

Your suppliers are part of your attack surface

Third Party Risk Hub — send, verify, track.

Most third-party risk programmes stop at attestation. A spreadsheet goes out, a supplier fills it in, the answers are filed, and nobody looks again until the renewal — by which point the certificate has lapsed and the exposed service has been sitting there for eight months. The Hub closes both gaps: **every answer is checked against independently observed evidence**, and the checking carries on after the form is filed.

Caldera Freight Systems

security@caldera-freight.example · caldera-freight.example

completed

weak · 42%

3 new alerts

Assessed 15 Sept 2026 · Last scanned 23 Sept 2026

38%

High Risk

-19 pts · 4 scans

Duty security manager, 24/7 hotline, 1-hour acknowledgement target.

critical

depot-systems

Edit tags

View Responses

Re-send

Re-scan

View Scan

Refresh Incident Contact

One supplier, one record. Self-reported score beside the externally observed one, unacknowledged alerts, a trend across the last twelve scans, the agreed incident contact and your own tags. Illustrative data.

Send

PAGE 2

A token-gated questionnaire the supplier completes with no account, no password and no software. Use the 26 standard questions, trim them, or send only your own — all weighted and scored server-side.

Verify

PAGE 3

Risk Purview scans the supplier's own domain against eight independent evidence sources and reports where the answers and the observed evidence disagree.

Track

PAGE 4

A weekly re-scan raises alerts on drift. Renewals are chased automatically. When something goes wrong, one screen notifies the suppliers who need to know.

WHAT SITS BEHIND A SUPPLIER RECORD

Two scores, never one

A supplier carries a **self-reported** score from the questionnaire and an **externally observed** Risk Purview score from the scan, deliberately kept apart. When they disagree, that disagreement is the finding — and the one thing a supplier cannot self-certify away.

200 suppliers in the standard pool

Tags up to 10 per supplier, filterable portfolio-wide

CSV export of the current view

Trend last 12 scans per supplier

Incident contact captured from the supplier

White-label supplier-facing pages

WHY IT LANDS ON YOUR DESK

Every framework you already run asks about suppliers

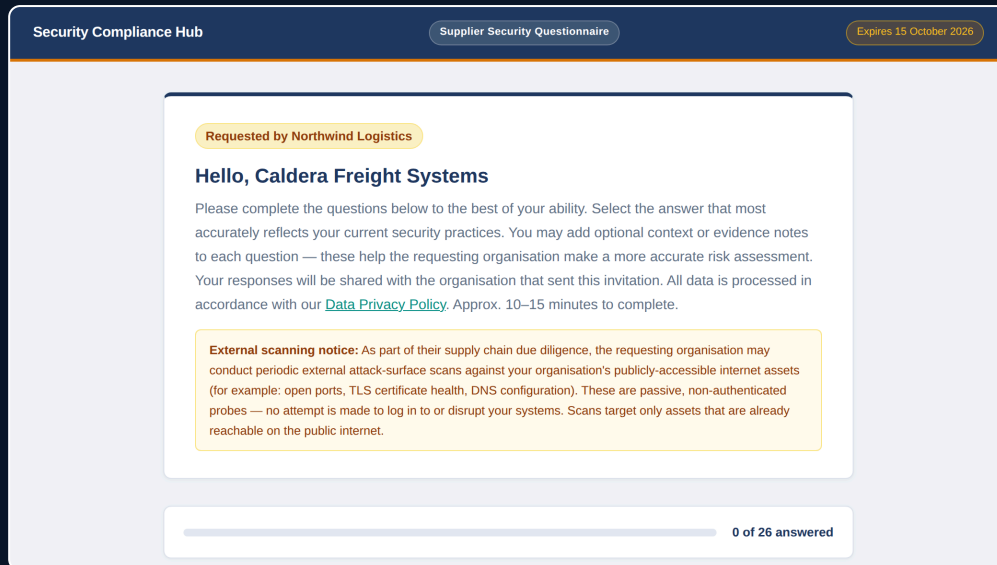
FRAMEWORK	WHERE	WHAT IT EXPECTS OF YOU
NIS2 Directive	Art. 21(2)(d)	Supply chain security named as a required measure in its own right.
DORA	Art. 28 & 30	ICT third-party risk management and specific contractual provisions.
NCSC CAF	A4	Understanding and managing supply chain risk to the essential function.
ISO 27001:2022	A.5.19 – A.5.22	Supplier relationships, agreements, and monitoring of service delivery.
CRMA · PE Due Diligence	Theme 11	Supply chain and third-party risk as a scored maturity theme.

