



Defence Supplier Mark Assurance Scheme

Defence Supplier Mark Control Set

Normative annex to WMA-SBD-001

Reference	WMA-SBD-CAT-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 Control Set
Reference	WMA-SBD-CAT-001
Version	1.0
Status	Normative annex to WMA-SBD-001
Parent framework	WMA-SBD-001 v1.0
Supersedes	WMA-SBD-CAT-001 draft v0.1, withdrawn without having been used in assessment
Version line	Independent of the parent framework, under WMA-SBD-001 clause 16.3.1
Review	Annually, and on any change to the normative references at WMA-SBD-001 Section 3
Classification	OFFICIAL

C1. How to read this document

- C1.1** This document contains the requirements against which an Organisation is scored. The parent framework governs how they are applied, and this document is read with it rather than in isolation.
- C1.2** Terms carry the meanings at WMA-SBD-001 Section 5. The scoring scale is at Section 8, and the evidence sufficiency rules attaching to each type marker are at Section 9.
- C1.3** Where this document and the parent framework conflict, the framework governs, under clause 16.8.

C2. Requirement anatomy

Every requirement carries the following fields.

Field	Content
Reference	The permanent identifier, in the form Sn.nn
Title	A short description
Type	One of the seven markers at WMA-SBD-001 9.1, determining which evidence sufficiency rules apply
Applies to	Operational scope, Cyber scope, or Both
Applies where	The condition that brings the requirement into play, stated where the requirement is conditional. Absent where the requirement applies to every engagement in the assessed scope.
Requirement	The obligation, expressed using the conventions at WMA-SBD-001 5.1
Evidence expected	What an Assessor examines. Indicative rather than exhaustive.
Scoring note	Supplementary guidance where the generic rules at Section 9 need refinement for this requirement. Absent where the generic rules suffice.
Linked DC	The disqualifying condition the requirement relates to, where one applies
Source	The normative reference the requirement derives from
Principle	The government and MOD principles the requirement supports, feeding Annexes A and B

C3. Numbering

- C3.1** References take the form Sn.nn, where Sn is the section and nn is a sequential number within it. Examples: S1.01, S3.07, S5.12.
- C3.2** References are permanent. A reference attaches to a requirement for the life of the scheme.
- C3.3** Where a requirement is withdrawn, its reference is retired. A retired reference is never reissued to a different requirement. The change log records the retirement.
- C3.4** Where a requirement is added, it takes the next unused number in its section. Numbering is not resequenced to close gaps.
- C3.5** Where a requirement is redrafted without changing what it examines, it keeps its reference and the change log records the redraft. Where redrafting changes what it examines, the previous reference is retired and a new one is issued.
- C3.6** The purpose of C3.2 to C3.5 is that an assurance statement issued in 2026 remains readable in 2032, and that a prime contractor comparing two assessments conducted under different versions can see what moved.

C4. Applicability

- C4.1** The Applies to field determines whether a requirement is scored at a given assessment scope. A requirement marked Cyber is recorded Out of Scope at an Operational assessment, and its points are removed from the section denominator under WMA-SBD-001 8.5.3.
- C4.2** The Applies where field states a condition. Where the condition did not arise during the assessment period and does not arise in the Organisation's normal delivery, the requirement is recorded Not Applicable under 8.5, with the evidence obligation at 8.5.2 and subject to the applicability cap at 8.5.4.
- C4.3** A conditional requirement is not disapplied because the Organisation chose not to do something it should have done. Where an Organisation undertook work requiring a Security Aspects Letter and none was sought, the requirement applies and scores 0. It is not recorded Not Applicable on the basis that no letter exists.
- C4.4** C4.3 is the distinction between a circumstance that did not arise and an obligation that was not met, and it is the most frequent error in self-assessment.

C5. Section index

Ref	Section	Weight at Combined scope	Requirements	Points
S1	Governance and Accountability	15%	6	12
S2	Risk Management and Project Implementation	20%	9	18
S3	Contractual, Statutory and Personnel Security	20%	10	20
S4	Information and Asset Handling	13%	9	18
S5	Cyber and Technical Security	12%	9	18
S6	Incident Management and Continuous Assurance	10%	6	12
S7	Supply Chain	10%	5	10
	Total	100%	54	108

Points by scope: Combined 108 across 54 requirements; Operational 90 across 45, dropping S5; Cyber 106 across 53, dropping S4.06 alone.

C6. Disqualifying condition links

Condition	Linked requirements
DC-1	S1.02
DC-2	S1.01
DC-3	S2.01
DC-4	S3.02
DC-5	S3.04, S3.05
DC-6	S3.10
DC-7	S4.07 and S2.08 by reference
DC-8	S6.01, S6.03
DC-9	S6.02
DC-10	S7.01, S7.02, S7.04
DC-11	No requirement. Misrepresentation is conduct during assessment rather than a security control.

C7. What this document does not contain

- C7.1** This document does not contain guidance on how to meet a requirement. Guidance would engage the consultancy separation at WMA-SBD-001 6.9.4.
- C7.2** The Evidence expected field lists what an Assessor examines. It does not list what an Organisation should create, and an Organisation producing exactly the artefacts listed has not thereby met the requirement.
- C7.3** C7.2 is the boundary that keeps this scheme from becoming a documentation exercise. The requirement is the obligation. The evidence field describes where an Assessor looks for proof that the obligation was met.

S1. Governance and Accountability

Weight at Combined scope: 15 per cent. Six requirements, twelve points available.

This section examines whether security risk is owned by a named person who exercises that ownership, whether the Organisation has written down how it manages security, whether it has stated what risk it will accept, and whether the people holding security roles are competent and resourced to perform them.

S1.01 — Named accountability for security risk

Type	G, governance and accountability
Applies to	Both
Linked DC	DC-2
Source	GovS 007. Secure by Design principle 1. ISN 2023/09 paragraphs 10 and 11.
Principle	Gov 1. MOD 1, MOD 3.

Requirement

The Organisation shall name one individual who holds accountability for security risk across all engagements within scope. That individual shall hold a position at director level, or shall hold Senior Responsible Owner authority for the work.

The accountability shall not be delegated, shared between individuals, or held collectively. 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.

The named individual shall approve the engagement security risk assessment for each engagement the Organisation identifies as sensitive, shall be notified of every reportable incident, and shall be the escalation point for security concerns.

The name and position shall be recorded in the security procedure and on each Project Security Plan.

Evidence expected

- The security procedure, naming the individual and their position
- Signed approvals across the sampled engagements, dated before mobilisation
- Incident notification records showing the individual was informed
- Testimony from delivery personnel identifying the individual without prompting
- At least one record of a security decision taken by that individual

Scoring note

The exercise test at WMA-SBD-001 9.2 governs. An individual who has approved every plan submitted with no recorded question, no refusal, and no condition attached has evidenced signature and scores 1.

Where no occasion requiring a security decision arose during the assessment period, the Assessor records this and 2 remains available on the approval record and the testimony together.

Where the Organisation operates a delegated security function, the Assessor tests whether delivery personnel can identify the person to whom a security concern is escalated. Identification of the immediate route scores the same as identification of the accountable individual. A delivery worker who can name neither scores the requirement at 0.

S1.02 — Documented security procedure

Type	P, process and procedure
Applies to	Both

Linked DC	DC-1
Source	GovS 007. ISN 2026/04 Annex B paragraph 5. Secure by Design policy.
Principle	Gov 1, Gov 9. MOD 2.

Requirement

The Organisation shall hold a documented procedure, or a documented set of policies and procedures, describing how security requirements are identified, assessed, controlled and evidenced across engagements within scope.

The procedure shall state its scope, the roles at S1.01 and their holders, the activity required at each phase from pre-contract enquiry through to close-out, and the retention applying to the records it generates.

The procedure shall be reviewed at intervals of no more than twenty-four months, and shall be reviewed on receipt or amendment of a Security Aspects Letter, following a security incident, and on a change to the contractual or regulatory environment affecting the work.

The procedure shall be issued to all personnel and subcontractors performing work within scope.

Evidence expected

- The procedure, carrying a version number, issue date and review date
- The review record, showing what was examined and what changed
- The distribution record
- Testimony that personnel know where the procedure is held and what it requires of them
- Records generated by the procedure across the sampled engagements

Scoring note

The currency rule at WMA-SBD-001 9.3 governs. A procedure carrying no review date, or last reviewed more than twenty-four months before the assessment with no evidence of use, scores 0 and the Assessor tests DC-1.

A procedure that is current and has not been applied because the circumstance has not arisen is handled under 8.5 rather than scored 0.

A procedure describing an organisation other than the one assessed, whether by name, by structure or by the work it describes, scores 0. This is found where a template has been adopted without adaptation.

Where the position is held across a set, the Assessor tests whether personnel performing the work can locate what applies to them. A set that is complete centrally and unnavigable at delivery level scores 1.

