

NHS DSPT Evidence Preparation & Assurance Checklist



IG-Smart Ltd · Practical Guide Collection · 25 October 2026

General information and original working aids; not legal advice, certification, clinical authorisation or regulatory approval. NHS identity appearing in retained illustrative artwork does not imply NHS approval or endorsement.

Use this guide to make a better-evidenced decision. This is general information and an original working aid, not a client-specific legal opinion, certification, clinical safety authorisation or regulatory approval. Apply the relevant jurisdiction, current requirements and competent professional review to your circumstances. Examples are illustrative unless expressly attributed.

Your first three steps

1. Confirm the organisation category and current portal requirements.
2. Map each requirement to an owner, current evidence and verification record.
3. Check cycle-specific assurance requirements before agreeing an audit or submission decision.

A 2026–27 version 9 practitioner guide to applicability, evidence ownership, assertions, audit readiness and defensible submission

Executive proposition: Data Security and Protection Toolkit (DSPT) readiness is not achieved by uploading a large folder of policies. It requires an organisation-specific answer to the applicable outcomes, assertions and evidence, supported by current proof of control operation, accountable owners and explicit treatment of gaps.

For: NHS trusts, ICBs, relevant NHS suppliers, health and social care organisations, DSPT leads, IG managers, DPOs, CISOs, internal audit, assurance committees and accountable executives. **Scope:** a readiness and evidence governance aid, not an NHS-issued checklist, official assessment, auditor opinion or guaranteed standards-met submission.

Executive briefing: what changed for the 2026–27 cycle?

The DSPT is an online self-assessment used by organisations with access to NHS patient data and systems. Requirements differ by organisation category, so a trust, key IT supplier and smaller care provider should not rely on the same generic evidence inventory. [S1]

Current cycle: The DSPT portal provides **2026–27 version 9 category-specific requirements** and states a **30 June 2027 submission deadline**. Use the requirements and applicable framework assigned to your organisation, rather than a single generic worksheet. [S2]

Official source detail: For category 3/4 item 10.2.1, the current v1.1 worksheet asks whether IT-system suppliers have robust cyber security arrangements. Its guidance includes certification checks and an explanation of assurance activities where suppliers lack certification. It does not establish a universal requirement for every supplier to hold ISO 27001 or Cyber Essentials Plus. Use the exact worksheet and category assigned to the organisation. [S2]

Important source limitation: the linked Strengthening Assurance page still describes **2025-26 version 8** guidance and a 30 June 2026 validity date. It does **not** establish the independent-assessment or mandated-audit requirements for version 9. Confirm the current category and cycle with the DSPT portal or NHS England before commissioning an assessment or making a submission claim. [S3]

The aim is not “pass on the first try” marketing. It is to create a defensible, current record: **applicable requirement → accountable owner → operational evidence → independent challenge where required → resolved or managed exception → authorised submission**.

1. Establish your organisation category first

The DSPT portal publishes category-specific requirements, including outcome/indicator material for relevant NHS bodies and assertion/evidence items for other sectors and supplier categories. Confirm how your organisation is registered and which current worksheet applies. Do not paste an older-year response set onto this cycle without reconciling changes.

Readiness question	Required action	Evidence
Registered entity	Confirm legal entity and DSPT organisation profile	Organisation code, owner and access rights
Assigned category	Identify the correct 2026–27 category and framework	Applicable version 9 requirement file
Submission responsibility	Confirm accountable approving executive and operational leads	Governance appointment and delegation
Current status	Record previous publication and open improvement plan	Last outcome, approved improvement records
Independent assurance	Verify whether mandatory audit requirements apply	Current strengthening-assurance guidance
Dependencies	Map NHS systems, services, suppliers and information flows	Data/system inventory and contracts

Essential distinction: a supplier's DSPT return does not automatically discharge a deploying trust's obligations. Likewise, ISO/IEC 27001 certification may support relevant evidence but cannot be treated as universal proof that every DSPT assertion has been met.

2. The IG-Smart DSPT Evidence Traceability Chain — seven stages

Gate	Control question	Evidence	Escalation
D1 Scope	Are entity, category and active requirement version correct?	Versioned applicability register	Wrong profile or omitted entity
D2 Accountability	Is each assertion or outcome allocated to a real owner?	RACI and delegated sign-off	Unowned mandatory requirement
D3 Implementation	Is the control actually operating?	Procedure, configuration, ticket, logs	Policy only, no implementation proof
D4 Evidence	Is the artefact current, relevant and retrievable?	Secure location, dates, scope	Stale or unrelated evidence
D5 Challenge	Has evidence been meaningfully reviewed?	Peer/independent review record where applicable	Unsupported claim or conflict
D6 Remediation	Are gaps tracked and managed to closure?	Action, risk, exception, retest	Critical exposure concealed
D7 Submission	Is the final response supportable and approved?	Versioned submission register and authorised sign-off	Unreconciled mandatory item

This chain is original IG-Smart working guidance, not the official DSPT assertion list and not a substitute for it.

