in place
Annex	Sources

Written from published UK Government and Ministry of Defence security requirements and National Cyber Security Centre guidance. Independent of government, and not produced or endorsed by any government department or the National Cyber Security Centre. Free to use within your own organisation. It may not be republished or sold without written permission. Your contract and its security conditions take precedence over anything written here.

SECTION 1

The question this framework answers

Suppliers to government regularly ask how they can show that a device is fit to hold OFFICIAL-SENSITIVE information. The accurate answer is that no device, operating system or product carries a certification for OFFICIAL-SENSITIVE, and government guidance tells buyers not to look for one.

"Don't look for assurance that a system is 'good for OFFICIAL-SENSITIVE'. A system that can handle OFFICIAL data may be appropriate to handle sensitive information."

Cabinet Office and Government Digital Service, 'OFFICIAL-SENSITIVE' data and IT, GOV.UK

What a supplier can build is an evidenced assurance position: company-owned, centrally managed devices configured to a written baseline drawn from National Cyber Security Centre guidance and used only with approved corporate services, under the security conditions each customer sets. Independent Cyber Essentials testing sits alongside it wherever the contract calls for it.

Every organisation's arrangements will look different, because each contract and each team is different. The framework sets a common standard, and each organisation fits it to its own people and platforms.

What this framework gives you

- A traceable line from government policy, through contract conditions and technical guidance, to each setting on each device
- A baseline for endpoints and the services behind them, with the evidence each control should produce
- An evidence pack and a form of words for a customer's security team that describes the arrangements accurately and does not overclaim
- The stages for putting it in place, and a record of where the published sources differ and the position taken

SECTION 2

How OFFICIAL-SENSITIVE works

The Government Security Classifications Policy (version 2.0, August 2024) has three classifications: OFFICIAL, SECRET and TOP SECRET. OFFICIAL-SENSITIVE is OFFICIAL information carrying an additional marking.

"The -SENSITIVE marking should be applied to OFFICIAL information that is not intended for public release and that is of at least some interest to threat actors (internal or external), activists or the media."

Government Security Classifications Policy, version 2.0, paragraph 25

The policy's Quick Read states that OFFICIAL-SENSITIVE is not a separate classification tier. In practice the information sits on the same class of system as other OFFICIAL information, with tighter handling by people and any extra conditions the customer attaches in the contract.

What this means for a supplier

The policy applies to suppliers as well as civil servants. Guidance 1.6 on contractors confirms that contractors handle government information entrusted to them, or produced by them under contract, in line with the policy. Two further points shape everything that follows.

- Guidance 1.1 says handling significant OFFICIAL or OFFICIAL-SENSITIVE information on a privately managed device through non-corporate channels "can only be justified in exceptional circumstances".
- For MOD work the position is firmer. Industry Security Notice 2022/10 on remote working requires company issued and managed devices within the UK, and personal devices and accounts are not used for MOD information.

A framework for government information therefore starts from company ownership of the device and the account.

SECTION 3

The authority chain

No single publication covers endpoints for government suppliers. The framework draws on several, each doing a different job. Full titles and links are in the Annex.

Layer	Source	What it gives you
Policy	Government Security Classifications Policy v2.0, with Guidance 1.1, 1.4 and 1.6	What the markings mean, and the baseline behaviours including remote working
Standard	Government Functional Standard GovS 007: Security, v2.0	The expectation that departments set security requirements for suppliers and assure them
Governance	Information Asset Owner Hub, security.gov.uk	Knowing what is held, who is accountable and how it is disposed of
Central government	Procurement Policy Note 014 and the model security schedules on security.gov.uk	When Cyber Essentials is required, and the contract schedules for OFFICIAL data
MOD cyber	DEFCON 658, Defence Standard 05-138 Issue 4 and the Cyber Security Model	The Cyber Risk Profile level and the controls it requires
MOD handling	Industry Security Notice 2026/04, the Security Aspects Letter and DEFCON 660	The OFFICIAL and OFFICIAL-SENSITIVE conditions that bind you once issued
MOD topic notices	Industry Security Notices 2020/07, 2022/10, 2023/04, 2024/06 and 2025/03	Encryption products, remote working, email and transfer, cloud services and incident reporting
Technical	National Cyber Security Centre Device Security Guidance and platform guides	How to set up and manage each type of endpoint
Services	National Cyber Security Centre Cloud Security Principles	How to judge and set up the services where the information lives
Independent assurance	Cyber Essentials and Cyber Essentials Plus (v3.3), and Defence Cyber Certification	External confirmation that stated controls are in place

