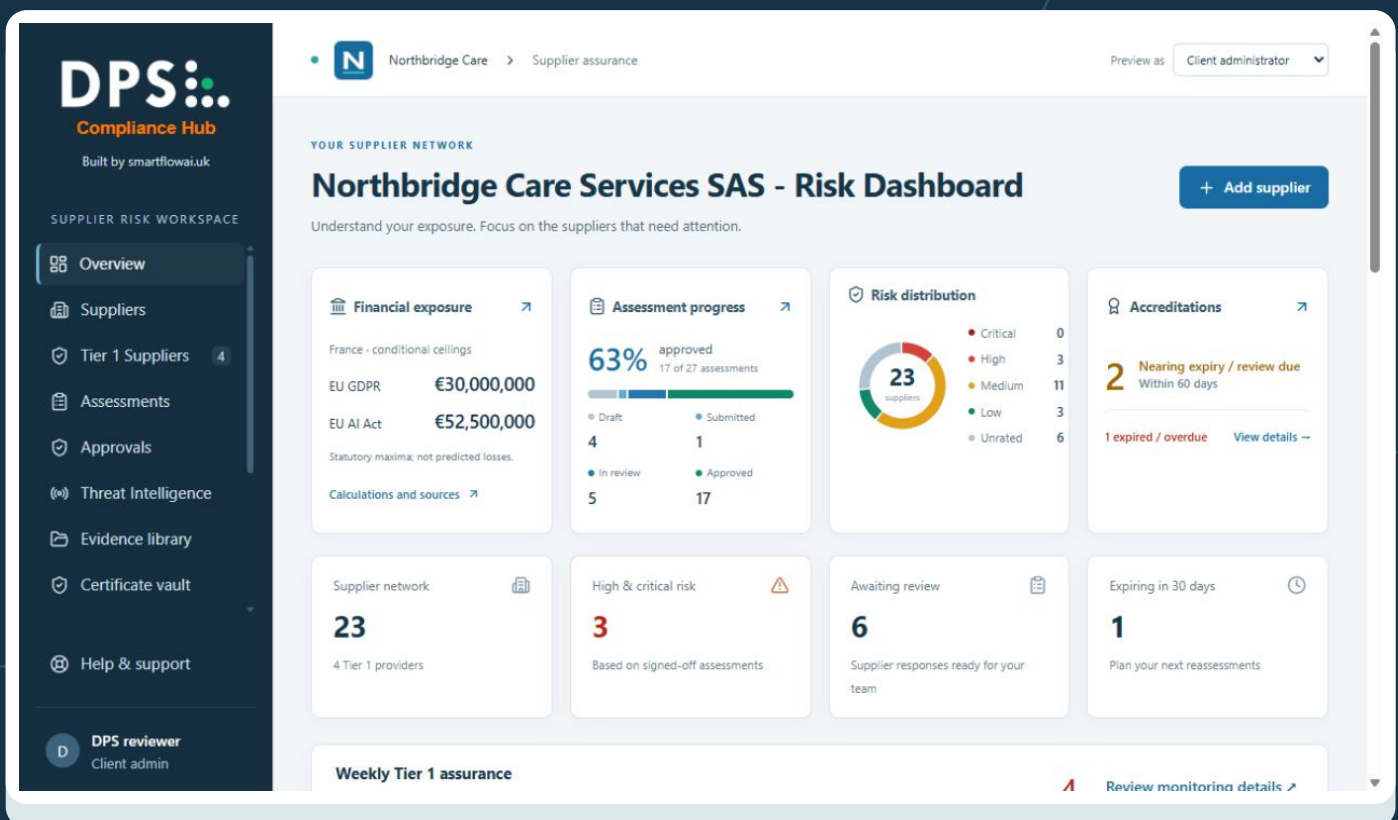


Supplier confidence. Built on evidence.

Know your suppliers. Understand your exposure.
Make risk decisions you can explain.



ASSESS / REVIEW / APPROVE / MONITOR

One workspace for your team.
A clearer assurance process for your suppliers.

Their service. Your exposure.

A supplier incident can become your operational disruption, procurement problem or data-protection risk.

Bring the whole risk story together.

The service you rely on. The information it handles. The evidence behind its controls. The decision your organisation makes.

01

Protect business continuity

Understand which services matter most, the consequences of an outage and the assurance needed to support your decision.

02

Support responsible procurement

Give procurement a practical risk summary, recommendations and a traceable approval rather than a collection of attachments.

03

Keep follow-up visible

Turn findings into classified risks and actions with owners, dates and status. Prioritise the work that needs attention.

04

Demonstrate due diligence

Keep evidence, review rationale and decision history together to support management, customer and assurance discussions.

The right route. The same clear process.

Match the assessment to the supplier, the service and the level of assurance you need.

01

Outside-in

Evaluate public information before engagement. Capture the checks, limitations and recommendations for procurement.

02

Standard

Collect supplier answers and evidence across the questionnaire. Review controls in the context of the service and processing.

03

Tier 1

Assess major providers against your specific use of their service, contractual evidence and ongoing published information.