3. Evidence quality: what actually proves a control?

A policy establishes intent. Strong assurance additionally requires evidence that the control works within the correct service and review period. A privileged-access policy, for example, should be supported where appropriate by relevant identity-system settings, access review samples, exceptions and accountable approval. An incident-response plan should be supported by a realistic exercise, after-action report and completed remediation—not only a document bearing the latest year.

Evidence verification rubric

Evidence maturity	What it shows	Risk of overclaim
Stated	Policy, procedure or management assertion	No observed operation
Implemented	Configuration, documented process or completed task	May not be verified over time
Tested	Observed outcome, sampling or drill	Scope and sampling may be narrow
Challenged	Independent or competent review of relevant claims	Objectivity and scope still matter
Sustained	Repeated evidence, resolved exceptions and monitored performance	Not absolute assurance or immunity

Do not assign numerical confidence values as if they were official DSPT scoring criteria. Use the portal's prescribed assessment method for formal submissions.

4. Thirteen thematic evidence domains for planning

This is an IG-Smart planning overlay, not a reproduction of the official v9 assertions. Map each field to actual current DSPT requirement IDs before final use.

Planning domain	Indicative artefacts to request	Challenge question
Senior governance	Risk committee minutes, owners, risk appetite	Is executive scrutiny demonstrable?
Data mapping	Patient data inventory, flows and access permissions	Is the actual NHS boundary known?
Identity and privileges	MFA, privileged access review, leavers	Can exceptions be traced and closed?
Asset security	Asset inventory, supported versions, exposure	Are critical assets outside coverage?
Vulnerability	Scans, prioritisation, remediation evidence	Are exploitable overdue issues owned?
Secure design	Security architecture, change controls, supplier assurance	Have shared responsibilities been tested?
Monitoring	Logging scope, alert escalation, test incidents	Can consequential misuse be detected?
Incident readiness	Exercises, reporting criteria and communications	Can relevant reporting deadlines be met?
Continuity	BIA, backup/restore and recovery exercise	Was recovery tested for actual services?

Planning domain	Indicative artefacts to request	Challenge question
Workforce	Role-specific training and competency evidence	Does training alter operational practice?
Supplier assurance	Contract, evidence reviews, subprocessor oversight	Do critical suppliers introduce unowned risk?
Privacy	DPIA, rights, lawful processing and breach governance	Are obligations applied to actual flows?
Audit and exceptions	Review programme, findings, action verification	Is the submission evidence internally consistent?

5. A linked evidence ledger every team can use

Use a stable record ID to join these two views. Keep the official requirement ID and category alongside the evidence; the example is a structure, not a real submission or claim of conformity.

View A - requirement and source

Record ID	Current requirement ID	Accountable owner	Evidence reference and version	Service, system and period covered
D-001	Insert actual portal requirement	Named owner	Controlled source link	Record the precise boundary

View B - verification and decision

Record ID	Reviewer and review date	Finding and limitations	Action, owner and due date	Decision and authority
D-001	Named reviewer; actual date	Supported / gap / not established, with reasons	Specific corrective action	Open / escalated / verified closure

Do not treat a source link as verification. Identify what was examined, what it establishes and what remains unknown. Keep access-controlled records outside the public website and do not place patient data in a general worksheet.

6. Common avoidable preparation failures

Wrong version: evidence mapped to the prior year's assertions or an inapplicable category. **Owner ambiguity:** policies signed by the IG lead despite implementation belonging to another team. **Policy-as-proof:** comprehensive wording without logs, tests or exceptions. **Historical tests:** a prior-year restore reused despite material infrastructure change. **Supplier blind spot:** treating an assurance certificate as proof of the exact NHS-hosted service. **Scope drift:** changing subsidiaries, services or data flows without reassessment. **Unresolved remediation:** logging an issue as complete without a verified outcome. **Inconsistent claims:** published answers contradicting other operational records.

A readiness review should mark these as traceable problems with a named owner and resolution condition—not rewrite the narrative until it sounds compliant.

