

Enterprise Supplier Assurance Evidence Matrix



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. Map the supplier legal entity, service, access and critical dependencies.
2. Choose applicable controls and challenge evidence against the actual service.
3. Use the workbook to track gaps, then record a human decision and review triggers.

A board-defensible framework for vendor tiering, evidence verification, residual-risk decisions and continuous third-party oversight

Executive briefing: the three questions that matter before contract signature

Supplier assurance is frequently reduced to collecting an ISO certificate, a completed questionnaire and a penetration-test cover sheet. Those are useful artefacts. They are not, by themselves, a conclusion that the organisation can safely and lawfully depend on the supplier.

An ISO/IEC 27001 certificate must be checked for **holder, issuer, scope, sites, validity and relevance to the particular service**. A SOC 2 report requires attention to its period, boundaries, control exceptions, subservice organisations and complementary user-entity controls. A penetration test is time-bound, scoped and may not cover the deployed configuration, subcontractors or current threats. A cloud provider's strong platform controls do not automatically establish the customer's tenant security. These are examples of evidence interpretation, not reasons to dismiss third-party evidence altogether.

Before onboarding a material supplier, an accountable decision-maker should be able to answer:

1. **Dependency:** If this supplier fails, is compromised, changes subcontractors or becomes unavailable, which services, people, data and legal duties are affected?
2. **Evidence:** What proportionate proof supports the relevant controls, what is excluded, and which controls remain unverified or only self-attested?
3. **Decision:** Is the residual exposure within approved appetite, are binding conditions in place, and who has authority to accept or prohibit the arrangement?

The NCSC recommends understanding supplier risk, building proportionate requirements, checking arrangements and improving oversight throughout the relationship. It does not recommend treating questionnaire completion as assurance in itself. [S1][S2] ISO/IEC 27036-2:2022 addresses the security of supplier–acquirer relationships through definition, implementation, operation, monitoring and improvement. [S3]

The first-page decision card

Decision point	Required answer	If absent
Supplier and service identity	Legal entity, scope, owners, fourth parties, locations	Do not assume the organisation has assessed the correct entity or service
Inherent risk	Criticality, data sensitivity, privileged access, resilience, concentration, safety	Tier provisionally; seek missing facts
Mandatory safeguards	Applicable contracts, processing terms, access controls, incident duties, clinical/sector requirements	Hold or escalate; no numeric score can cure a mandatory gap
Evidence confidence	Current artefacts, correct scope, verified provenance, reviewer conclusion	Record unverified; do not mark 'compliant'
Residual-risk ownership	Specific unresolved exposures, mitigations, authorised decision	No silent acceptance by procurement or the assessor
Review triggers	Change, incidents, expiry, subprocessor variation, concentration	Decision expires or is reassessed on material change

Executive rule: An amber supplier with one evidenced, owned remediation plan may be a more defensible choice than a 'green' supplier whose unverified claims have been mis-scored as passed. Neither colour is a substitute for the decision record.

1. The legal and standards perimeter: apply only what actually applies

Supplier risk management draws on overlapping but non-interchangeable frameworks. The applicable duties depend on the organisation's role, sector, location, data, contract and actual supplier service. No single checklist establishes compliance with all of them.

Framework or regulatory context	What it contributes	Practical boundary
UK NCSC supply-chain guidance	Risk-led supplier identification, proportional checking, contractual influence, reassessment and board reporting	Guidance, not a universal certification checklist [S1][S2]
ISO/IEC 27001:2022 and ISO/IEC 27002:2022	Information security management; supplier relationship, agreements, ICT supply chain and review/change management controls often mapped to Annex A 5.19–5.22	A supplier's certificate does not automatically cover the service or every control; ISO standards are copyright-protected
ISO/IEC 27036-1:2021, -2:2022, -3:2023	Supplier relationship concepts, security requirements and ICT supply-chain guidance	The workbook is IG-Smart's interpretation, not a reproduction of proprietary standard text [S3][S4]
NIST SP 800-161 Rev. 1, Update 1 (2024)	Enterprise cyber supply-chain risk management, acquisition and multilevel risk integration	US-origin guidance; not automatically a UK statutory mandate [S5]
UK GDPR: Articles 28 and 32, plus transfer rules where relevant	Appropriate processor assurances, contractual terms, security and accountability	Not every supplier is a processor; first establish roles, processing, transfer facts and contractual responsibility [S6][S7]

Framework or regulatory context	What it contributes	Practical boundary
FCA / PRA outsourcing and operational resilience, where applicable	Important business service dependency mapping, outsourcing controls, materiality and accountability	Applicability varies by firm and activity. UK financial-sector CTP oversight and the 2027 reporting regime have their own boundaries [S8]
EU DORA (Regulation 2022/2554), where applicable	ICT third-party risk management, register, contractual controls for EU financial entities	DORA applies to specified EU financial entities and related defined parties; do not apply it automatically to every UK supplier [S9]
NHS DSPT, DTAC and clinical safety, where applicable	Specific organisational, product or deployment evidence; healthcare security and safety	Separate obligations, dependent on context. Supplier assurance cannot substitute for DCB0129/DCB0160 safety activity or a contracting body's decision
EU AI Act or AI-specific governance, where applicable	AI-specific actor duties, technical assurance and supply-chain responsibilities	Applicability and dates vary; generic supplier tiering does not replace legal classification

2026-specific source note: Current ICO international-transfer guidance explains the UK protection test; UK law now uses the phrase '**data protection test**' while the ICO continues to use 'transfer risk assessment (TRA)' in its guidance. A spreadsheet field labelled 'TRA/IDTA needed?' is only an intake prompt, never a legal conclusion. [S10] The FCA reports additional operational incident and third-party reporting requirements effective in March 2027 for firms within scope. [S8]

The three assurance boundaries often missed

- **Certification versus service evidence:** ISO/IEC 27001 certification is evidence of a scoped management system, not a claim that every supplied service is immune to compromise or that a buyer's configuration is compliant.
- **Controller accountability versus processor assurances:** Article 28 contractual safeguards and supplier diligence assist the controller, but outsourcing processing does not extinguish the controller's own legal obligations. [S6]
- **Operational dependence versus contract value:** A low-cost integration can have a critical privileged path into production; a high-value contract may have no access to regulated data or important services. Contract spend is not a sufficient risk proxy.

