PROSIKON

Vendor Due Diligence Platform

Know your vendors.
Prove your due diligence.

Secure, scored, and audit-ready third-party cybersecurity assessments in one platform.

Start your 7-day free trial



by Arrakis Consulting

prosikon.arrakisconsulting.com

WHY PROSIKON

Third-party risk is your risk.

Every vendor you connect to your data, systems, or customers extends your attack surface. Regulators, auditors, and boards now expect you to prove — not just claim — that each one was assessed, scored, and reviewed.

Most programs still run on spreadsheets and email threads. Questionnaires go out in different versions, answers come back without evidence, scoring depends on who reviewed it, and when the auditor asks who approved a vendor and why, nobody can find the record.

Prosikon replaces that with one secure, invite-only platform that runs the full vendor due diligence cycle — from the first invitation to the next scheduled review — with every decision documented along the way.

Weighted
scoring that reflects the controls that matter most

Evidence
attached to the exact question it answers

Verified
with external scans of the vendor's internet footprint

Audit-ready
decisions, justifications and access all logged



Prosikon at a glance

Structured questionnaires
Weighted categories, point-based questions, conditional follow-ups and instant-fail controls.

Secure vendor invites
Unique links and QR codes with a one-time security code — no public sign-up.

Live risk dashboards
Invite status, score distribution, risk matrix, overdue and unassigned vendors at a glance.

External verification
Shodan exposure, Pentest-Tools scans, DNS records and breach research per vendor.

Decisions with justification
Manager suggestions and client final decisions, each with a recorded reason.

Automated reporting
Scheduled monthly reports, review reminders and domain-restricted email delivery.

Public

HOW IT WORKS

From invitation to decision.

Prosikon runs the whole assessment cycle in one place, so nothing falls between the cracks.

01

Configure your assessment

Build weighted categories such as Access Control, Incident Response and Data Protection. Add scored questions, conditional follow-ups and auto-fail criteria mapped to your frameworks.

02

Invite vendors securely

Send a unique link or QR code with a one-time security code. Each vendor gets private, isolated access — no public sign-up and no visibility into other vendors.

03

Vendors answer and upload evidence

Respondents sign in with a magic link or Microsoft, answer only the questions that apply to them, and attach certificates, policies and audit reports to individual answers.

04

Verify with external intelligence

Run external attack-surface scans, pull DNS records and review breach history to corroborate what the questionnaire claims.

05

Score, decide and justify

Weighted scoring produces an overall posture percentage. Vendor managers suggest an outcome; the client company records the final decision with written justification.

06

Report and schedule the next review

Set the next review date, send scheduled reports to approved recipients, and keep a full audit trail across every step.

Built for repeatability

Every vendor goes through the same structured process with the same scoring rules — so results can be compared fairly across your entire supply chain and defended in front of an auditor.

Public

COMMAND CENTER

See your entire vendor portfolio at once.

The Prosikon dashboard turns hundreds of assessments into a clear picture of where your third-party risk sits today.



Dashboard: live totals, invite status and vendor score distribution.

- **Headline metrics** — total questions, categories, invites sent, completed, unassigned and overdue vendors — with red alerts you can click to see exactly which vendors need attention.
- **Invite status** — track how many vendors have not accepted, are in progress, or have completed their assessment.
- **Score distribution** — see how vendors cluster across risk bands, with certification-based passes shown separately.
- **One-click export** — download a vendor risk report as a PDF, optionally with full vendor responses.