S1.03 — Security risk appetite

Type	G, governance and accountability
Applies to	Both
Source	Secure by Design principle 3 and the associated activity on establishing risk appetite. ISN 2023/09 paragraph 16.
Principle	Gov 3. MOD 1, MOD 3.

Requirement

The Organisation shall define and record a security risk appetite, approved by the individual at S1.01.

The appetite shall state the level of residual security risk the Organisation accepts without escalation, the level requiring escalation to the individual at S1.01, and the level at which work will not proceed.

The appetite shall be expressed so that it can be applied to an engagement-level risk assessment, and shall be reviewed annually and on a material change to the work the Organisation undertakes.

Evidence expected

- The recorded appetite, with approval and date
- Engagement risk assessments showing residual ratings tested against it
- A record of escalation on an occasion where a rating exceeded the appetite
- Testimony from an Engagement Security Lead describing what the appetite required of them on a specific engagement

Scoring note

A risk matrix may express the appetite where it states what the Organisation accepts without escalation, what it escalates to the individual at S1.01, and what stops work, and where it has been approved by that individual.

A matrix carrying action bands with no approval and no evidence of application scores 1.

A score of 2 requires the appetite to have been approved and applied to a live decision. Where no engagement approached the escalation threshold during the assessment period, 2 remains available where the appetite is approved and the Engagement Security Lead can describe what it requires of them.

An appetite expressed only as a commitment to accept no security risk scores 1, since it cannot be applied to a decision.

S1.04 — Resourcing of security activity

Type	G, governance and accountability
Applies to	Both
Source	Secure by Design principle 1, outcome on resourcing. ISN 2023/09 paragraphs 12 and 19.
Principle	Gov 1. MOD 2.

Requirement

The Organisation shall make resource available for the security activity its engagements require, covering briefing time, assessment time, secure storage, provision of Controlled Devices, personnel screening, and maintenance of competence under S1.05.

Where the Organisation prices work for a customer, the cost of security activity should be identified within the price.

The Organisation shall record any occasion on which a security activity was not performed for want of resource, and the decision taken in consequence.

Evidence expected

- Evidence of provision, such as screening costs, device procurement, storage arrangements and training expenditure
- Pricing or estimating records identifying security activity
- Any record of an activity deferred or omitted, with the decision
- Testimony from delivery personnel on whether time is available to perform what the procedure requires

Scoring note

An Organisation asserting that resource is available, with no instance of it having been applied, scores 1.

Evidence that a security activity was funded where commercial pressure ran against it evidences this requirement more strongly than a budget line. The Assessor asks the Engagement Security Lead whether they have ever been refused something they asked for on security grounds, and records the answer.

S1.05 — Competence of security role holders

Type	R, record and register
Applies to	Both
Source	ISN 2023/09 paragraph 20.
Principle	Gov 1. MOD 2.

Requirement

The Organisation shall hold a competence record for each individual performing a role under S1.01, stating the basis of that individual's competence for the security activity they perform, the date competence was last reviewed, and the person who reviewed it.

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.

The record shall state a basis specific to the security activity. A professional qualification in the Organisation's delivery discipline, recorded without more, does not state a basis.

Where the Organisation does not hold competence internally for a security activity its engagements require, it shall record how that activity is resourced.

Evidence expected

- The competence record
- Qualifications, credentials, training or continuing professional development records relied upon
- Any retained adviser arrangement, and evidence of it being used
- Testimony from a role holder describing what they were relied upon to do and what prepared them for it

Scoring note

Score	Position
0	No record, or a record naming individuals and roles with no basis stated against any of them
1	A basis stated for each role holder, reviewed within twenty-four months
2	A basis stated and corroborated, whether by training or continuing professional development records, by evidence of the competence being applied to a live security decision, or by an external arrangement under the fourth limb having been used in practice

A sole director whose basis rests on stated experience of delivering into the environment concerned meets this requirement, provided the record states what that experience consists of. Years in the industry, recorded as a number with nothing attached, does not.

The contemporaneity test at 9.4 applies to the review dates.

Where competence is managed through a corporate framework, the Assessor tests whether the framework covers the individuals actually performing the roles at S1.01 on the sampled engagements. A framework covering job families without covering those individuals scores 1.

S1.06 — Identification of applicable security obligations

Type	C, contractual and statutory
Applies to	Both
Source	ISN 2022/05. Secure by Design activity on understanding security obligations. GovS 007.
Principle	Gov 1, Gov 3. MOD 1.

Requirement

The Organisation shall identify, for each engagement within scope, the security obligations applying to it. Identification shall cover:

- The security conditions of the contract
- Any Security Aspects Letter and any Security Grading Guide referenced by it
- The Defence Conditions and Defence Standards invoked
- Industry Security Notices extant at contract award and published during the contract
- The security regulations of any establishment at which work is performed
- Statutory obligations arising

Identification shall be recorded before mobilisation and shall be kept under review for the duration of the engagement.

Evidence expected

- The obligations record for each sampled engagement
- Contract extracts showing the conditions invoked
- Copies or references of the Defence Conditions and Industry Security Notices relied upon
- Evidence of review where a relevant Industry Security Notice was published during the engagement
- Testimony from the Engagement Security Lead describing which obligations applied and where they came from

Scoring note

An Organisation identifying the contract without identifying the conditions it invokes has not met this requirement.

Where an Industry Security Notice bearing on the work was published during a sampled engagement and the Organisation cannot show it was seen, the requirement scores no higher than 1.

An Organisation relying wholly on the prime contractor to tell it what applies scores 1. Reliance on the customer is reasonable in fact. It does not evidence identification by the Organisation.

Where obligations are identified at bid stage by a function other than the delivery team, the Assessor tests the handover. Identification that did not reach the Engagement Security Lead scores 1.

S2. Risk Management and Project Implementation

Weight at Combined scope: 20 per cent. Nine requirements, eighteen points available.

This section examines whether the Organisation assesses security risk for the engagement in front of it rather than in general, whether the controls it applies follow from that assessment, and whether the position is maintained as the engagement changes.

S2.01 — Engagement-level security risk assessment

Type	P, process and procedure
Applies to	Both
Linked DC	DC-3
Source	Secure by Design principle 3. ISN 2023/09 paragraphs 15 and 26.
Principle	Gov 3. MOD 1, MOD 3.

Requirement

The Organisation shall complete a security risk assessment for each engagement within scope, before mobilisation.

The assessment shall identify risks specific to the engagement, shall record the controls selected against each, and shall record a residual position tested against the appetite at S1.03.

A corporate risk register, a health and safety risk assessment, or an assessment applied unchanged across engagements does not satisfy this requirement.

Evidence expected

- The assessment for each sampled engagement, dated before the engagement start
- Variation between assessments, reflecting the engagements they cover
- Approval where the engagement was identified as sensitive
- Testimony from the person who completed it, describing a risk they identified and why

Scoring note

Identical assessments across engagements of materially different sensitivity evidence a template rather than an assessment. The Assessor scores 0 and tests DC-3.

Pre-populated risks are acceptable. The test is whether engagement-specific risks were added, whether inapplicable ones were removed, and whether the ratings differ where the engagements differ.

An assessment dated after mobilisation scores 1 at most, and the Assessor records how far after.

S2.02 — Threat assessment

Type	P, process and procedure
Applies to	Both
Source	Secure by Design activity on sourcing a threat assessment. ISN 2023/09 paragraph 21.
Principle	Gov 3. MOD 1, MOD 2.

Requirement

The Organisation shall establish, for each engagement within scope, the threat picture bearing on it, covering who would have interest in the information the engagement produces or the access it confers, and what capability they would bring.

Where the Organisation cannot produce a threat assessment itself, it shall seek one from the customer, the prime contractor, or the establishment, and shall record the request and the response.

Evidence expected

- The threat picture recorded against sampled engagements
- Requests made to the customer or prime, with responses
- Threat material provided by the customer, where the Organisation is permitted to hold it
- Testimony describing who the Organisation considered the threat to be on a specific engagement

Scoring note

An Organisation that asked and received nothing has met the second limb. The Assessor scores on the request and the record, not on the answer received.

Clause 7.10 applies where the customer holds threat material the Organisation may not see. Withholding by the customer does not reduce the score.

A generic statement that hostile actors exist scores 0. A statement identifying the interest a specific site, dataset or system would attract scores 1 as a minimum.

S2.03 — Threat modelling

Type	P, process and procedure
Applies to	Both
Source	Secure by Design principle 7 and the activity on threat modelling. NCSC Secure Design Principles.
Principle	Gov 3, Gov 7. MOD 1, MOD 4.

Requirement

The Organisation shall examine, for each engagement within scope, how the engagement itself could be exploited, covering the access it creates, the information it generates, the presence of its personnel, and the aggregation effect at S4.02.