SECTION 4

Framework structure

The framework has seven parts. Parts A and B come first, because the contract and the information decide how strong the endpoint controls need to be. Parts C to F are the controls. Part G turns them into evidence.

Part	Title	Outcome
A	Contract and requirement capture	You know what each customer requires before any information arrives
B	Information governance	Each holding of government information has a named owner and a register entry
C	Endpoint baseline	Every endpoint that can reach government information is built and held to one written standard
D	Services, storage and transfer	Information stays in approved corporate services and moves only by approved routes
E	People and physical handling	Staff are screened and briefed, and follow clear rules when working away from the office
F	Incidents, loss and disposal	Losses reach the right authority in time, and devices leave service without leaving data behind
G	Evidence and assurance statement	You can show a customer's security team what you have and how you know it works

A note on the owner role

Government guidance places the information asset owner inside the government organisation, and that person stays accountable for the asset when it is shared with a supplier. A supplier should adopt the same principles for its own holding and name an internal owner, without describing that person as the customer's information asset owner. This framework calls the role the Government Information Owner.

PART A

Contract and requirement capture

The customer sets the strength of the controls, so this part comes first. Before accepting OFFICIAL-SENSITIVE material, hold the customer's written requirements and check your arrangements against them.

Central government contracts

- Procurement Policy Note 014 applies to central government departments, their executive agencies and non-departmental public bodies, and NHS bodies. It covers contracts that involve personal data or systems holding OFFICIAL information, among others.
- Evidence of Cyber Essentials, or equivalent controls verified independently, is needed at the point data is passed to the supplier, and is renewed every twelve months. The buyer decides whether Cyber Essentials Plus is needed, according to the risk.
- Many contracts now use the model security schedules on security.gov.uk, graded by the sensitivity of the data. Read the schedule in your contract line by line against Part C, and record the controls in your Security Management Plan.

MOD contracts: cyber

- 1 Risk assessment**
The MOD delivery team gives the contract a Risk Assessment Reference and a Cyber Risk Profile level from Level 0 to Level 3.
- 2 Questionnaire**
The supplier completes the Supplier Assurance Questionnaire through the Supplier Cyber Protection Service, scored against the level.
- 3 Implementation plan**
Where the level is not met, a Cyber Implementation Plan is agreed and becomes part of the contract.
- 4 Repeat and flow down**
DEFCON 658 requires the questionnaire at least once in each contract year, records kept for six years after the contract ends, and equivalent provisions in relevant subcontracts.

PART A, CONTINUED

Cyber Risk Profile levels and handling conditions

Issue 4 of Defence Standard 05-138 (May 2024, mandatory from 3 December 2025 under Industry Security Notice 2025/07) replaced the old profiles of Very Low, Low, Moderate and High with four numbered levels.

Level	Name	Controls	Cyber Essentials requirement
Level 0	Basic	3	Cyber Essentials
Level 1	Foundational	101	Cyber Essentials and Cyber Essentials Plus
Level 2	Advanced	139	Cyber Essentials and Cyber Essentials Plus
Level 3	Expert	144	Cyber Essentials and Cyber Essentials Plus

Control counts from clause 2.2 of Defence Standard 05-138 Issue 4. Control 0001 requires Cyber Essentials at every level and control 0002 requires Cyber Essentials Plus at Levels 1 to 3. Some published descriptions of Defence Cyber Certification place the Plus requirement at Level 2 and above. The level markings in the issue attached to your contract govern.