A CONSISTENT DECISION JOURNEY

Assess

Scope and evidence

Review

Findings and gaps

Approve

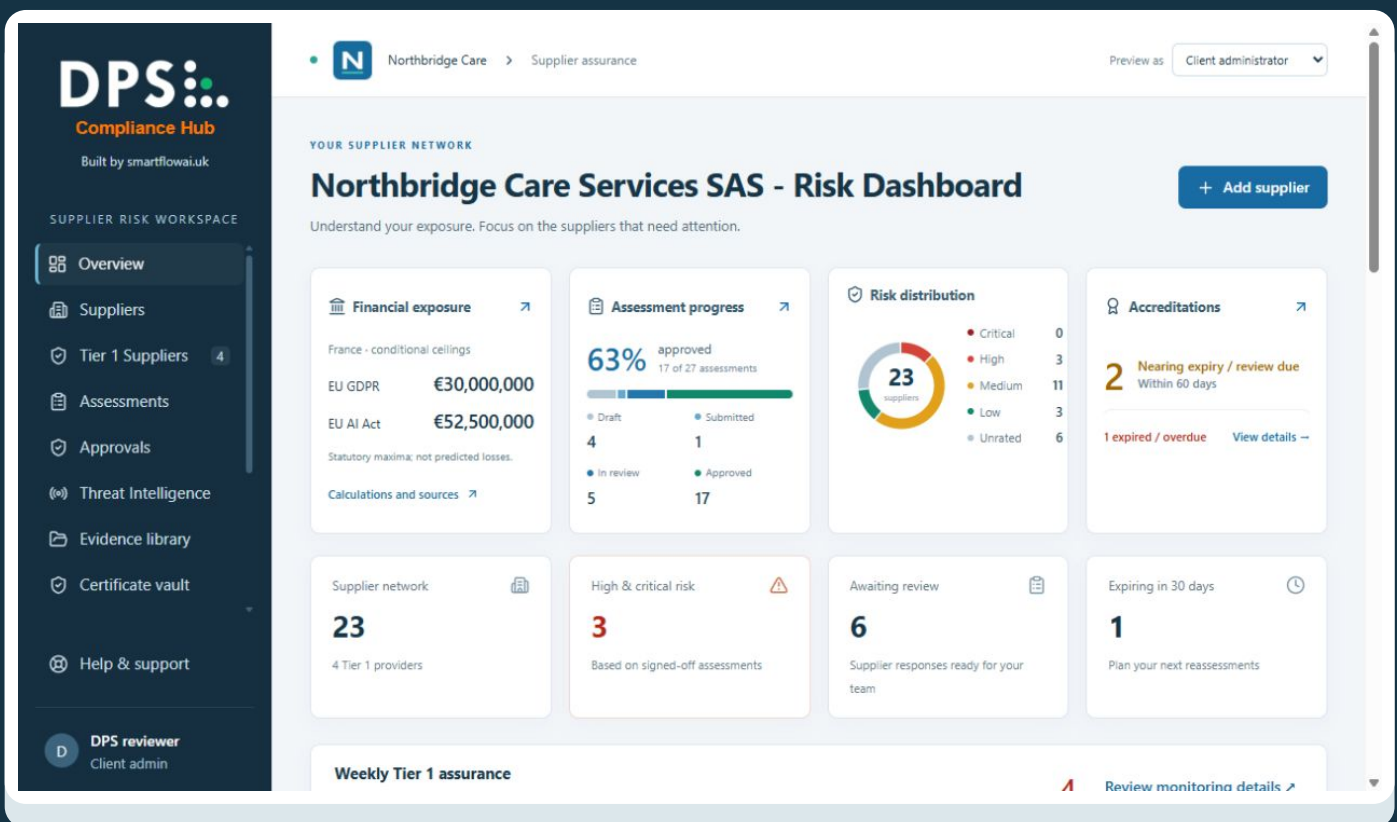
Decision and conditions

Monitor

Changes and actions

See the risk. Find the next action.

Move from an overall view of the supplier network to the individual suppliers that need your team's attention.



01

A clearer management view

Assessment progress, risk distribution, accreditation flags and current supplier priorities in one place.

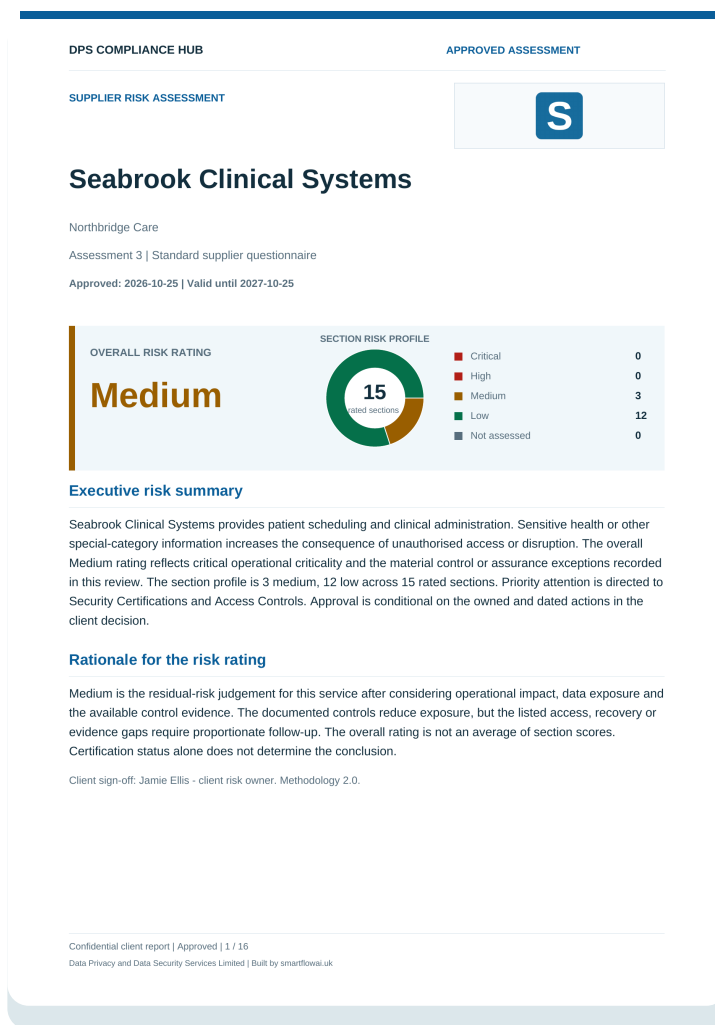
02

Drill down with purpose

Use supplier and assessment filters to focus on the service, finding, action or decision that needs review.

