



Defence Supplier Mark Assurance Scheme

Defence Supplier Mark Assurance Standard

The requirements against which an organisation is assessed

Reference	WMA-SBD-001
Scheme	Westmark Defence Supplier Mark
Version	1.1
Date of issue	September 2026
Classification	OFFICIAL
Scheme Owner	Westmark Assurance, a trading name of Ross Macdonald Consultancy Ltd (SC848204)

Document control

Document title	Defence Supplier Mark Assurance Standard
Reference	WMA-SBD-001
Version	1.1
Date of issue	September 2026
Classification	OFFICIAL
Status	Normative
Scheme Owner	Westmark Assurance, a trading name of Ross Macdonald Consultancy Ltd (SC848204)
Normative annex	WMA-SBD-CAT-001 Defence Supplier Mark Control Set
Supersedes	BC-METH-001 v1.0 Assurance Methodology, withdrawn on issue of this framework
Review frequency	Annually as a minimum, and on any change to the publications at Section 3 that affects a requirement in this framework or in WMA-SBD-CAT-001
Retention	This framework and all superseded versions are retained for seven years from the date of withdrawal

Version history

Version	Date	Summary
1.0	July 2026	First issue. Replaces BC-METH-001 v1.0 and the SBD-PROC-001 document suite v1.0.
1.1	September 2026	Re-issued under the two-scheme structure as the Westmark Defence Supplier Mark Assurance Standard. Scheme line added, outcome names changed to Westmark Defence Supplier Mark and Westmark Defence Supplier Conditional, control set renumbered WMA-SBD-CAT-001, templates renumbered WMA-SBD-TPL-001 to 006. No change to any requirement, weighting or threshold.

1. Purpose and status

1.1 What this framework does

WMA-SBD-001 sets out the requirements against which Westmark Assurance assesses an organisation's Secure by Design posture, and the basis on which an assurance outcome is awarded and withdrawn.

It serves two audiences. For the assessed organisation it states what has to be in place and what evidence will be examined. For the assessor it states how each requirement is scored, what constitutes corroboration, and what conditions prevent a positive outcome irrespective of score.

1.2 What this framework does not do

An assurance outcome awarded under this framework is an independent judgement by Westmark Assurance that the organisation's delivery is consistent with the Secure by Design principles published by government and with the contractual security obligations placed on suppliers to MOD and government customers.

It does not constitute, and shall not be represented as:

- Government or MOD certification, accreditation or approval
- Compliance with the government Secure by Design policy, which places its obligations on departments and arm's length bodies rather than on their suppliers
- A Facility Security Clearance, or any form of National Security Vetting
- Cyber Essentials, Cyber Essentials Plus, Defence Cyber Certification, or ISO/IEC 27001 certification
- Completion of a Supplier Assurance Questionnaire, or compliance with Defence Standard 05-138
- A substitute for any assessment, audit or inspection carried out by a Contracting Authority, a prime contractor, or a Designated Security Authority

Organisations holding an outcome under this framework are bound by the claim wording at Section 14. Representation beyond that wording is a breach of the scheme terms and is grounds for withdrawal.

1.3 The basis of the distinction

The government Secure by Design principles are mandatory for government departments and arm's length bodies, and optional for other parts of the public sector. Third party suppliers to those organisations are directed to liaise with their security contacts to understand the specific requirements that apply to them. Secure by Design is itself not an assurance process.

An organisation in the supply chain therefore has no route to certify against the government approach. What it can demonstrate is that its own delivery is designed and evidenced so that its customer can discharge the obligations the approach places on them. That is what this framework assesses.

2. Scope and applicability

2.1 Organisations within scope

This framework may be applied to any organisation that delivers, or seeks to deliver:

- Site-based work onto MOD establishments, government premises, Crown Estate sites or critical national infrastructure, including survey, inspection, condition assessment, measured work, maintenance, construction and facilities services
- Digital, cyber or technical services to a government or government-aligned customer
- Any of the above beneath a prime contractor or another supplier, at any tier
- Work involving the handling, generation or transmission of information classified OFFICIAL or above

The framework applies to organisations of any size. Proportionality is handled through the scoring criteria at Section 9 rather than by exempting smaller organisations from requirements.

2.2 Assessment scopes

An assessment is conducted against one of three scopes, fixed at scoping stage and recorded on the assurance statement.

Scope	Applies to	Sections assessed
Operational	Organisations delivering site-based work with no access to customer systems or data beyond the deliverable	S1, S2, S3, S4, S6, S7
Cyber	Organisations delivering digital or technical services	All seven
Combined	Organisations delivering both	All seven

Where a section is outside the assessed scope, its weighting is redistributed across the assessed sections in proportion to their stated weights. A scoped-out section is recorded as out of scope on the assurance statement. It is never recorded as a pass.

An organisation cannot select its own scope where the evidence contradicts it. Where the assessor finds during sampling that the organisation performs work outside the declared scope, the assessment is suspended and rescoped.

2.3 Matters outside this framework

This framework does not assess health and safety performance, quality management, environmental management, financial standing, or the technical competence of the organisation in its own discipline. Where an assessor observes a matter of that kind that bears on security, it is recorded as an observation and reported. It does not affect the score.

2.4 Framework sections

Ref	Section
S1	Governance and Accountability
S2	Risk Management and Project Implementation
S3	Contractual, Statutory and Personnel Security
S4	Information and Asset Handling
S5	Cyber and Technical Security
S6	Incident Management and Continuous Assurance
S7	Supply Chain

Section weightings are at Section 10. The requirements themselves are in WMA-SBD-CAT-001, which is a normative annex to this framework and carries its own version line.

3. Normative references

The following publications are referenced in this framework and in WMA-SBD-CAT-001. Assessors apply the version extant at the assessment date. Where a publication is withdrawn or replaced between issue of this framework and an assessment, the assessor applies the successor and records the substitution in the assessment file.

3.1 Government security policy and standards

- Government Functional Standard GovS 007: Security
- Government Security Classifications Policy
- Secure by Design principles, Government Cyber Unit, published at security.gov.uk
- Secure by Design policy, published at security.gov.uk
- Cyber Assessment Framework, National Cyber Security Centre
- Baseline Personnel Security Standard

The Security Policy Framework published in 2014 is superseded by the Government Functional Standards, including GovS 007, and is not a reference in this framework.

3.2 MOD policy and contractual instruments

- Industry Security Notice 2023/09, Secure by Design Requirements
- Industry Security Notice 2026/04, Security Aspects Letters and Contractual Security Conditions, together with its Annex B, UK OFFICIAL and UK OFFICIAL-SENSITIVE Contractual Security Conditions
- Industry Security Notice 2022/05, Release of JSP 440 to Industry
- The extant Industry Security Notices on incident reporting and on subcontracting or collaborating on classified MOD programmes
- DEFCON 76, Conditions that Apply to Work at UK Government Establishments
- DEFCON 531, Disclosure of Information
- DEFCON 658, Cyber
- DEFCON 659A, Security Measures
- DEFCON 660, OFFICIAL-SENSITIVE Security Requirements
- Defence Standard 05-138 Issue 4
- Cyber Security Model version 4, Defence Cyber Protection Partnership
- MOD Form 1686 and MOD Form 680 procedures

JSP 440 is not released to industry as a default. Requirements reaching a supplier are laid down in GovS 007, the contract together with any Security Aspects Letter, the DEFCONs and DefStans invoked by the contract, extant Industry Security Notices, and List X Notices to Facility Security Clearance holders. An organisation is not assessed against JSP 440, and an assessor does not request sight of it.

3.3 Technical guidance

- NCSC 10 Steps to Cyber Security
- NCSC guidance on Transport Layer Security for external facing services
- NCSC Secure Design Principles
- Cyber Essentials and Cyber Essentials Plus scheme requirements

3.4 Statute

- Official Secrets Act 1989
- National Security Act 2023
- Data Protection Act 2018 and the UK General Data Protection Regulation

4. Alignment basis

4.1 Government Secure by Design principles

The ten published principles are: 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.

Principle	Framework sections
1. Create responsibility for cyber security risk	S1
2. Source secure technology products	S5, S7
3. Adopt a risk-driven approach	S2
4. Design usable security controls	S2, S5
5. Build in detect and respond security	S5, S6
6. Design flexible architectures	S5
7. Minimise the attack surface	S4, S5
8. Defend in depth	S4, S5
9. Embed continuous assurance	S6
10. Make changes securely	S2, S5

Principles 2, 4, 6 and 10 have limited application to an organisation assessed under Operational scope. Their treatment is governed by the scoping rule at 2.2 and they are recorded as out of scope rather than as a shortfall.

4.2 MOD Secure by Design principles

ISN 2023/09 sets out seven principles: understand and define context; plan the security activities; implement continuous risk management; define security controls; engage and manage the supply chain; assure, verify and test; enable through life management.

MOD principle	Framework sections
1. Understand and define context	S1, S2
2. Plan the security activities	S2
3. Implement continuous risk management	S2, S6
4. Define security controls	S4, S5
5. Engage and manage the supply chain	S7
6. Assure, verify and test	S6
7. Enable through life management	S6

4.3 Contractual security obligations

Sections S3 and S4 carry the requirements arising from the contractual security conditions rather than from the principles. These cover the Security Aspects Letter, the DEFCON conditions, personnel screening, statutory obligations, and the handling, return and destruction of classified material. They are assessed on every engagement irrespective of scope, because they attach to the contract rather than to the type of work performed.

4.4 Relationship to the Cyber Assessment Framework

Where an organisation's customer is subject to GovAssure, the assessor records the mapping between the organisation's evidence and the relevant CAF outcomes at Annex C. This supports the customer's own reporting. It confers no CAF standing on the organisation.

5. Conventions and definitions

5.1 Normative conventions

Term	Meaning
shall	A requirement. Failure to meet it affects the score, and where the requirement is identified as disqualifying it prevents a positive outcome.
should	A recommendation. An organisation departing from it is expected to explain the alternative it has adopted. Departure without explanation affects the score.
may	A permission. No score attaches to the choice.
the Organisation	The legal entity undergoing or holding an assessment, as named on the assurance statement. Where the entity trades under more than one name, the assessment attaches to the legal entity and the trading names within the assessed scope are listed on the certificate.
the Assessor	The individual conducting the assessment on behalf of Westmark Assurance.
the Scheme Owner	Westmark Assurance, a trading name of Ross Macdonald Consultancy Ltd.
the Customer	The party to whom the Organisation delivers, whether a government department, the Ministry of Defence, a prime contractor, or another supplier in the chain.

Where a defined term appears in this framework or in WMA-SBD-CAT-001, it carries the meaning given in this section. Where a contract, a Security Aspects Letter or a Defence Condition defines the same term differently for a specific engagement, that definition governs the engagement and this framework is read consistently with it.

5.2 Scheme terms

Term	Definition
Assessment	The examination of an Organisation against this framework and the control set, conducted at a defined scope and resulting in an outcome.
Control Set	WMA-SBD-CAT-001, the normative annex containing the requirements against which an Organisation is scored. Each version carries its own reference and change log.
Outcome	One of the three results defined at Section 11: Westmark Defence Supplier Mark, Westmark Defence Supplier Conditional, or Not Confirmed. No other result is recorded.
Confidence Level	The Assessor's judgement of the strength and consistency of evidence supporting a Westmark Defence Supplier Mark outcome, recorded as High, Moderate or Limited. It is a separate judgement from the score.
Disqualifying Condition (DC)	A condition which, where found, prevents an outcome of Westmark Defence Supplier Mark irrespective of the score achieved. The conditions are at Section 12.
Project Sample	The set of engagements selected by the Assessor for examination. The Organisation may propose candidates and cannot direct the selection.
Corroboration	Evidence of a single matter drawn from more than one independent source. A single document, a single interview, or a single observation does not corroborate itself.
Documentary evidence	Procedures, risk assessments, project plans, briefing records, incident logs, training records, subcontractor assessments, Security Aspects Letters and acknowledgements, and Supplier Assurance Questionnaire records.
Observational evidence	Site walk-throughs, observation of working practice, and review of physical and technical controls in use.
Testimonial evidence	Structured interviews with delivery personnel, project leads, and the individual holding

Term	Definition
	accountability for security within the Organisation.
Record evidence	Correspondence, meeting minutes, change records, access logs, and other artefacts generated during normal delivery rather than produced for the assessment.
Assessment File	The Assessor's contemporaneous record of the assessment, retained for seven years.
Assurance Statement	The document issued to the Organisation recording the outcome, the scope, the sample, any limitations, and any improvement actions.

5.3 Contractual and defence terms

Term	Definition
Contracting Authority (CA)	The party placing the contract and issuing the security requirements. Where the Organisation subcontracts classified work, it becomes the Contracting Authority in respect of that subcontract.
Security Aspects Letter (SAL)	The written notice from the Contracting Authority identifying which aspects of a tender or contract are classified and at what level. The security obligations become legally effective on its issue.
Security Grading Guide (SGG)	A document referenced by a SAL setting out the classification of components, assemblies or elements of the work in greater detail than the SAL itself.
Defence Condition (DEFCON)	A standard contract condition invoked by an MOD contract. Those bearing on this framework are listed at 3.2.
Defence Standard (DefStan)	A technical standard invoked by an MOD contract, including Defence Standard 05-138.
Industry Security Notice (ISN)	Policy direction issued by the MOD to the defence supply base and published on GOV.UK.
Defence Related Classified Material	Any information or asset given a security classification by the MOD, including material owned by a third party such as NATO or another nation for which the MOD is responsible.
Facility Security Clearance (FSC)	Clearance of a facility permitting classified material above OFFICIAL-SENSITIVE to be held on the Organisation's own premises.
Facility Security Controller	The individual appointed by an FSC holder as the point of contact for the Contracting Authority and the Designated Security Authority.
Designated Security Authority	The national authority responsible for security oversight of the Organisation.
Cyber Risk Profile (CRP)	The level assigned to a contract by the Contracting Authority under the Cyber Security Model, determining the control set applying under Defence Standard 05-138.
Risk Assessment Reference	The reference issued with a Cyber Risk Profile, required before a Supplier Assurance Questionnaire can be completed.
Supplier Assurance Questionnaire (SAQ)	The self-assessment completed through the Supplier Cyber Protection Service against the controls applying to the assigned Cyber Risk Profile.
Cyber Implementation Plan (CIP)	The plan submitted where a Supplier Assurance Questionnaire outcome is Not Met, setting out equivalent mitigations or the actions required to reach compliance.
Defence Industry WARP	The MOD Defence Industry Warning, Advice and Reporting Point, to which loss or compromise of Defence Related Classified Material is reported in addition to the Contracting Authority.
MOD Form 1686	The form used to seek approval to subcontract or collaborate on classified work.
MOD Form 680	The form governing release of classified defence material to a foreign entity for promotion

Term	Definition
	or sale.