Industry Security Notice 2026/01 confirmed that the requirements apply to the supplier as a single legal entity, so the whole company is in view, including systems that never touch the contract directly. Under Industry Security Notice 2026/02, a Defence Cyber Certification certificate is accepted as assured evidence at the matching level, and a higher level covers those below it. The MOD Cyber Security Model page still says certificate holders are not yet exempt from parts of the questionnaire, so plan to complete both until the MOD confirms otherwise.

MOD contracts: handling

- DEFCON 660 applies to MOD contracts with OFFICIAL-SENSITIVE aspects and requires security requirements to be flowed down.
- Where a supplier will hold OFFICIAL-SENSITIVE material, the requirements come through a Security Aspects Letter. A signed acknowledgement is returned before work begins. No letter is needed where only OFFICIAL material is handled.
- The letter attaches the OFFICIAL and OFFICIAL-SENSITIVE Contractual Security Conditions, currently Annex B to Industry Security Notice 2026/04. Those conditions also bring in DEFCON 658 and Defence Standard 05-138, so the cyber and handling requirements meet in one place.

PART A, CONTINUED

Requirement capture checklist

Item	Central government	MOD
Security conditions	Security schedule in the contract	Security Aspects Letter and its conditions, with signed acknowledgement returned
Cyber requirement	Cyber Essentials, or Plus where the buyer specifies	Risk Assessment Reference, Cyber Risk Profile level, questionnaire result or Cyber Implementation Plan
Storage and services	As the schedule states	As the conditions state, with cloud services aligned to the Cloud Security Principles
Devices	As the schedule states	Company issued and managed devices in the UK, and encryption of portable devices
Incident reporting	As the schedule states, normally to the contract manager	Defence Industry WARP, and DEFCON 658 for cyber incidents
Subcontracting	As the schedule states	Flow-down under DEFCON 658 and DEFCON 660
Printing, media and travel	As the schedule states	As the conditions and notices state
Retention and return	As the schedule states	Records kept six years after contract end under DEFCON 658

PART B

Information governance

This part applies the principles of the government's information asset owner guidance to the supplier's own holding of customer information: know what is held, review the risks to it, keep it protected and marked, and keep the record current.

The Government Information Owner

Name a senior person as Government Information Owner for each customer or contract. That person decides who may access the information and approves any exception to the baseline. Disposal at contract end needs their sign-off. The role needs the authority to say no, so in a smaller company it will usually sit with a director.

The government information register

Field	What to record
Holding	Contract name and reference, customer, and a plain description of the information
Classification and marking	OFFICIAL, or OFFICIAL-SENSITIVE where the customer has marked it so, with any handling instructions
Owner	The named internal owner, and the customer's security contact
Governing requirements	Security schedule or Security Aspects Letter, and the Cyber Risk Profile level for MOD work
Permitted locations	The specific corporate services and folders where the information may be held
Permitted endpoints	Company-owned endpoints meeting Part C, by device type
Authorised people	Named individuals or a named group, with screening status
Sharing	Approved recipients, subcontractors and transfer methods
Retention and disposal	Retention period, return or destruction arrangements and the record of disposal
Review	Last and next review dates, at least yearly and on any contract change

PART C

Endpoint baseline

An endpoint is any device a person uses to reach government information: desktop computers, laptops, tablets and mobile phones. Servers and the cloud services that hold the information are covered in Part D.

Every endpoint that can reach government information meets this baseline, and no endpoint that does not meet it can open that information. The outcomes are the same on every platform. Where a contract condition or Defence Standard control sets a specific figure, that figure is used.