Supplier-type evidence prompts: apply the controls to the real service

The same procurement questionnaire can miss material differences between a cloud provider, an off-site records warehouse and a clinical safety-critical subcontractor. For each supplier category below, tailor the request to **actual processing, access, dependencies and contractual responsibilities**, rather than requiring every document in the same way.

Supplier category	High-value additional evidence to consider	Decision trap to avoid
IT managed service provider / privileged support	Access boundaries, privileged identity, subcontracted support, logging, change approvals, separation of clients and tested recovery	Treating the MSP's generic certificate as proof for the specific client's tenant and administrators
Data centre / cloud hosting / backups	Physical security, access logs, service-specific availability, key custody, restoration tests, geographical and fourth-party dependencies	Confusing the cloud provider's controls with the customer's application, configuration or data responsibilities

Supplier category	High-value additional evidence to consider	Decision trap to avoid
SaaS / enterprise software / AI-enabled tools	Processor roles, subprocessor chain, SSO/ MFA, application testing, development/ change controls, data flows, model integrations and retention	Assuming the brand name or standard contract demonstrates the actual deployed configuration
Marketing technology / analytics / data brokers	Lawful collection provenance, controller/ processor or joint-control analysis, consent/ PECR issues where relevant, profiling, transfers and deletion	Treating contractual promises of 'GDPR compliance' as proof of lawful sourcing and onward use
Off-site records, archives and backup media	Chain of custody, indexed retrieval, secure transport, physical premises controls, retention, secure destruction and incident recovery	Assuming physical custody and electronic data protection have identical safeguards
Pharmacovigilance / clinical service suppliers	Patient safety and pharmacovigilance accountability, relevant data protection, validation, reporting chains, subcontractors and incident escalation	Treating ordinary IT security evidence as sufficient for safety-critical regulated work
Facilities, maintenance, security and call centres	Site/visitor access, identity checks, supervised access, call recording and disclosure arrangements, continuity, subcontracting and staff training	Excluding the provider from governance because it is not labelled a technology supplier

Remote versus onsite review: Select a proportionate method based on the control that must be evidenced, the consequences of failure, access to reliable records and any contractual or sector requirement. Neither an onsite visit nor a remote documentary review is inherently mandatory or sufficient for every Tier 1 supplier. Record why the method supports the decision.

2. IG-Smart's Seven-Gate Supplier Evidence-to-Decision Method

Original working model — not a regulator-approved methodology. Each gate must produce traceable outputs. The gates are deliberately sequential: a polished assurance score cannot rectify a misidentified supplier or a missed legal mandate.

Gate	Decision	Minimum defensible output	Stop / escalation trigger
G1 — Define the dependence	What service, entity, environment, access, data and fourth parties are involved?	Scope statement, dependency map, service owner	Legal entity, hosted service or important dependency unknown
G2 — Determine exposure	What is the inherent effect of loss, compromise, misuse or supplier failure?	Human-reviewed tier, materiality rationale, regulatory overlays	Unrecognised patient-safety, regulated-data or critical-service exposure
G3 — Set evidence requirements	Which control claims must be demonstrated, at what depth?	Tier-specific evidence request and mandatory safeguards	Evidence demands do not address the actual risk
G4 — Verify claims	Is each artefact genuine, recent, appropriately scoped and independently interpreted?	Source reference, verifier, date, exceptions and limitations	Certificate mismatch; report is out of period; critical scope excluded
G5 — Establish contractual protection	Are responsibilities, access, incident, audit, subcontracting, exit and data terms enforceable?	Agreed contract/control schedule; owner sign-off	Mandatory processor terms, safety or resilience obligations absent

Gate	Decision	Minimum defensible output	Stop / escalation trigger
G6 — Decide residual risk	Which issues remain? Can they be accepted within authority and appetite?	Findings, mitigations, owner, expiry, signed accept/condition/ reject decision	Critical unmitigated risk; unauthorised waiver; unowned exception
G7 — Monitor change	What triggers re-evaluation throughout the relationship and at exit?	Monitoring plan, reassessment calendar, triggers and exit evidence	Material supplier or service change without review

Do not report 'seven gates passed = secure'. The purpose is to ensure no critical decision element becomes invisible. A separate quality assurance review should sample whether the process operated effectively.

3. Inherent-risk tiering: classify first, score only after scoping

The initial tier determines how much assurance work is needed; it must not be inferred from the percentage of documents already collected. Consider at least:

1. **Business criticality:** effect on important functions, regulatory delivery, finances and end users.
2. **Data exposure:** volume and sensitivity, special-category/health data, confidentiality and international processing.
3. **Privilege and connectivity:** direct production access, administrative control, network trust, code deployment, integration rights and support access.
4. **Concentration and substitutability:** single points of failure, geographic or provider concentration, recovery feasibility, fourth-party opacity.
5. **Human or clinical safety consequence:** whether failure or misuse can create clinical or other consequential human harm.
6. **Regulated-service classification:** whether sector-specific outsourcing, ICT, reporting, safety or processor duties are engaged.