5.4 Personnel and access terms

Term	Definition
Baseline Personnel Security Standard (BPSS)	The pre-employment screening standard covering identity, right to work, employment history and criminal record checking. It is the floor for access to OFFICIAL and OFFICIAL-SENSITIVE material and sits beneath National Security Vetting rather than alongside it.
National Security Vetting (NSV)	Clearance at Counter Terrorist Check, Security Check, Developed Vetting or Enhanced levels, granted to an individual by the vetting authority.
Cleared Personnel	Individuals holding current National Security Vetting at the level the contract requires, verified by the Organisation as current at the point of access.
Escort Arrangement	A written arrangement agreed with the site security authority under which an individual without the required clearance is permitted access under supervision. The arrangement is set by the establishment. It is not a matter the Organisation determines for itself.
Need to Know (NTK)	The principle that access to classified material is confined to individuals whose duties require it, who have been made aware of the requirement to protect it.
Aftercare	The continuing obligation on a clearance holder to report changes in personal circumstances bearing on suitability, and the Organisation's obligation to receive and act on those reports.

5.5 Information, asset and device terms

Term	Definition
Controlled Information	Any information, data, drawing, plan, photograph, measurement, model, configuration or output relating to a controlled site or a government-aligned engagement, whether provided by the Customer or generated by the Organisation, and subject to handling restrictions under the Government Security Classifications Policy.
Controlled Site	Any location where operational, personnel or physical security considerations apply, including MOD establishments, government premises, Crown Estate land, utilities and network infrastructure, and the premises of a prime contractor delivering into those customers.
Aggregation	The effect by which separate items of information, each individually of low sensitivity, combine to produce a holding of higher sensitivity. For survey and inspection work, the combination of layout, access arrangement and condition data is the common instance.
Authority Property	Samples, patterns, specifications, plans, drawings or other material issued by or on behalf of the Contracting Authority, which remain the property of the Contracting Authority and are returned on completion or destroyed on direction.
Portable Electronic Device (PED)	Any device capable of holding, processing or transmitting information and capable of being carried by one person, including laptops, tablets, phones, cameras, survey instruments with onboard storage, data loggers, drones and removable media.

Device categories

The distinction below governs how a device is handled. It turns on what the device holds or can reach, and does not turn on who owns it.

Category	Definition	Handling
Controlled Device	Any Portable Electronic Device that holds, processes or transmits Controlled Information, or that has access to a Customer system, network or account. Ownership is immaterial. A device owned by the individual falls into this category the moment it is used for engagement purposes, including receipt of engagement email or the taking of a site photograph.	Subject in full to the requirements at S4 and S5, including encryption, the prohibition on leaving the device unattended in a vehicle, separation of encryption tokens from the device, and access revocation at close-out.
Personal Device	A Portable Electronic Device holding no Controlled Information, with no access to any Customer system, network or account, and not used for any engagement purpose.	May be left secured in a vehicle when visiting a site, where the site instruction permits. Not brought into an area where the establishment prohibits it. Never used to capture, store or transmit anything relating to the engagement.

Three points govern the boundary.

1. A Personal Device becomes a Controlled Device on first engagement use and remains one until the Organisation has confirmed and recorded the removal of engagement data and access.
2. Establishments frequently restrict or prohibit Personal Devices on site, and some restrict storage in vehicles within the establishment perimeter. The site instruction prevails over this framework in every case.
3. The Organisation's briefing shall state which category applies to each device an individual carries, before that individual arrives on site.

5.6 Risk, engagement and incident terms

Term	Definition
Engagement	A discrete piece of work delivered under a contract, task order or instruction.
Operational Engagement	An engagement involving physical access to a controlled site, or the production of Controlled Information about a site or asset.
Cyber Engagement	An engagement involving the delivery, configuration, testing or assessment of digital systems, software or technical services, or access to a Customer system or data.
Risk Appetite	The level of security risk the Organisation's accountable owner is prepared to accept, stated in advance of assessment rather than derived from the scores produced.
Threat Assessment	An assessment of the actors, capabilities and intent bearing on the engagement, sourced from the Customer or from an appropriate authority where the Organisation cannot produce it itself.
Threat Modelling	The structured examination of how an engagement could be attacked or exploited, conducted at design stage and distinct from the scoring of identified risks.
Project Security Risk Assessment	The engagement-level record of identified security risks, the controls selected, and the reasoning.
Project Security Plan (PSP)	The assembled record for an engagement, comprising the risk assessment, the controls applied, the briefing records, the SAL and its acknowledgement where issued, and the close-out record.
Security Incident	Any event, actual or suspected, that may have compromised Controlled Information, site security, personnel safety arising from a security cause, or the integrity of a system under engagement.
Near Miss	An event which, had circumstances differed, would have constituted a Security Incident.
Compromise	Loss of confidentiality, integrity or availability of Controlled Information, whether or not the recipient is known and whether or not the material has been recovered.

6. Roles, competence and independence

6.1 Accountability

- 6.1.1** The Organisation shall name a single individual who holds accountability for security risk across all engagements within scope. That individual shall hold a position at director level or hold Senior Responsible Owner authority for the work.
- 6.1.2** The accountability shall not be delegated, shared between individuals, or held by a committee. Activity supporting the accountability may be delegated to a security function, a compliance function or a named deputy, provided the delegation is documented and the accountability itself remains with the named individual.
- 6.1.3** The named individual shall be recorded by name and position in the Organisation's security procedure, on each Project Security Plan, and on any assurance statement issued under this framework.
- 6.1.4** Where the named individual changes, the Organisation shall record the date of change and notify the Scheme Owner within twenty working days where an outcome is held.

6.2 Roles within the Organisation

Role	Holds	Requirement
Accountable Owner	Accountability for security risk across the Organisation	Approves the security risk appetite, approves the Project Security Plan for engagements the Organisation classifies as sensitive, receives notification of every reportable incident, and is the escalation point for security concerns
Security Lead	Responsibility for maintaining the security procedure and its supporting records	Maintains the procedure, the training record, the incident record, and the register of Security Aspects Letters and their acknowledgements
Engagement Security Lead	Responsibility for security on a specific engagement	Completes or commissions the engagement security risk assessment before mobilisation, delivers or arranges the briefing, acts as the single point of contact for security queries during delivery, and reports incidents without delay
Facility Security Controller	Responsibility arising from a Facility Security Clearance, where held	Acts as the point of contact for the Contracting Authority and the Designated Security Authority, and receives Security Aspects Letters issued to a clearance holder
All personnel and associates	Individual obligation	Comply with the procedure and with any engagement or site instruction, complete required briefing before access, report suspected breach or unusual activity, and confine collection and retention to what the deliverable requires

6.3 Role concentration in smaller organisations

- 6.3.1** The Accountable Owner, the Security Lead and the Engagement Security Lead may be the same individual where the size of the Organisation makes separation impracticable.
- 6.3.2** Where roles are concentrated, the Organisation shall record the concentration and shall identify how a security decision receives a second view. Acceptable arrangements include a nominated deputy, a retained external adviser, or a documented referral route to the Customer's security function.
- 6.3.3** An Organisation in which one individual holds every role with no second view available shall not score above 1 on the governance requirements at S1. This is a limit on score rather than a disqualification, and it reflects that a single point of judgement carries no internal check.
- 6.3.4** Concentration of roles shall be recorded on the assurance statement as a stated limitation.

6.4 Competence

- 6.4.1** MOD policy requires that individuals assigned to Secure by Design activity are suitably qualified and experienced. The Organisation shall hold a record demonstrating that each person performing a role at 6.2 meets that expectation for the work they perform.
- 6.4.2** The competence record shall state, for each role holder: the basis of their competence, any qualification or credential relied upon, the date it was last reviewed, and the person who reviewed it.
- 6.4.3** Competence may rest on qualification, on credential, on training, or on experience. Experience is a sufficient basis where the record states what that experience consists of and how it bears on the activity performed.
- 6.4.4** Where the Organisation lacks internal competence for a security activity, it shall record how the activity is resourced, whether through a retained adviser, the Customer's security function, or a subcontracted specialist. Sourcing competence externally is acceptable. Leaving the activity unresourced is not.

6.5 Resourcing

- 6.5.1** The Accountable Owner shall make resource available for the security activities the Organisation's engagements require, including briefing time, assessment time, secure storage, device provision, and personnel screening.
- 6.5.2** Where the Organisation prices work for a Customer, the cost of security activity should be identified within the price rather than absorbed. An Organisation that cannot show how security activity is funded will be examined closely at S1, because unfunded activity tends not to occur.

6.6 Scheme roles

Role	Held by	Function
Assessor	An individual authorised by the Scheme Owner	Conducts the assessment, selects the project sample, gathers and tests evidence, applies the scoring criteria, and prepares the assurance statement or finding report
Technical Reviewer	An individual authorised by the Scheme Owner, other than the Assessor	Reviews the assessment file and the proposed outcome before issue, and confirms that the scoring is supported by the evidence recorded
Scheme Owner	Westmark Assurance	Owns this framework and the control set, authorises Assessors, maintains the register, and decides on suspension and withdrawal

6.7 Assessor competence

- 6.7.1** An Assessor shall demonstrate working knowledge of the publications at Section 3, current at the date of authorisation.
- 6.7.2** An Assessor shall hold experience of delivery or oversight in the sector being assessed. An Assessor without operational experience of site-based defence work does not assess an Organisation at Operational scope.
- 6.7.3** The Scheme Owner shall hold a competence record for each Assessor, reviewed annually, recording the scopes the Assessor is authorised to assess.
- 6.7.4** An Assessor shall complete continuing professional development covering the normative references, and shall record it.

6.8 Technical review

- 6.8.1** Every outcome shall be reviewed by a Technical Reviewer before issue.
- 6.8.2** Where the Scheme Owner does not have a second authorised individual available, the review shall be performed under a documented arrangement with an external reviewer bound by the confidentiality terms at Section 15.
- 6.8.3** An outcome issued without technical review shall not be issued. Where review is unavailable, the assessment is held and the Organisation is informed of the delay and its cause.

6.9 Independence and conflict of interest

- 6.9.1** The credibility of an outcome under this framework rests on the Assessor having no interest in the result. This section is applied without exception and without commercial discretion.
- 6.9.2** Related body. For the purposes of this section, a Related Body is any legal entity which, in relation to the Scheme Owner: is under common ownership or common control; shares a director, member, partner or controlling individual; shares personnel who perform assessment or consultancy work; holds a financial interest in the Scheme Owner, or in which the Scheme Owner holds a financial interest; or operates under a standing commercial arrangement with the Scheme Owner covering referral, revenue sharing, joint delivery, subcontracting or reseller terms. Separate incorporation does not by itself take an entity outside this definition. The test is whether an informed observer would consider the relationship capable of affecting the Assessor's judgement.
- 6.9.3** Consultancy separation. The Scheme Owner shall not assess an Organisation which, within the period beginning two years before the assessment date and ending on expiry of the outcome, has received security consultancy, advisory, implementation, documentation drafting or training services from the Scheme Owner or from a Related Body.
- 6.9.4** Template provision. Issuing the template paperwork forming Part B of this scheme, unmodified and available on the same terms to every Organisation, does not constitute consultancy. Tailoring a template to an Organisation's circumstances, drafting its procedure, populating its risk assessment, or advising on how to raise a score does constitute consultancy and engages 6.9.3.
- 6.9.5** Register of Related Bodies. The Scheme Owner shall maintain a register of Related Bodies, reviewed annually and on any change of control, directorship or standing commercial arrangement. The register is disclosed to any Contracting Authority or prime contractor on request.
- 6.9.6** Declaration. Before assessment begins, the Scheme Owner shall disclose in writing to the Organisation, and to any prime contractor commissioning the assessment, the existence of any Related Body providing services in the security field. The disclosure is made whether or not the Organisation has used that body.
- 6.9.7** Prior relationship. An Assessor shall not assess an Organisation in which the Assessor, or a person connected to the Assessor, holds a financial interest, a directorship, an employment relationship, or a family connection.
- 6.9.8** Referral. The Scheme Owner may refer an Organisation requiring consultancy to another provider, and shall not receive a fee, commission or other benefit for the referral.
- 6.9.9** Emergent conflict. Where a conflict arises during an assessment, the Assessor shall stop, notify the Scheme Owner, and record the matter. The assessment is reassigned or terminated. It is not completed by the conflicted Assessor.
- 6.9.10** Declaration before assessment. The Assessor shall complete a conflict declaration before each assessment, recording any relationship with the Organisation, its personnel, or its Customer. The declaration is retained on the assessment file.
- 6.9.11** Fee structure. Assessor remuneration shall not vary with the outcome awarded. The Scheme Owner shall not offer, and shall not accept, a fee arrangement contingent on an Organisation achieving a particular outcome.
- 6.9.12** Prime contractor relationship. Where an assessment is commissioned by a prime contractor in respect of a supplier, the Assessor's obligations of accuracy run to both. The Assessor shall not discuss emerging findings with the commissioning prime before the assurance statement is issued, and shall not accept direction from either party on the sample, the scoring, or the outcome.

6.10 Assessor conduct

Conduct obligations governing hospitality, contemporaneous recording, confidentiality during assessment, and the testing of adverse findings are at Section 15.

7. The assessment process

7.1 Stages

Stage	Purpose	Output
1. Enquiry and eligibility	Establish that the Organisation falls within the applicability at Section 2	Eligibility record
2. Scoping	Fix the assessed scope, the control set version, and the assessment terms	Signed assessment agreement
3. Pre-assessment submission	Obtain the documentary set and the engagement list	Submission log
4. Sample selection	Select the engagements to be examined	Sample record with selection reasoning
5. Evidence gathering	Examine documents, interview personnel, observe practice	Evidence record against each requirement
6. Findings testing	Give the Organisation opportunity to produce further evidence against any adverse view	Response record
7. Scoring and technical review	Apply the criteria, review the file, confirm the outcome	Scored assessment, reviewer sign-off
8. Issue	Issue the assurance statement or the finding report	Statement or report, register entry

Stages are sequential. An Assessor shall not score a requirement before the findings testing at stage 6 has been completed in respect of that requirement.