Type	Particular risks	Additional requirements
Desktops	Use by others in shared or open offices, and unlocked sessions	Kept on company premises unless issued for home working. Screen locked whenever the user steps away
Laptops	Loss or theft, and being overlooked in public	Full disk encryption with authentication before the operating system starts, where supported. Privacy screen in public
Tablets and phones	Loss or theft, unmanaged apps, messaging, cameras and screenshots	Enrolled into management from first start. Government information kept in managed apps, with copying to unmanaged apps blocked
Removable media and peripherals	Uncontrolled copies leaving the organisation	Controlled through the removable media rules in this part and the printing rules in Part E

PART C, CONTINUED

Common baseline for every endpoint

Industry Security Notice references apply to MOD contracts. Central government contracts follow the security schedule.

Area	Requirement	Source	Evidence
Ownership	Company-owned device, issued to a named user for company business only. No personally owned devices.	Classifications Policy Guidance 1.1, Industry Security Notice 2022/10	Asset register entry, signed acceptable use agreement
Choice and support life	A model and operating system the manufacturer will support with security updates for the device's planned life, replaced before support ends.	National Cyber Security Centre Choosing devices	Purchase specification, support end dates
Enrolment	Enrolled into organisation management from first start, so the user cannot remove it.	National Cyber Security Centre platform guides	Enrolment profile, device inventory
Management	Managed through Microsoft Intune or an equivalent service that configures and enforces this part, including remote lock and wipe.	National Cyber Security Centre platform guides	Compliance policy exports, compliance report
Encryption	All stored data encrypted with the platform's built-in encryption, with recovery information held by the organisation and never kept with the device.	Defence Standard 05-138 control 2317, Industry Security Notice 2020/07, Industry Security Notice 2026/04	Encryption compliance report

PART C, CONTINUED

Common baseline, continued

Area	Requirement	Source	Evidence
Sign-in	Biometric, PIN or passcode unlock, and multi-factor authentication on every cloud service, with phishing-resistant methods preferred.	National Cyber Security Centre platform guides, Cyber Essentials v3.3	Authentication policy, sign-in logs
Administration	Users work without administrator rights, and separate administrator accounts are used by as few people as practicable. Jailbroken or rooted devices are blocked.	National Cyber Security Centre platform guides, Cyber Essentials v3.3	Privileged role listing, compliance report
Conditional access	Government information reachable only from compliant, company-managed devices with multi-factor authentication. Non-compliant devices blocked.	National Cyber Security Centre platform guides	Conditional access policy export, blocked sign-in samples
Updates	Automatic updates for the operating system and applications, and firmware where the platform allows. High-risk updates within 14 days.	Cyber Essentials v3.3, Industry Security Notice 2026/04	Update policy, patch compliance report
Malware protection	Endpoint protection with detection and response on Windows and macOS. Phones and tablets checked for threats through management.	National Cyber Security Centre platform guides, Industry Security Notice 2026/04	Endpoint protection health report

PART C, CONTINUED

Common baseline, continued

Area	Requirement	Source	Evidence
Firewall	Operating system firewall on and centrally managed on desktops and laptops.	Industry Security Notice 2026/04	Firewall policy export
Applications	Applications only from a company catalogue or managed app store, with controls on what can run. Office macros disabled unless a named workflow needs them.	National Cyber Security Centre platform guides	Application policy, installed software report
Removable media	USB storage blocked by default. Where a need is approved, only encrypted, company-owned media.	Defence Standard 05-138 control 2310	Device control policy, exception log
Screen lock	Locks after no more than 15 minutes of inactivity. Phones and tablets lock sooner.	Industry Security Notice 2026/04	Configuration profile export
Logging	Sign-in attempts and changes to privileges and passwords recorded and retained. Security alerts monitored.	Industry Security Notice 2026/04, National Cyber Security Centre logging guidance	Log retention settings, alert handling record

PART C, CONTINUED

How each platform meets the baseline

An organisation only needs the platforms it uses, and fewer platforms means less to manage and evidence.