Four illustrative assurance tiers

Tier	Typical characteristic	Illustrative due-diligence depth	Monitoring posture
Tier 1 — Critical	Patient safety, essential operating service, extremely sensitive processing, extensive privileged access or difficult-to-replace infrastructure	Full scoped evidence review; mandatory controls; legal/ operational overlay; contract and continuity review; authorised residual-risk decision	Enhanced, event-triggered and scheduled reviews appropriate to actual risk
Tier 2 — High	Material sensitive data, core system integration, meaningful business interruption or significant outsourced control	Substantive evidence assessment and material exception register	Regular service/risk monitoring with event triggers
Tier 3 — Moderate	Limited integration, bounded data exposure or recoverable non-critical service	Targeted questionnaire plus sample evidence and core contract checks	Scheduled and event-led reassessment
Tier 4 — Low	No material data/system access and readily replaceable service	Confirm scope, baseline controls and relevant contractual terms	Proportionate recheck when scope or risk changes

The tiers are **IG-Smart proposal labels**, not a mandated classification under ISO, NCSC, DORA, NHS or FCA rules. Organisation-specific materiality assessments and legal definitions override them where applicable. A human owner must approve the tier; an Excel formula may only suggest one.

Mandatory non-compensatory safeguards

Regardless of the weighted score, withhold unconditional approval where an applicable requirement is materially unmet. Typical examples include:

- No valid Article 28 processor agreement when required, or subprocessor engagement without required authorisation.
- Unresolved critical exposure affecting essential/clinical services or direct privileged access.
- Inability to establish what regulated personal data is processed or where restricted transfers occur.
- Lack of agreed incident notification cooperation for a critical supplier, where needed by law or contract.
- A material clinical-safety requirement left without the responsible clinical owner.
- A supplier refusal to provide proportionate assurance needed for a critical dependency, with no adequate alternative assurance.
- Unauthorised acceptance of material risks by a person without the relevant delegated authority.

Not every information gap is automatically a legal breach. Classify '**unknown**' separately from '**failed**', identify the consequence of the uncertainty and escalate proportionately.

4. Evidence reliability: a questionnaire is not a control test

IG-Smart evidence confidence ladder

Level	Evidence	What it can and cannot show
E0 — Unsubstantiated assertion	Sales statements, unchecked 'yes' answers, unsupported claims	Directional only; insufficient for material control assurance
E1 — Documented design	Policies, procedures, diagrams, contractual descriptions	Evidence that a control is described, not necessarily used effectively
E2 — Operational artefact	Time-stamped logs, sampled tickets, access recertifications, test outputs	Evidence of operation for a defined period/population, subject to representativeness
E3 — Independent or appropriately segregated review	Scoped assurance reports, independent test results, audit findings	Stronger challenge; still bounded by scope, period, sampling and exceptions
E4 — Corroborated and current	Multiple consistent sources, remediated exceptions, follow-up checks and live monitoring	Stronger confidence in the specified claim, never proof that risk is zero

Evidence level is not a single maturity score. For a simple control, a current operational artefact may be more decision-useful than an unrelated external certificate. Assess **identity, provenance, scope, currency, testing coverage, auditor independence, exceptions, applicability and configuration-specific responsibility**.

The 'five questions' test for every supplier artefact

1. **Whose?** Does it name the contracted legal entity, specific product, site, operating subsidiary and relevant subcontracted scope?
2. **What?** Which control assertion does it support—and which does it not address?

3. **When?** What period does it cover? Has a material change or incident occurred since?
4. **Who assessed it?** Is the assessor suitably competent and independent for the claimed conclusion?
5. **What remains?** Are exclusions, complementary customer controls, known vulnerabilities, outstanding findings or remediation conditions disclosed?

Evidence quality rule: 'Evidence received' and 'evidence verified' must be separate workflow states. Evidence should not receive full credit solely because a supplier uploaded a file.

5. The 36-control Enterprise Supplier Assurance Evidence Matrix

The matrix is a **reference library**. For each supplier, select only the controls relevant to the service and risk tier; justify each 'not applicable' finding. The source artefact may be reused across controls only where its content genuinely supports each claim. **M** denotes a potential mandatory gate **when applicable**, not an automatically universal legal requirement. The 1–5 weight is an illustrative prioritisation starting point, not a regulatory prescription.

ID	Assurance domain and required conclusion	Typical evidence to request and independently interpret	Illustrative weight	Gate?
SA-01	Entity and scope: supplier legal entity and service boundaries established	Contracted entity, product/service map, company records	3	M
SA-02	Accountability: named service, security and executive owners	RACI, contacts, escalation authority	3	
SA-03	Subcontracting: fourth parties and outsourced dependencies identified	Subprocessor list, architecture, fourth-party map	4	M
SA-04	Service/data locations: hosting, support and transfer locations understood	Data-flow and hosting location schedule	4	M
SA-05	Assurance scope: certificates/report boundaries match service	Valid scoped ISO certificate or assurance report	4	
SA-06	Policy governance: security governance and review cadence exist	Approved policies, accountability and review records	2	
SA-07	Risk management: supplier operates its own risk process	Risk criteria, register sample, management oversight	3	
SA-08	Independent review: external or segregated testing interpreted	Auditor report, scope, exceptions, remediation	3	
SA-09	Access management: least privilege and joiner/mover/leaver	IAM policy, access recertification sample, logs	5	M