The examination shall be recorded and shall inform the controls selected at S2.05.

Evidence expected

- The record, whether held separately or within the risk assessment
- Evidence that a control was selected in response to something the examination identified
- Testimony describing how the engagement could be exploited, from the person who conducted it

Scoring note

This requirement is met where the examination is recorded within the risk assessment. Clause 9.11.3 prohibits requiring a separate document.

The distinction from S2.01 is direction. S2.01 asks what could go wrong. This asks how someone would set about making it go wrong. An Organisation whose only answer is the risk list scores 1.

For an Operational engagement, an answer addressing what the survey output would tell a hostile reader scores 2 where corroborated.

S2.04 — Identification of information and assets

Type	R, record and register
Applies to	Both

Source	Secure by Design activities on documenting service assets and assessing their importance. ISN 2023/09 paragraph 14e.
Principle	Gov 3, Gov 7. MOD 1.

Requirement

The Organisation shall identify, for each engagement within scope, the information and assets it will receive, generate, hold and transmit, together with the classification applying to each.

Identification shall record where each item will be held, who will have access, and the retention applying.

Evidence expected

- The identification for sampled engagements
- Consistency between what was identified and what the engagement produced
- The classification recorded against each item
- Access arrangements recorded and evidenced

Scoring note

Identification covering material received from the customer while omitting material the Organisation generated scores 1. The output of a survey is the item most likely to be missed and is frequently the more sensitive holding.

Where identification exists and the engagement produced items not on it, the Assessor tests whether the omission was noticed.

S2.05 — Controls selected, traceable and workable

Type	P, process and procedure
Applies to	Both
Source	Secure by Design principles 4 and 8, and the activity on agreeing a security controls set. ISN 2023/09 paragraphs 33 and 34.
Principle	Gov 4, Gov 8. MOD 4.

Requirement

The Organisation shall select controls that address the risks identified, shall record the reasoning linking each control to the risk it addresses, and shall apply controls across more than one layer so that failure of a single control does not expose controlled information or site access.

Controls shall be workable by the personnel required to apply them in the conditions in which they work.

Evidence expected

- Controls recorded against the risks they address
- Evidence of layering, with the backstop identified
- Testimony from delivery personnel on whether the controls are workable
- Any record of a control being changed because it was found unworkable

Scoring note

The workability limb is tested through interview. Where delivery personnel describe a documented control they do not apply because it obstructs the work, the requirement scores 0 and the Assessor records the finding under S6 as well.

A control list with no traceability to identified risks scores 1, whatever its content.

Evidence that a control was revised after personnel reported it unworkable scores towards 2, since it evidences the feedback loop the requirement seeks.

S2.06 — Project Security Plan approved before mobilisation

Type	R, record and register
Applies to	Both
Source	GovS 007. ISN 2023/09 paragraph 22.
Principle	Gov 1, Gov 9. MOD 2.

Requirement

The Organisation shall assemble, for each engagement within scope, a Project Security Plan comprising the risk assessment, the controls applied, the obligations identified at S1.06, any Security Aspects Letter and its acknowledgement, the briefing records, and the close-out record.

The plan shall be approved before mobilisation by the individual at S1.01 where the engagement is identified as sensitive, and shall be retained under S6.

Evidence expected

- The assembled plan for sampled engagements
- Approval dated before mobilisation
- Completeness of the plan against the engagement it covers

Scoring note

The plan may be a folder, a file structure or a record set. Clause 9.11.3 prohibits requiring a bound document.

A plan assembled at close-out rather than maintained through the engagement scores 1, and the Assessor tests contemporaneity under 9.4.

S2.07 — Risk reviewed through delivery

Type	P, process and procedure
Applies to	Both
Source	Secure by Design principles 3 and 9. ISN 2023/09 paragraphs 24 to 29.
Principle	Gov 3, Gov 9. MOD 3, MOD 7.

Requirement

The Organisation shall keep the security risk position under review for the duration of each engagement, and shall reassess on:

- A change to the scope, the site, the systems or the information handled
- An unexpected discovery during delivery
- A security incident or near miss
- A change to the threat picture notified by the customer or the establishment
- Addition of a subcontractor

Review shall be recorded, including where review concluded that no change was required.

Evidence expected

- Review records across sampled engagements
- Evidence of reassessment following a trigger that occurred
- Testimony describing an occasion on which the position was revisited

Scoring note

Where a trigger occurred during a sampled engagement and no reassessment is recorded, the requirement scores 0.

Where no trigger occurred, 2 remains available on the review record and testimony that personnel know what would prompt reassessment.

For engagements running beyond three months, review at intervals of no more than three months is expected in addition to trigger-based review.

S2.08 — Security impact of change evaluated

Type	P, process and procedure
Applies to	Both
Source	Secure by Design principle 10 and the activity on evaluating the security impact of changes.
Principle	Gov 10. MOD 3.

Requirement

The Organisation shall evaluate the security impact of a proposed change before implementing it, covering changes to the method of delivery, the systems or devices used, the personnel deployed, the subcontractors engaged, and the storage or transmission arrangements applied.

Where a change requires access beyond the scope agreed, the Organisation shall obtain written authority from the site security authority or the customer technical authority before proceeding.

Evidence expected

- Change records showing security impact considered
- Written authority obtained where scope was extended
- Testimony describing a change and what was considered before it was made

Scoring note

Access taken beyond agreed scope without written authority is examined against DC-7 where controlled information was exposed, and scores 0 under this requirement in any event.

An Organisation with no changes during the assessment period is handled under 8.5 rather than scored 0. The Assessor tests whether personnel can describe what they would do.

S2.09 — Close-out

Type	P, process and procedure
Applies to	Both
Source	Secure by Design principle 10 and the activity on retiring components securely. ISN 2026/04 Annex B paragraphs 15 and 37.
Principle	Gov 10, Gov 7. MOD 7.

Requirement

The Organisation shall complete a recorded close-out for each engagement within scope, covering:

- Return of passes, keys, tokens and credentials to the issuing authority
- Removal of access from customer systems, with confirmation
- Return of Authority Property, or destruction where directed
- Secure disposal of working material not forming part of the deliverable

-
- Confirmation that nothing has been left on site
 - A security review recording anything learned

Evidence expected

- Close-out records for sampled engagements
- Confirmation of return or revocation, from the receiving party where obtainable
- Disposal records
- The review record and any change made in consequence

Scoring note

Close-out asserted without confirmation from the receiving party scores 1 where confirmation was obtainable.

Return of Authority Property is the limb most frequently absent. An Organisation that disposed of customer-issued drawings rather than returning them has not met this requirement, whatever the security of the disposal.

A review recording that nothing was learned, on every engagement across the sample, scores 1.

S3. Contractual, Statutory and Personnel Security

Weight at Combined scope: 20 per cent. Ten requirements, twenty points available.

This section examines the obligations that arise from the contract and from statute rather than from the Secure by Design principles. Four disqualifying conditions attach here, more than any other section, because these obligations are binary facts a Contracting Authority can establish for itself.

Applicability cap: 40 per cent under WMA-SBD-001 8.5.6. Four of the ten requirements in this section are conditional, against a control set average below one fifth. The higher cap reflects that an Organisation delivering to government outside MOD will properly record several requirements as Not Applicable.

S3.01 — Contract security conditions identified and applied

Type	C, contractual and statutory
Applies to	Both
Source	ISN 2026/04 paragraphs 18, 19 and Annex B paragraphs 5, 12, 16. DEFCON 660. DEFCON 531.
Principle	Gov 1. MOD 1, MOD 5.

Requirement

The Organisation shall identify the security conditions incorporated in each contract within scope, shall apply them, and shall give notice of them to every individual working on the contract.

Where the contract incorporates the OFFICIAL and OFFICIAL-SENSITIVE Contractual Security Conditions, the Organisation shall hold a copy and shall apply its provisions on storage, access, distribution, transmission and destruction.

Evidence expected

- The conditions held against each sampled engagement
- Evidence that they were given to personnel, and testimony that personnel received them
- Application evidenced in the engagement records
- Correspondence where a condition was queried with the Contracting Authority

Scoring note

Holding the conditions without evidence that they reached the people applying them scores 1. Clause 9.11.6 governs at scale.

The obligation under DEFCON 531 runs to giving employees notice before they receive information. Notice given after access scores 1.

S3.02 — Security Aspects Letter received and acknowledged

Type	C, contractual and statutory
Applies to	Both
Applies where	The Organisation has undertaken, or tendered for, work classified at OFFICIAL-SENSITIVE or above
Linked DC	DC-4
Source	ISN 2026/04 paragraphs 3, 7, 8, 9, 10, 11.
Principle	Gov 1, Gov 3. MOD 1, MOD 2.