A risk rating. With the reasoning.

Give decision-makers an executive summary, a clear assessment scope and the evidence behind the conclusion.



From detail to decision

Understand the profile

Colour-coded ratings and a section risk distribution.

Test the rationale

Findings and evidence references explain the rating.

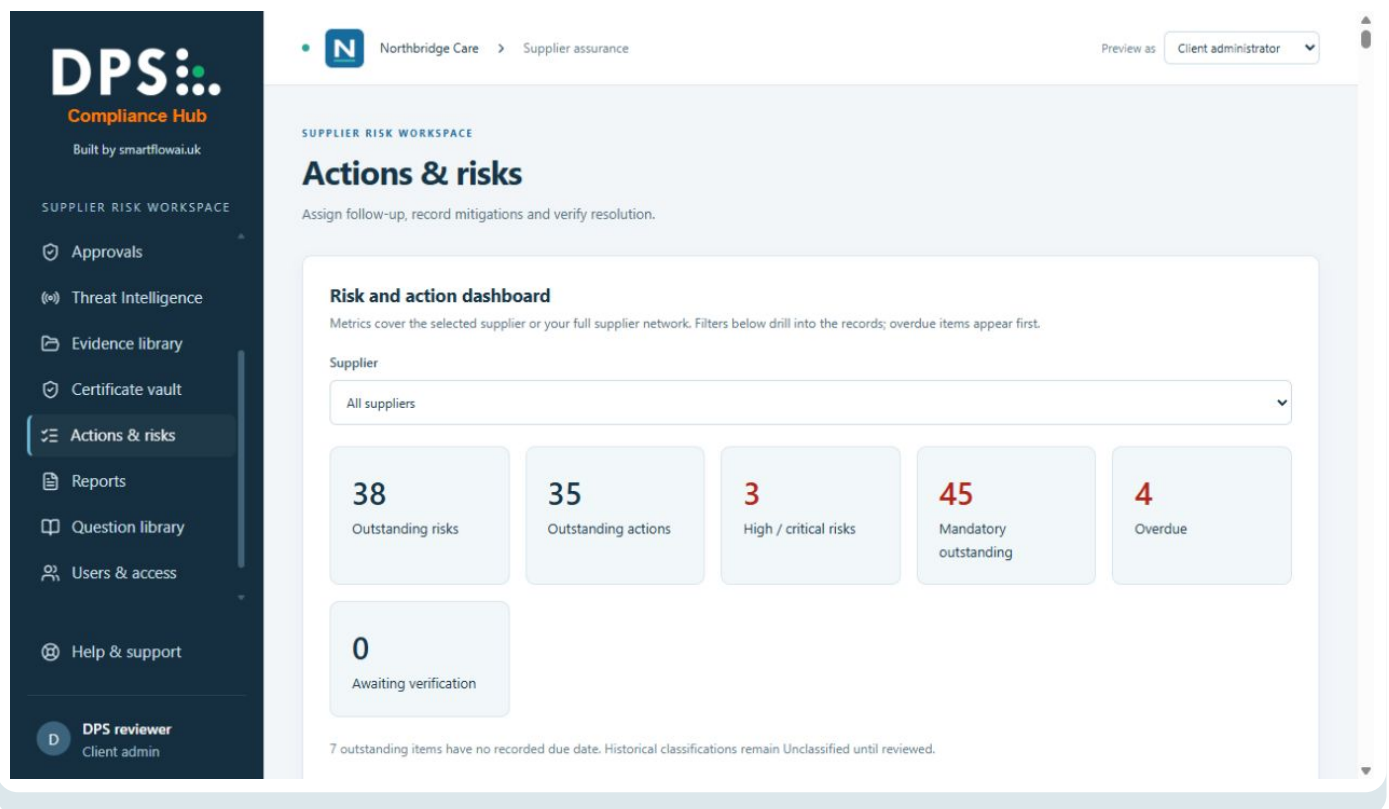
Agree the next step

Procurement recommendations, actions and approval history.

AI supports analysis and drafting. Your authorised reviewers retain responsibility for the approval and acceptance of risk.

Findings become owned actions.

Give risks and actions a clear home, then keep the decision and the follow-up connected.



01

Manage what remains open

Create, amend and remove client risks and actions. Track mandatory classifications, owners, due dates and progress.

02

Keep approval accountable

Procurement reviews outside-in recommendations. Client administrators approve standard assessments and outstanding conditions, with a dated audit trail.

Risk does not stand still. Neither should assurance.

Stay aware of changes across critical providers, software dependencies and supporting evidence.

DPS:.. Compliance Hub
Built by smartflowaiuk

SUPPLIER RISK WORKSPACE

- Overview
- Suppliers
- Tier 1 Suppliers** 4
- Assessments
- Approvals
- Threat Intelligence
- Evidence library
- Certificate vault
- Help & support

DPS reviewer
Client admin

Northbridge Care > Supplier assurance

Preview as Client administrator

Tier 1 Suppliers
Service-specific reviews backed by public assurance and permitted documentary evidence.