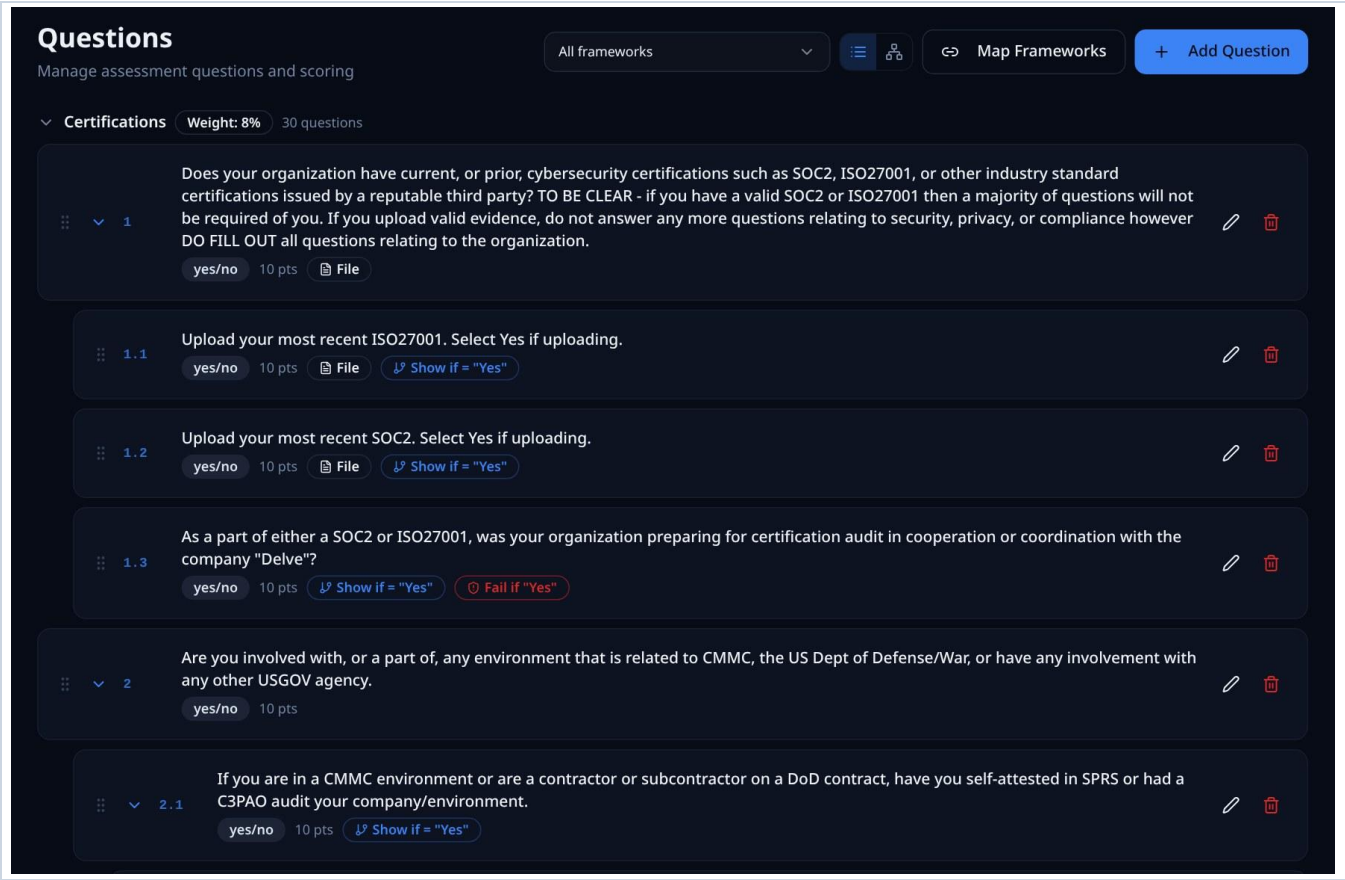
Risk matrix: vendors plotted by impact and likelihood, filterable by client company.