Requirement

The Organisation shall obtain the Security Aspects Letter applying to each engagement classified at OFFICIAL-SENSITIVE or above, shall return a signed acknowledgement before work begins, and shall hold a register recording receipt, acknowledgement, review and amendment.

Where the Organisation undertakes work it knows or ought to know is classified at OFFICIAL-SENSITIVE or above and no Security Aspects Letter has been issued, it shall raise the absence with the Contracting Authority in writing before work begins and shall record the response.

Where the letter is unclear, or imposes an obligation the Organisation cannot meet, it shall raise the matter with the Contracting Authority.

Evidence expected

- The letter for each applicable sampled engagement, with any Security Grading Guide referenced
- The signed acknowledgement, dated before the engagement start date
- The register, showing review at intervals of no more than twelve months and at each contract amendment
- Evidence that the aspects defined in the letter appear in the engagement risk assessment and the briefing

Scoring note

An acknowledgement dated after work began evidences the acknowledgement and not the sequence. It scores 1.

A register listing letters received, with no evidence that their content reached the people doing the work, scores 1.

Absence of a Security Grading Guide referenced by a letter is a shortfall against this requirement rather than a separate one.

Where the Contracting Authority failed to issue a letter and the Organisation identified that, raised it and recorded the response, the requirement scores 2 where corroborated and DC-4 is not engaged.

S3.03 — Work at government establishments

Type	C, contractual and statutory
Applies to	Operational
Applies where	Work is performed at an MOD or other government establishment
Source	ISN 2026/04 paragraph 22. DEFCON 76 section 10.
Principle	Gov 8. MOD 4.

Requirement

The Organisation shall obtain the security regulations of each establishment at which its personnel work, shall brief its personnel on them before access, and shall apply them in preference to its own arrangements where the two differ.

Where establishment regulations restrict Personal Devices, storage in vehicles within the perimeter, photography, or movement between areas, the Organisation shall record the restriction and shall brief it specifically.

Evidence expected

- Establishment regulations or instructions held for sampled engagements
- Briefing records referencing the specific establishment
- Testimony from personnel describing a restriction particular to a site they attended
- Records of escort or access arrangements agreed with the site security authority

Scoring note

A briefing covering the Organisation's own procedure with no site-specific content scores 1, however thorough the procedure.

The device categories at WMA-SBD-001 5.5 are tested here. Personnel who cannot say which of their devices fall into which category, for the site they attended, evidence a briefing that did not reach them.

Where an establishment issued no written regulations and the Organisation recorded what it was told at induction, that record satisfies the first limb.

S3.04 — Baseline personnel screening

Type	C, contractual and statutory
Applies to	Both
Linked DC	DC-5
Source	ISN 2026/04 Annex B paragraph 17. Baseline Personnel Security Standard.
Principle	Gov 1. MOD 5.

Requirement

The Organisation shall confirm, before granting any individual access to controlled material, a controlled site, or a customer system, that the individual has undergone baseline recruitment checks covering proof of identity, legal entitlement to work, and verification of employment record, together with criminal record checking where permissible.

The confirmation shall be recorded against the individual with the date of check.

This applies to every individual, including those operating under an escort arrangement, and including associates and agency personnel.

Evidence expected

- The screening record for individuals working on sampled engagements
- Dates of check preceding first access
- The arrangement by which associates and agency personnel are screened
- Testimony on what happens when a new person joins an engagement

Scoring note

The record states status and date. The underlying screening evidence is examined and is not copied to the assessment file, under WMA-SBD-001 15.7.4.

Screening completed after access was granted scores 1 and the Assessor tests DC-5 in respect of the period before it.

Long-serving personnel engaged before the Organisation began defence work are within this requirement.

Retrospective verification recorded with its date satisfies it. Absence of any record for those individuals scores 0 and engages DC-5.

An Organisation relying on an agency's assurance that its personnel are screened, with no verification of any kind, scores 1.

S3.05 — Clearance and escort arrangements

Type	C, contractual and statutory
Applies to	Both
Applies where	The contract or establishment requires National Security Vetting or an escort arrangement
Linked DC	DC-5
Source	ISN 2026/04 Annex B paragraph 16. GovS 007.
Principle	Gov 1, Gov 7. MOD 5.

Requirement

The Organisation shall confirm that each individual requiring clearance holds it at the level required and that it is current at the point of access, and shall check expiry dates before mobilisation.

Where an individual does not hold the clearance required, the Organisation shall hold a written escort arrangement agreed with the site security authority before access, and shall not treat an escort arrangement as a matter it determines for itself.

Access shall be confined to individuals whose duties require it, under the need to know principle.

Evidence expected

- Clearance status and expiry recorded against individuals on sampled engagements
- The written escort arrangement, agreed with the site security authority
- Evidence of a check performed before mobilisation
- Testimony describing what happens where a clearance is close to expiry

Scoring note

Clearance recorded once at recruitment, with no check before subsequent engagements, scores 1.

An escort arrangement described in the Organisation's own records with no evidence of agreement by the site scores 0.

S3.06 — Aftercare and change of personal circumstances

Type	H, human factor and behaviour
Applies to	Both
Source	GovS 007. UKSV aftercare guidance.
Principle	Gov 1. MOD 5.

Requirement

The Organisation shall require personnel holding clearance, escort approval, or access to controlled material to report a change in personal circumstances bearing on their suitability to hold that access, shall provide a route by which such a report is made confidentially, and shall record how a report received is handled.

The Organisation shall make clear that reporting does not of itself affect an individual's clearance or their ability to work, and that failure to report a relevant matter is itself a security concern.

Evidence expected

- The obligation stated in the briefing and in the procedure
- The reporting route, and evidence that personnel know it
- Testimony from personnel on what they would report and to whom
- The handling record for any report received, examined at a level that does not disclose its content

Scoring note

Personnel who describe the obligation as applying only to criminal matters evidence an incomplete briefing and score 1.

Where interviews disclose that personnel would hesitate to report because of the consequences they expect, the requirement scores no higher than 1 and the finding is recorded under S6.

The Assessor shall not examine the content of an individual aftercare report. Existence, date and handling are sufficient.

S3.07 — Statutory obligations

Type	C, contractual and statutory
Applies to	Both
Source	ISN 2026/04 Annex B paragraph 8. Official Secrets Act 1989. National Security Act 2023.
Principle	Gov 1. MOD 5.

Requirement

The Organisation shall inform every individual given access to controlled material that the provisions of the Official Secrets Act 1989 and the National Security Act 2023 apply to information associated with the contract, shall obtain a signed record of that notice, and shall retain it.

Where a contract or Security Aspects Letter requires a declaration in a particular form, the Organisation shall use that form and shall retain a copy.

Evidence expected

- The signed record for individuals on sampled engagements
- The form required by the contract, where one is specified
- Testimony that individuals understood what they signed

Scoring note

A signature on a form the signatory cannot describe in substance scores 1, under WMA-SBD-001 9.5.

The obligation continues after the engagement ends. Personnel who believe it ceased at close-out evidence an incomplete briefing.

S3.08 — Classification ceiling and facility clearance

Type	C, contractual and statutory
Applies to	Both
Source	ISN 2026/04 paragraph 7. ISN 2022/05.
Principle	Gov 7. MOD 1.

Requirement

The Organisation shall record whether it holds Facility Security Clearance, and shall state the classification ceiling of work it can accept.

Where Facility Security Clearance is not held, the Organisation shall not hold, produce or process classified material above OFFICIAL-SENSITIVE on its own premises, and shall state that limit at tender stage.

Where Facility Security Clearance is held, the Organisation shall name its Facility Security Controller and shall route Security Aspects Letters and List X Notices through that individual.

Evidence expected

- The recorded position on clearance and ceiling
- Tender or proposal material stating the limit, where clearance is not held
- The named Facility Security Controller and evidence of the routing, where clearance is held
- Testimony that the person accepting work knows the ceiling

Scoring note

An Organisation that has never considered its ceiling scores 0, whether or not it has exceeded it.

The requirement is met by an accurate statement of a limited position. A sole director practice recording that it holds no facility clearance, works at OFFICIAL-SENSITIVE at customer premises only, and states this in proposals, scores 2 where corroborated.

S3.09 — Disclosure, publicity and export control

Type	C, contractual and statutory
Applies to	Both
Source	ISN 2026/04 Annex B paragraphs 12, 40, 41, 42. DEFCON 531.
Principle	Gov 7. MOD 5.

Requirement

The Organisation shall obtain prior approval from the Contracting Authority before releasing any material arising from a contract within scope, covering publicity literature, website content, media comment, exhibition display, lectures, and technical or scientific papers.

The Organisation shall not disclose the contract or any provision of it to any person other than an individual directly employed by it or by a subcontractor, without written consent.

Where the Organisation would release classified defence material to a foreign entity for promotion or sale, it shall obtain approval through the MOD Form 680 procedure.