+ Add supplier

Search suppliers or se All risk ratings All relationships Due soonest (overdue first) 4 suppliers

SUPPLIER	RELATIONSHIP	RISK RATING	ASSESSMENT	REVIEW CADENCE
A AWS Tier 1 - AWS	In contract	High	In review Draft - client approval pending Previous: Accepted subject to actions	Weekly monitoring
G Google Tier 1 - Google	In contract	Medium	In review Draft - client approval pending Previous: Accepted subject to actions	Weekly monitoring
H HubSpot Tier 1 - HubSpot	In contract	Medium	In review Draft - client Previous: Accepted subject to	Weekly monitoring

Weekly

Tier 1 review

Refresh the public-source assessment and bring changed status to the dashboard.

10 minutes

Published service health

Check configured official outage feeds and flag published issues for review.

Connected

Threat Intelligence

Compare threat information with declared providers and supporting technologies.

Public incidents require service, region and customer-impact verification. Certificate expiry and review flags also help direct assurance follow-up.

Clear requests. Less avoidable back-and-forth.

Help suppliers understand the scope, provide useful evidence and see what the client needs next.

The screenshot displays the DPS Compliance Hub interface. On the left is a dark sidebar with the logo 'DPS:.. Compliance Hub' and 'Built by smartflowai.uk'. Below this is a 'SUPPLIER RISK WORKSPACE' section with links: 'My organisation', 'My assessment' (highlighted), 'Documents', 'Certificate vault', 'Open risks', 'Threat updates', 'Users & access', 'Help & support', and 'Supplier contact' (with a 'Supplier admin' link below it). The main content area has a light blue header with 'GOV' and 'Security Governance'. Below this, it says 'Establish who owns security and how risk decisions are governed.' A question '01 Is a named senior owner accountable for the security of the services supplied to this client?' is shown with a subtext 'Role description, named accountable owner and reporting line.' The 'Response' dropdown is set to 'Partial'. Below this is a text box for 'Explain your response' containing 'Synthetic demonstration response describing the example control and its implementation. This is not a real supplier assertion.' There is a section for 'Supporting documents - optional' with a list of example files: 'Example supplier security policy.pdf', 'Example supplier resilience test record.pdf', and 'example-question-evidence.pdf'. At the bottom, there is a 'Choose file' button, a 'No file chosen' status, and an 'Upload and attach' button. A note below says 'Upload PDF, Word, Excel or text evidence (up to 5 MB). A successful security scan is required: the file is'. At the very bottom, it says 'Responses saved' and a 'Save responses' button.

01

Work in context

Save questionnaire progress, follow evidence guidance and declare certifications, insurance and software dependencies.

02

Put their work to use

Export questions and answers to Excel or PDF. Respond to assigned actions and keep supporting assurance documents together.

Turn assurance into customer confidence.

Complete your own assessment and organise the evidence prospective customers need, without making it publicly available.

Your organisation. Your evidence. Your control.

A dedicated client assessment brings questionnaire responses, certifications, insurance and evidence into your organisation's risk posture. The view also considers approved supplier-network findings.

01 Prepare

Complete the assessment and review the AI-assisted posture.

02 Agree confidentiality

Use an NDA by default, or record the decision that one is not required.

03 Grant access

Invite a named prospective client for temporary, read-only access.

04 Control disclosure

Share permitted responses and evidence; retain access and request history.

Access can be revoked. The workflow supports a three-month deletion follow-up where a prospective client does not engage. Your own assessment does not consume supplier assessment allowances.

A workspace for your team. DPS support when you need it.

Use the software to run your own process, or add practical support for onboarding and ongoing supplier due diligence.

The workspace

Your team leads the review.

Bring structure

Use consistent assessments, evidence and decision records.

Retain oversight

See the portfolio, priorities, approval status and follow-up.

Build capability

Use role-based guidance and training to support adoption.

Supplier Risk Management

DPS helps manage the process.

Start well

Agree scope, configure the workspace and onboard suppliers.

Keep work moving

Coordinate questionnaire completion, evidence requests and review activity.

Add review capacity

DPS can manage agreed risk-review tasks under your documented authority.

Practical expertise. Clear accountability.

Optional services are agreed in the Order Form, including responsibilities, scope and delegated authority.

Support your obligations. Strengthen your assurance.

Supplier assessments help evidence a proportionate process. Applicable duties depend on the organisation, service, sector and jurisdiction.

UK and EU GDPR

Controllers must select processors providing sufficient guarantees, use appropriate contracts and oversee processing. Documented assessment and review help support that accountability.

NIS2 and DORA

For organisations within scope, NIS2 addresses supply-chain security and DORA sets requirements for ICT third-party risk in financial services. Assess applicability before relying on either framework.

ISO/IEC 27001 and 27701

Organised supplier evidence, risk treatment and recorded decisions can support information-security and privacy-management processes. Software use does not itself confer certification.

Good practice, beyond minimum duties

The NCSC supply-chain security principles support understanding dependencies, setting expectations and maintaining assurance. A repeatable process gives teams a stronger basis for action.

Official references: [EU GDPR](#) / [DORA](#) / [ISO/IEC 27701](#). Click each topic for its primary source. Reviewed 26 October 2026. The ICO guidance is under review following the Data (Use and Access) Act 2025.

Choose your capacity. Keep the process consistent.

Four levels. A 12- or 24-month commitment.
Annual and monthly payment options.

LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
20 Outside-in / year	40 Outside-in / year	60 Outside-in / year	100 Outside-in / year
40 Standard / year	60 Standard / year	100 Standard / year	200 Standard / year

Very competitively priced. Price on application.

Tell DPS about your supplier population, service criticality and internal review capacity. We will help identify the right licence and any optional onboarding or managed-service support.