ID	Assurance domain and required conclusion	Typical evidence to request and independently interpret	Illustrative weight	Gate?
SA-10	Privileged access: administrators and support access controlled	PAM/MFA proof, break-glass and session records	5	M
SA-11	Authentication: appropriate MFA and credential protection	Configuration evidence, access design and enforcement	4	
SA-12	Logging and detection: relevant events generated and reviewed	Log architecture, alert samples, response coverage	4	
SA-13	Asset and environment scope: assets and segregation known	Inventory, architecture, environment diagrams	3	
SA-14	Vulnerability management: vulnerabilities found, triaged and treated	Scan coverage, SLAs, exception and remediation evidence	5	M
SA-15	Independent security testing: tests fit the actual attack surface	Scoped pen-test summary, retest evidence, limitations	4	
SA-16	Secure change and software supply chain: controls over code/releases/dependencies	SDLC, change records, dependency/CI controls	4	
SA-17	Cryptographic protection: data protected appropriately	Encryption design, key ownership and key rotation	4	
SA-18	Tenant and cloud responsibility: provider/customer controls apportioned	Shared-responsibility matrix, tenancy hardening	5	M
SA-19	Incident preparation: triage, containment and contact arrangements	Incident plan, exercise and communication proof	5	M
SA-20	Notification cooperation: actionable reporting and evidence preservation	Contract clause, notification route, exercise	5	M
SA-21	Resilience: recovery objectives and dependencies assessed	BIA, RTO/RPO, recovery test and failure-mode evidence	5	M
SA-22	Concentration and substitution: material single-point dependencies handled	Substitution plan, concentration assessment	4	
SA-23	Exit and portability: practical transition and data retrieval	Exit plan, export test, termination rights	4	M

ID	Assurance domain and required conclusion	Typical evidence to request and independently interpret	Illustrative weight	Gate?
SA-24	Article 28 processor terms: compliant contract where role requires	Signed DPA, prescribed particulars and terms	5	M
SA-25	Subprocessor authorisation: appropriate permissions and flow-down	Authorisation record, notification and chain clauses	5	M
SA-26	Restricted transfers: roles, transfer mechanism and assessment established	Transfer map, adequacy/safeguard, TRA/data protection test where required	5	M
SA-27	Privacy rights and deletion: DSAR support, retention and disposal	Rights workflow, retention/deletion and return evidence	4	
SA-28	Data minimisation and purpose: processing limited to agreed purpose	Data inventory, processing instructions and configurations	4	
SA-29	Contractual assurance rights: reporting/audit and cooperation proportionate	Executed schedule, alternative independent assurance terms	4	M
SA-30	Material service/change duties: change and subservice notification	Contract terms, change notice process and samples	4	
SA-31	Security remedies: findings, timeframes and verification defined	Contractual remediation and service-credit clauses as appropriate	4	
SA-32	Regulatory classification: regulated outsourcing/ICT status documented	FCA/PRA/DORA applicability memorandum where relevant	5	M
SA-33	Clinical/safety overlay: risk ownership and deployment boundaries clear	DCB0129/0160 artifacts where relevant, clinical owner	5	M
SA-34	AI systems and data use: model suppliers, training use and assurance understood	Model/service inventory, AI terms, data-use limitations	4	
SA-35	Oversight and review: monitoring cadence and triggers assigned	Owner, KPIs/KRIs, meeting minutes, next review	4	
SA-36	Residual decision: senior authorised decision and limits recorded	Exception register, decision memo, approval date	5	M

Use the workbook rather than treating this table as a completed audit. The matrix should record an evidence reference, reviewer, status, scope, confidence, age, exceptions and decision for each relevant control. No supplier is automatically 'compliant' because all 36 rows appear in a spreadsheet.

Tier-specific evidence depth: a practical baseline

Question	Tier 1	Tier 2	Tier 3	Tier 4
Confirm legal entity, service and role	Required	Required	Required	Required
Verify high-impact security and access claims	Detailed, scoped	Substantive	Targeted	Baseline if applicable
Identify fourth parties and critical dependence	Detailed and documented	Documented	Where relevant	When discovered
Privacy/transfer contractual duties	Fully applied if engaged	Fully applied if engaged	Fully applied if engaged	Fully applied if engaged
Independent report or comparable alternative evidence	Strongly preferred where justified	Risk-led	Optional when proportionate	Usually not needed
Formal resilience/exit evidence	Detailed, risk-led	Proportionate	If relevant	When relevant
Senior risk acceptance	When required by delegated authority	If material residual risk	If outside appetite	If outside appetite
Monitoring plan	Enhanced + material change	Risk-led periodic + change	Periodic/event-led	Change-led

Legal requirements do not disappear because a supplier is 'low tier'. A low-tier processor still requires appropriate UK GDPR processing terms, for example. [S6]

6. From evidence to residual risk: do not confuse control confidence with risk acceptability

Four concepts must remain separate in the decision record:

- **Inherent risk:** exposure before the buyer relies on mitigating controls.
- **Control evidence confidence:** the strength and scope of verified material supporting the specific control claim.
- **Residual risk:** exposure remaining after considering controls and the organisation's deployment, shared responsibilities, vulnerabilities and dependencies.
- **Decision authority:** the person or committee authorised to accept, condition, pause or reject the arrangement.

Suggested scoring approach in the companion workbook

A 0–4 reviewer confidence value may be applied to a **verified, in-scope control**, with an illustrative prioritisation weight of 1–5. The workbook can calculate:

Evidence confidence (%) = $100 \times \text{SUM}(\text{weight} \times \text{verified confidence}/4) / \text{SUM}(\text{weight of applicable recorded controls})$

This is an **evidence confidence indicator**, not a cyber-risk probability, provider grade, legal compliance percentage or likelihood of breach. The denominator should exclude only documented, reviewer-approved non-applicable items. If the applicable control set is incomplete, the indicator remains provisional. A single missing mandatory safeguard overrides any otherwise favourable percentage.

Residual risk must be a separate assessed conclusion. One practical method uses the organisation's existing impact/likelihood scales plus documented mitigations, rather than inventing a universal supplier-risk scoring threshold. Where risk appetite is not approved, use 'decision pending' rather than an artificial green/amber/red conclusion.