Evidence expected

- Approvals obtained, or a record that no release was made
- The Organisation's own published material, checked against its engagements
- The internal route by which a proposed release is checked
- Testimony from anyone responsible for marketing

Scoring note

The Assessor examines the Organisation's website and published material directly, and compares it against the sampled engagements. Named customers, site photographs, or descriptions of defence work published without evidence of approval score 0.

The Form 680 limb is recorded Not Applicable for an Organisation that does not release material to foreign entities. That is a circumstance that does not arise rather than an obligation unmet.

Social media activity by individual personnel is examined under S3.03 and S6 rather than here.

S3.10 — Cyber contractual obligations

Type	C, contractual and statutory
Applies to	Both
Applies where	A contract held by the Organisation incorporates DEFCON 658
Linked DC	DC-6
Source	ISN 2026/04 paragraph 20. Defence Standard 05-138 Issue 4. Cyber Security Model version 4.
Principle	Gov 2, Gov 3. MOD 5.

Requirement

Where a contract incorporates DEFCON 658, the Organisation shall:

- Obtain the Cyber Risk Profile and Risk Assessment Reference from the Contracting Authority

- Complete a Supplier Assurance Questionnaire through the Supplier Cyber Protection Service against the controls applying to that profile
- Submit a Cyber Implementation Plan where the outcome is Not Met
- Renew the questionnaire on the anniversary of contract award, within the window stated
- Flow DEFCON 658 down to any subcontractor, in accordance with S7
- Retain the records demonstrating compliance for six years after termination of the contract

Evidence expected

- The Cyber Risk Profile and Risk Assessment Reference held
- The questionnaire submission and its date
- Any Cyber Implementation Plan, with progress against it
- The renewal record, and the retention arrangement

Scoring note

This requirement applies to Operational engagements as readily as to Cyber ones. DEFCON 658 attaches to contracts involving MOD Identifiable Information rather than to digital work, so a survey contract may carry it.

A questionnaire completed once with no renewal on the contract anniversary scores 1.

An outcome of Not Met with no Cyber Implementation Plan scores 0 and engages DC-6, unless the Organisation evidences that it has raised the position with the Contracting Authority.

The Assessor examines whether the questionnaire position is accurate against what is found at S5. A questionnaire asserting controls the assessment finds absent is examined against DC-11.

S4. Information and Asset Handling

Weight at Combined scope: 13 per cent. Nine requirements, eighteen points available.

This section examines how the Organisation classifies, stores, transmits, minimises, returns and destroys the information and assets it handles, and how it protects the systems and devices those holdings sit on.

S4.01 — Classification and marking

Type	C, contractual and statutory
Applies to	Both
Source	Government Security Classifications Policy. ISN 2026/04 Annex B paragraph 4.
Principle	Gov 7. MOD 1.

Requirement

The Organisation shall apply the classification stated in the Security Aspects Letter, or in the contract where no letter has been issued, to material provided to it and to material it generates.

The Organisation shall mark every OFFICIAL-SENSITIVE document it originates or copies. Material at OFFICIAL requires marking where it is transmitted overseas.

Where the Organisation considers a classification to be wrong, it shall raise the matter with the Contracting Authority and shall apply the higher of the two positions pending the response.

Evidence expected

- Marking on outputs from sampled engagements
- The basis on which classification was determined for material the Organisation generated
- Correspondence querying a classification, with the response
- Testimony on how an individual decides what to mark a photograph or a field note

Scoring note

Marking applied to final deliverables while working material carries none scores 1. Field notes, photographs and interim drawings attract the classification of what they contain.

An Organisation that has never considered the classification of material it generates, as distinct from material it receives, scores 0.

S4.02 — Aggregation

Type	P, process and procedure
Applies to	Both
Source	Government Security Classifications Policy. NPSA guidance on aggregation.
Principle	Gov 7. MOD 1.

Requirement

The Organisation shall examine, for each engagement within scope, whether the material it holds or produces attracts a higher classification in combination than any single item attracts alone.

The examination shall be recorded within the engagement risk assessment or the identification at S2.04, shall be repeated where the holding grows, and shall record the classification applied in consequence.

Evidence expected

- The recorded examination for sampled engagements

- Evidence of an uplift applied where aggregation warranted it, or a recorded conclusion that it did not
- Testimony describing what the combined holding would tell a hostile reader
- The point at which the examination was repeated on a long engagement

Scoring note

This is the requirement most frequently absent in survey and inspection work, where layout, access arrangement and condition data combine into a holding materially more sensitive than any single drawing.

A statement in a policy that aggregation may require a higher rating, with no examination against any engagement, scores 0.

Where the examination concluded that no uplift was required and recorded why, the requirement is met.

S4.03 — Storage

Type	T, technical control
Applies to	Both
Source	ISN 2026/04 Annex B paragraphs 9 and 11.
Principle	Gov 8. MOD 4.

Requirement

The Organisation shall hold controlled material in access-controlled, encrypted systems, and shall hold physical material at OFFICIAL-SENSITIVE under lock and key in a lockable room, cabinet, drawer or safe, with keys and combinations controlled.

Storage locations shall be recorded, and access shall be confined to individuals with a need to know.

Evidence expected

- Direct verification of the systems in use, under WMA-SBD-001 9.6
- Physical storage observed at the Organisation's premises
- The control arrangement for keys and combinations
- Access lists, and evidence that they are reviewed

Scoring note

Direct verification is required for a score above 0, under 9.6. An assertion that storage is encrypted scores 0.

Key control is the limb most often absent. A lockable cabinet whose key sits in an unsecured drawer does not meet the requirement.

Where the Organisation holds material only on customer systems and holds nothing itself, the requirement is scored on the access controls it applies to those systems, and the physical limb is recorded Not Applicable.

S4.04 — Transmission

Type	T, technical control
Applies to	Both
Source	ISN 2026/04 Annex B paragraphs 20, 21, 22, 23. NCSC guidance on Transport Layer Security.
Principle	Gov 8. MOD 4.

Requirement

The Organisation shall transmit OFFICIAL-SENSITIVE material over the internet only when encrypted using an approved cryptographic technique, with Transport Layer Security enabled at both sender and recipient, or by an approved file transfer platform or encrypted physical media.

Unencrypted transmission of OFFICIAL-SENSITIVE material shall be made only with the prior approval of the Contracting Authority, and each occasion shall be recorded.

The Organisation shall confirm the recipient before transmitting, and shall record the recipients of each output.

Evidence expected

- Direct verification of the transmission arrangement in use
- The recipient record for outputs from sampled engagements
- Any record of unencrypted transmission, with the approval relied upon
- Testimony on what an individual does when a customer asks for a file by ordinary email

Scoring note

The last evidence item is the substance of this requirement. Personnel who would send the file scores 0 whatever the policy states.

Reliance on the recipient's arrangements without confirming that Transport Layer Security operates at their end scores 1.

S4.05 — Controlled Devices

Type	T, technical control
Applies to	Both
Source	ISN 2026/04 Annex B paragraphs 27, 28, 29, 30.
Principle	Gov 7, Gov 8. MOD 4.

Requirement

The Organisation shall identify which devices are Controlled Devices under WMA-SBD-001 5.5, shall encrypt every Controlled Device, and shall apply the following to each:

- The device is not left unattended in a public location
- The device is not left unattended in a vehicle, whether in view, in the boot or in a luggage compartment
- Where a vehicle is in motion, the device is secured out of sight
- Any token or password associated with the encryption package is held separately from the device whenever it is not in use, unattended or in transit
- Removable media carrying personal data is not taken outside a secure site unencrypted

Evidence expected

- The device register, showing category against each device
- Direct verification of encryption across the estate identified
- Testimony from delivery personnel on what they do with equipment overnight when working away
- Any incident or near miss involving a device, and what followed

Scoring note

Estate coverage is tested under 9.6. Encryption verified on company laptops while surveyors photograph sites on personal phones does not cover the estate, since those phones are Controlled Devices.

The vehicle limb is tested through interview rather than through policy. Personnel who describe leaving equipment in a locked boot overnight evidence a control that has not reached them.

Survey instruments, data loggers and cameras with onboard storage are Controlled Devices and are frequently omitted from a device register built around IT equipment.

S4.06 — Site discipline

Type	H, human factor and behaviour
Applies to	Operational
Source	DEFCON 76. ISN 2026/04 Annex B paragraph 16. Establishment security regulations.
Principle	Gov 7, Gov 8. MOD 4.

Requirement

The Organisation shall require its personnel on a controlled site to display identification, to remain within the areas authorised, to present their own credentials at access-controlled points, to keep working material on their person or secured, and to complete an end of day check confirming that nothing has been left.

The Organisation shall operate a photographic protocol stating what may be captured, and shall require incidental capture outside scope to be reported and deleted.