Allowances renew on each licence anniversary. New assessments and reassessments count once when created. Editing, AI draft regeneration and exports do not add units. Tier 1 weekly reviews and your own client posture assessment are separate. Usage alerts are issued at 85%.

Everything, in one reference.

33 capability areas / 253 functions

The following reference describes released workspace functionality. Access depends on the user role, configuration and agreed service scope.

01

Workspace and branding

- 01.01 Separate client workspaces with supplier-specific records and access.
- 01.02 Client company name in the Risk Dashboard heading.
- 01.03 Client branding, clear header logo and DPS favicon.
- 01.04 Supplier logos on supplier records and assessment reports.
- 01.05 DPS Compliance Hub branding and client-facing workspace identity.
- 01.06 Responsive layouts, searchable lists, colour-coded ratings and role-aware navigation.

02

Identity and user access

- 02.01 Microsoft Entra sign-in and multi-factor authentication.
- 02.02 DPS administration, Client administrator, Reviewer, Client member, Procurement, Supplier administrator and Supplier member access.
- 02.03 Supplier users restricted to their assigned supplier within the client workspace.
- 02.04 Time-limited guest access, expiry checks and administrator revocation.
- 02.05 Invitations are tied to the authenticated directory identity; an entered email alone grants no access.
- 02.06 Seven-day read-only Client viewer access for an invited client trial.
- 02.07 Dedicated Prospective client access restricted to the inviting organisation's approved security posture and authorised materials.

03

Supplier onboarding and profiles

- 03.01 Create suppliers with relationship, operational criticality and assessment route.
- 03.02 Relationship stages: initial evaluation, tender and contract.
- 03.03 Standard supplier or Tier 1 trust-centre route; Tier 1 provider selection appears only for that route.
- 03.04 Standard supplier levels: outside-in public evaluation or detailed supplier questionnaire.
- 03.05 Organisation profile covering legal identity, contacts, service scope, locations, data categories and volume.
- 03.06 Service applicability flags for personal and special-category data, hosting, system access, development, AI and sector-specific work.
- 03.07 Supplier branding and service-specific profile completion.
- 03.08 NDA issue, supplier return and client acceptance, with assessment access gated when required.

04

Client business context

- 04.01 Company name and address, incorporation country, group membership and group name.
- 04.02 Annual worldwide turnover, currency, financial year and company or group basis.
- 04.03 Core products and services and legal-entity employee count.
- 04.04 Security certifications held by the client.
- 04.05 DPO appointment, identity and contact details.
- 04.06 Primary incident management contacts, email addresses, telephone numbers and web routes.

Client business context / continued

- 04.07 Applicable legislation and confirmed financial assumptions used in risk analysis.

05

Assessment search and licence usage

- 05.01 Search assessments by supplier name and filter by supplier, assessment type and status.
- 05.02 Separate outside-in, standard and Tier 1 assessment views, with combined filters and a matching-result count.
- 05.03 Current assessments shown first, with an option to include earlier versions.
- 05.04 Annual outside-in and standard usage meters show consumed units, limits, remaining allowances and percentage used.
- 05.05 Licence-year dates, licence level and contract duration remain visible while results are filtered.

06

Licence administration

- 06.01 DPS administrators set the licence level, start date and a 12- or 24-month term.
- 06.02 Four annual allowance levels: Level 1 includes 20 outside-in and 40 standard assessments; Level 2 includes 40 and 60; Level 3 includes 60 and 100; Level 4 includes 100 and 200.
- 06.03 Separate annual allowances reset on each licence anniversary.
- 06.04 Each newly created assessment or reassessment consumes one unit in the relevant allowance.
- 06.05 Editing an existing assessment, regenerating an AI draft and exporting do not consume additional assessment units.
- 06.06 Tier 1 weekly monitoring does not consume outside-in or standard assessment units.
- 06.07 Client and DPS notifications at 85% usage; new assessments are blocked when the relevant allowance is exhausted or the licence has expired.

Licence administration / continued

- 06.08 Licence configuration history retains the administrator, date, reason and previous values. In-term upgrades preserve consumed usage.

07

Questionnaire structure and applicability

- 07.01 29 configurable assessment sections and 136 catalogue questions, including mandatory software dependencies.
- 07.02 Simplified language with contextual evidence guidance.
- 07.03 Yes, Partial, No and Not applicable responses, with explanations; contextual questions use descriptive responses.
- 07.04 Section applicability decisions and reasons, with profile conflicts highlighted for review.
- 07.05 Core governance, certifications, resilience and software-dependency coverage.
- 07.06 Dedicated questions for ISO/IEC 27001, ISO/IEC 27701, SOC 2 report type, Cyber Essentials and Cyber Essentials Plus.
- 07.07 Specialist sections for UK government, NHS, OT, Consumer Duty, financial risk and ESG where applicable.
- 07.08 Client-defined question sections and additional questions.
- 07.09 Questionnaire progress, draft saving, submission confirmation and locked submitted answers.
- 07.10 Reassessment carries previous answers forward for supplier confirmation; changes are not silently treated as verified.

08

Software and technology dependency inventory

- 08.01 Mandatory software-supplier section for detailed assessments and corresponding outside-in research.
- 08.02 Checkbox selection of Tier 1 providers, other software providers and underlying technologies.

Software and technology dependency inventory / continued

- 08.03 Capture runtimes, languages and components such as PHP, Java, .NET, Node.js, Python, WordPress and databases.
- 08.04 Supplier confirmation of selections, with unknown details explicitly identified.
- 08.05 Questions on monitoring outages across the software supplier network.
- 08.06 Declared dependencies inform risk assessment and evidence-led threat matching.