It runs alongside your own assessments, not instead of them. The Hub already answers "how good are we?". This answers the other half — *how good is everyone we depend on?* — on the same platform. With Risk Operations, **Add to risk register** on a supplier's card opens a risk filled in from its record, and the card shows the supplier's open risks.

The questionnaire

26 questions · 8 domains · no account, no password, no software.

Response rate is the whole game. A supplier who has to create an account, remember a password and learn an interface will not finish — so they never have to. The link is single-use and token-gated, the page is one scrolling form, and it takes ten to fifteen minutes. **Every answer takes an optional free-text note**, because "partially" without a reason is not much use to either side.



The supplier's own view. Note the scanning notice — consent is obtained on the page, before any probe runs. Illustrative data.

THE EIGHT DOMAINS

Governance & Policy	3 q	Policy, named accountability, contractual obligations.
Certification & Assurance	3 q	CE, ISO 27001, SOC 2 and independent testing.
Access Control	4 q	MFA, privilege, joiners and leavers, remote access.
Data Handling	3 q	Classification, encryption, retention and disposal.
Network Security	3 q	Segmentation, perimeter, monitoring.
Incident Response	3 q	Plan, notification commitment, exercising.
Resilience & Continuity	3 q	Backup, recovery objectives, tested restore.
Vulnerability Management	4 q	Patching, scanning, disclosure, remediation SLA.

ADD YOUR OWN QUESTIONS

- ▶ **Up to 100 authored**, 100 in any single send, with the standard questions or instead of them
- ▶ **Genuinely scored** — weight 1, 2 or 3, on the same four-point scale, not informational padding
- ▶ **Your own domains**, rendered after the canonical eight
- ▶ **Import from CSV** if the questions already exist somewhere else

Custom questions never distort your benchmark.

Two scores are computed on submission: a merged score including your own questions — the one you act on — and, when all 26 standard questions were asked, a standard-only score, so peer comparison stays comparing like with like.

ONCE IT'S OUT THE DOOR

Live links behave themselves

Snapshotted at send

The question set is frozen into the link. Editing or deleting a custom question afterwards never changes a questionnaire already in a supplier's inbox.

Expiry and revocation

Pick 7, 30 or 90 days, or no expiry. Revoke at any time. Anything outstanding past its window — or past 14 days with no expiry set — is flagged Overdue.

Your brand, not ours

Your logo and accent colour on every supplier-facing page, and the sender identity the supplier sees is the organisation actually asking.

Scoring happens on the server, not in the browser. A supplier cannot influence their own score by editing what the page sends. Answers are weighted, banded into high / medium / low, and written straight onto the supplier record.

Risk Purview

What they told you, checked against what the internet already shows.

Point Risk Purview at the supplier's domain and it assembles an independent picture from eight evidence sources — no credentials, no agent, nothing installed at the supplier. Every probe is passive and touches only assets that are already reachable on the public internet, and the supplier is told so on the questionnaire page before any scan runs. The output is a composite observed score, a set of severity-ranked signals, and — **the part that actually changes conversations** — the contradictions.

WEAK

42%

Externally observed risk level, derived from attack surface, breach intelligence, and Companies House evidence. For comparison: **38%** self-reported.

⚠ Self-reported High Risk · Externally observed weak — investigate contradictions below.

CONTRADICTIONS

3

CRITICAL

Claimed: MFA is enforced on all remote access

⚠ Port 3389 (RDP) answers directly from the internet with no gateway or MFA broker in front of it.

HIGH

Claimed: All internet-facing systems run supported, patched software

⚠ Observed banner matches a build with 3 known CVEs, the oldest published 14 months ago.

MEDIUM

Claimed: Email authentication is fully configured

⚠ SPF present but no DMARC record found for caldera-freight.example.

The headline output is disagreement.

Claimed MFA on all remote access, against RDP answering directly from the internet. Claimed patched internet-facing systems, against a banner matching three known CVEs. Illustrative data.

WHERE THE EVIDENCE COMES FROM

Shodan exposed services, CVEs

crt.sh certificate transparency

HIBP disclosed breaches

Enzoic non-disclosed exposure

Companies House UK registry

Google Public DNS

TLS probe grade, expiry, protocol

DNS probe SPF, DMARC, DKIM

WHAT A CONTRADICTION IS

Not a low score. A specific, cited clash between one stated answer and one observed fact, ranked critical to low, each carrying the claim it contradicts and the evidence that contradicts it. A supplier can argue with a score. It is considerably harder to argue with an open port.