7. Independent assessment and mandatory audit boundaries

The DSPT portal publishes **Strengthening Assurance** materials, but the source linked here is explicitly for version 8 (2025-26). Do not reuse its mandated areas, eligibility or terms of reference as confirmed version 9 requirements. Establish the applicable current-cycle assessment and auditor requirements with the portal or NHS England, record the response, and then agree scope and independence. Readiness support is not automatically an independent assessment, and not every registered organisation has identical audit obligations. [S3]

Before an audit: reconcile control ownership; confirm auditor eligibility/competence; agree evidence access and sampling; disclose conflicts; verify whether mandatory v9 audit areas apply; preserve findings without suppressing open gaps.

Audit-ready evidence pack structure

- **00 — Scope and requirement version:** registration details, category, dated framework extract.
- **01 — Governance:** accountabilities, approvals, audit programme.
- **02 — Control evidence:** one indexed record per relevant requirement.
- **03 — Testing:** samples, exercise results and scope limits.
- **04 — Gaps:** risks, exceptions, remedial actions and retests.
- **05 — External dependency:** supplier evidence and contracts.
- **06 — Submission record:** responses, reviewer challenge and approval.

8. Illustrative readiness scenarios

NHS trust with legacy device support. Evidence states all servers are patched, but clinical legacy devices run under an authorised exception. Readiness should expose the actual residual risk, compensating controls, governance approval and current plan instead of erasing the exception.

Key software supplier. It has ISO/IEC 27001 certification but outsourced incident support and privileged cloud support are not included in the evidence supplied. The assurance team checks entity, scope and current v9 category obligations rather than assuming certification proves every requirement.

Health charity with NHS data access. Its internal spreadsheet uses NHS trust requirements instead of the organisation's applicable DSPT category. Correct the applicability record and map evidence to the officially assigned worksheet before claiming submission readiness.

9. Executive readiness briefing

Organisation and profile: __; **DSPT 2026–27 v9 applicability source:** __; **deadline and internal submission date:** __; **requirement owner completion:** __; **material evidence gaps:** __; **independent assessment applicability:** __; **unacceptable unmitigated risks:** __; **remediation budget and owners:** __; **submission approver:** __; **decision:** submit / conditional preparation / defer and remediate; **re-review trigger:** __.

A submitted self-assessment should be represented accurately. An internal readiness checklist, a portal submission, an independently audited assessment and a published DSPT outcome are distinct events.

10. Fifteen evidence preparation questions

1. Which exact organisation profile and category applies?

2. Are we using the latest requirements for the current cycle?
3. Have we reviewed changes from the preceding version?
4. Who is authorised to approve the submission?
5. Who owns implementation for every requirement?
6. Does the evidence show operation rather than policy intent?
7. Is its scope exactly the covered legal entity and service?
8. Is evidence within an appropriate review period?
9. What control assumptions rely on critical suppliers?
10. Which exceptions are material and still active?
11. Can issues be retested and closed objectively?
12. Does the applicable category require independent assurance?
13. Can we provide evidence without exposing sensitive information?
14. Have internal challenge and executive review occurred?
15. What changes after submission will require monitoring?

11. Frequently asked buyer questions

Is DSPT a certification of the software product? No. The DSPT is an organisation-focused assessment; check its actual subject and publication status.

Are all v9 requirements identical for NHS trusts and suppliers? No. Refer to the current category-specific requirements.

Does ISO 27001 replace DSPT? No. Certification within a scope can support some evidence but does not complete the organisation's DSPT duties.

What is the 2026–27 deadline? The official DSPT portal states 30 June 2027 as of this edition; verify current portal status before publication or use.

Can an organisation submit despite gaps? Submission rules and representations depend on current official requirements; gaps must never be hidden or falsely represented.

Does a successful portal result prove every control works? No. The assessment has a defined method and evidential limitations; manage ongoing cyber/privacy risks continuously.

12. Next steps

Next step: Submit a Requirement identifying organisation type, current DSPT version/category, intended submission date and most material evidence gaps.

Sources

- [S1] DSPT official portal <https://www.dsptoolkit.nhs.uk/>
- [S2] DSPT, 2026–27 version 9 outcomes, assertions and evidence (current category-specific release) <https://www.dsptoolkit.nhs.uk/News/169>
- [S3] DSPT, Strengthening Assurance: 2025-26 version 8 (historical; not evidence of version 9 audit requirements) <https://www.dsptoolkit.nhs.uk/Help/64>
- [S4] NHS England, Data Security and Protection Toolkit overview <https://digital.nhs.uk/services/data-security-and-protection-toolkit>