09 Question-level document evidence

- 09.01 Supplier document upload and linking to an individual assessment question.
- 09.02 Configurable mandatory evidence requirements for specific questions.
- 09.03 Submission blocked until mandatory clean evidence is linked and other required tasks are complete.
- 09.04 Evidence metadata includes ownership, timestamps, content type and cryptographic hash.
- 09.05 Client review documents can remain private to the client.
- 09.06 Evidence library with supplier scope and retained document access.
- 09.07 Previous evidence retained for audit and reassessment.

10 Secure upload processing

- 10.01 Private upload quarantine and dedicated Azure storage.
- 10.02 Microsoft Defender malware scanning before accepted evidence is released.
- 10.03 Integrity checks prevent document substitution after malware scanning.
- 10.04 Scan-result integrity enforced independently of the uploading application.

Secure upload processing / continued

- 10.05 File size and format validation, including limits on unsafe content.
- 10.06 Encrypted managed workspace storage with versioning and recovery records.
- 10.07 Uploads remain disabled unless the scanner acceptance check succeeds.

11 Certificate evidence vault

- 11.01 Supplier-only declaration of accreditations held, or explicit confirmation that none are held.
- 11.02 Current certificates and assurance reports uploaded into a dedicated vault.
- 11.03 AI proposes holder, issuer, scope and relevant dates for human confirmation.
- 11.04 Certificate expiry tracking and report freshness or review dates.
- 11.05 SOC 2 handled as an assurance report, with reporting period and agreed review date rather than an invented certificate expiry.
- 11.06 Replacement evidence linked to the previous record; history retained.
- 11.07 Dashboard counts for nearing expiry, expired and overdue assurance evidence.
- 11.08 Branded reminders to active supplier administrators and members, with notification logs.

12 Outside-in public assessment

- 12.01 Early supplier evaluation before supplier invitation or completed supplier profile.
- 12.02 Eight research topics: trust centre, legal terms, breaches or enforcement, data processing, residency, financial identity, software dependencies and operational issues.
- 12.03 Service scope and proposed data use captured before analysis.
- 12.04 Dated searches, source references, evidence links, research notes and uncertainty recorded by topic.

Outside-in public assessment / continued

- 12.05 Evidence located, no relevant result, unable to verify and not-applicable states distinguished.
- 12.06 Public-source collection validates addresses and records restricted or unavailable evidence.
- 12.07 Evidence-led AI review and a client assessment PDF.
- 12.08 No result is treated as uncertainty, not proof of an incident-free or risk-free supplier.

13**AI-assisted risk analysis**

- 13.01 Analysis uses the client business, regulatory exposure, supplier criticality and service scope.
- 13.02 Ten contextual factors cover business fit, financial exposure, criticality, history, personal data, special-category data, volume, residency, subprocessors and controls.
- 13.03 Supplier answers and clean documents combined with attributable outside-in evidence.
- 13.04 Overall rating, section ratings, detailed rationale and evidence references.
- 13.05 Executive summary and review text editable by authorised client reviewers.
- 13.06 Rating overrides require a documented reason and retain review provenance.
- 13.07 Proposed actions classified Mandatory, Preferred or Guidance - Optional.
- 13.08 Evidence limits and unknowns disclosed; human review remains required.
- 13.09 Cyber and professional indemnity cover are reviewed for declared amounts, currency, dates, insured entity, relevant scope, limits, excess, exclusions and evidential gaps.

14**Assessment PDF reports**

- 14.01 Professional supplier heading and contained supplier logo or clear initials when no logo is available.
- 14.02 Prominent colour-coded overall risk rating and finding severity counts.

Assessment PDF reports / continued

- 14.03 Executive risk summary and rationale for the overall rating.
- 14.04 Assessment route, dates, approval status, scope and coverage.
- 14.05 Section risk dashboard, section rationale and detailed contextual risk analysis.
- 14.06 Findings and action plan, client acceptance and recorded conditions.
- 14.07 Combined supplier documents and outside-in evidence register, with source links and integrity details.
- 14.08 Draft and approved report downloads limited to client roles.
- 14.09 Approved assessment snapshots retained as versioned records.
- 14.10 Front-page section-risk doughnut chart and a named section-by-section risk matrix.
- 14.11 Editable executive summaries and rating rationale explain material findings and service-specific business exposure.

15**Client risk sign-off**

- 15.01 Explicit client review and approval before report finalisation.
- 15.02 Acceptance as assessed or acceptance subject to owned and dated follow-up actions.
- 15.03 Applicability exclusions and conflicting scope decisions reviewed before finalisation.
- 15.04 Signer identity, sign-off date, rationale and risk acceptance recorded.
- 15.05 Acceptance conditions tracked through completion and separate reviewer verification.
- 15.06 Original sign-off evidence and report snapshots remain immutable.

16

Procurement approvals and expanded sign-off

- 16.01 Procurement reviewer role and time-limited guest membership checks.
- 16.02 Editable procurement recommendations derived from outside-in findings.
- 16.03 Named Procurement reviewer assigned an outside-in assessment for approval.
- 16.04 Approve, approve subject to actions, request changes or reject with an explicit rationale.
- 16.05 Assessment and outstanding-item fingerprint prevents approving a changed review silently.
- 16.06 Conditional approval requires owned and dated actions.
- 16.07 Approval decision, reviewer and date visible on the supplier dashboard.
- 16.08 Dedicated approval queue and sign-off history.
- 16.09 Standard client sign-off captures explicit acceptance of outstanding risks and actions.