Worked example: a fictional health-data SaaS vendor

Illustrative scenario only — no real client, provider, test or finding is represented.

A supplier hosts a clinical workflow application containing patient information. It offers a valid ISO certificate and a recent penetration-test letter. The buyer discovers: (a) the certification scope excludes the operational support subsidiary that can access customer tenants; (b) MFA enforcement is evidenced for employees but privileged break-glass access remains untested; and (c) an overseas subprocessor is listed without a documented transfer assessment.

An aggregate score could look reassuring because many policies exist. A defensible decision is **hold pending scope and legal clarification**, not 'pass with 86%'. The evidence owner should verify the support entity and privileged-control path, assess processor/subprocessor roles and any restricted transfer, and determine whether bounded corrective action can make the arrangement acceptable. Only an authorised buyer can decide whether and when to proceed.

Residual-risk decision categories

Outcome	Meaning	Required record
Approved	Applicable mandatory safeguards verified and residual risk accepted within authority	Scope, approved tier, evidence and decision
Approved with conditions	Risks and conditions have been expressly accepted under appropriate authority; no unlawful mandatory gap waived	Conditions, owners, completion dates, escalation and rollback
Deferred / Hold	Material fact, control or legal requirement unresolved; decision cannot yet be made	Blocking item, owner, evidence request and review date
Rejected	Unacceptable exposure or impossible / unavailable mitigation	Decision reason, alternatives and retention schedule
Unassessed	Insufficient baseline information to conduct assurance	Minimum inventory and classification actions

'Approved with conditions' is **not** a licence to commence activity prohibited by law or to ignore a safety-critical concern. In the workbook, readiness and decision approval are distinct fields deliberately requiring human sign-off.

7. Who owns what: independence and three-lines accountability

Participant	Accountable contribution	Must not be assumed to do
Business / service owner	Owens the dependency, service outcomes, business case, operational controls and supplier relationship	Delegate risk acceptance to an assessor merely because the assessor completed a questionnaire
Procurement	Checks procurement process, contracting, vendor records and milestone dependencies	Certify legal compliance or independently verify technical controls without competence
Information Security / vCISO	Defines risk-led assurance scope and tests technical evidence	Treat certification as a substitute for service-specific validation
DPO / privacy governance	Advises on role, Article 28, international flows, lawful processing and privacy impact	Assume statutory accountability for the controller's management decisions
Legal / contracts	Validates contractual and regulatory conditions	Determine technical evidence adequacy in isolation
Operational resilience / clinical safety	Validates critical-service, recovery and clinical implications where relevant	Transfer clinical responsibility to a generic vendor scoring model
Internal audit or independent assurance	Tests the assurance programme's design/ operation subject to competence and independence	Audit its own control implementation without addressing self-review conflicts
Senior risk owner / board committee	Accepts or rejects material residual risk within documented delegated authority	Infer acceptance from silence or contract signature alone
Supplier and fourth parties	Supply evidence, perform contractual controls and report changes/incidents	Assign the buyer's own risk ownership or assurance decision

Independence boundary: An adviser who helps design supplier processes may still provide valuable implementation support, but the independence and limitations of any subsequent assurance work must be assessed and disclosed. Do not describe IG-Smart's implementation as independent certification.

8. The supplier assurance lifecycle: from request to retirement

Stage 1 — Pre-selection

Define the service, data, end users, dependencies, internal owners, planned integrations and credible failure scenarios. Avoid distributing a generic 200-question pack before understanding what matters. Identify prospective processor roles, regulated outsourcing definitions and fourth-party reliance early. Start a single supplier record and link evidence to the actual product/service, not just the vendor's corporate marketing website.

Stage 2 — Risk-led due diligence

Assign an approved tier, choose relevant control checks, request proportionate evidence, and assess provenance and scope. Separate facts from supplier assertion, control design from operation, and limitations from noncompliance. Confirm which controls rely on buyer configuration (cloud tenant hardening, encryption keys, access provisioning, local clinical safety, etc.).

Stage 3 – Contracts and onboarding

Ensure commercial schedules reflect the control and reporting commitments on which approval depends. Where personal data are processed on behalf of the buyer, check Article 28 terms. For high-consequence services, clarify incident notification, audit/assurance rights, restoration, data retrieval, fourth-party visibility, exit assistance and unresolved remediations. Avoid assuming a general right to unrestricted penetration testing of cloud infrastructure.

Stage 4 – Run and monitor

Collect agreed security/operational metrics, assess material changes, scrutinise incident reports and follow up remediation. Reassess fourth parties, location changes, critical integrations, major vulnerabilities and new AI/data uses. Ask whether deployed configuration still matches the assessed version. Supplier 'annual review completed' is not a sufficient effectiveness metric by itself.

Stage 5 – Exit or substitution

Verify data return/deletion under the applicable legal and contractual arrangements; recover or revoke privileged access, API tokens and keys; validate portability where required; record transition and continuity dependencies; and preserve the necessary audit trail. If deletion cannot occur because of a legal retention obligation, document the continuing basis and controls.

The NCSC's five-stage assessment guidance directly supports integrating assurance throughout supplier relationships and continuous improvement. [S2]

9. Contractual assurance: the terms that turn a questionnaire into an enforceable relationship

The following are procurement drafting considerations, not a substitute for legal advice or model clauses. Tailor them to supplier type, bargaining position, location, clinical or financial-sector rules and the actual service.