7.2 Enquiry and eligibility

- 7.2.1** The Scheme Owner shall establish at enquiry that the Organisation performs, or is bidding to perform, work within the applicability at Section 2.
- 7.2.2** An Organisation with no current or prospective engagement within scope shall not be assessed. The framework assesses delivery. It does not assess an intention to deliver.
- 7.2.3** Where an Organisation has never delivered an engagement of the type it seeks assessment for, the Scheme Owner may offer a readiness review. A readiness review produces no outcome, carries no certificate, appears on no register, and shall not be represented as an assessment.

7.3 Scoping

- 7.3.1** Scope is fixed before assessment begins and is recorded in the assessment agreement. It shall state the assessed scope at 2.2; the legal entity assessed and the trading names within scope; the sites, regions or business units within scope where the Organisation operates in a way that makes this material; the version of WMA-SBD-CAT-001 applying; and the sections in scope and any section recorded as out of scope, with the reason.
- 7.3.2** The Organisation declares the types of work it performs. The Assessor tests that declaration during sampling. Where the evidence contradicts the declared scope, 2.2 applies and the assessment is suspended and rescoped.
- 7.3.3** Scope shall not be narrowed after sampling has begun in order to exclude an engagement the Assessor has selected.

7.4 Control set version currency

- 7.4.1** An assessment is conducted against the version of WMA-SBD-CAT-001 extant on the date the assessment agreement is signed.

- 7.4.2 Where a new version of WMA-SBD-CAT-001 is issued after signature and before the assessment concludes, the assessment continues against the version at signature. The Assessor records the superseding version on the assessment file and notes it on the assurance statement.
- 7.4.3 An outcome awarded against a superseded version remains valid until its expiry date. It is not withdrawn or downgraded by the issue of a new control set.
- 7.4.4 Reassessment is conducted against the version extant at the date the reassessment agreement is signed.
- 7.4.5 Where a change to the publications at Section 3 introduces a requirement the Scheme Owner judges to be of immediate effect, the Scheme Owner may issue the new control set with a stated application date and may require holders to confirm their position on the affected requirements. This is the sole circumstance in which a change to the control set reaches a live outcome, and it is exercised by exception.

7.5 Pre-assessment submission

- 7.5.1 The Organisation shall submit, before the assessment date:
- Its security procedure and any supporting policy
 - Its record of named accountability and the competence records at 6.4
 - A list of engagements delivered within the assessment period, sufficient for the Assessor to select a sample
 - Its incident record for the assessment period
 - Its training and briefing records
 - Its subcontractor assessment records
 - Its register of Security Aspects Letters and acknowledgements, where any have been issued to it
 - Its Supplier Assurance Questionnaire position, where DEFCON 658 applies to any contract it holds
- 7.5.2 The engagement list shall state, for each engagement: the customer, the contract or task reference, the period, the type of work, the classification of information handled, whether a Security Aspects Letter was issued, and whether any incident or near miss was reported.
- 7.5.3 The assessment period is the twelve months preceding the assessment date, or the period since the Organisation began delivering work within scope, whichever is shorter.
- 7.5.4 Where the Organisation withholds a document, the Assessor records the withholding, the reason given, and the effect on the evidence available. Clause 7.10 governs the treatment.

7.6 Sample selection

- 7.6.1 The Assessor selects the sample. The Organisation may propose candidates and shall not direct the selection.
- 7.6.2 A sample comprises between three and six engagements. The number is set by the Assessor having regard to the range of work, the classifications handled, and the consistency of the evidence encountered.
- 7.6.3 Selection shall reflect the range of work delivered, and shall include any engagement during the assessment period in which a security incident or near miss was reported; any engagement for which a Security Aspects Letter was issued; at least one engagement delivered beneath a prime contractor, where the Organisation works in that position; and at least one engagement in each assessed scope, where the Organisation holds a Combined scope.
- 7.6.4 Where the Organisation has delivered fewer than three engagements within scope during the assessment period, the Assessor records this. The limitation appears on the assurance statement and caps the confidence level at Limited.
- 7.6.5 Where an engagement selected by the Assessor cannot be examined because the customer withholds consent, the Assessor records the refusal, selects a replacement, and notes the substitution on the assurance statement. Repeated customer refusal across a sample is recorded as a limitation on the evidence available.

7.7 Evidence

- 7.7.1 Evidence falls into the four categories defined at 5.2. The Assessor draws on more than one category across the assessment as a whole.

- 7.7.2** Corroboration. A score of 2 against any requirement requires corroboration. A single document, a single interview, or a single observation does not corroborate itself. Corroboration is the distinction between this framework and a documentary compliance review, and it is applied without exception.
- 7.7.3** Record evidence generated during normal delivery carries greater weight than material produced in response to the assessment. The Assessor records which of the two a given item is.
- 7.7.4** The Assessor shall not accept a statement of intent as evidence of practice. A procedure describing what the Organisation will do evidences the existence of the procedure. Evidence that the procedure operates is drawn from records, observation and interview.

7.8 Interviews

- 7.8.1** The Assessor interviews, as a minimum: the individual holding accountability at 6.1, at least one Engagement Security Lead, and at least two individuals performing delivery work.
- 7.8.2** Delivery personnel are interviewed without a director or manager present, unless the individual requests otherwise. Where an Organisation declines to permit this, the Assessor records the refusal and the confidence level is capped at Limited.
- 7.8.3** Interviews test understanding rather than recall of document titles. An individual who cannot name the procedure but describes the correct action on discovering a security incident evidences the outcome the requirement seeks.

7.9 Observation

- 7.9.1** Where the assessed scope is Operational or Combined, the assessment shall include observation of working practice, either on a live engagement or at the Organisation's own premises.
- 7.9.2** Observation on a customer site is arranged through the Organisation and is subject to the customer's consent and the site's own access requirements. The Assessor complies with the establishment's security regulations and holds the clearance or escort arrangement the site requires.
- 7.9.3** Where site observation cannot be arranged, the Assessor observes at the Organisation's premises and records the substitution. An assessment conducted with no observation of any kind caps the confidence level at Limited.
- 7.9.4** Remote assessment is permitted for documentary review and interview. An assessment conducted wholly remotely shall be recorded as such on the assurance statement.

7.10 Evidence that cannot be produced

- 7.10.1** An Organisation delivering into defence and government environments will encounter matters it cannot show an Assessor. Customer threat assessments, security requirements, and material covered by a Security Aspects Letter may be withheld from the Assessor by the customer or by the classification itself. Export controls, third party intellectual property and commercial confidentiality produce the same effect.
- 7.10.2** Withholding on any of these grounds shall not of itself reduce a score.
- 7.10.3** Where evidence is withheld, the Assessor examines what can be shown of the surrounding process: that the Organisation received the material; that it was handled at the classification applying to it; that it was acted upon, evidenced through the decisions and records it produced; and that the individuals who needed it had access and those who did not were excluded.
- 7.10.4** The Assessor records the withholding, the ground given, and the alternative evidence examined. Where the alternative evidence is sufficient, the requirement is scored normally. Where it is insufficient, the requirement is scored on what could be examined, and the limitation appears on the assurance statement.
- 7.10.5** An Organisation shall not invoke this clause to withhold its own internal records. The clause covers material whose disclosure is restricted by the customer, by classification, by export control, or by a third party's rights. It does not cover a procedure the Organisation has chosen not to produce.

7.11 Findings testing

- 7.11.1** Where the Assessor forms a view that may be adverse to the Organisation, the Assessor shall put the view to the Organisation and give it opportunity to produce further evidence before the finding is settled.

7.11.2 The opportunity is given during the assessment rather than after the outcome is issued. An Organisation encountering an adverse finding for the first time in the assurance statement has not been assessed in accordance with this framework.

7.11.3 The Organisation's response, and the Assessor's treatment of it, are recorded on the assessment file.

7.11.4 This clause does not create a negotiation. The Assessor decides what the evidence supports.

7.12 Suspension of an assessment

The Assessor shall suspend an assessment where:

- The declared scope is contradicted by the evidence, pending rescoping under 7.3.2
- A conflict of interest emerges under 6.9
- Access to evidence or to personnel is obstructed to a degree that prevents examination of a section
- The Organisation is subject to a live investigation by a Contracting Authority or a Designated Security Authority into a matter within scope of this framework

A suspended assessment produces no outcome. The Organisation is informed in writing of the ground, and of what is required to resume.

7.13 The assessment file

7.13.1 The Assessor records observations contemporaneously. Reconstruction after the event is not contemporaneous recording.

7.13.2 The assessment file comprises the scoping record, the submission log, the sample record and its selection reasoning, the evidence record against each requirement, the interview record, the observation record, the findings testing record, the conflict declaration, the scoring, the technical review, and the statement or report issued.

7.13.3 The file is retained for seven years from the date the outcome is issued or the assessment is terminated. Retention is set at seven years so that the file outlives the six year contractual retention period applying to the Organisation's own records, allowing an assessment to be reconstructed for as long as the underlying evidence is required to exist.

7.13.4 The file is held at OFFICIAL as a minimum, and at the highest classification of any material it contains.

8. Evidence and scoring

8.1 The scale

Every requirement in WMA-SBD-CAT-001 is scored on a three point scale.

Score	Label	Meaning
0	Absent	The requirement is not met. Either nothing is in place, or something is in place which does not operate.
1	Established	The requirement is met. Evidence rests on a single source, or practice varies across the sampled engagements.
2	Embedded	The requirement is met, evidence is corroborated from more than one source, and practice is consistent across every sampled engagement to which the requirement applied.

No half marks, no intermediate values, and no fourth score. Where an Assessor is undecided between two scores, the lower applies.

8.2 What each score requires

Score 0

Awarded where any of the following is found:

- Nothing is in place addressing the requirement
- A document exists describing the requirement, with no record, observation or testimony that it operates
- The requirement operates in some part of the Organisation and is absent from the work sampled
- Practice contradicts the documented position

A document without operation scores 0. This is the most frequent scoring decision an Assessor makes, and it follows from 7.7.4.

Score 1

Awarded where the requirement is met and one or more of the following applies:

- Evidence comes from a single source, uncorroborated
- The requirement is met on some sampled engagements and missed on others
- The requirement operates through the personal practice of an individual with nothing to sustain it if that individual is unavailable
- Records exist but are incomplete across the assessment period
- The Organisation acted correctly following a prompt from a customer or a prime rather than through its own process

Score 2

Awarded only where all of the following apply:

- The requirement is met
- Evidence is corroborated in accordance with 8.3
- Practice is consistent across every sampled engagement to which the requirement applied
- The requirement operates through the Organisation's own process rather than through external prompting
- Records covering the requirement are complete for the assessment period

8.3 Corroboration

8.3.1 Corroboration means evidence of the same matter drawn from more than one independent source. Independence is judged by origin rather than by document count. Two documents produced by the same person on the same day for the same purpose are one source.

- 8.3.2 The following are independent of one another: a record generated during delivery, and testimony from a person who was not its author; testimony from a delivery worker, and observation of the practice described; a record held by the Organisation, and confirmation from the customer or prime; a record generated during delivery, and a separate record generated for a different purpose that is consistent with it.
- 8.3.3 The following do not corroborate: a procedure and a checklist derived from the same procedure; two individuals repeating a briefing they received together, with no record and no observation; a completed template with no evidence that the activity it records took place; testimony from the author of the document being tested.
- 8.3.4 Corroboration is required for a score of 2 and is not required for a score of 1.

8.4 Consistency across the sample

- 8.4.1 Where a requirement applied to four sampled engagements and was met on three, the score is 1. Consistency is assessed across the engagements to which the requirement applied, and partial consistency does not reach 2.
- 8.4.2 Where a requirement applied to only one sampled engagement, a score of 2 remains available if corroboration is present, and the Assessor records that consistency could be tested on a single engagement only. This is a factor in the confidence level at Section 11.
- 8.4.3 Where a requirement applied to no sampled engagement, 8.5 governs.

8.5 Requirements that do not apply

- 8.5.1 A requirement is recorded as Not Applicable where the circumstance it addresses did not arise during the assessment period and does not arise in the Organisation's normal delivery.
- 8.5.2 Not Applicable is a finding of fact and requires evidence. The Assessor shall record the basis on which the circumstance is judged not to arise. An assertion by the Organisation is not sufficient.
- 8.5.3 A requirement recorded as Not Applicable is removed from both the points achieved and the points available for the section. It is never scored as though met.
- 8.5.4 The applicability cap. Where more than the cap stated at 8.5.6 of the requirements in a section are recorded as Not Applicable, the section is recorded as Insufficient Basis. A section carrying that record contributes no score, has its weighting redistributed across the remaining sections, appears on the assurance statement as Insufficient Basis with the reason, and caps the overall confidence level at Limited. The cap exists so that an Organisation cannot raise its percentage by narrowing what it does.
- 8.5.5 Where a circumstance recorded as Not Applicable subsequently arises, the Organisation shall notify the Scheme Owner within twenty working days. Section 13 governs the review that follows.
- 8.5.6 The applicability cap is one third unless WMA-SBD-CAT-001 states a different cap for a section. A section-specific cap is stated in the control set against the section concerned, together with the reason, and is available only where the section carries a materially higher proportion of conditional requirements than the control set as a whole. No section-specific cap exceeds 40 per cent.

8.6 Requirements linked to a Disqualifying Condition

- 8.6.1 Certain requirements in WMA-SBD-CAT-001 are marked as linked to a Disqualifying Condition. The link is stated against the requirement.
- 8.6.2 A score of 0 against a linked requirement obliges the Assessor to test whether the corresponding condition at Section 12 is met. A score of 0 does not of itself establish the condition. The condition is established on its own terms.
- 8.6.3 Where the condition is established, Section 12 applies and no outcome of Westmark Defence Supplier Mark is available irrespective of the score achieved.