Platform	Enrolment	Encryption	Applications
Windows	Windows Autopilot	BitLocker, with TPM and startup PIN	App Control for Business or AppLocker
macOS	Apple Automated Device Enrolment	FileVault, recovery key held by the management service	Gatekeeper, with apps through management
iOS and iPadOS	Automated Device Enrolment, supervised	Built-in data protection, unlocked by the passcode	Company app catalogue
Android	Zero-touch enrolment, organisation-managed	Built-in encryption, unlocked by the passcode	Managed Google Play
ChromeOS	Enterprise enrolment through the Google Admin console	User data encrypted by default	Extensions and apps on an allow list, developer mode off

The compliance gate

The controls only give assurance if a device that falls out of line loses access automatically. Set a compliance policy for each platform and a conditional access policy that relies on them. A device is compliant only when it is enrolled and managed, encrypted, at or above the minimum operating system version, protected by a passcode or biometric, not jailbroken or rooted, and, on desktops and laptops, running endpoint protection and a firewall. A device that fails any check loses access until it is fixed, and the record of that check is the evidence.

ChromeOS is managed through the Google Admin console, which Intune compliance policies do not cover. Use an equivalent way to block unmanaged or out-of-date ChromeOS devices, or keep ChromeOS out of scope.

PART C, CONTINUED

Licensing and encryption notes

Licensing for smaller businesses

Microsoft 365 Business Premium, available to organisations of up to 300 users, includes Intune and Defender for Business. It also includes Entra ID P1, which provides conditional access. For most small and medium suppliers on Microsoft 365 it covers the baseline without separate products. Larger organisations, or those wanting Defender for Endpoint Plan 2, will need Enterprise licensing or add-ons. Equivalent services from other providers can meet the same outcomes.

Encryption assurance

- The Commercial Product Assurance scheme has closed, so contracts should not ask for CPA-certified encryption.
- For MOD work, Industry Security Notice 2020/07 lists BitLocker as an approved product for internal drives, and the conditions in Industry Security Notice 2026/04 require any portable device holding OFFICIAL-SENSITIVE information to be encrypted.
- Defence Standard 05-138 control 2317 requires full disk encryption on all endpoints at Levels 1 to 3, to an industry standard such as AES-256 or a FIPS equivalent.
- On Windows, National Cyber Security Centre guidance recommends BitLocker with a TPM and a PIN. On other platforms the built-in encryption in the platform guide is used.
- Where a customer names a different product or standard, the customer's requirement applies.

PART D

Services, storage and transfer

Most of the protection for government information sits in the services where it is stored and the routes by which it moves. The endpoint is the way in.

Where information may be held

- Only in the company's own tenant or file store, in the locations named in the register. Never in personal cloud storage or personal email accounts.
- For MOD work, cloud services holding MOD information align with the National Cyber Security Centre Cloud Security Principles, reviewed at least yearly (Industry Security Notice 2024/06). Principle 14, secure use of the service, covers the settings the customer of the service is responsible for. For central government work, follow the schedule.
- Local copies on a device kept to the minimum needed, and removed when the work is done.
- Document labelling tools can mark and protect files, provided the markings match the Classifications Policy and the customer's requirements.

How information may move

- OFFICIAL information may be emailed over the internet without additional encryption.
- For MOD work, OFFICIAL-SENSITIVE information travels encrypted using an approved technique such as TLS at version 1.2 or higher (Industry Security Notices 2026/04 and 2023/04).
- Where a file is encrypted for transfer on MOD work, its password is at least nine characters and is sent by a separate route.
- OFFICIAL-SENSITIVE information is never sent to a personal device or personal account.
- Sharing with subcontractors happens only where the register and the contract allow it, after the subcontractor has accepted equivalent requirements.

PART E

People and physical handling

The classification policy relies heavily on people behaving well. These controls are simple, and they are the ones most often missed.