Clause / schedule	Buyer decision to make	Evidence or negotiation point
Identity and service scope	Who does what, where and for how long?	Entities, products, environments, deliverables
Information security baseline	Which safeguards are contractual promises?	Security schedule matched to risk assessment
Processor role / UK GDPR Article 28	Is the supplier a processor?	Mandatory particulars and protections if yes [S6]
Subprocessor governance	What approval and notice rights are necessary?	List, change mechanism and downstream obligations
Subcontractor and fourth-party control	How do key outsourced dependencies affect service?	Flow-down duties and evidence access
Locations and cross-border flows	Where is data accessed, stored or transferred?	Data flow and lawful transfer mechanism [S10]
Incident notification	Who contacts whom, what is reported, by when?	Defined trigger, practical channels and evidence preservation

Clause / schedule	Buyer decision to make	Evidence or negotiation point
Security testing and audit rights	Which proportionate audit approaches apply?	Access, limitations, pooled assurance, frequency
Vulnerability and remediation	What are fix/mitigation obligations?	Severity model, exceptions, owner and retest
Service resilience	What continuity/recovery objectives are justified?	BIA, SLA/SLO, restoration evidence
Customer responsibilities	Which shared controls remain with the buyer?	Tenant configuration and access responsibility matrix
Regulatory cooperation	What support is required for lawful audits or notices?	Contractual duties aligned to applicable sector law
Material change and assignment	What triggers prior consent or notice?	Service, ownership, location, subcontractor changes
Exit and data portability	Can the organisation switch providers safely?	Tested exit path, format, assistance and escrow if relevant
Data retention and deletion	What happens when service ends?	Return/deletion procedure and certification where appropriate
Evidence cadence	What must be supplied during service?	Periodic review pack and change-triggered updates

Legal point: ICO guidance identifies specific minimum Article 28 contractual provisions where controller–processor processing occurs. The exact legal arrangements must be established rather than relying on a generic vendor DPA badge. [S6][S7]

Financial-sector point: Where EU DORA applies, particular contractual provisions and registers may be legally required for ICT services; UK FCA/PRA duties follow their own rulebooks and are not interchangeable with DORA merely because the supplier operates internationally. [S8][S9]

10. Ongoing monitoring: seven useful signals, not 100 decorative KPIs

Indicator	What it reveals	Appropriate response
Evidence currency	Certificate, report, test or policy in/out of relevant period	Recheck scope and refresh only where material
High-severity remediation ageing	Critical or high findings not resolved or accepted	Escalate to authorised risk owner
Privileged-access exceptions	Break-glass, excessive standing access, failed recertification	Restrict/monitor access and assess exposure
Incident and near-miss changes	Supplier-reported or independently identified events	Reassess service impact and contractual notifications
Subprocessor, location and ownership changes	Previously assessed dependency is no longer identical	Reclassify legal and operational exposure
Resilience test variance	RTO/RPO test failure, prolonged outage or concentration drift	Demand mitigation and continuity decision

Indicator	What it reveals	Appropriate response
Exit readiness	Ability to extract, transfer, revoke and delete safely	Prioritise alternative and exit actions

Reassessment triggers that override an annual diary

- A significant supplier incident, breach or material vulnerability affecting scope.
- A new clinical workflow, regulated data category or safety consequence.
- Transfer of processing to another country or fourth party.
- Material change in API privileges, cloud tenant, software architecture or production access.
- Expiry, suspension or narrowing of assurance evidence.
- Acquisition, insolvency, material financial distress or concentration increase.
- Material service outage, failed restoration exercise or repeated SLA failure.
- A regulator's new requirement applicable to this particular buyer and arrangement.
- Significant AI functionality or data-use change introduced by the supplier.
- Approaching termination, contract renewal or change of important business service.

Avoid claiming that 'continuous assurance' means continuous invasive scanning. It means **ongoing ownership, appropriate evidence collection, exception management and event-driven review**.

11. Sector overlays: one assurance model, different decisions

NHS / clinical digital health

For a supplier delivering a clinically consequential solution, distinguish supplier product evidence from the NHS deploying organisation's clinical risk management. Assess relevant DCB0129 and DCB0160 accountabilities, DTAC and DSPT conditions as the actual procurement/deployment dictates. A good cyber supplier grade does not authorise use of a clinically unsafe product. Where clinical responsibility or hazard acceptance is unresolved, route to qualified clinical safety leadership.

Financial services

For a UK FCA/PRA-regulated buyer, map important business services, outsourcing/materiality and operational resilience obligations before assigning the diligence programme. The FCA makes clear that firms remain accountable for applicable regulatory responsibilities when they outsource. Its 2026 guidance also flags forthcoming reporting changes effective in March 2027 for relevant firms. [S8]

For EU financial entities within DORA, Article 28 and Article 30 requirements may require specified ICT third-party governance and contract features. A UK vendor can be a relevant provider to an EU entity, but that does not mean every UK buyer is directly regulated by DORA. [S9]

Life sciences and research

Where CROs, research platforms, clinical trial systems or pharmacovigilance providers handle sensitive or regulated information, assess both privacy and domain-specific controls. A data hosting certificate cannot replace the sponsor's or responsible entity's clinical/research governance. Confirm data use, research agreements, validated systems where applicable and cross-border flows on the actual facts.

Enterprise SaaS and AI-enabled vendors

Assess privileged integrations, data-use boundaries, AI training and secondary-use settings, model/service suppliers, change notification and customer configuration. AI software risks are not reducible to one 'AI compliant' question. Apply the appropriate AI, privacy, cyber and contractual overlays according to actual role, service and jurisdiction.

12. Four illustrative procurement situations

Scenario A — Low spend, high privilege: A £2,000/year support utility receives production administrator access. Its low cost does not justify Tier 4. Verify identity, access restrictions, session logging, incident procedures, contract authority and safe revocation. Consider a higher tier based on access and potential impact.