BEYOND THE CONTRADICTIONS

The rest of the picture

Attack surface

Resolved addresses, open ports, known CVEs matched to observed banners, and subdomains from certificate transparency.

Breach intelligence

Disclosed breach events and non-disclosed credential exposure against the supplier's domain, with the data classes involved.

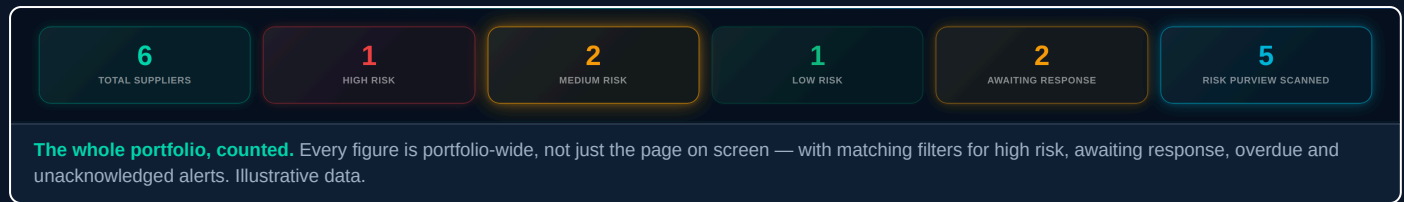
Certificate and email posture

TLS grade, issuer, protocol and days to expiry; SPF, DMARC and DKIM presence — the two that quietly decay between reviews.

Honest about its own limits. A CDN-fronted or heavily proxied domain shows the CDN's posture, not the supplier's, and the report says so rather than scoring it as clean. Risk Purview is external observation used to interrogate an answer — it is not a penetration test, and it is never presented as one.

It keeps watching after the form is filed

Weekly re-scans, six alert types, chased renewals, and a way to reach every affected supplier at once.



DRIFT DETECTION — WHAT RAISES AN ALERT

ALERT	RAISED WHEN
New signal	A risk signal appears that the previous scan did not see.
Severity escalation	An existing signal moves up a severity rank.
New contradiction	Observed evidence starts clashing with a stored answer.
Score drop	The observed score falls by 10 points or more.
New breach	A breach or credential exposure is reported since the last scan.
Certificate expiring	TLS expiry crosses inside 30 days.

CHASED, NOT REMEMBERED

- ▶ **Weekly re-scan** across the portfolio, with per-supplier failures skipped rather than breaking the sweep
- ▶ **Annual renewal reminders** at 30 days, 7 days, on the day and overdue — one digest per owner, not one email per supplier
- ▶ **Alerts clear when seen**, not when dismissed: the badge zeroes the moment you open the findings behind it

Executive portfolio report. An AI analysis across the whole supplier base — concentration, the suppliers actually worth your attention, and what to do about them.

WHEN SOMETHING GOES WRONG

Incident communications, both directions

INBOUND — WHO DO WE CALL?

Each supplier is asked, over its own secure link, how it would notify you of an incident and who to contact. The answer is summarised onto the supplier record, so the escalation path exists before the 2 a.m. call rather than being improvised during it.

OUTBOUND — THE RED BUTTON

Notify affected suppliers in one pass: compose from a template, segment by selection, tag or risk tier, preview, then confirm by typing SEND. Recipients acknowledge with one click and the responses are tracked per supplier.

Sending is gated separately. Reaching hundreds of external contacts needs its own authority on top of Hub access — plus a per-send recipient cap, a cooldown between sends and a daily volume ramp, so nobody fires a mass broadcast by accident.

Tags ▼

All 6
High risk 1
Medium 2
Low 1
Awaiting 2
Overdue 1
Alerts 4

Finding the ones that matter. Live search across name, email and domain, your own tags, and one-press filters for each risk band, awaiting a response, overdue and unacknowledged alerts. Illustrative data.

FOR PRACTICES RUNNING THIS ON BEHALF OF OTHERS

MSP and vCISO portfolios

Every client organisation gets its own isolated supplier portfolio, scans, alerts and tags — reachable from the client's own tab in the MSP Portal, never pooled and never visible across clients. Team members can be scoped to only the clients they are engaged on, and given read-only access. Questionnaire branding shows the client's identity rather than yours, where that is what the supplier should see.

WHAT IT TAKES TO START

1 · Add the supplier

Name, a contact address and the domain — the domain is what makes Risk Purview possible.

2 · Send the questionnaire

Choose the questions (standard, your own or both), pick an expiry, and send it branded as you.

3 · Scan straight away

Risk Purview doesn't wait for the supplier to answer — the domain alone is enough.