Evidence expected

- The protocol, and briefing records covering it
- Testimony describing what an individual did on a specific site
- End of day check records
- Any report of incidental capture, and what followed

Scoring note

A report of incidental capture, correctly handled, evidences this requirement more strongly than an absence of reports. The Assessor asks whether anyone has ever photographed something they should not have, and treats a candid answer as evidence rather than as a shortfall.

Personnel who describe holding a door for a colleague at an access-controlled point evidence a briefing that did not land.

S4.07 — Minimisation and output review

Type	P, process and procedure
Applies to	Both
Source	Secure by Design principle 7. ISN 2026/04 Annex B paragraph 16.
Principle	Gov 7. MOD 1, MOD 4.

Requirement

The Organisation shall confine collection to what the deliverable requires, shall review each output before issue to confirm that it contains nothing beyond the agreed scope, and shall issue outputs only to named recipients with a need to know.

Evidence expected

- Evidence of the review, recorded against outputs from sampled engagements
- The recipient list for each output
- Any instance of material removed from an output at review
- Testimony on who performs the review and what they look for

Scoring note

An instance of something being removed at review is the strongest evidence available for this requirement. Its absence across the sample suggests review as a formality.

Distribution to a group mailbox or a shared folder without a named recipient list scores 1.

S4.08 — Return, destruction and retention

Type	P, process and procedure
Applies to	Both
Source	ISN 2026/04 Annex B paragraphs 7, 15, 37.
Principle	Gov 7, Gov 10. MOD 7.

Requirement

The Organisation shall return Authority Property on completion of the contract, or destroy it where the Contracting Authority so directs, and shall record which course was taken.

The Organisation shall destroy controlled material no longer required by a method making reconstitution very difficult or impossible. Where material cannot be destroyed by such a method, it shall be returned to the Contracting Authority.

The Organisation shall apply the retention period stated by the Contracting Authority, and shall hold a retention schedule covering the records this framework generates.

Evidence expected

- Return records, with confirmation from the receiving party where obtainable
- Destruction records, stating method
- The retention schedule
- Testimony on what happens to a customer's drawings at the end of a job

Scoring note

Return of Authority Property is the limb most frequently absent. An Organisation that securely destroyed customer-issued drawings rather than returning them has not met the requirement, whatever the security of the destruction.

Cross-cut shredding to DIN 66399 Level P-4 or above satisfies the destruction limb for paper. The Assessor records the standard applied rather than requiring a particular one.

A retention schedule that states a single period for everything scores 1, since contractual retention varies by record type.

S4.09 — Protection of systems holding controlled information

Type	T, technical control
Applies to	Both
Source	ISN 2026/04 Annex B paragraphs 25 and 26. NCSC 10 Steps to Cyber Security.
Principle	Gov 7, Gov 8. MOD 4.

Requirement

The Organisation shall apply the NCSC 10 Steps to Cyber Security proportionately to each system storing, processing or generating controlled information, and shall as a minimum:

- Run operating systems, applications and firmware that remain supported

- Patch in line with the manufacturer's schedule, and document the risk accepted where a patch cannot be applied
- Operate anti-virus software with current updates
- Take backups, and hold a documented contingency plan
- Protect any connection to the internet or an untrusted system by a firewall
- Lock unattended terminals automatically after no more than fifteen minutes
- Overwrite storage media before disposal

Evidence expected

- Direct verification of patch status, support status and endpoint protection across the estate identified at S4.05
- The contingency plan, and evidence that a backup has been restored or tested
- Screen lock setting observed
- The documented risk decision where a system cannot be patched

Scoring note

Estate coverage under 9.6 governs. Verification on office equipment while field devices are unmanaged does not cover the estate.

A current Cyber Essentials certificate evidences the majority of this requirement within its scope, and the Assessor records the scope and date rather than retesting what the certificate covers.

Backups asserted but never restored or tested score 1.

S5. Cyber and Technical Security

Weight at Combined scope: 12 per cent. Nine requirements, eighteen points available. Cyber scope only.

This section examines the delivery of digital and technical services into a customer environment. It does not examine the Organisation's own IT hygiene, which sits at S4.09 and applies at every scope.

S5.01 — Scope of system access agreed and bounded

Type	P, process and procedure
Applies to	Cyber
Source	ISN 2023/09 paragraph 14. ISN 2026/04 Annex B paragraph 13.
Principle	Gov 7. MOD 1.

Requirement

The Organisation shall agree, before access is taken, the systems, environments and data within the scope of each engagement, the duration of access, and the process by which access is removed.

The Organisation shall record the agreement and shall confine its activity to the scope agreed.

Evidence expected

- The recorded scope for sampled engagements, agreed before access
- Evidence that activity remained within it
- Any request for access beyond scope, with the written authority obtained
- Testimony describing what an engineer does on finding a system outside scope

Scoring note

An Organisation given broad administrative access by a customer, with no scope agreed, scores 1 at most. The obligation to seek definition rests on the Organisation and is not discharged by the customer's failure to impose one.

Access taken beyond scope without written authority scores 0 and is examined under S2.08 and DC-7.

S5.02 — Credential lifecycle

Type	T, technical control
Applies to	Cyber
Source	ISN 2026/04 Annex B paragraphs 26a and 26b. Defence Standard 05-138 Issue 4 access control provisions.
Principle	Gov 7, Gov 8. MOD 4.

Requirement

The Organisation shall operate named accounts for each individual, shall scope credentials to the need of the engagement, shall time-bound them where the customer's systems permit, and shall obtain confirmation from the customer that access has been revoked at close-out.

Credentials shall not be shared between individuals, stored in personal password managers, or reused across engagements.

Evidence expected

- Direct verification of account arrangements on a sampled engagement
- Revocation confirmation from the customer at close-out
- The credential handling arrangement, verified rather than described

- Testimony on where an engineer keeps engagement credentials

Scoring note

Revocation asserted by the Organisation without customer confirmation scores 1, where confirmation was obtainable.

Shared accounts used because the customer issued only one are scored on what the Organisation did about it. An Organisation that raised the position and recorded the response scores 1 as a minimum. One that accepted it silently scores 0.

Multi-factor authentication is examined here. Its absence where the customer's systems offer it scores 0.

S5.03 — Access control and privileged accounts

Type	T, technical control
Applies to	Cyber
Source	ISN 2026/04 Annex B paragraphs 26a, 26b, 26d, 26i.
Principle	Gov 7, Gov 8. MOD 4.

Requirement

The Organisation shall apply least privilege to the access it holds and to the access it configures for others, shall hold current lists of authorised users for systems it administers, and shall require administrators to perform standard user functions from standard accounts rather than from privileged ones.

Evidence expected

- Direct verification of privilege levels held on a sampled engagement
- Authorised user lists, with evidence of review
- The account arrangement operated by the Organisation's own engineers
- Testimony on how a privilege escalation request is handled

Scoring note

Privileged accounts used for routine work score 0, irrespective of the policy.

Where the Organisation administers a system for the customer, the authorised user list is examined for currency. A list containing leavers scores 1.

S5.04 — Logging and monitoring

Type	T, technical control
Applies to	Cyber
Source	ISN 2026/04 Annex B paragraph 26f. Secure by Design principle 5.
Principle	Gov 5. MOD 4, MOD 7.

Requirement

The Organisation shall enable security logging on systems it delivers, configures or administers, capturing as a minimum all logon attempts whether successful or failed, logoff including timeout, and the creation, deletion or alteration of access rights, privileges and passwords.

Each record shall capture event type, user identity, date and time, and device identity. Records shall be held so that they are inaccessible to users without a need to know.

Where the Organisation does not administer the system, it shall record what logging the customer operates over its own activity.

Evidence expected

- Direct verification of logging configuration on a sampled engagement
- A log extract demonstrating the fields captured
- The access arrangement protecting the records
- The recorded position on customer-operated logging, where the third limb applies

Scoring note

Logging enabled by default with no verification that the required events and fields are captured scores 1.

The third limb matters more than it appears. An Organisation working on a customer system that does not log its activity is exposed on any subsequent dispute, and an Organisation that identified and recorded that position evidences the requirement.

S5.05 — Vulnerability management

Type	P, process and procedure
Applies to	Cyber
Source	Secure by Design principle 5 and the activities on vulnerability management and discovery. ISN 2023/09 paragraph 42.
Principle	Gov 2, Gov 5. MOD 6.

Requirement

The Organisation shall operate a process for identifying, recording, prioritising and remediating vulnerabilities in what it delivers, and shall report a vulnerability discovered in a customer environment to the customer rather than acting on it unilaterally.

Findings from security testing shall be recorded and acted upon, and shall be made available to the customer.

Evidence expected

- The vulnerability record, with dates of identification and remediation
- Evidence of a vulnerability reported to a customer, and the handling that followed
- Prioritisation applied, and the basis for it
- Testimony on what an engineer does on finding an unexpected weakness

Scoring note

The testimony item is decisive. An engineer who describes fixing something quietly evidences a process that has not reached delivery.