17

Risk Dashboard and supplier drilldown

- 17.01 Client financial exposure, assessment progress, risk distribution and accreditation alerts in the summary row.
- 17.02 Supplier network, high or critical risk, awaiting review and assessment-expiry metrics.
- 17.03 Search for a supplier or service.
- 17.04 Filter by risk rating and relationship.
- 17.05 Sort by due date with overdue assessments first, highest risk or supplier name.
- 17.06 Live validity countdown: green, amber within two calendar months and red after expiry.
- 17.07 Direct supplier and PDF report access from the attention list.
- 17.08 Compact Tier 1 service notifications and weekly assurance alerts with detailed drilldown.

18

Risks and actions

- 18.01 Overall risk and action metrics and supplier-specific drilldown.
- 18.02 Filters for supplier, search text, severity, classification, status and overdue items.
- 18.03 Outstanding, mandatory, overdue, high or critical and awaiting-verification counts.
- 18.04 Risk treatments show supplier, severity, classification, due date, status and progress.
- 18.05 Client follow-up actions with an owner and due date.
- 18.06 Supplier progress updates and client verification before closure.
- 18.07 Classification changes require a recorded reason.
- 18.08 Risk acceptance conditions remain linked to the signed-off assessment.

19

Client administration of risks and actions

- 19.01 Client administrators add, amend or remove risks and client actions.
- 19.02 Editable titles, risk details, severity, mitigation, classification, owners and due dates.
- 19.03 Recorded reason and before-and-after history for each change.
- 19.04 Removal retains the record and audit evidence rather than erasing history.
- 19.05 Changing an acceptance condition is recorded as an amendment and invalidates prior condition verification.

20

Tier 1 supplier assurance

- 20.01 Microsoft, Google, AWS and HubSpot provider routes.
- 20.02 Service-specific trust-centre collection and permitted restricted evidence.

Tier 1 supplier assurance / continued

- 20.03 Evidence coverage for SLAs, terms, data agreements, subprocessors, RPO, RTO, uptime and availability history.
- 20.04 Weekly background assessment reviews, separate from the approved baseline.
- 20.05 Changed status or risk requires client attention and acknowledgement.
- 20.06 Weekly draft can be promoted for a new client review.
- 20.07 Tier 1 uses weekly monitoring rather than a validity expiry or due-in countdown.
- 20.08 Supplier search and filters appear above Tier 1 monitoring panels.
- 20.09 Dated outside-in public-source assessments for Microsoft 365, Google Workspace, AWS and HubSpot, with linked official evidence and explicit customer-specific gaps.
- 20.10 Separate published SLA commitments, recovery design targets and customer-measured availability.
- 20.11 Public research findings remain separate from client-approved ratings until an authorised sign-off.
- 20.12 Service-specific onboarding captures the service purpose, client-suggested criticality, outage impact, personal and special-category data, residency and known data volume.
- 20.13 AI review uses the client's service context alongside business background and supplied public evidence.

21

Published service outages

- 21.01 Official public provider service-health feeds checked in batches every ten minutes.
- 21.02 Provider notices, source coverage and related supplier records.
- 21.03 Compact Risk Dashboard notification with drilldown.
- 21.04 Detailed Tier 1 service-health view and official source links.
- 21.05 Unknown coverage and failed checks distinguished from confirmed healthy status.

Published service outages / continued

- 21.06 Public incident reports are not treated as proof that the client's account, region or contracted service is affected.

22

Threat Intelligence

- 22.01 Latest published items first, with ten-minute batch refresh.
- 22.02 Public sources include vulnerability catalogues, exploitation information and vendor advisories, including PHP advisories.
- 22.03 Public exposure rating and evidence-based severity filtering.
- 22.04 CVSS, source references, publication and retrieval details where available.
- 22.05 AI checks supplier answers and dependency declarations for attributable matches.
- 22.06 Supplier suggestions include the supporting statement or evidence quotation.
- 22.07 Users review recipients and choose whether to share a threat advisory.
- 22.08 Declared use does not automatically imply a vulnerable version, compromise or proven customer impact.

23

Regulatory financial exposure

- 23.01 Client location, relevant legislation, turnover basis and local currency inform the calculation.
- 23.02 GDPR conditional statutory ceilings, with source and calculation detail.
- 23.03 EU AI Act exposure where the client role, undertaking size and applicability support the scenario.
- 23.04 Financial assumptions and currency conversion provenance recorded.
- 23.05 Separate optional client breach-cost scenario.
- 23.06 Statutory maxima are not predicted fines or expected breach losses and are not added together.

Regulatory financial exposure / continued

- 23.07 Full applicability and legislative-source drilldown from the dashboard.

24

Management PowerPoint reporting

- 24.01 Reports is a dedicated navigation section.
- 24.02 Client PowerPoint template uploaded in Settings, with safe template validation.
- 24.03 Assessment status and risk-distribution charts.
- 24.04 Tier 1 risk overview, assessments due or expired within 30 days, new suppliers and outside-in outcomes.
- 24.05 Actions and risk overview and executive commentary.
- 24.06 AI-assisted report planning and section customisation.
- 24.07 Editable native PowerPoint charts and tables with embedded data.
- 24.08 Saved historical report archive with template hash, content hash, dated data snapshot and audit metadata.
- 24.09 Branded executive metrics, assessment charts and paginated tables, with concise editable commentary.
- 24.10 Title slide and table of contents before the detailed management reporting sections.
- 24.11 Readable risk-distribution chart with separate rating counts; historical originals are retained while compatible downloads correct shared slide-note relationships.

25

Supplier assessment exports

- 25.01 Supplier PDF export of saved assessment questions and answers.
- 25.02 Supplier Excel export for alternative use.
- 25.03 Export respects supplier scope and applicable sections.