Scenario B — Major cloud provider with scoped reports: A cloud supplier provides extensive third-party assurance. The buyer remains responsible for identity policy, configurations, encryption choices and application-level recovery. Requesting another general penetration test of the hyperscaler is unlikely to answer tenant-specific questions. Verify shared controls instead.

Scenario C — Healthcare SaaS with a strong cyber certificate: The supplier can demonstrate information security controls but cannot identify who owns the clinical safety case for the actual deployment. Cyber due diligence may proceed, but clinical readiness remains a separate hold until clinical safety responsibilities and evidence are resolved.

Scenario D — EU financial entity using a UK SaaS provider: Assess whether the EU financial entity is subject to DORA and whether the contract supports applicable ICT third-party arrangements. Do not assume the UK supplier itself has become an EU financial entity or that UK FCA obligations are identical.

The scenarios are fictional teaching examples, not descriptions of IG-Smart clients, investigations, deal values or actual supplier failures.

13. Twenty-five procurement questions enterprise buyers should ask

Scope and dependency

1. Which legal entity supplies this specific product and holds contractual responsibility?
2. Which system and business services rely on the supplier, and which are genuinely critical?
3. What production, data, administrator and network access exists at launch and in support?
4. Which fourth parties are essential to service delivery and incident recovery?
5. Where are data stored, accessed, backed up or routed, including support and telemetry?

Governance and evidence

1. What is the scope, validity and issuer of the proposed ISO or independent assurance evidence?
2. Which key controls are verified by operational artefacts rather than supplier statements?
3. What exceptions, scope exclusions or customer-responsibility controls remain?
4. What is the most recent independently assessed failure, and what remediation was evidenced?
5. How does the supplier manage privileged access and break-glass events?

Security and privacy

1. How are vulnerabilities identified, prioritised, mitigated and retested?
2. Which relevant application, cloud, API and code-release components were tested?
3. How does the supplier prevent unauthorised use of customer data for secondary purposes or AI model training?
4. What personal-data controller/processor roles apply to the proposed processing?
5. How are subprocessors authorised and notified, and how are equivalent protections flowed down?
6. If a restricted transfer occurs, what mechanism and assessment are relied upon?

Resilience and accountability

1. What has actually been tested against the buyer's recovery needs?
2. What are the practical limits of the provider's SLA and recovery guarantees?
3. How quickly and through which channel will the buyer learn of a material incident?
4. What information will the supplier preserve and share so the buyer can investigate?
5. Who owns known control exceptions and who can approve temporary conditions?
6. What substitute, exit, portability and credential revocation arrangements exist?

Regulatory and lifecycle

1. Does the arrangement trigger special clinical, outsourcing, financial-sector or AI obligations?
2. What events will trigger contract amendment, a new assessment or board escalation?
3. Can we reconstruct the approval decision a year later from the evidence, dates, reviewer notes and authorised sign-off?

14. One-page board and procurement decision briefing

SUPPLIER ASSURANCE DECISION – EXECUTIVE RECORD

Field	Required entry
Supplier and contracted entity	[Legal entity, group relationship, service identifier]
Decision owner / assurance reviewer	[Roles; independence/conflict assessment if relevant]
Business service and dependencies	[Critical outcomes; important-business-service/clinical impact]
Approved inherent tier	[1–4 with documented rationale and regulatory overrides]
Data, access and fourth-party footprint	[Sensitive data, privilege, processing/transfer locations, dependencies]
Applicable legal and contractual safeguards	[Specific requirements and counsel/SME review where needed]
Evidence verified	[Control sample, scope, period, assurance reports, principal limitations]
Open high/critical matters	[Finding IDs, potential harm, owner, mitigation, due date]
Residual risk and appetite	[Assessment, known unknowns and authorised acceptance rationale]
Proposed decision	[Approve / Conditions / Hold / Reject]
Conditions precedent	[Must be satisfied before access, data migration or clinical use]
Approval authority, date, next review	[Signature/record; events triggering earlier reassessment]

Board discussion prompts: Does this supplier create concentration or a material single point of failure? Which claims were actually tested? What remains legally or clinically conditional? Which person is accountable if a key supplier control fails? Can we exit safely and recover our data and services?

15. Ten concise enterprise FAQs

Is ISO/IEC 27001 certification sufficient to approve a supplier?

No. It can be valuable scoped assurance, but the buyer must confirm certificate relevance, service-specific controls, shared responsibilities, material exceptions and its own risk appetite. A certificate is not a warranty against incidents.

Must every supplier complete the same questionnaire?

No. NCSC guidance supports proportionate, risk-based assurance. Applicable legal duties remain applicable regardless of tier. [S1][S2]

Can a supplier have a high score and still be rejected?

Yes. The weighted indicator summarises recorded evidence confidence. It cannot override an unmitigated critical exposure, a missing mandatory legal safeguard, or an unauthorised risk acceptance.

What is the difference between an inherent and residual risk tier?

An inherent tier describes exposure and diligence depth before credit is given for controls. Residual risk is a separately assessed conclusion after considering actual mitigations and context. The workbook intentionally does not calculate residual risk from collected-document percentages.

What is an evidence exception?

A time-bounded, documented variance from a specified requirement. It needs a reason, business consequence, alternative mitigation, owner, authority and review date. A waiver is not an assertion of legal compliance.

Should a vendor always provide a complete penetration-test report?

Not necessarily. Sensitive technical reports may require controlled disclosure or a credible alternative. Assess the scope, tester independence, findings, remediation and residual relevance; a cover letter alone may be insufficient for a high-risk service.

Is a SOC 2 Type II report equivalent to ISO/IEC 27001 certification?

No. They are different forms of independent assurance with different criteria, reporting boundaries and conclusions. Interpret the actual report, period and scope rather than equating badges.

Does appointing a processor transfer UK GDPR accountability?