An Organisation with no vulnerabilities identified during the assessment period is examined on whether it looks. Absence of findings without any means of discovery scores 0.

S5.06 — Secure configuration and design

Type	T, technical control
Applies to	Cyber
Source	ISN 2023/09 paragraphs 31, 32 and Annex A. Secure by Design principles 6, 7, 8.
Principle	Gov 6, Gov 7, Gov 8. MOD 4.

Requirement

The Organisation shall configure what it delivers so that unnecessary functionality, services, accounts and data are removed, shall apply layered controls so that failure of one does not expose the whole, and shall design so that future security controls can be introduced without rework.

Where the customer operates approved architectural patterns or standard tooling, the Organisation shall use them in preference to its own.

Evidence expected

- Configuration standards or baselines held, and evidence of application
- A build or handover record showing what was removed or disabled
- Evidence of customer patterns applied where they exist
- Testimony describing a design decision taken on security grounds

Scoring note

Delivery on vendor default configuration scores 0.

The layering limb is tested by asking what happens when a named control fails. An answer identifying the backstop scores towards 2.

Where the customer specified a configuration the Organisation considered weak, the requirement is scored on whether the Organisation recorded the position rather than on the configuration delivered.

S5.07 — Third-party products and components

Type	S, supply chain
Applies to	Cyber
Source	Secure by Design principle 2 and the activity on managing third-party product security risks. ISN 2023/09 paragraph 37.
Principle	Gov 2. MOD 5.

Requirement

The Organisation shall assess the security of third-party products, libraries, components and services it introduces into a customer environment, shall record the assessment, and shall keep the position under review while the component remains in use.

Where a vulnerability is identified in a component the Organisation introduced, it shall inform the customer.

Evidence expected

- The assessment record for components introduced on sampled engagements
- The inventory of components in use
- Evidence of review, and of a customer being informed where a vulnerability arose
- The route by which the Organisation learns of vulnerabilities in components it has used

Scoring note

An Organisation with no means of learning about vulnerabilities in components it introduced cannot meet the review limb and scores 1 at most.

Components introduced before the assessment period remain within the requirement where they remain in use.

An inventory listing products without version information scores 1.

S5.08 — Testing and validation

Type	P, process and procedure
------	--------------------------

Applies to	Cyber
Source	ISN 2023/09 paragraphs 39, 41, 42, 43. Secure by Design principle 9.
Principle	Gov 9. MOD 6.

Requirement

The Organisation shall validate that the security controls it delivers operate as intended, before the system handles customer data and at the design points the engagement defines.

Acceptance testing shall evaluate security controls alongside functional ones, and non-conformances shall be addressed before the system is used.

Evidence expected

- Test records covering security controls on sampled engagements
- Non-conformances raised, and evidence of closure before go-live
- The point in the engagement at which testing occurred
- Any independent testing commissioned, with its findings

Scoring note

Functional testing that incidentally covers security is not security testing. The record identifies what security property was tested.

An Organisation that went live with an open non-conformance scores 0 unless it evidences the customer's recorded acceptance of the position.

Repeatable or automated testing scores towards 2 where evidenced.

S5.09 — Secure change and decommissioning

Type	P, process and procedure
Applies to	Cyber
Source	Secure by Design principle 10 and the activity on retiring components securely. ISN 2026/04 Annex B paragraph 26k.
Principle	Gov 10. MOD 7.

Requirement

The Organisation shall evaluate the security impact of a change before deploying it, shall record the evaluation, and shall apply a route by which a change can be reversed.

Where the Organisation retires a system, service or component, it shall remove the access, credentials, data and connections associated with it, shall overwrite storage media before disposal, and shall confirm the position with the customer.

Evidence expected

- Change records showing security evaluated before deployment
- Rollback arrangements, and evidence of use where a change was reversed
- Decommissioning records, with customer confirmation
- Testimony on what happens to data when a component is retired

Scoring note

Decommissioning is the limb most frequently absent. Systems left running with live credentials after an engagement ends are found by asking what happened to the last environment the Organisation stood up.

Change evaluation performed for operational impact with security considered only where someone raised it scores 1.

S6. Incident Management and Continuous Assurance

Weight at Combined scope: 10 per cent. Six requirements, twelve points available.

Two disqualifying conditions attach here. The weight understates the section's significance deliberately, because the failures that matter most are handled at Section 12 of the framework rather than by score.

S6.01 — Incident recognition and reporting

Type	P, process and procedure
Applies to	Both
Linked DC	DC-8
Source	Secure by Design principle 5. GovS 007. ISN 2026/04 Annex B paragraph 31.
Principle	Gov 5. MOD 3, MOD 7.

Requirement

The Organisation shall operate a documented process for recognising and reporting security incidents and near misses.

The process shall state what constitutes an incident, the reporting route, the timescale applying at each step, and the point of contact. It shall be given to personnel before they begin work on an engagement.

An incident shall reach the individual at S1.01 within the timescale stated.

Evidence expected

- The process, with its definitions and timescales
- Briefing records covering it, and testimony that personnel received it
- Incident records showing the route and the timing actually followed
- Testimony describing what an individual would do in a specific scenario

Scoring note

A process defining incidents only as loss of information, omitting unauthorised access, suspected surveillance, approaches for information about the engagement, and compromise of credentials, scores 1.

Where reportable events occurred during the assessment period and the process was not invoked, the requirement scores 0 and the Assessor tests DC-8.

Testimony is tested by scenario under 9.7. An individual who names no procedure but describes the correct action evidences the requirement.

S6.02 — External reporting

Type	C, contractual and statutory
Applies to	Both
Linked DC	DC-9
Source	ISN 2026/04 Annex B paragraphs 31, 32, 33. The extant Industry Security Notice on incident reporting.
Principle	Gov 5. MOD 5, MOD 7.

Requirement

Where a security incident affects controlled material, the Organisation shall report it to the Contracting Authority within the timescale the contract states, and immediately where none is stated.

Where Defence Related Classified Material has been lost or otherwise compromised, the Organisation shall also report immediately to the MOD Defence Industry Warning, Advice and Reporting Point, and shall follow the instructions in the extant Industry Security Notice on incident reporting.

The Organisation shall hold the reporting contact details in advance and shall not rely on locating them at the time.

Evidence expected

- The reporting contact details held, and where they are held
- Reports made during the assessment period, with their timing
- Any acknowledgement or advice received in response
- Testimony from the individual who would make the report, on who they would contact

Scoring note

An Organisation operating a competent internal process while holding no external route scores 1. Internal handling does not discharge the external obligation.

Failure to report an actual loss or compromise of Defence Related Classified Material to both recipients scores 0 and engages DC-9.

Where no incident occurred during the assessment period, 2 remains available on the recorded route together with testimony identifying it correctly. An individual who would report to the customer alone, unaware of the Warning, Advice and Reporting Point, evidences a route that has not reached them and scores the requirement at 1.

S6.03 — Recording and investigation

Type	R, record and register
Applies to	Both
Linked DC	DC-8
Source	ISN 2026/04 Annex B paragraphs 31 to 33. GovS 007.
Principle	Gov 5, Gov 9. MOD 3.

Requirement

The Organisation shall complete a written record of each security incident within twenty-four hours, or within the period the contract states where shorter.

The record shall state what occurred, what material or access was affected, the actions taken, and the notifications made.

The Organisation shall investigate proportionately to the incident, shall record the cause, and shall record any change to controls arising.

Evidence expected

- Incident records across the assessment period
- Investigation records, proportionate to the incidents they cover
- Completeness of the log against events disclosed in interview
- Evidence of a control changed in consequence

Scoring note

Contemporaneity is tested under 9.4. Records created together after the event score 0.

A log holding fewer entries than interviews disclose is incomplete, and the Assessor tests whether the omission engages DC-8.

A record stating what happened without stating what changed scores 1.

S6.04 — Reporting culture

Type	H, human factor and behaviour
Applies to	Both
Source	Secure by Design principle 5. NPSA guidance on insider risk and reporting.
Principle	Gov 5. MOD 3.

Requirement

The Organisation shall state to its personnel that there is no penalty for reporting in good faith, including the report of an individual's own error, and shall provide a route by which any person can report.

The Organisation shall not treat a report that turns out to be nothing as a failure by the person who made it.

Evidence expected

- The statement, in the briefing and in the procedure
- Testimony from delivery personnel on whether they would report their own mistake
- Near miss records
- Any instance of a self-reported error, and how it was handled

Scoring note

This requirement is scored on testimony rather than on the statement. Where personnel would hesitate to report their own error, it scores no higher than 1 whatever the procedure says, and the finding is recorded.

An instance of a self-reported error handled without sanction scores 2 where corroborated. It is the strongest evidence available for this requirement.