8.7 The scoring record

For every requirement, the Assessor records:

Field	Content
Requirement reference	The WMA-SBD-CAT-001 reference
Score	0, 1, 2, Not Applicable, or Out of Scope
Evidence relied upon	Each item examined, identified sufficiently to be retrieved from the file
Sources	The origin of each item, and whether the sources are independent of one another
Engagements	Which sampled engagements the requirement applied to, and the position on each
Corroboration	Present or absent, with the basis where present
Findings testing	Whether an adverse view was put to the Organisation, and its response
Assessor note	The reasoning where the score is not self-evident from the evidence listed

A score recorded without an evidence entry is incomplete and shall not pass technical review.

8.8 Section and overall scoring

- 8.8.1** A section score is the points achieved divided by the points available within that section, expressed as a percentage. Points available is twice the number of requirements scored, after removal of any recorded as Not Applicable or Out of Scope.
- 8.8.2** The overall score is the weighted sum of the section scores, using the weightings at Section 10.
- 8.8.3** Scores are calculated to one decimal place and reported to the nearest whole number. Rounding is applied once, at the overall score. Section scores are not rounded before weighting.
- 8.8.4** An overall score falling within one percentage point below a threshold at Section 11 shall be reviewed by the Technical Reviewer, who examines whether any single scoring decision determines the outcome. Where one decision does determine it, the reviewer tests that decision specifically and records the review. The threshold is not adjusted.

8.9 What the Assessor does not do

- 8.9.1** The Assessor does not advise the Organisation how to raise a score, propose wording, supply a control, or identify which requirement to address first. Improvement actions attached to a Westmark Defence Supplier Conditional outcome state what is deficient. They do not state how to remedy it.
- 8.9.2** The Assessor does not score an Organisation against a requirement outside the assessed scope, against a superseded control set version, or against the Assessor's own view of good practice where that view exceeds the requirement as written.
- 8.9.3** Where an Assessor considers a requirement in WMA-SBD-CAT-001 to be unclear, wrongly calibrated or out of date, the Assessor scores the requirement as written and raises the matter with the Scheme Owner for consideration at the next review of the control set.

9. Evidence sufficiency by requirement type

9.1 Purpose of this section

Section 8 sets the scale. This section sets what an Assessor accepts as evidence for each type of requirement, so that a score of 2 for a governance requirement carries the same meaning as a score of 2 for a technical control. Each requirement in WMA-SBD-CAT-001 carries a type marker, and the sufficiency rules below attach to the marker.

Marker	Requirement type
G	Governance and accountability
P	Process and procedure
R	Record and register
C	Contractual and statutory
T	Technical control
H	Human factor, behaviour and awareness
S	Supply chain

9.2 Type G, governance and accountability

What is being tested: that a named individual holds security risk, exercises it, and is reachable when something goes wrong.

Score	Sufficiency
0	Accountability unnamed, held collectively, or named on paper with no evidence of exercise
1	A named individual, evidenced by the procedure and by one of: a signed approval, a decision record, or testimony from a delivery worker who identifies them correctly
2	A named individual, evidenced by signed approvals across the sampled engagements, and testimony from delivery personnel who identify them without prompting, and at least one instance of the accountability being exercised on a live matter

The exercise test. A governance requirement reaches 2 only where the Assessor can point to an occasion on which the accountability did something. Approval of a plan, refusal of a proposal, resourcing of a control, or a decision recorded following an incident all qualify. An individual who has approved every plan submitted without a recorded question has evidenced signature rather than accountability, and scores 1. Where the Organisation has had no occasion requiring a security decision during the assessment period, the Assessor records this and 2 remains available on the strength of the approval record and the testimony.

9.3 Type P, process and procedure

What is being tested: that a documented process operates in the way it is written.

Score	Sufficiency
0	No document, or a document with no evidence of operation, or practice contradicting the document
1	Document present, and evidence of operation on some sampled engagements, or evidence from a single source
2	Document present, evidence of operation on every sampled engagement to which it applied, corroborated by a source independent of the document itself

Currency. A procedure carrying no review date, or last reviewed more than twenty-four months before the assessment with no evidence of use, does not evidence an operating process and scores 0. A current procedure that has never been applied because the circumstance has not arisen is governed by 8.5 rather than scored 0.

9.4 Type R, record and register

What is being tested: that a record exists, is complete for the assessment period, and was made when the event occurred.

Score	Sufficiency
0	No record, or a record with material gaps across the assessment period, or a record reconstructed for the assessment
1	Record present and substantially complete, with minor gaps the Organisation can explain
2	Record complete for the assessment period, contemporaneous, and consistent with an independent source

Contemporaneity. The Assessor tests whether entries were made at the time. Metadata, sequence, internal consistency, and correspondence with dated events all bear on this. A register in which every entry carries the same creation date scores 0 irrespective of its content.

Completeness. A record is complete where it covers every occasion on which the underlying activity occurred. An incident log holding two entries where interviews disclose four reportable events is incomplete, and the Assessor tests whether the omission engages the disqualifying condition on incident reporting.

9.5 Type C, contractual and statutory

What is being tested: that an obligation arising from a contract, a Security Aspects Letter, a Defence Condition or statute has been received, understood and discharged.

Score	Sufficiency
0	The obligation was not received, not acknowledged where acknowledgement was required, or not discharged
1	The obligation was received and discharged, evidenced from a single source, or discharged inconsistently across the sampled engagements
2	The obligation was received, acknowledged in the form required, discharged on every applicable engagement, and the discharge is corroborated

These requirements are binary at the point of receipt. A signed Security Aspects Letter acknowledgement either exists or does not. A Supplier Assurance Questionnaire is either current or is not. Where the artefact is absent, the score is 0 and no allowance is made for the Organisation's general diligence.

Where the customer did not issue what it should have issued, the Assessor scores the Organisation on what it did about that. An Organisation that identified the absence of a Security Aspects Letter on classified work and raised it with the Contracting Authority evidences the requirement. An Organisation that proceeded without noticing does not.

Statutory requirements covering the Official Secrets Act 1989 and the National Security Act 2023 are evidenced by the declaration record and by testimony that individuals understood what they signed. A signature on a form the signatory cannot describe scores 1.

9.6 Type T, technical control

What is being tested: that a technical control is configured, operating, and applied to the estate it is supposed to cover.

Score	Sufficiency
0	Control absent, unconfigured, applied to part of the estate only, or asserted with no verification
1	Control present and verified on a sample of the estate, or evidenced by policy and testimony without direct verification
2	Control present, directly verified by the Assessor or by a report the Assessor can trace to the estate, applied to the whole estate in scope, and corroborated

Direct verification. For technical requirements the Assessor accepts an observed configuration screen, a management console report, a certificate or scheme report from an independent scheme, or an extract the Assessor can tie to named devices or accounts. A statement that encryption is enabled, standing alone, scores 0.

Certification as evidence. A current Cyber Essentials or Cyber Essentials Plus certificate is accepted as evidence of the controls within its scope, and the Assessor records the scope and date. It does not evidence requirements outside that scope, and it does not substitute for the assessment.

Estate coverage. A control applied to company-issued devices while engagement work is performed on other devices is not applied to the estate in scope. The Assessor establishes what the estate actually is before testing coverage.

9.7 Type H, human factor and behaviour

What is being tested: that the people doing the work understand their obligations and act on them.

Score	Sufficiency
0	No briefing, no record, or delivery personnel unable to describe the obligation when asked
1	Briefing delivered and recorded, and personnel able to describe the obligation in general terms
2	Briefing delivered and recorded, personnel able to describe the specific action they would take, and at least one instance evidencing that they did so

The interview governs this type. A briefing record signed by four people who cannot say what they would do on finding a document left in a corridor scores 0, whatever the record shows. This is the clearest instance in the framework of practice overriding paperwork, and it is deliberate.

Understanding is tested by scenario rather than by recall. The Assessor asks what the individual would do, and does not ask them to name the procedure or quote its clauses.

Reporting culture. Where interviews disclose that individuals would hesitate to report a mistake of their own, the requirement scores no higher than 1 irrespective of the briefing record, and the Assessor records the finding under S6.

9.8 Type S, supply chain

What is being tested: that the Organisation applies to its subcontractors what its customer applies to it.

Score	Sufficiency
0	Subcontractors engaged on work in scope with no security assessment before engagement, or with no oversight during delivery
1	Assessment before engagement evidenced, with oversight during delivery evidenced on some engagements or from a single source
2	Assessment before engagement, flow-down of the applicable conditions, and oversight during delivery, evidenced across every sampled engagement using a subcontractor and corroborated

Flow-down is evidenced by the subcontract, rather than by the Organisation's statement that flow-down occurs. The Assessor examines the subcontract document or the terms incorporated into it.

Self-declaration by the subcontractor is a single source. An Organisation relying wholly on a signed statement from its subcontractor, with no verification of any kind, scores 1 at best.

Where the Organisation engages no subcontractors, the requirements are governed by 8.5 and the applicability cap applies, subject to 10.7.

9.9 Evidence the Assessor does not accept for any requirement type

- A marketing statement, website text or tender response, as evidence of practice
- A document dated within the assessment window that describes activity before that window, without corroboration
- A template supplied by the Scheme Owner as part of Part B, presented unpopulated
- An assurance given by a third party which the Assessor cannot trace to a named person and a date

- An artefact the Organisation declines to allow the Assessor to record on the assessment file, where the ground for declining is not one recognised at 7.10

9.10 Weight of evidence where sources conflict

- 9.10.1** Where documentary evidence and testimony conflict, the Assessor establishes which describes what happened. Testimony from a person who performed the work generally carries greater weight than a record produced by someone who did not.
- 9.10.2** Where observation conflicts with both, observation prevails for the practice observed, and the Assessor records that the conflict was found.
- 9.10.3** A conflict between sources is itself a finding. Where an Organisation's records materially misdescribe its practice, the Assessor considers whether the disqualifying condition on misrepresentation is engaged, and records the consideration whether or not the condition is met.

9.11 Proportionality

- 9.11.1** A requirement states an outcome. The Organisation chooses the means by which it achieves that outcome.
- 9.11.2** The sophistication of the means is not scored. An outcome achieved by simple means in a small organisation scores the same as the same outcome achieved by elaborate means in a large one.
- 9.11.3** An Assessor shall not require a separate document where the outcome is evidenced within an existing one; require a document at all where the outcome is evidenced by observed practice and corroborated record; treat volume of documentation as evidence of control; score down an Organisation for holding one procedure where a larger organisation would hold several; or require a role to be held by a different person from the one holding it, beyond what 6.3 provides.
- 9.11.4** Proportionality applies to every assessment. It is not a concession granted to organisations below a size threshold, and no size threshold is defined.
- 9.11.5** Where an Assessor considers that a requirement cannot be met proportionately by an Organisation of the size assessed, the Assessor records the observation and raises it under 8.9.3. The requirement is scored as written, and the matter is considered at the next review of the control set.
- 9.11.6** Where an Organisation operates at a scale at which policy is set centrally and work is delivered elsewhere, the Assessor tests whether the central position reaches the delivery point. Existence of a corporate position is scored at 1 where the sampled engagements do not evidence its application. Reach is the test at scale, in the same way that basis is the test where roles are concentrated under 6.3.

10. Section weightings

10.1 Status

Weightings are fixed for the version of this framework in which they appear. An Assessor shall not vary a weighting for an individual assessment, and the Scheme Owner shall not vary one by agreement with an Organisation or with a commissioning prime contractor.

10.2 Base weightings

Applying to an assessment at Combined scope.

Ref	Section	Weight
S1	Governance and Accountability	15%
S2	Risk Management and Project Implementation	20%
S3	Contractual, Statutory and Personnel Security	20%
S4	Information and Asset Handling	13%
S5	Cyber and Technical Security	12%
S6	Incident Management and Continuous Assurance	10%
S7	Supply Chain	10%
	Total	100%

10.3 Reasoning

S2 and S3 carry the heaviest weight at 20 per cent each. S2 holds the substance of the Secure by Design approach, being the risk-driven activity performed before delivery starts. S3 holds the obligations that arise from the contract and from statute, which are the obligations a Contracting Authority can point to when something has gone wrong.

S1 at 15 per cent reflects that named accountability is the first principle in both the government and MOD sets, and that its absence undermines every other section. It sits below S2 and S3 because accountability without applied practice is worth less than applied practice with imperfect accountability.

S4 at 13 per cent covers the handling of information, assets and sites. It is weighted below S3 because a substantial part of the handling requirement arises from the contractual conditions scored at S3, and weighting both equally would count the same obligation twice.

S5 at 12 per cent covers technical control. It is lower than an information security scheme would set it because this framework assesses an organisation delivering into a customer environment rather than one operating its own estate at scale.

S6 at 10 per cent covers incident management and continuous assurance. The weight understates its significance deliberately, because the most serious failures in this area are handled by the disqualifying conditions at Section 12 rather than by score.

S7 at 10 per cent covers supply chain. Where an Organisation subcontracts sensitive work, this is the section a prime contractor reads first, and MOD treats supply chain engagement as a principle in its own right. Where an Organisation subcontracts nothing, 10.7 applies.

10.4 Redistribution

10.4.1 Where a section is out of scope under 2.2, recorded as Insufficient Basis under 8.5.4, or recorded as Not Engaged under 10.7, its weight is redistributed across the remaining assessed sections in proportion to their base weights.

10.4.2 Redistribution is calculated at full precision. The tables below show results to one decimal place for reference. The calculation itself uses unrounded values, and rounding is applied once at the overall score in accordance with 8.8.3.

10.4.3 The redistribution factor is 100 divided by the sum of the base weights of the assessed sections.

10.5 Operational scope

S5 out of scope. Redistribution factor 100 divided by 88.

Ref	Section	Weight
S1	Governance and Accountability	17.0%
S2	Risk Management and Project Implementation	22.7%
S3	Contractual, Statutory and Personnel Security	22.7%
S4	Information and Asset Handling	14.8%
S6	Incident Management and Continuous Assurance	11.4%
S7	Supply Chain	11.4%

10.6 Cyber scope

A Cyber assessment carries no section-level redistribution and uses the base weightings at 10.2. Requirements within S4 marked Operational are recorded Out of Scope under WMA-SBD-CAT-001 C4.1, and their points leave the S4 denominator.

10.7 Sections recorded as Not Engaged

10.7.1 An Organisation that does not subcontract any work within scope may have S7 recorded as Not Engaged.

10.7.2 Not Engaged is available for S7 only. No other section may be recorded on this basis.

10.7.3 Not Engaged is declared at scoping under 7.3, before sampling begins. It shall not be recorded after the Assessor has selected the sample.