No. The controller retains applicable duties and must establish appropriate Article 28 terms and safeguards. The processor also has its own duties. [S6][S7]

Does DORA apply to all UK companies selling software to banks?

No. DORA's primary obligations apply to specified EU financial entities and related in-scope parties. Contractual requirements can flow to providers serving those entities. Analyse each relationship on its facts. [S9]

When should supplier assurance be repeated?

When risk, service scope, evidence, fourth parties, applicable law or material incidents change—and at a cadence proportionate to the supplier's criticality. An annual checkbox is not a substitute for event-driven review.

Make the evidence request fit the supplier

The following are **illustrative review lenses, not claims about any named supplier or completed IG-Smart engagement**. Select only the tests relevant to the agreed service and risk. A generic questionnaire alone can miss the most consequential dependency.

Supplier type	Evidence that often matters	Challenge the assumption
Managed IT and security service providers	Privileged access, staff access control, incident escalation, subcontractors and recovery interfaces	Does the contract cover the systems and operating hours the business relies on?
Data centres, offsite records and backup-tape stores	Physical access, custody, media tracking, environmental resilience, retrieval and restore tests	Does secure storage also provide usable recovery within the required time?
SaaS, cloud and software providers	Product-specific assurance, shared responsibilities, configuration, data location, support access and exit	Does an enterprise certificate actually cover this service, region and configuration?
Marketing providers and data brokers	Data provenance, permitted uses, transparency, processor/controller roles, retention and tracking	Can the proposed collection, sharing and secondary use be justified, not merely described?
Pharmacovigilance and healthcare suppliers	Data integrity, timely safety information, special-category data, continuity and specialist oversight	Which safety or regulatory duties remain with the commissioning organisation?
Facilities, maintenance and security suppliers	Physical and remote access, subcontractors, continuity and interfaces with operational technology	Can a non-IT supplier still disrupt a critical service or expose sensitive information?
Call centres and customer-support providers	Identity checks, recordings, agent access, scripts, retention, outsourced locations and continuity	Are stated controls evidenced in the actual delivery locations and channels?

Use remote document review where it can answer the question. Where justified, agree site visits, interviews, observation or authorised technical testing. Onsite attendance is not proof of effectiveness, and penetration testing requires explicit scope and permission. Treat privacy impact assessments as a distinct assessment where triggered, not a universal questionnaire substitute.

16. Practical implementation: what to do with this guide

1. **Start with the supplier inventory.** Record the exact service, legal entity, internal owner, dependency and access/data map.

2. **Approve a risk tier.** Treat the workbook's calculated suggestion as a screening signal, not delegated authority.
3. **Choose applicable controls.** Use the 36-item library to build a proportionate evidence request; document omissions and legally mandatory overlays.
4. **Verify rather than collect.** Record each claim's source, date, limits, reviewer and confidence.
5. **Escalate blockers.** Track critical and high findings, contractual gaps, unauthorised transfers and clinical/operational concerns separately from the overall score.
6. **Make a human decision.** Document residual risk, conditions, authority and the point at which service/data access may proceed.
7. **Monitor and reclassify.** Set review triggers and a defensible lifecycle record.

Next step: Where a regulated buyer needs a bounded review, ongoing vendor oversight or an independently scoped assurance programme, IG-Smart can help define the supplier population, testing depth, accountability, evidence and reporting model. **Talk to a Senior Practitioner** or **Submit a Requirement** through the website enquiry routes. Final engagement scope, independent-assurance boundaries, pricing and outputs remain subject to proposal.

Using the revised evidence workbook safely

Set the assessment date on **START HERE** and use unique supplier and control IDs. The matrix now checks unknown IDs, duplicate supplier/control records, unresolved applicability, confidence values, evidence references, reviewers, future artefact dates and stale review dates. A percentage is **neither a probability nor a compliance conclusion**. A records-ready flag means only that the configured record checks have passed; independently examine the findings, exception and contract registers and obtain the required human approvals.

Confirm the supplied workbook's actual configured capacity and supported row-expansion procedure. Extend formulas, validations and summary ranges together before adding further rows; the library does not define universally required controls. Never paste past the configured capacity and assume the summary includes the additional records. Conditional acceptance cannot authorise processing, deployment or service use while a mandatory legal or safety condition remains unmet.

Sources

- [S1] UK NCSC — Principles of supply chain security (12 principles). <https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security>
- [S2] UK NCSC — How to assess and gain confidence in your supply chain cyber security. <https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security>
- [S3] ISO/IEC 27036-2:2022 — Cybersecurity: Supplier relationships, Part 2, Requirements (official abstract). <https://www.iso.org/standard/82060.html>
- [S4] ISO/IEC 27036-3:2023 — Guidelines for hardware, software and services supply chain security (official abstract). <https://www.iso.org/standard/82890.html>
- [S5] NIST SP 800-161 Rev. 1 Update 1 (2024), Cybersecurity Supply Chain Risk Management Practices. <https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final>
- [S6] ICO — Contracts and liabilities between controllers and processors. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/contracts-and-liabilities-between-controllers-and-processors-multi/>
- [S7] ICO — Contracts (UK GDPR Article 28 guide). <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/contracts/>

- [S8] FCA — Outsourcing and operational resilience (updated July 2026). <https://www.fca.org.uk/firms/outsourcing-and-operational-resilience>
- [S9] Regulation (EU) 2022/2554 — Digital Operational Resilience Act, notably Articles 28 and 30. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2554>
- [S10] ICO — International transfers and transfer risk assessment / data protection test (current guidance). <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/>
- [S11] NCSC — Check your supplier arrangements. <https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security/check-your-arrangements>
- [S12] ISO/IEC 27036-1:2021 — Supplier relationships: overview and concepts. <https://www.iso.org/standard/82905.html>