An absence of near miss reports across the period, in an Organisation performing site work, suggests under-reporting rather than an absence of near misses. The Assessor examines which it is.

S6.05 — Lessons and improvement

Type	P, process and procedure
Applies to	Both
Source	Secure by Design principle 9. ISN 2023/09 paragraphs 44 to 46.
Principle	Gov 9. MOD 7.

Requirement

The Organisation shall record what it learns from incidents, near misses, close-out reviews and customer feedback, and shall reflect that learning in the procedure, the briefing and the engagement risk assessment.

Where a lesson produced no change, the Organisation shall record the reason.

Evidence expected

- The lessons record
- A traceable change to a document arising from a recorded lesson
- Version history showing when the change was made
- Testimony on whether briefings have altered over the period

Scoring note

A lessons log with no traceable change to any document across the assessment period scores 1.

A single traceable change, from a recorded lesson through to an amended briefing, scores towards 2 and evidences the loop the requirement seeks.

A close-out review recording that nothing was learned, on every engagement in the sample, is examined under S2.09 as well as here.

S6.06 — Continuous assurance and audit

Type	P, process and procedure
Applies to	Both
Source	Secure by Design principle 9. ISN 2026/04 Annex B paragraph 46. ISN 2023/09 paragraph 25.
Principle	Gov 9. MOD 6, MOD 7.

Requirement

The Organisation shall review its own security position at intervals of no more than twelve months, covering the operation of the procedure, the currency of its records, the competence at S1.05, and any change to the obligations identified at S1.06.

The Organisation shall retain records so that it can demonstrate compliance on request, and shall cooperate with any audit or inspection by the Contracting Authority, the prime contractor, or a Designated Security Authority.

Evidence expected

- The review record, stating what was examined and what was found
- The retention arrangement, applied
- Any audit or inspection by a customer or prime, and the Organisation's response
- Evidence of action following an audit finding

Scoring note

A review that examined nothing in particular and concluded that everything was satisfactory scores 1.

Where the Organisation has been audited by a customer or prime, its response to that audit evidences this requirement more strongly than an internal review conducted alone.

An Organisation that has never been audited and conducts a substantive internal review scores 2 where the review is corroborated by a change arising from it.

S7. Supply Chain

Weight at Combined scope: 10 per cent. Five requirements, ten points available.

This section may be recorded Not Engaged under WMA-SBD-001 10.7 where the Organisation engages no subcontractors on work within scope. The declaration is made at scoping and verified during sampling. Associates engaged on a day rate are subcontractors for this section.

S7.01 — Assessment before engagement

Type	S, supply chain
Applies to	Both
Linked DC	DC-10
Source	ISN 2023/09 paragraphs 35 to 38. Secure by Design principle 2.
Principle	Gov 2. MOD 5.

Requirement

The Organisation shall assess the security arrangements of a subcontractor before engaging it on work within scope, shall record the assessment, and shall record the decision to engage.

The assessment shall address the subcontractor's handling of controlled information, the screening of its personnel, its incident reporting, and its own use of further subcontractors.

Where the Organisation identifies a shortfall and engages the subcontractor regardless, it shall record the shortfall, the reason for proceeding, and the additional control applied.

Evidence expected

- The assessment record for each subcontractor used on sampled engagements, dated before engagement
- The engagement decision, and who took it
- Any recorded shortfall, with the control applied in consequence
- Testimony on how a new subcontractor is brought on

Scoring note

An assessment dated after the subcontractor began work scores 0 and the Assessor tests DC-10.

Self-declaration by the subcontractor is a single source under 9.8. An Organisation relying wholly on a signed statement, with no verification of any kind, scores 1.

A recorded shortfall accepted with a compensating control evidences the requirement more strongly than an assessment finding nothing, since it demonstrates that the assessment carries consequence.

S7.02 — Flow-down of security conditions

Type	C, contractual and statutory
Applies to	Both
Linked DC	DC-10
Source	ISN 2026/04 paragraphs 2, 17, 20 and Annex B paragraphs 34, 35, 36. DEFCON 660. DEFCON 658.
Principle	Gov 2. MOD 5.

Requirement

The Organisation shall incorporate the applicable security conditions into each subcontract for work within scope, covering the OFFICIAL and OFFICIAL-SENSITIVE Contractual Security Conditions where they apply to the head contract.

Where the subcontracted work is classified, the Organisation acts as Contracting Authority and shall issue its own Security Aspects Letter to the subcontractor, shall obtain a signed acknowledgement before work begins, and shall seek permission to subcontract where the extant Industry Security Notice requires it.

Where the head contract incorporates DEFCON 658, the Organisation shall flow it down and shall complete a Risk Assessment for the subcontract using the Supplier Cyber Protection Service.

Where the Organisation would subcontract OFFICIAL-SENSITIVE work to a facility in a third country, it shall obtain approval using MOD Form 1686.

Evidence expected

- The subcontract, or the terms incorporated into it, showing the conditions flowed down
- Security Aspects Letters issued by the Organisation, with acknowledgements
- Risk Assessment references issued for subcontracts where DEFCON 658 applies
- Any MOD Form 1686 submitted, with the approval

Scoring note

Flow-down is evidenced by the subcontract rather than by the Organisation's statement that flow-down occurs. The Assessor examines the document.

A purchase order carrying no security terms, issued for work under a contract with security conditions, scores 0 and the Assessor tests DC-10.

The Security Aspects Letter limb is the one most often missed. An Organisation that received a letter and did not pass the relevant aspects to a subcontractor working on the same classified material has not met this requirement, and DC-4 is examined in addition.

S7.03 — Subcontractor personnel

Type	S, supply chain
Applies to	Both
Source	ISN 2026/04 Annex B paragraphs 16, 17. GovS 007.
Principle	Gov 1, Gov 7. MOD 5.

Requirement

The Organisation shall apply to subcontractor personnel the same requirements it applies to its own, covering baseline screening at S3.04, clearance or escort at S3.05, statutory notice at S3.07, and briefing at S4.06 and S6.01.

The Organisation shall confirm the position for each named individual rather than accepting a general assurance about the subcontractor's workforce.

Evidence expected

- Screening and clearance status recorded against named subcontractor individuals on sampled engagements
- Briefing records covering subcontractor personnel
- The signed statutory notice for those individuals
- Testimony from a subcontractor worker, where one is available during the assessment

Scoring note

A general assurance covering the subcontractor's workforce, without confirmation against the named individuals who attended, scores 1.

Where subcontractor personnel attended a site and no briefing record exists for them, the requirement scores 0.

Testimony from a subcontractor worker, where the Assessor can obtain it, is the strongest corroboration available for this requirement.

S7.04 — Oversight during delivery

Type	S, supply chain
Applies to	Both
Linked DC	DC-10
Source	ISN 2023/09 paragraph 36. ISN 2026/04 Annex B paragraph 46.
Principle	Gov 2, Gov 9. MOD 5, MOD 6.

Requirement

The Organisation shall maintain oversight of a subcontractor for the duration of the work, shall require the subcontractor to report security incidents to it on the same terms as its own personnel, and shall retain the right to audit the subcontractor's security arrangements.

Oversight shall be recorded, and shall be proportionate to the sensitivity of the work subcontracted.

Evidence expected

- Oversight records across the sampled engagements
- The incident reporting obligation stated in the subcontract, and any incident reported under it
- The audit right, and evidence of it being exercised where the work warranted
- Testimony on what the Organisation would do on learning of a problem at a subcontractor

Scoring note

Assessment before engagement with nothing afterwards is the pattern this requirement addresses, and it scores 0 where the work was sensitive. The Assessor tests DC-10, which is engaged by absent oversight as well as by absent assessment.

An audit right that has never been exercised is acceptable where the work did not warrant it. The Assessor records the basis on which the Organisation judged that.

S7.05 — Subcontractor close-out

Type	S, supply chain
Applies to	Both
Source	ISN 2026/04 Annex B paragraphs 15, 37. Secure by Design principle 10.
Principle	Gov 7, Gov 10. MOD 7.

Requirement

The Organisation shall confirm, on completion of subcontracted work, that credentials issued to subcontractor personnel have been revoked, that controlled material held by the subcontractor has been returned or destroyed, and that passes, keys and tokens have been returned.

The Organisation shall obtain confirmation from the subcontractor and shall record it.

Evidence expected

- Close-out confirmations obtained from subcontractors on sampled engagements
- Revocation records for credentials issued

-
- Destruction or return records covering material the subcontractor held
 - Testimony on what happens when a subcontractor finishes

Scoring note

Close-out asserted by the Organisation without confirmation from the subcontractor scores 1.

Material held by a subcontractor is the holding most frequently overlooked at close-out, because the Organisation's own close-out at S2.09 addresses what it holds itself. The Assessor asks specifically what the subcontractor still has.