10.7.4 The Assessor shall verify the declaration during sampling. Where any sampled engagement discloses a subcontractor engaged on work within scope, the declaration falls, S7 is assessed, and the Assessor records that the declaration was contradicted by the evidence.

10.7.5 Where S7 is recorded as Not Engaged, its weight is redistributed under 10.4, no confidence cap arises, and the assurance statement and certificate state that the Organisation was assessed on the basis that it engages no subcontractors on work within scope.

10.7.6 The Organisation shall notify the Scheme Owner before engaging a subcontractor on work within scope during the currency of the outcome. Section 13 governs the review that follows.

10.8 Relationship to 8.5.4

Clause 8.5.4 is read subject to 10.7. The applicability cap and the Insufficient Basis record apply to requirements recorded as Not Applicable within an assessed section. They do not apply to S7 where Not Engaged has been declared and verified under 10.7. The distinction is between a circumstance that did not arise during the assessment period, which the cap addresses, and a circumstance that does not arise in the Organisation's model of delivery, which 10.7 addresses through disclosure on the certificate rather than through a scoring penalty.

10.9 Section floors

10.9.1 An outcome of Westmark Defence Supplier Mark is not available where any assessed section scores below 50 per cent, irrespective of the overall score.

10.9.2 A section scoring below 40 per cent generates a mandatory improvement action, irrespective of the outcome awarded.

10.9.3 The floors exist because a weighted average allows strength in one area to conceal absence in another. An Organisation scoring 95 per cent across six sections and 20 per cent on contractual and statutory security reaches an overall figure above the Confirmed threshold while holding a deficiency a Contracting Authority would treat as disqualifying in itself.

10.9.4 Where a floor is breached and no disqualifying condition is met, the outcome is Westmark Defence Supplier Conditional and the improvement actions address the section that breached the floor.

10.10 Review of weightings

Weightings are reviewed on each issue of this framework. A change to weightings shall be recorded in the change log with the reasoning, and takes effect for assessments agreed after the issue date in accordance with 7.4.

11. Outcomes, thresholds and confidence

11.1 The three outcomes

One of three outcomes is recorded at the end of every assessment. No other outcome label is used, and no qualifier, grade, band, star or tier is added to any of them.

Outcome	Requirements
Westmark Defence Supplier Mark	Overall score of 80 per cent or above, no assessed section below 50 per cent, no disqualifying condition met, and the evidence consistent across the project sample. A confidence level is recorded.
Westmark Defence Supplier Conditional	Overall score of 60 per cent or above, no disqualifying condition met, and the outcome not qualifying as Confirmed. Improvement actions are attached and must be completed within the period stated.
Not Confirmed	Overall score below 60 per cent, or any disqualifying condition met. No assurance statement is issued.

11.2 Westmark Defence Supplier Mark

- 11.2.1** All of the following shall be satisfied: overall weighted score of 80 per cent or above; no assessed section scoring below 50 per cent, in accordance with 10.9.1; no disqualifying condition at Section 12 met; evidence consistent across the project sample, in accordance with 11.5; and technical review completed under 6.8.
- 11.2.2** A confidence level is recorded in accordance with 11.6. The confidence level qualifies the outcome and is stated wherever the outcome is claimed.
- 11.2.3** An outcome of Westmark Defence Supplier Mark is valid for twenty-four months from the date of issue, subject to Section 13.

11.3 Westmark Defence Supplier Conditional

- 11.3.1** Westmark Defence Supplier Conditional is a positive outcome carrying defined improvement actions. It is not a failure and it is not a probationary form of Confirmed. It records that the Organisation's position is sound in substance with identified deficiencies to be addressed.
- 11.3.2** The outcome is awarded where the overall score is 60 per cent or above, no disqualifying condition is met, and one or more of the following applies: the overall score is below 80 per cent; an assessed section scores below 50 per cent; or the evidence is inconsistent across the project sample to the degree described at 11.5.
- 11.3.3** Improvement actions. The assurance statement states each action, the requirement it relates to, and the date by which it is to be completed. The completion period is set by the Assessor having regard to what the action requires, within a range of three to six months from issue. A single completion date applies to all actions attached to an outcome.
- 11.3.4** Improvement actions state what is deficient. They do not state how to remedy it, in accordance with 8.9.1.
- 11.3.5** Verification. The Organisation submits evidence of completion by the stated date. The Scheme Owner verifies. Verification is conducted by examination of the evidence submitted, and may include a site visit where the action concerns practice rather than documentation.
- 11.3.6** On verification. Where all actions are verified as complete, the outcome converts to Westmark Defence Supplier Mark for the remainder of the original validity period, and a confidence level is recorded at that point. Conversion does not extend validity.
- 11.3.7** On failure to complete. Where actions are not completed by the stated date, the outcome lapses. The register is updated. The Organisation shall cease all claim in accordance with Section 14.
- 11.3.8** Extension. The Scheme Owner may extend the completion date once, by up to three months, on written request received before the original date, where the Organisation evidences that completion is under way and delayed by a cause outside its control. An extension is recorded on the register.
- 11.3.9** An outcome of Westmark Defence Supplier Conditional is valid for twenty-four months from the date of issue, subject to completion of the improvement actions and to Section 13.

11.4 Not Confirmed

- 11.4.1** Recorded where the overall score is below 60 per cent, or where any disqualifying condition at Section 12 is met irrespective of score.
- 11.4.2** No assurance statement is issued and no certificate is issued.
- 11.4.3** The Organisation receives a finding report setting out the outcome, the basis for it, the evidence supporting it, the score achieved by section, and each disqualifying condition met with the evidence relied upon.
- 11.4.4** The Organisation holds no outcome and shall make no claim of any kind arising from the assessment, including any statement that an assessment was undertaken, in accordance with 14.3.
- 11.4.5** A Not Confirmed outcome is recorded on the assessment file and is not published on the register. The register records outcomes held. It does not publish the identity of organisations that did not achieve one.
- 11.4.6** Reassessment. An Organisation recorded as Not Confirmed may seek reassessment no earlier than six months from the date of the finding report. Reassessment is a full assessment against the control set current at the date of the reassessment agreement. It is not a review of the previous finding.
- 11.4.7** Where a Not Confirmed outcome arose from the disqualifying condition on material misrepresentation, the reassessment interval is twelve months and the previous finding is disclosed to any prime contractor commissioning the reassessment.

11.5 Consistency across the project sample

- 11.5.1** Consistency is assessed across the sample as a whole, distinct from the consistency test applied to an individual requirement at 8.4.
- 11.5.2** The sample is consistent where the Organisation's security position holds across the engagements examined, allowing for proportionate variation between engagements of different sensitivity.
- 11.5.3** The sample is inconsistent where any of the following is found: one engagement was managed to a materially different standard from the others, with no explanation grounded in the risk; security practice was applied on engagements for a customer that audits, and absent on engagements for a customer that does not; practice deteriorated across the assessment period rather than being sustained; or a single engagement carries the whole of the evidence for several sections.
- 11.5.4** Inconsistency prevents Westmark Defence Supplier Mark under 11.2.1. Where the score would otherwise support Confirmed, the outcome is Westmark Defence Supplier Conditional and the improvement actions address the inconsistency found.
- 11.5.5** The second limb of 11.5.3 is examined specifically. An Organisation performing to standard only where it is watched has not evidenced a security posture, and the Assessor records the finding whether or not it determines the outcome.

11.6 Confidence levels

- 11.6.1** A confidence level is recorded within a Westmark Defence Supplier Mark outcome. It expresses the Assessor's judgement of the strength and consistency of the evidence. It is a separate judgement from the score, and a high score does not produce a high confidence level.

Level	Basis
High	Evidence is consistent, corroborated from multiple sources, and observed across the full project sample. The Assessor would expect materially similar findings on reassessment.
Moderate	Evidence is present and sufficient, drawn from a narrower sample or a smaller range of sources, or less consistent between engagements.
Limited	Evidence meets the threshold while resting substantially on stated process, on a single engagement, or on corroboration that could not be fully tested.

11.6.2 Mandatory caps. Confidence is capped at Limited where any of the following applies: fewer than three engagements were available for sampling, under 7.6.4; unaccompanied interview with delivery personnel was declined, under 7.8.2; no observation of any kind was conducted, under 7.9.3; or a section is recorded as Insufficient Basis, under 8.5.4.

11.6.3 Cap at Moderate. Confidence is capped at Moderate where the assessment was conducted wholly remotely under 7.9.4, or where a requirement applied to a single sampled engagement across more than one section under 8.4.2.

11.6.4 Where more than one cap applies, the lowest governs.

11.6.5 The Assessor records the reasoning for the confidence level on the assessment file in every case, including where a cap determined it.

11.6.6 Confidence is recorded for Westmark Defence Supplier Mark only. An Westmark Defence Supplier Conditional outcome carries improvement actions rather than a confidence level, and a confidence level is recorded on conversion under 11.3.6.

11.7 Score and outcome are distinct

11.7.1 The score determines eligibility for an outcome. It does not determine the outcome by itself. An Organisation scoring 94 per cent with a disqualifying condition met is recorded as Not Confirmed.

11.7.2 The numeric score is disclosed to the Organisation, by section and overall, and is not published on the register or permitted in any claim, in accordance with 14.5.

11.7.3 Where an assessment is commissioned by a prime contractor under a Track 2 arrangement, the section scores are disclosed to the commissioning prime with the Organisation's written consent, obtained at scoping. Where consent is withheld, the prime receives the outcome, the scope, the confidence level, any improvement actions, and any limitation recorded.

11.8 Summary of determination

The Assessor applies the following in order. The first condition met determines the outcome.

Step	Test	Outcome
1	Is any disqualifying condition at Section 12 met?	Not Confirmed
2	Is the overall score below 60 per cent?	Not Confirmed
3	Is the overall score below 80 per cent?	Westmark Defence Supplier Conditional
4	Does any assessed section score below 50 per cent?	Westmark Defence Supplier Conditional
5	Is the sample inconsistent under 11.5.3?	Westmark Defence Supplier Conditional
6	Otherwise	Westmark Defence Supplier Mark, with a confidence level recorded under 11.6

12. Disqualifying conditions

12.1 Effect

- 12.1.1** An outcome of Westmark Defence Supplier Mark shall not be awarded where any disqualifying condition in this section is found, irrespective of the overall score and irrespective of any section score.
- 12.1.2** Where a disqualifying condition is found, the outcome is Not Confirmed. Westmark Defence Supplier Conditional is not available as an intermediate position.
- 12.1.3** These conditions are applied consistently across every assessment. They are not subject to waiver, mitigation by performance elsewhere, or agreement with the Organisation or a commissioning prime contractor.

12.2 Applicability

- 12.2.1** A condition applies only where the circumstance it addresses arises in the Organisation's delivery. A condition addressing Security Aspects Letters does not apply to an Organisation that has never been issued one and has undertaken no work requiring one.
- 12.2.2** Where a condition does not apply, the Assessor records it as such with the basis, in the same manner as a requirement recorded Not Applicable under 8.5.2.
- 12.2.3** A condition is not disapplied because the circumstance arose on an engagement outside the project sample. Where the Assessor becomes aware of the circumstance from any source, it is examined.

12.3 Evidence standard

- 12.3.1** A disqualifying condition shall be established on corroborated evidence in accordance with 8.3. A single source does not establish a condition.
- 12.3.2** The Assessor shall put the proposed finding to the Organisation under 7.11 and give it opportunity to produce further evidence before the finding is settled. A condition settled without that opportunity has not been established in accordance with this framework.
- 12.3.3** Every finding of a disqualifying condition shall be reviewed by the Technical Reviewer under 6.8, who examines whether the evidence recorded establishes the condition on its own terms.
- 12.3.4** The Assessor records the condition, the evidence, the Organisation's response, and the basis for the conclusion.

12.4 Relationship to scoring

- 12.4.1** A score of 0 against a linked requirement obliges the Assessor to test whether the corresponding condition is met, under 8.6.2. It does not establish the condition.
- 12.4.2** A condition may be established where the linked requirement scored above 0, because the conditions are drawn more narrowly than the requirements and address a specific state of affairs rather than a general shortfall.
- 12.4.3** Scoring continues to completion even where a condition has been found. The finding report states the score achieved, so that the Organisation understands its position across the framework rather than only the matter that determined the outcome.

12.5 The conditions

Ref	Condition	Test
DC-1	No security procedure	The Organisation holds no documented procedure governing how security requirements are identified, assessed and controlled. Or a procedure exists, has not been reviewed within the preceding twenty-four months, and cannot be shown to be in use.
DC-2	No named accountability	No individual holds accountability for security risk, or accountability is held collectively, or the individual named cannot be identified by any person interviewed and no record evidences the accountability being exercised during the assessment period.

Ref	Condition	Test
DC-3	No engagement-level security risk assessment	Across the project sample, the Organisation cannot produce an engagement-level security risk assessment for work delivered into a sensitive environment. A corporate risk register, a health and safety risk assessment, or a generic assessment applied unchanged across engagements does not satisfy this test.
DC-4	Classified work undertaken without security aspects being defined	A Security Aspects Letter was issued and no signed acknowledgement was returned before work began. Or the Organisation undertook work it knew or ought to have known was classified at OFFICIAL-SENSITIVE or above, no Security Aspects Letter or equivalent written notice was issued, and the Organisation neither raised the absence with the Contracting Authority nor recorded any consideration of it.
DC-5	Personnel granted access without screening	An individual was granted access to controlled material, a controlled site, or a customer system without the baseline screening required for that access, and without a clearance or written escort arrangement where the contract or establishment required one.
DC-6	Cyber contractual obligations not discharged	The Organisation holds a contract carrying DEFCON 658 and has no Supplier Assurance Questionnaire current for that contract, or has an outcome of Not Met with no Cyber Implementation Plan submitted, and cannot evidence that the position has been raised with the Contracting Authority.
DC-7	Unmanaged information exposure	Controlled information was stored, transmitted or disposed of in a manner creating foreseeable exposure, the Organisation became aware of it, and no action was taken. The condition turns on the absence of action following discovery rather than on the exposure itself.
DC-8	Incident reporting absent or unused	No incident reporting process exists. Or a process exists and was not invoked on any identifiable occasion during the assessment period, where evidence establishes that reportable events occurred.
DC-9	Loss or compromise not reported to the required recipients	Defence Related Classified Material was lost or compromised and the Organisation did not report it to the Contracting Authority, or did not report it to the Defence Industry Warning, Advice and Reporting Point, and cannot evidence that it was directed otherwise in writing by the Contracting Authority.
DC-10	Uncontrolled subcontractor activity	A subcontractor was engaged on sensitive work with no security assessment before engagement. Or a subcontractor operated on sensitive work with no oversight during delivery and with the applicable security conditions not incorporated into the subcontract.
DC-11	Material misrepresentation or obstruction	The Organisation provided information to the Assessor which is subsequently shown to be false or materially misleading. Or the Organisation obstructed access to evidence the Assessor required, other than on a ground recognised at 7.10. Or the Organisation made a claim in respect of an outcome under this framework which breaches Section 14 and which was not corrected on notice.