Topic	Rule	Source
Screening	Everyone with access holds a Baseline Personnel Security Standard check or equivalent, and any higher clearance the contract requires	Baseline Personnel Security Standard, Industry Security Notice 2026/04
Briefing	Each authorised person is briefed on the baseline behaviours and the customer's conditions before access, and the briefing is recorded	Classifications Policy Guidance 1.1
Working in public	Use a privacy screen wherever you could be overlooked, and take calls about OFFICIAL-SENSITIVE matters somewhere private	Classifications Policy Guidance 1.4
Unattended devices	Never left unattended in a public place or in a vehicle, with tokens and PINs kept apart from the device. Desktops are locked when the user steps away	Industry Security Notice 2026/04
Location	MOD work is done within the UK on company devices. Taking government information abroad needs prior agreement	Industry Security Notice 2022/10, Guidance 1.4
Printing	Kept to a minimum, and never on a public or personal printer	Industry Security Notice 2022/10, Guidance 1.4
Paper disposal	Destroyed so that reconstitution is very difficult or impossible, for example by cross-cut shredding	Industry Security Notice 2026/04

Guide 2 covers physical security and Guide 3 covers personnel security in more detail.

PART F

Incidents, loss and disposal

Reporting

For MOD work, all security incidents affecting defence related material go to the Defence Industry WARP (DefenceWARP@mod.gov.uk, 03001 583 640 in office hours) under Industry Security Notice 2025/03. Cyber incidents are also reported as DEFCON 658 requires, including to your prime if you are a subcontractor. The conditions in Industry Security Notice 2026/04 say a loss is reported immediately, while the notice allows up to 72 hours for OFFICIAL-SENSITIVE and five working days for OFFICIAL. This framework adopts immediate reporting for any lost or stolen device that could reach government information, because the stricter requirement satisfies both.

For central government work, follow the route in the security schedule, normally the contract manager. Where you process personal data for the department, the UK GDPR requires you to tell it about a breach without undue delay.

A lost or stolen device

- 1 Report**
The user tells the Government Information Owner at once.
- 2 Lock and wipe**
The device is locked and wiped remotely, and the user's sessions and tokens are revoked.
- 3 Notify**
The loss goes to the customer by the contractual route, and to the Defence Industry WARP for MOD work.
- 4 Record**
The register records what the device could reach and whether it was encrypted and compliant at its last check-in.
- 5 Review**
The owner reviews the cause and records any change to the baseline.

Disposal and reuse

National Cyber Security Centre sanitisation guidance treats a factory reset of an encrypted device, which deletes the encryption keys, as proportionate for OFFICIAL data. The MOD conditions add that an erasure product is used to overwrite the data. For devices that have held MOD information, do both, or use a destruction provider that issues a certificate, and keep the record with the asset register entry.

PART G

Evidence and assurance statement

The evidence pack

A customer's security team will want to see how the arrangements work in practice. Keep the following together and current.

- The written endpoint baseline from Part C, with its version and approval date
- The government information register from Part B
- Compliance and conditional access policy exports
- A current device compliance report showing every in-scope endpoint by type
- The Cyber Essentials or Cyber Essentials Plus certificate, with its scope
- For central government work, the Security Management Plan and its latest review
- For MOD work, the Risk Assessment Reference, questionnaire result, any Cyber Implementation Plan and any Defence Cyber Certification certificate
- Signed Security Aspects Letter acknowledgements
- Screening and briefing records
- The incident and loss procedure, and the log of any incidents
- Disposal and erasure records

PART G, CONTINUED

Describing the arrangements

The strongest accurate statement describes what the organisation has done and which guidance it followed. The example below can be adapted, completing the bracketed details and removing anything that does not apply.

Example assurance statement

Endpoints used to process UK Government information, including desktops, laptops, tablets and mobile phones, are company-owned devices, configured and managed to our documented endpoint baseline, which is aligned with the National Cyber Security Centre Device Security Guidance and its platform guides. Controls include centrally managed configuration, full disk encryption, secure boot, endpoint detection and response, removal of local administrator rights, managed updating and security logging. Access to government information is restricted to compliant managed devices through conditional access with multi-factor authentication. Our arrangements are subject to [Cyber Essentials / Cyber Essentials Plus] certification, certificate number [number], valid until [date]. Government information is handled in line with the Government Security Classifications Policy and the security requirements set by the contracting authority.