Supplier assessment exports / continued

- 25.04 Confidential client risk reports and private client evidence are excluded.

26

Notifications and email

- 26.01 Branded certificate reminders, assessment workflow notices and selected advisories.
- 26.02 Outbox records pending, sent, failed, suppressed and uncertain delivery states.
- 26.03 Sender and recipient checks remove revoked or expired recipients.
- 26.04 Provider acceptance is recorded as sent; inbox delivery is not inferred from provider acceptance alone.
- 26.05 Branded notices use the authorised email sender for the deployment.

27

Role-based support

- 27.01 DPS service desk for client requests and escalations.
- 27.02 Client queue for supplier issues, fresh requests to DPS and escalation to DPS.
- 27.03 Supplier help, tool issues, assessment queries and appeals.
- 27.04 Tickets linked to supplier or assessment where appropriate.
- 27.05 Assignment, priority, status, replies and role-limited internal visibility.
- 27.06 Support history retained with the request.

28

Training videos and guidance

- 28.01 25 DPS, client and supplier training videos.
- 28.02 Conversational British English male narration with explicit acronym pronunciation.
- 28.03 DPS Compliance Hub 16:9 thumbnails aligned across each row.

Training videos and guidance / continued

- 28.04 Centred floating player can be moved and made smaller while the workspace remains usable.
- 28.05 Transcript and guidance available for each course.
- 28.06 Optional captions, switched off by default.
- 28.07 British pronunciation distinguishes record as a noun and verb.
- 28.08 Client training includes a dedicated video on approving outside-in and standard reports.
- 28.09 Updated courses cover approvals, client management of risks and actions, report options and licence administration.

29**Existing supplier assessment import**

- 29.01 Import previous supplier questionnaire questions and responses from CSV or XLSX.
- 29.02 Preview mapped questions, responses, sections and evidence references before committing an import.
- 29.03 Capture the supplier name, services, criticality, PII and special-category processing, record volume and original assessment date.
- 29.04 Retain the original source file, parsed responses and source references for review.
- 29.05 AI reviews the supplied imported questions and context without requiring completion of the normal catalogue.
- 29.06 A committed imported assessment consumes one Standard assessment unit; previewing does not consume an allowance.

30**Client Risk Posture**

- 30.01 Dedicated full organisational questionnaire with all 29 sections and 136 questions.
- 30.02 Client self-assessment and reassessment are excluded from supplier assessment allowances.
- 30.03 Confirm section applicability and explain exclusions while retaining the question history.

Client Risk Posture / continued

- 30.04 Private client evidence area with certification, cyber insurance and professional indemnity categories.
- 30.05 AI review considers applicable answers, client business context and supplied evidence.
- 30.06 Separate internal-control and supplier-network risk positions inform the combined posture.
- 30.07 Approved Tier 1 and standard supplier findings influence network exposure; unassessed, expired and pending coverage remains visible.
- 30.08 Section risk matrix, executive summary, risk rationale and recommended actions.
- 30.09 Client-admin approval and recorded amendments before prospective-client disclosure.
- 30.10 Changed questionnaire, business or supplier findings invalidate the current-review status and restrict disclosure until refreshed.
- 30.11 Export the complete questions and saved answers to Excel.
- 30.12 Download a dated PDF posture overview with scope, section conclusions, findings, evidence and approval status.

31**Private prospective-client assurance reviews**

- 31.01 Named Microsoft sign-in with a seven-day access expiry and administrator revocation.
- 31.02 NDA required by default, with an explicit recorded reason for any waiver.
- 31.03 The client is the information Provider and prospective client the Recipient in the confidentiality workflow.
- 31.04 Prepare an editable pre-populated NDA or use an approved uploaded version with the required retention terms.
- 31.05 Send the NDA for signature, receive the signed return and record client acceptance before document access.
- 31.06 Read-only access to the approved posture and full questionnaire responses after the access conditions are met.

Private prospective-client assurance reviews / continued

- 31.07 Client-selected evidence and certificates can be downloaded by the authorised prospect.
- 31.08 Downloads and material access decisions are recorded for audit.
- 31.09 Three-month non-engagement deadline, access expiry, deletion-request follow-up and recorded deletion acknowledgement.
- 31.10 Record an engagement reference to distinguish an active client relationship from a non-engagement deletion follow-up.

32

Supplier confidentiality agreements

- 32.01 Pre-populated editable NDA with the client as Recipient and supplier as Provider.
- 32.02 Client company information and known supplier details are drawn from the workspace profiles.
- 32.03 Review the purpose, effective date, governing law, courts and agreement clauses before issue.
- 32.04 Client administrators can retain reusable NDA clause wording.
- 32.05 Alternative upload and selection of an existing approved NDA.
- 32.06 Branded request email with the NDA attached where size permits, otherwise available through the secure workspace.
- 32.07 Supplier confirmation of its company details produces a new issued version before signed return.
- 32.08 Signed return, client acceptance, assessment-access gating and retained version/audit history.

33

Legal information and product resources

- 33.01 Dedicated Supplier Risk Workspace privacy policy, controller and DPO contact details.
- 33.02 SaaS terms linked from the footer, with Cyprus governing law, licence allowances and committed payment terms.

Legal information and product resources / continued

- 33.03 Order-form provisions for optional onboarding, setup and managed supplier due-diligence services.
- 33.04 DPS Compliance Hub Trust Centre links.
- 33.05 Downloadable product brochure and full feature reference.

Make supplier risk a decision you can stand behind.

See how the Supplier Security Workspace can support your organisation, your suppliers and your next procurement decision.

Arrange your demonstration

info@dataprivacyservices.co.uk



Explore the workspace

dpscompliancehub.com