12.6 Notes on individual conditions

DC-2 is satisfied by the absence of accountability rather than by imperfection in how it is exercised. An individual who is named, identified by staff, and has approved plans meets the test even where the quality of that exercise scores poorly at S1.

DC-4 does not penalise an Organisation for a failure by the Contracting Authority. Where no Security Aspects Letter was issued and the Organisation identified that, raised it, and recorded the response, the condition is not met and the matter is scored at S3.

DC-5 applies to baseline screening as much as to National Security Vetting. An Organisation using escorted uncleared personnel remains obliged to have screened them to the baseline standard for access to OFFICIAL and OFFICIAL-SENSITIVE material. This is the condition most frequently found among organisations new to defence work.

DC-6 applies only where DEFCON 658 is invoked in a contract the Organisation holds. The condition addresses the absence of the required position rather than the content of the position. A low Cyber Risk Profile properly assessed and evidenced does not engage it.

DC-9 stands separately from DC-8 because an Organisation may operate an internal incident process competently while failing to make the external report the contractual conditions require. Internal handling does not discharge the external obligation.

DC-11 covers three distinct behaviours in one condition because the effect on the scheme is the same in each case. The third limb applies to a holder of an existing outcome and is the route by which a claim breach reaches withdrawal under Section 13.

12.7 Conditions found after issue

12.7.1 Where a disqualifying condition is found after an outcome has been issued, whether during a review under Section 13, during a reassessment, or on information received, the Scheme Owner shall examine whether the condition existed at the date of assessment.

12.7.2 Where the condition existed at the date of assessment and was not disclosed to the Assessor, the outcome is withdrawn and DC-11 is considered in respect of the non-disclosure.

12.7.3 Where the condition arose after the date of assessment, the outcome is suspended and Section 13 governs.

12.7.4 A withdrawal under this clause is recorded on the register for twelve months and is disclosed at any subsequent assessment.

12.8 Notification

12.8.1 The Organisation is informed in writing of any disqualifying condition found, the evidence, and the basis for the conclusion.

12.8.2 Where the assessment was commissioned by a prime contractor under a Track 2 arrangement, the prime is informed that the outcome is Not Confirmed. The detail of the condition is disclosed to the prime only with the Organisation's consent, except where the condition is DC-9 or DC-11.

12.8.3 The exception at 12.8.2 exists because a failure to report loss of classified material, and a material misrepresentation to an assessor, each bear directly on whether the prime can rely on the Organisation. Withholding those findings from a party who commissioned the assessment would leave the Scheme Owner complicit in the position it identified.

12.8.4 The Scheme Owner does not report a disqualifying condition to a Contracting Authority, a Designated Security Authority, or any other body, except where required by law or where the Organisation consents. The Scheme Owner is not a regulator and holds no reporting duty into the defence security system.

13. Outcome lifecycle

13.1 Validity

13.1.1 An outcome is valid for twenty-four months from the date of issue, subject to this section.

13.1.2 Validity is not extended by conversion of a Westmark Defence Supplier Conditional outcome under 11.3.6, by completion of improvement actions, or by any review conducted during the period.

13.1.3 An outcome expires at the end of its validity period whether or not reassessment has been sought. There is no automatic renewal and no period of grace.

13.1.4 The Scheme Owner shall notify a holder of impending expiry at four months and at two months before the expiry date.

13.2 Continuing obligations of a holder

A holder shall notify the Scheme Owner of each of the following within twenty working days of it occurring, other than where a shorter period is stated.

Event	Reference	Period
Change in the individual holding accountability for security risk	6.1.4	20 working days
A circumstance previously recorded Not Applicable arising	8.5.5	20 working days
Engagement of a subcontractor on work within scope, where S7 was recorded Not Engaged	10.7.6	Before engagement
Change of control, ownership or legal form of the Organisation		20 working days
Change of registered name, or addition or removal of a trading name within scope		20 working days
Delivery of work of a type outside the assessed scope		Before delivery
Lapse, withdrawal or reduction in scope of any certification relied upon as evidence at assessment		20 working days
A security incident involving loss or compromise of controlled information		10 working days
A circumstance that would engage a disqualifying condition at Section 12		10 working days
Investigation or enforcement action by a Contracting Authority or a Designated Security Authority into a matter within scope		10 working days
Insolvency, administration, receivership or an arrangement with creditors		10 working days

Failure to notify is itself a ground for suspension under 13.6, and where the failure was deliberate it engages DC-11.

13.3 Annual declaration

13.3.1 At the twelve month point in the validity period, a holder shall submit an annual declaration confirming that the matters at 13.2 have been notified or that none has arisen; that the individual holding accountability remains in post, or the identity of the successor; that the assessed scope remains an accurate description of the work delivered; that any improvement actions verified under 11.3.5 remain in effect; and the number of engagements within scope delivered in the preceding twelve months.

13.3.2 The declaration is signed by the individual holding accountability at 6.1.

13.3.3 The declaration is a self-declaration. It is not an assessment, it produces no score, and it does not alter the outcome or the confidence level.

13.3.4 A declaration not received within twenty working days of the due date results in suspension under 13.6.

13.3.5 Where a declaration discloses a matter engaging 13.4, the Scheme Owner determines the review type under 13.5.

13.4 Triggers for review

The Scheme Owner shall consider whether a review is required on:

- Receipt of a notification under 13.2
- Receipt of an annual declaration disclosing a change
- Information received from a Contracting Authority, a prime contractor, or a customer of the holder
- Information received from any source alleging a matter that would engage a disqualifying condition
- A claim by the holder which appears to breach Section 14
- Issue of a control set version with a stated application date under 7.4.5

13.5 Types of review

Type	Conducted by	Scope	Outcome
Desk review	Assessor or Scheme Owner	Examination of documents submitted in response to the trigger	Outcome unaffected, or escalation to targeted review
Targeted review	Assessor	Examination of the sections or requirements affected by the trigger, which may include interview and observation	Outcome unaffected, outcome amended, suspension, or withdrawal
Full reassessment	Assessor	Assessment in accordance with Section 7 against the control set current at the date of the reassessment agreement	New outcome replacing the existing one

13.5.1 The Scheme Owner determines the review type having regard to what the trigger affects and to the evidence available.

13.5.2 A change in the individual holding accountability is examined by desk review as a minimum, and by targeted review where the assessment relied on the exercise test at 9.2.

13.5.3 A change of control is examined by targeted review as a minimum.

13.5.4 Delivery of work outside the assessed scope requires full reassessment before the outcome extends to that work. The existing outcome remains valid for the scope assessed, and the holder shall not claim it in respect of the new work.

13.5.5 The cost of a review is borne by the holder in accordance with the scheme terms, and the fee shall not vary with the review's conclusion.

13.6 Suspension

13.6.1 The Scheme Owner shall suspend an outcome where an annual declaration is overdue under 13.3.4; a notification required under 13.2 was not made and the matter has come to light; a disqualifying condition has arisen since the date of assessment, under 12.7.3; a review has been triggered and the holder does not provide the evidence required to conduct it; or a claim breaching Section 14 has not been corrected on notice, pending the withdrawal decision under 14.8.

13.6.2 Effect of suspension. From the date of suspension the holder shall cease all claim to the outcome in every medium; remove the Westmark Assurance mark within ten working days; and inform any party to whom the outcome was claimed in a live tender.

13.6.3 The register records the outcome as suspended, with effect from the date of suspension.

13.6.4 Duration. Suspension continues until the matter is resolved. Where it remains unresolved three months after the date of suspension, the outcome is withdrawn.

13.6.5 Reinstatement. On resolution, the outcome is reinstated for the remainder of its original validity period. Reinstatement does not extend validity, and the register records the period of suspension for twelve months following reinstatement.

13.7 Withdrawal

- 13.7.1** The Scheme Owner shall withdraw an outcome where a disqualifying condition existed at the date of assessment and was not disclosed, under 12.7.2; a suspension has run for three months without resolution, under 13.6.4; a claim breaching Section 14 was not corrected, or was repeated, or asserted government or MOD certification, under 14.8; the holder ceases to exist as a legal entity, or the assessed entity is no longer the entity delivering the work; or the holder requests withdrawal under 13.8.
- 13.7.2** Effect of withdrawal. The outcome ceases on the date of the withdrawal decision. The obligations at 13.6.2 apply.
- 13.7.3** The register records the withdrawal for twelve months. Where the ground was non-disclosure of a disqualifying condition or misrepresentation, the record is disclosed at any subsequent assessment.
- 13.7.4** A withdrawn outcome is not reinstated. An Organisation seeking an outcome after withdrawal is fully reassessed, subject to the interval at 11.4.6 or 11.4.7 where the ground engaged those clauses.

13.8 Voluntary surrender

- 13.8.1** A holder may surrender an outcome at any time by written notice.
- 13.8.2** Surrender takes effect on receipt. The obligations at 13.6.2 apply.
- 13.8.3** The register records the outcome as surrendered. Surrender is recorded without adverse notation, and is distinguished on the register from withdrawal.
- 13.8.4** The Scheme Owner shall not accept surrender where a review or an investigation into a disqualifying condition is in progress. In that circumstance the review concludes and the outcome is determined under 13.6 or 13.7.

13.9 Reassessment

- 13.9.1** A holder seeking to maintain an outcome beyond its validity period shall be reassessed before expiry.
- 13.9.2** Reassessment is a full assessment under Section 7 against the control set current at the date of the reassessment agreement, in accordance with 7.4.4.
- 13.9.3** The Assessor conducting a reassessment may be the Assessor who conducted the previous assessment. Where the same Assessor conducts three consecutive assessments of the same Organisation, the fourth shall be conducted by a different Assessor. Where no other Assessor is available, the technical review of that assessment shall be conducted externally.
- 13.9.4** The previous assessment file is available to the Assessor conducting a reassessment. The Assessor examines whether matters previously found have been sustained, and records the comparison.
- 13.9.5** A reassessment produces its own outcome. A previous outcome creates no presumption in favour of the same result.

13.10 Appeal

- 13.10.1** An Organisation may appeal against an outcome of Not Confirmed; a finding of a disqualifying condition; a confidence level recorded; a suspension or withdrawal decision; or an improvement action attached to a Westmark Defence Supplier Conditional outcome.
- 13.10.2** Grounds. An appeal shall state which of the following is relied upon: the framework or the control set was applied incorrectly; evidence submitted was not considered; the evidence recorded does not support the finding made; or a procedural requirement of this framework was not observed. Disagreement with a judgement properly made on evidence properly considered is not a ground of appeal.
- 13.10.3** Period. An appeal shall be lodged within twenty working days of the decision appealed against.
- 13.10.4** Independence. An appeal shall be determined by an individual who conducted neither the assessment nor its technical review, and who has no relationship with the Organisation engaging 6.9.7. Where the Scheme Owner has no such individual available internally, the appeal shall be determined by an external reviewer appointed under a standing arrangement and bound by the terms at Section 15.
- 13.10.5** Determination. The appeal is determined within thirty working days of being lodged. The determination may uphold the decision; set aside the decision and substitute a different outcome, confidence level or improvement action; or direct that the assessment, or a defined part of it, be conducted again.

13.10.6 The determination is final within the scheme. It is issued in writing with reasons.

13.10.7 Effect pending determination. A suspension remains in effect during an appeal. A withdrawal takes effect on the decision date and is reversed where the appeal succeeds. An outcome is not issued while an appeal against Not Confirmed is pending.

13.10.8 Fee. An appeal fee is payable on lodging, at the rate stated in the scheme terms. The fee is refunded where the appeal succeeds in whole or in part.

13.11 Complaints

13.11.1 A complaint about the conduct of an assessment, an Assessor, or the administration of the scheme is made in writing to the Scheme Owner.

13.11.2 A complaint is acknowledged within five working days and determined within thirty working days.

13.11.3 A complaint about an Assessor is determined by an individual other than that Assessor.

13.11.4 A complaint is distinct from an appeal. A complaint about conduct does not alter an outcome. Where a complaint discloses a procedural failure affecting an outcome, the Scheme Owner refers the matter to the appeal route and informs the Organisation.

13.11.5 The Scheme Owner maintains a record of complaints, their determination, and any change to the scheme arising. The record is reviewed at each issue of this framework.

14. Representation of outcomes

14.1 Governing principle

An organisation holding an outcome under this framework may describe that outcome accurately and may not describe it as anything else. The wording at 14.3 and 14.4 is the full extent of what may be claimed. Departure from it, including paraphrase that alters meaning, is a breach of the scheme terms.

This section is binding on the organisation from the date the assurance statement is issued and continues to bind it after the outcome lapses, to the extent that it governs claims that may no longer be made.

14.2 Elements every claim must carry

A claim made in any medium shall state the outcome awarded, using the label at Section 11; the assessed scope; the date of assessment; the version of WMA-SBD-CAT-001 against which the assessment was conducted; the certificate reference; and the expiry date of the outcome.

A claim omitting any of these is incomplete and is treated as a breach. The requirement exists so that a prime contractor reading the claim can establish what was assessed, when, and against which control set, without contacting Westmark Assurance.

14.3 Permitted claim wording: short form

For use in email signatures, capability statements, website footers and similar. The bracketed fields are completed by the organisation. No other text may be added within or adjacent to the claim in a way that qualifies it.

Westmark Defence Supplier Mark — Westmark Assurance Defence Supplier Mark Assurance Standard (WMA-SBD-001), [Operational / Cyber / Combined] scope, [confidence level] confidence. Assessed [date] against WMA-SBD-CAT-001 v[x.x]. Certificate [ref]. Valid until [date].