Statements to avoid

- "Our devices are OFFICIAL-SENSITIVE approved" or "certified for OFFICIAL-SENSITIVE". No such approval exists.
- "Compliant with Defence Standard 05-138" without the level. Compliance is always at a stated Cyber Risk Profile level.
- "Cyber Essentials certified devices". Cyber Essentials certifies an organisation's defined scope, and devices sit within that scope.
- Any statement that the supplier is the information asset owner for the customer's information.

SECTION 5

Putting it in place

The baseline is a set of requirements that only work together. A device meets it because the environment around it enforces it, so the baseline is put in place across the whole environment before any single device can be shown to meet it. The Government Information Owner signs off at each point where a decision is theirs.

- 1 Capture the requirements**
Work through the security conditions and Cyber Risk Profile levels for current and expected contracts, and record them against Part A.
- 2 Appoint the owner and start the register**
Name the Government Information Owner and open a register entry for each holding.
- 3 Agree the baseline**
Fit Part C to your platforms and the highest level any contract requires, and have a director approve it.
- 4 Implement it centrally**
Identity and multi-factor authentication, conditional access, device management, encryption, updates, endpoint protection, application and media controls, logging and the approved storage locations.
- 5 Test the devices**
Test one device of each type against every control, and collect the evidence it produces.
- 6 Turn on the compliance gate**
Run conditional access in report-only mode first, then enforce it once every device passes.
- 7 Roll out and brief**
Bring the remaining devices into line and brief everyone who will handle government information.
- 8 Seek independent assurance**
Cyber Essentials or Cyber Essentials Plus with the full scope in view, and the MOD questionnaire or Defence Cyber Certification where required. Where you want the whole arrangement assessed, the Westmark Defence Supplier Mark examines it.

HOW THE MARK LOOKS AT THIS AREA

Under the Westmark Defence Supplier Mark, the devices and services in this framework are examined as part of information handling at every scope, and in full at Cyber and Combined scope, alongside the other areas of security.

ANNEX

Sources

Sources checked in September 2026. Where a source is withdrawn or replaced, its successor applies.

Government Security Classifications Policy v2.0 and Guidance 1.1, 1.4, 1.6

Cabinet Office, August 2024 · gov.uk/government/publications/government-security-classifications

'OFFICIAL-SENSITIVE' data and IT

Cabinet Office and GDS, February 2017 · gov.uk/guidance/official-sensitive-data-and-it

GovS 007: Security, v2.0

Cabinet Office, September 2021 · gov.uk/government/publications/government-functional-standard-govs-007-security

Information Asset Owner Hub

Government Security Group · security.gov.uk/policy-and-guidance/information-asset-owner-hub

PPN 014: Cyber Essentials Scheme

Cabinet Office, February 2025 · gov.uk/government/publications/ppn-014-cyber-essentials-scheme

Contracting securely: model security schedules

Government Security Group · security.gov.uk/policy-and-guidance/contracting-securely

Cyber Security Model

Ministry of Defence · gov.uk/guidance/cyber-security-model

Defence Standard 05-138 Issue 4

Ministry of Defence, May 2024 · gov.uk/government/publications/cyber-security-for-defence-suppliers-def-stan-05-138-issue-4

Industry Security Notices, including 2020/07, 2022/10, 2023/04, 2024/06, 2025/03, 2025/07, 2026/01, 2026/02 and 2026/04

Ministry of Defence · gov.uk/government/publications/industry-security-notices-isns

Device Security Guidance and platform guides

National Cyber Security Centre · ncsc.gov.uk/collection/device-security-guidance

Cloud Security Principles

National Cyber Security Centre · ncsc.gov.uk/collection/cloud/the-cloud-security-principles

Cyber Essentials requirements v3.3

National Cyber Security Centre and IASME, April 2026 · ncsc.gov.uk/cyberessentials

Baseline Personnel Security Standard v7.0

Cabinet Office, June 2024 · gov.uk/government/publications/government-baseline-personnel-security-standard

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.