Westmark Defence Supplier Conditional — Westmark Assurance Defence Supplier Mark Assurance Standard (WMA-SBD-001), [Operational / Cyber / Combined] scope. Assessed [date] against WMA-SBD-CAT-001 v[x.x], with improvement actions outstanding. Certificate [ref]. Valid until [date].

An organisation holding Westmark Defence Supplier Conditional shall state that improvement actions are outstanding wherever the outcome is claimed. Presenting a Conditional outcome without that qualification is a breach.

An organisation recorded as Not Confirmed holds no outcome and shall make no claim of any kind arising from the assessment, including any statement that an assessment was undertaken.

14.4 Permitted claim wording: tender positioning statement

For use in pre-qualification questionnaires, invitation to tender responses and framework submissions. The organisation may delete sentences that do not apply to its scope. It may not add to the text.

[Organisation] holds Westmark Defence Supplier Mark under the Westmark Assurance Defence Supplier Mark Assurance Standard (WMA-SBD-001), assessed at [scope] scope on [date] against control set WMA-SBD-CAT-001 v[x.x], certificate [ref].

The assessment is an independent examination of how [Organisation] identifies, controls and evidences security risk across the engagements it delivers. It examined a sample of [n] projects selected by the assessor, and drew on documentary, observational, testimonial and record evidence. It covered governance and named accountability for security risk, project-level security risk assessment, the handling of contractual security conditions and classified material, personnel screening, incident recognition and reporting, continuous assurance, and the management of subcontractors engaged on sensitive work.

The outcome is a judgement by Westmark Assurance. It is independent of government and of the Ministry of Defence, and it confers no certification, accreditation or approval by either. It does not substitute for any assessment carried out by a Contracting Authority, a prime contractor or a Designated Security Authority, and [Organisation] will support such assessment on request. The current status of this outcome may be verified at [verification address].

14.5 Prohibited claims

An organisation holding an outcome shall not state or imply any of the following. The list is illustrative of the boundary rather than exhaustive.

Standing the outcome does not confer

- Certification, accreditation, approval, endorsement or recognition by government, the Ministry of Defence, the National Cyber Security Centre, the Government Security Group, or any Contracting Authority
- Compliance with the government Secure by Design policy, or that the organisation meets the ten published Secure by Design principles
- Compliance with MOD Secure by Design, or with Industry Security Notice 2023/09
- Satisfaction of DEFCON 658, Defence Standard 05-138, or any Cyber Risk Profile requirement
- Cyber Essentials, Cyber Essentials Plus, Defence Cyber Certification, ISO/IEC 27001, or any other certification the organisation does not separately hold
- Facility Security Clearance, List X status, or any National Security Vetting standing for the organisation or its personnel
- Any standing under GovAssure or the Cyber Assessment Framework

Confusion with other schemes

- Any use of the term Secured by Design, which is a separate police-owned scheme concerned with physical product and development design
- Any use of a government crest, departmental logo, MOD branding, or the branding of a prime contractor

Overreach beyond what was assessed

- Extension of the claim to a scope that was not assessed, including any cyber claim by a holder of an Operational scope outcome
- Extension of the claim to a parent, subsidiary, group company, joint venture, franchise or trading name that was not itself assessed
- Extension of the claim to work of a type not represented in the assessed project sample
- Any statement that subcontractors of the organisation hold or are covered by the outcome

Currency and precision

- Continued claim after the outcome has lapsed, been suspended or been withdrawn
- Claim against a superseded version of WMA-SBD-CAT-001 without stating the version assessed
- Publication of the numeric score or percentage achieved, or of section-level scores
- Any statement that the organisation achieved the highest, or a leading, or a comparative result

14.6 Use of the Westmark Assurance mark

An organisation holding Westmark Defence Supplier Mark or Westmark Defence Supplier Conditional is granted a non-exclusive, non-transferable licence to display the Westmark Assurance outcome mark issued to it, for the duration of the outcome. Conditions of use:

- The mark is displayed only in the form issued, without alteration to its proportions, colour or setline
- The mark carries the certificate reference and expiry date, which are integral to it and shall not be cropped or obscured
- The mark is not applied to a product, a deliverable, a report, a drawing, a vehicle livery or an item of personal protective equipment
- The mark is not used in a manner suggesting that a specific project, deliverable or subcontractor was assessed
- The mark is removed from all media within ten working days of the outcome lapsing, being suspended or being withdrawn

14.7 Verification and the public register

Westmark Assurance maintains a register recording, for each outcome, the organisation, the scope, the outcome label and confidence level, the assessment date, the control set version, the certificate reference, and the expiry date.

The register is available to any Contracting Authority, prime contractor or customer seeking to verify a claim. Numeric scores are not published on the register. Suspended and withdrawn outcomes are shown as such for twelve months following the change of status. An organisation consents to this publication as a condition of assessment.

14.8 Breach

On becoming aware of a claim outside the terms of this section, Westmark Assurance will notify the organisation in writing identifying the claim and the term breached; require correction within ten working days, or a shorter period where the claim is made in a live tender; and record the breach on the assessment file.

Where correction is not made, or where the breach is repeated, or where the claim asserted government or MOD certification, the outcome is withdrawn under Section 13 and the register is updated. Westmark Assurance may notify a Contracting Authority or prime contractor to whom the claim was made. Withdrawal for misrepresentation is recorded on the register for twelve months and is disclosed in any subsequent assessment of the organisation.

14.9 Claims by Westmark Assurance

Westmark Assurance will not name an organisation as a client, publish a case study, or reference an assessment in its own marketing without the organisation's written consent. Consent is sought separately from the assessment and is never a condition of it.

15. Scheme terms, conduct and confidentiality

15.1 The assessment agreement

15.1.1 No assessment begins until the Organisation has signed an assessment agreement incorporating this framework and the scheme terms.

15.1.2 The agreement records the scoping decisions at 7.3, the fee, and the consents at 15.5.

15.1.3 By signing, the Organisation accepts this framework and the control set version stated; consents to the register entry and publication at 14.7; consents to the disclosures at 15.5; undertakes to provide access to evidence, personnel and premises as Section 7 requires; and accepts the continuing obligations at 13.2 for the period any outcome is held.

15.2 Assessor conduct

An Assessor shall:

- Record observations contemporaneously
- Decline hospitality beyond refreshment taken in the ordinary course of a working day, and offer none
- Decline any gift, benefit or inducement, of any value, offered by the Organisation or by a party connected to it
- Withhold emerging findings from any third party, including a commissioning prime contractor, until the assurance statement or finding report is issued
- Put any view that may be adverse to the Organisation before it is settled, under 7.11
- Comply with the security regulations of any establishment visited, and hold the screening, clearance or escort arrangement that establishment requires
- Complete the conflict declaration at 6.9.10 before the assessment begins

An Assessor shall not:

- Advise the Organisation how to raise a score, under 8.9.1
- Accept a fee, commission or benefit contingent on an outcome, under 6.9.11
- Solicit consultancy work from an Organisation during or arising from an assessment
- Discuss one Organisation's assessment with another Organisation, in any degree of anonymisation
- Remove classified material from an Organisation's premises or from an establishment
- Record classified material on the assessment file beyond what is required to evidence the finding

15.3 Assessor status and screening

15.3.1 An Assessor shall hold baseline screening to the standard applying to the material they will encounter, and shall hold National Security Vetting at the level required where the assessment involves access to material above OFFICIAL-SENSITIVE.

15.3.2 An Assessor shall not accept an assessment requiring access to material above the level for which they are cleared. Where such material arises during an assessment, the Assessor withdraws from examining it, records the withdrawal, and applies 7.10.

15.3.3 An Assessor accessing classified material is subject to the Official Secrets Act 1989 and the National Security Act 2023, and signs a declaration to that effect held by the Scheme Owner.

15.3.4 The Scheme Owner maintains a record of each Assessor's screening and clearance status, reviewed on expiry and annually.

15.4 Confidentiality

15.4.1 The Scheme Owner and every Assessor shall hold in confidence all information obtained in the course of an assessment, and shall not disclose it other than as permitted at 15.5.

15.4.2 The obligation survives completion of the assessment, expiry of any outcome, and termination of the agreement. It continues for seven years from the date the assessment file is closed, matching the retention at 7.13.3.

15.4.3 The obligation binds any external technical reviewer appointed under 6.8.2 and any external appeal reviewer appointed under 13.10.4, who shall each be engaged on terms incorporating this section.

15.4.4 Assessment material is held at OFFICIAL as a minimum and at the highest classification of any material it contains, under 7.13.4. The Scheme Owner shall not accept material above the classification its own arrangements permit it to hold, and shall apply 7.10 where that limit is reached.

15.5 Permitted disclosures

The Scheme Owner may disclose assessment information in the following circumstances and in no others.

Circumstance	Recipient	Extent
Register publication	Any party	The fields at 14.7
Verification of a claim	Any Contracting Authority, prime contractor or customer	The fields at 14.7
Track 2 assessment commissioned by a prime	The commissioning prime	Outcome, scope, confidence level, improvement actions, limitations. Section scores with the Organisation's consent under 11.7.3.
Disqualifying condition DC-9 or DC-11 found on a Track 2 assessment	The commissioning prime	The condition found and the basis for it, without the Organisation's consent, under 12.8.3
Technical review or appeal	The reviewer appointed	The assessment file
Legal requirement	As required	As required, with notice to the Organisation where lawful to give it
Consent	As stated in the consent	As stated in the consent

15.5.1 The disclosure at row four is made without the Organisation's consent. The Organisation's signature on the assessment agreement is its acknowledgement of that term, and the term is drawn to the Organisation's attention at scoping rather than buried in the schedule.

15.5.2 The Scheme Owner shall not disclose a finding to a Contracting Authority, a Designated Security Authority, the Ministry of Defence, or any regulator, except under the legal requirement row. The limit on the Scheme Owner's role at 12.8.4 governs.

15.5.3 The Scheme Owner shall not name an Organisation in marketing, publish a case study, or reference an assessment in its own material without written consent obtained separately from the assessment, under 14.9.

15.6 Obligations of the Organisation

The Organisation shall:

- Provide the pre-assessment submission at 7.5 by the date agreed
- Provide access to personnel for interview, including unaccompanied interview under 7.8.2
- Provide access to premises and, where the customer consents, to a live engagement under 7.9
- Give accurate information, and correct any information found to be inaccurate
- Notify the Assessor of any matter that would engage a disqualifying condition
- Obtain customer consent where an engagement in the sample requires it, and inform the Assessor promptly where consent is refused
- Inform the Assessor of any restriction on disclosure arising under 7.10, and the ground for it

15.7 Data protection

15.7.1 Assessment material includes personal data, including screening records, clearance status, training records and interview notes.

15.7.2 The Scheme Owner processes that data as controller for the purpose of conducting the assessment, maintaining the register, and administering the scheme.

- 15.7.3** The lawful basis is legitimate interests, being the operation of an assurance scheme the Organisation has commissioned, with contract as the basis where the processing is required to perform the assessment agreement.
- 15.7.4** The Scheme Owner shall not record more personal data than the finding requires. Screening status is recorded as held or not held with the date of check. The underlying screening evidence is examined and is not copied to the assessment file.
- 15.7.5** Interview notes record the substance of what was said and the role of the speaker. They shall not attribute a statement to a named individual in the assurance statement, the finding report, or any disclosure to a commissioning prime.
- 15.7.6** The Organisation shall inform its personnel that an assessment is taking place and that interview notes will be held by the Scheme Owner.
- 15.7.7** Retention follows 7.13.3. On expiry of the retention period the file is destroyed by a method preventing recovery, and the destruction is recorded.

15.8 Fees

- 15.8.1** Fees are stated in the assessment agreement and are payable irrespective of the outcome.
- 15.8.2** No fee, discount, rebate or other term shall vary with the outcome awarded, under 6.9.11.
- 15.8.3** Fees for a review under 13.5 and for an appeal under 13.10.8 are stated in the scheme terms.
- 15.8.4** The Scheme Owner shall not offer an assessment at a reduced fee in consideration of consultancy, tooling, licensing or any other engagement with the Organisation.

15.9 Termination

- 15.9.1** Either party may terminate the assessment agreement on written notice before the assessment concludes.
- 15.9.2** Termination by the Organisation after sampling has begun does not produce an outcome, and the Scheme Owner records that the assessment was terminated at the Organisation's request.
- 15.9.3** Where an assessment is terminated after the Assessor has identified a matter engaging a disqualifying condition, the Scheme Owner records the position on the assessment file. No outcome is issued and no report is published. The matter is disclosed at any subsequent assessment of the Organisation.
- 15.9.4** Clause 15.9.3 exists so that termination cannot be used to abandon an assessment that is going badly and start again elsewhere in the knowledge that nothing was recorded.

15.10 Liability

- 15.10.1** An outcome under this framework is an opinion formed on evidence examined within a defined scope, on a sample, at a point in time. It is not a warranty of the Organisation's security posture, and it is not relied upon by the Scheme Owner as such.
- 15.10.2** A party relying on an outcome does so on the terms at Section 14 and on the limitations recorded on the assurance statement.
- 15.10.3** Liability limits, insurance requirements and indemnities are stated in the scheme terms rather than in this framework.

Drafting note for the Scheme Owner: the operative limitation of liability wording belongs in the scheme terms and should be settled with a solicitor before the first certificate is issued. Clause 15.5.1 should be reviewed at the same time.

16. Framework governance

16.1 Ownership

16.1.1 This framework and the control set are owned by Westmark Assurance. No other party may issue, amend, extend or reproduce either, in whole or in part, without written permission.

16.1.2 An Organisation holding an outcome may reproduce this framework internally for the purpose of meeting it, and may provide a copy to a customer or prime contractor who asks on what basis its outcome was awarded.

16.1.3 The Part B templates are licensed to an Organisation on the terms at 16.9.

16.2 Review cycle

16.2.1 This framework is reviewed annually as a minimum.

16.2.2 A review is also conducted on a change to any publication at Section 3 affecting a requirement in this framework or the control set; withdrawal or replacement of any publication at Section 3; a determination on appeal that identified a defect in the framework; a pattern in the complaints record at 13.11.5; or a pattern of Assessor observations raised under 8.9.3.

16.2.3 The review examines the requirements, the weightings, the thresholds, the disqualifying conditions, and the evidence sufficiency rules against the outcomes actually awarded during the period.

16.2.4 The review record states what was examined, what changed, and what was considered and left unchanged. A review producing no change is recorded on the same terms as one that does.

16.3 Version numbering

Change type	Effect on version	Examples
Major	Whole number, 1.0 to 2.0	Addition, removal or material redrafting of a requirement. Change to a weighting, threshold, section floor or disqualifying condition. Change to the scoring scale or the evidence sufficiency rules.
Minor	Decimal, 1.0 to 1.1	Clarification of wording where meaning is unchanged. Correction of a cross-reference. Update to a normative reference where the requirement is unaffected. Editorial correction.

16.3.1 The framework and the control set carry independent version numbers. A change to one does not oblige a change to the other.

16.3.2 A major version of the control set may be issued against an unchanged framework, and this is the expected pattern where MOD policy moves.

16.4 Issue and application

16.4.1 A minor version applies from its issue date, including to assessments in progress, since meaning is unchanged.

16.4.2 A major version is issued with not less than three months notice before it becomes the current version for the purposes of 7.4.1. The notice period allows Organisations preparing for assessment to know which version they will be held to.

16.4.3 The exception at 7.4.5 permits a major version to be issued with a shorter or immediate application date where the Scheme Owner judges a change to the publications at Section 3 to require it. The Scheme Owner shall record the reasoning, and shall state on issue which requirements carry the shortened date.

16.4.4 Holders of a current outcome are notified of every issue, and of whether the issue affects them.

16.5 Change log

16.5.1 Every version carries a change log at Annex F recording, for each change: the clause or requirement affected, the nature of the change, the reason, and the version at which it took effect.

16.5.2 The change log is cumulative. Entries from superseded versions are retained.

16.5.3 Where a weighting, threshold or disqualifying condition changes, the log records the previous position alongside the new one.

16.6 Interpretation

16.6.1 The Scheme Owner is the sole authority on the interpretation of this framework and the control set.

16.6.2 Where an Assessor raises a matter under 8.9.3, or where an Organisation queries the meaning of a requirement, the Scheme Owner may issue an Interpretation Note.

16.6.3 An Interpretation Note carries a reference in the series WMA-IN-nnn and a date; states the requirement it addresses and the interpretation to be applied; is binding on every Assessor from its date; is published to Assessors and to Organisations holding or seeking an outcome; and is folded into the next version of the affected document and is then withdrawn.

16.6.4 An Interpretation Note clarifies a requirement as written. It shall not introduce a requirement, alter a weighting or threshold, or extend a disqualifying condition. A matter needing any of those is handled by a version change.

16.6.5 Interpretation Notes extant at an assessment date apply to that assessment, whether issued before or after the assessment agreement was signed. This departs from 7.4.1 because a note states what the version already means.

16.7 Corrections

16.7.1 An error of transcription, numbering or cross-reference is corrected by erratum, recorded in the change log and reflected in the next minor version.

16.7.2 Where an error has affected an assessment already conducted, the Scheme Owner examines whether the outcome would have differed. Where it would, the outcome is reviewed under 13.5 at the Scheme Owner's cost, and any adjustment operates in the Organisation's favour where the error was the Scheme Owner's.

16.8 Precedence

Where documents within the scheme conflict, the order is: this framework; WMA-SBD-CAT-001, the control set; Interpretation Notes, subject to 16.6.4; the Part B templates; guidance issued by the Scheme Owner.

A contract, a Security Aspects Letter, a Defence Condition or statute governs the Organisation's own obligations over anything in this scheme, under 5.1.

16.9 Part B templates

16.9.1 The Part B templates are provided to support an Organisation in producing the evidence this framework examines. Their use is voluntary.

16.9.2 Use of a template evidences nothing by itself. A populated template is scored on the same terms as any other document, under 9.9.

16.9.3 An Organisation may adapt a template to its circumstances. Adaptation does not affect scoring in either direction.

16.9.4 The Scheme Owner shall not adapt a template for a named Organisation, since that would constitute consultancy under 6.9.4.

16.9.5 The templates are issued unmodified and on the same terms to every Organisation, whether or not it proceeds to assessment.

16.10 Withdrawal of the framework

16.10.1 Where the Scheme Owner withdraws this framework, outcomes current at the date of withdrawal remain valid until their expiry date.

16.10.2 The register is maintained until the last outcome expires.

16.10.3 Holders are notified not less than six months before withdrawal takes effect.

Annex schedule

Ref	Title	Status	Version line
WMA-SBD-CAT-001	Defence Supplier Mark Control Set	Normative	Independent
Annex A	Mapping to the government Secure by Design principles	Informative	Framework
Annex B	Mapping to the MOD Secure by Design principles	Informative	Framework
Annex C	Mapping to Cyber Assessment Framework outcomes	Informative	Framework
Annex D	Part B template index	Informative	Framework
Annex E	Assessment output formats	Normative	Framework
Annex F	Change log	Normative	Framework

Informative annexes assist in reading the framework and carry no requirement. Normative annexes carry requirements and are read as part of the framework.

Annex A. Mapping to the government Secure by Design principles

Status: informative. This mapping shows where each published principle is examined. It does not create an entitlement to claim compliance with the principles, which is prohibited at 14.5.

Principle	Requirements	Count
1. Create responsibility for cyber security risk	S1.01, S1.02, S1.04, S1.05, S1.06, S2.06, S3.01, S3.04, S3.05, S7.03	10
2. Source secure technology products	S3.10, S5.05, S5.07, S7.01, S7.02, S7.04	6
3. Adopt a risk-driven approach	S1.03, S1.06, S2.01, S2.02, S2.03, S2.04, S3.02, S3.10	8
4. Design usable security controls	S2.05	1
5. Build in detect and respond security	S5.04, S5.05, S6.01, S6.02, S6.03, S6.04	6
6. Design flexible architectures	S5.06	1
7. Minimise the attack surface	S2.03, S2.04, S3.05, S3.08, S3.09, S4.01, S4.02, S4.05, S4.06, S4.07, S4.08, S4.09, S5.01, S5.02, S5.03, S5.06, S7.03, S7.05	18
8. Defend in depth	S2.05, S3.03, S4.03, S4.04, S4.05, S4.06, S4.09, S5.02, S5.03, S5.06	10
9. Embed continuous assurance	S1.02, S2.06, S2.07, S5.08, S6.03, S6.05, S6.06, S7.04	8
10. Make changes securely	S2.08, S2.09, S4.08, S5.09	4

A.1 Principles with single-requirement coverage

Principles 4 and 6 are each examined by one requirement. This is a stated position rather than an oversight.

Principle 4, design usable security controls, is directed at teams designing services for users. For a supplier, the analogous question is whether the controls it applies are workable by the people required to apply them, which is the second limb of S2.05 and is tested through interview. Padding the coverage with further requirements would examine the same thing twice.

Principle 6, design flexible architectures, applies to an organisation building or modernising a service. A supplier delivering into a customer's architecture influences it at the margins, which S5.06 examines. At Operational scope the principle has no application at all, and S5.06 is Out of Scope.

An Organisation assessed at Operational scope receives no examination against principles 2, 4, 6 or 10 beyond S2.08, S2.09, S3.10, S4.08 and S7.01 to S7.04. The assurance statement records the scope, and a reader can establish what was and was not examined from this annex.

Annex B. Mapping to the MOD Secure by Design principles

Status: informative. Principles as set out for the defence supply base in ISN 2023/09.

Principle	Requirements	Count
1. Understand and define context	S1.01, S1.03, S1.06, S2.01, S2.02, S2.03, S2.04, S3.02, S3.08, S4.01, S4.02, S4.07	12
2. Plan the security activities	S1.02, S1.04, S1.05, S2.02, S2.06, S3.02	6
3. Implement continuous risk management	S1.01, S1.03, S2.01, S2.07, S2.08, S6.01, S6.03, S6.04	8
4. Define security controls	S2.05, S3.03, S4.03, S4.04, S4.05, S4.06, S4.09, S5.02, S5.03, S5.04, S5.06	11
5. Engage and manage the supply chain	S3.01, S3.04, S3.05, S3.06, S3.07, S3.09, S3.10, S5.07, S6.02, S7.01, S7.02, S7.03, S7.04	13
6. Assure, verify and test	S5.05, S5.08, S6.06, S7.04	4
7. Enable through life management	S2.09, S4.08, S5.04, S5.09, S6.02, S6.05, S6.06, S7.05	8

B.1 Reading this mapping

The MOD principles are addressed to Delivery Teams inside the Ministry of Defence rather than to suppliers. Several of the obligations they carry, including capability registration and the appointment of a Delivery Team Security Lead, sit with the customer and have no supplier analogue.

This mapping shows where a supplier's own activity supports the customer in meeting each principle. It does not assert that the Organisation meets the MOD principles, and 14.5 prohibits a claim to that effect. Principle 5 carries the heaviest supplier-side weight, which is expected. From the customer's position, a supplier is the supply chain.

Annex C. Mapping to Cyber Assessment Framework outcomes

Status: informative and indicative.

C.1 Standing

- C.1.1** This mapping is provided to assist a customer subject to GovAssure in relating an Organisation's evidence to its own reporting. It confers no CAF standing on the Organisation, and 14.5 prohibits any claim to CAF standing.
- C.1.2** The mapping is at objective level by deliberate choice. A mapping at contributing outcome level would age with each NCSC reissue and would read as a claim to have been assessed against the framework.
- C.1.3** CAF version: [x.x], to be confirmed against the current NCSC issue at the date this annex is published, and re-verified at each framework review under 16.2.

C.2 Objective-level mapping

CAF objective	Sections principally bearing on it
A. Managing security risk	S1, S2, S7
B. Protecting against cyber attack	S3, S4, S5
C. Detecting cyber security events	S5, S6
D. Minimising the impact of incidents	S6

C.3 Limitations of this mapping

- The framework assesses an organisation delivering into a customer environment. CAF assesses an operator of essential functions. The unit of assessment differs, and the mapping is directional rather than equivalent.
- Objective D is thinly covered, since recovery of an essential function is the customer's concern rather than the supplier's.
- Nothing in this framework evidences a CAF profile, a GovAssure return, or an independent CAF assessment.

Annex D. Part B template index

Status: informative.

Ref	Template	Requirements supported
WMA-SBD-TPL-001	Security Procedure	S1.02, S1.03, S1.06, S2.05, S2.07, S2.08, S3.01, S3.03, S3.08, S4.01 to S4.09, S5.01 to S5.09, S6.01, S6.04, S6.05, S6.06, S7.01, S7.02, S7.04
WMA-SBD-TPL-002	Engagement Security Risk Assessment and Project Security Plan	S2.01 to S2.09, S4.02, S4.08
WMA-SBD-TPL-003	Self-Assessment Checklist	All, indicative only
WMA-SBD-TPL-004	Staff Security Briefing and Declaration	S3.03, S3.06, S3.07, S4.05, S4.06, S6.01, S6.04
WMA-SBD-TPL-005	Subcontractor Security Assessment and Flow-Down Pack	S7.01 to S7.05, and S3.02 where the Organisation issues a letter
WMA-SBD-TPL-006	Register Pack	S1.05, S1.06, S3.02, S3.04, S3.05, S3.07, S4.05, S4.09, S6.03, S6.05, S6.06

D.1 Requirements no template supports

The following are evidenced by practice, by testimony or by direct verification rather than by a document an Organisation completes.

Requirement	How evidenced
S1.01 accountability, exercise limb	A record of a decision taken, arising in the ordinary course
S1.04 resourcing	Provision applied, evidenced by expenditure and by testimony
S3.09 publicity	The Organisation's published material, examined directly by the Assessor
S4.03, S4.04, S4.09, S5.02 to S5.04 technical limbs	Direct verification under 9.6
S6.04 reporting culture	Testimony from delivery personnel

Using every template and completing every field does not produce an outcome. This table is where that becomes concrete.

Annex F. Change log

Status: normative.

F.1 Format

Version	Date	Type	Clause	Change	Reason
1.0	July 2026	Major	All	First issue	Replaces BC-METH-001 v1.0 and the SBD-PROC-001 suite v1.0

F.2 Rules

- F.2.1** The log is cumulative. Entries from superseded versions are retained.
- F.2.2** Where a weighting, threshold, section floor or disqualifying condition changes, the previous position is recorded.
- F.2.3** Where a requirement is withdrawn, the entry records the reference as retired and the reference is never reissued, under WMA-SBD-CAT-001 C3.3.
- F.2.4** Where a requirement is redrafted without changing what it examines, the entry records the redraft and the reference is retained. Where redrafting changes what it examines, the entry records retirement of the old reference and issue of a new one.
- F.2.5** Interpretation Notes issued under 16.6 are recorded on issue and again on withdrawal when folded into a version.
- F.2.6** An erratum under 16.7 is recorded with the correction and the date.

F.3 Predecessor position, recorded once at first issue

Superseded	Position under the predecessor	Position at v1.0
BC-METH-001 v1.0	Six critical failure conditions, CF-1 to CF-6	Eleven disqualifying conditions, DC-1 to DC-11
BC-METH-001 v1.0	Three outcomes at 80 per cent, 60 to 79 per cent, below 60 per cent	Retained, with section floors added at 50 and 40 per cent
BC-METH-001 v1.0	Confidence levels High, Moderate, Limited	Retained, with mandatory caps added at 11.6.2 and 11.6.3
BC-METH-001 v1.0	Sample of three to six projects, assessor selected	Retained
BC-METH-001 v1.0	Corroboration required for a score of 2	Retained
BC-METH-001 v1.0	Assessment file retained seven years	Retained
WMA-SBD-CAT-001 draft v0.1	Five sections, 28 controls	Seven sections, 54 requirements
WMA-SBD-CAT-001 draft v0.1	S1 20, S2 25, S3 20, S4 20, S5 15	S1 15, S2 20, S3 20, S4 13, S5 12, S6 10, S7 10
SBD-PROC-001 suite v1.0	Six Secure by Design principles	Ten government principles and seven MOD principles, mapped at Annexes A and B
SBD-GUIDE-006 v1.0	Organisation-drafted tender positioning statement	Section 14, scheme-issued claim wording

F.3 exists so that anyone comparing the old suite to this one can see what moved and why, without reading both. It is written once and never amended.

Annex E, Assessment Output Formats, is a normative annex issued as a separate document at first issue and folded into this framework at the next version.