Public

ASSESSMENT DESIGN

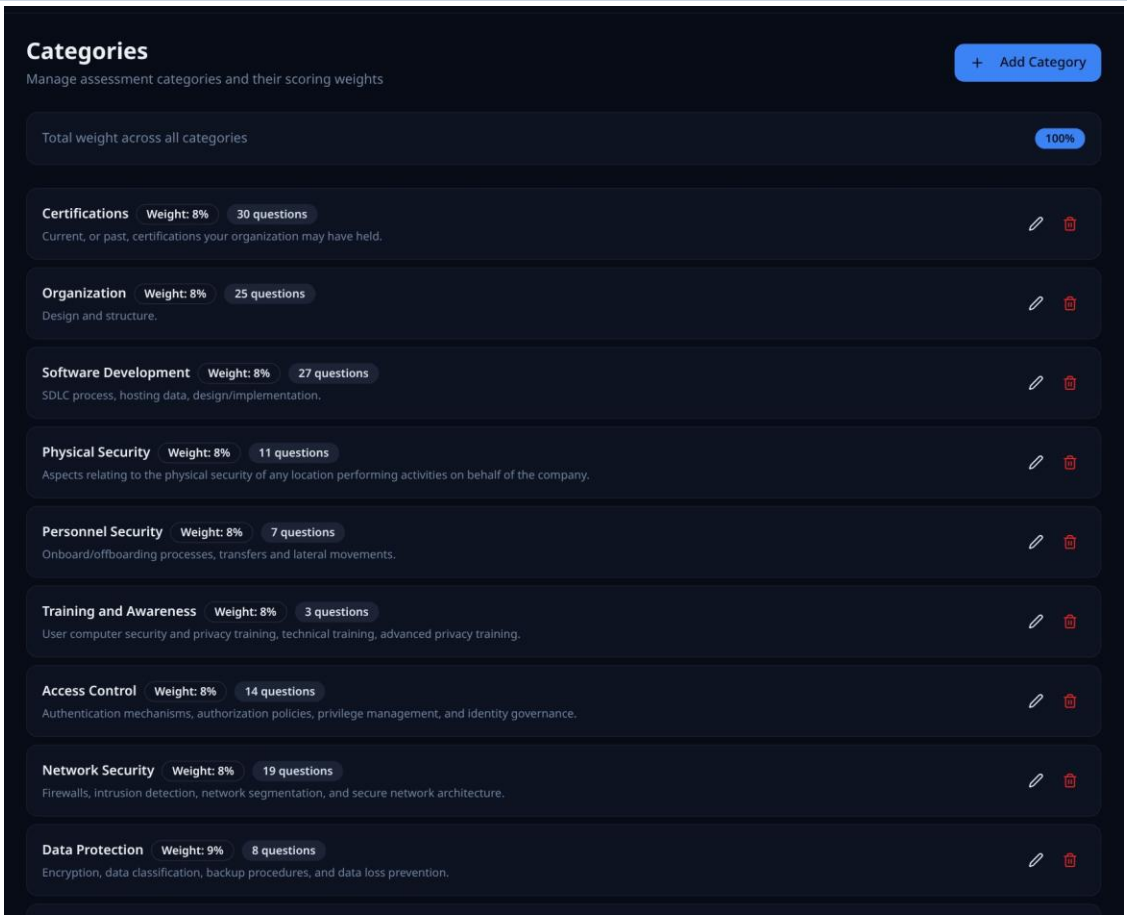
Questionnaires that score what matters.

Design assessments once and reuse them across every vendor. Prosikon handles the logic, numbering and scoring for you.



Question builder with hierarchical numbering, conditional follow-ups and auto-fail rules.

- **Weighted categories** — each category carries a weight, so the overall percentage reflects your priorities rather than a flat question count.
- **Points per question** — yes/no, multiple choice, text and file-upload questions, each with its own point value.
- **Conditional follow-ups** — sub-questions appear only when an answer triggers them, numbered 1, 1.1, 1.1.1 so vendors never lose their place.
- **Auto-fail controls** — flag critical questions that instantly fail a vendor, with regulatory references attached.
- **Framework mapping** — map questions to NIST SP 800-53, ISO 27001, CIS Controls and CMMC so one response set evidences several requirements.
- **Drag-and-drop ordering** — reorder questions and categories visually; numbering updates automatically.



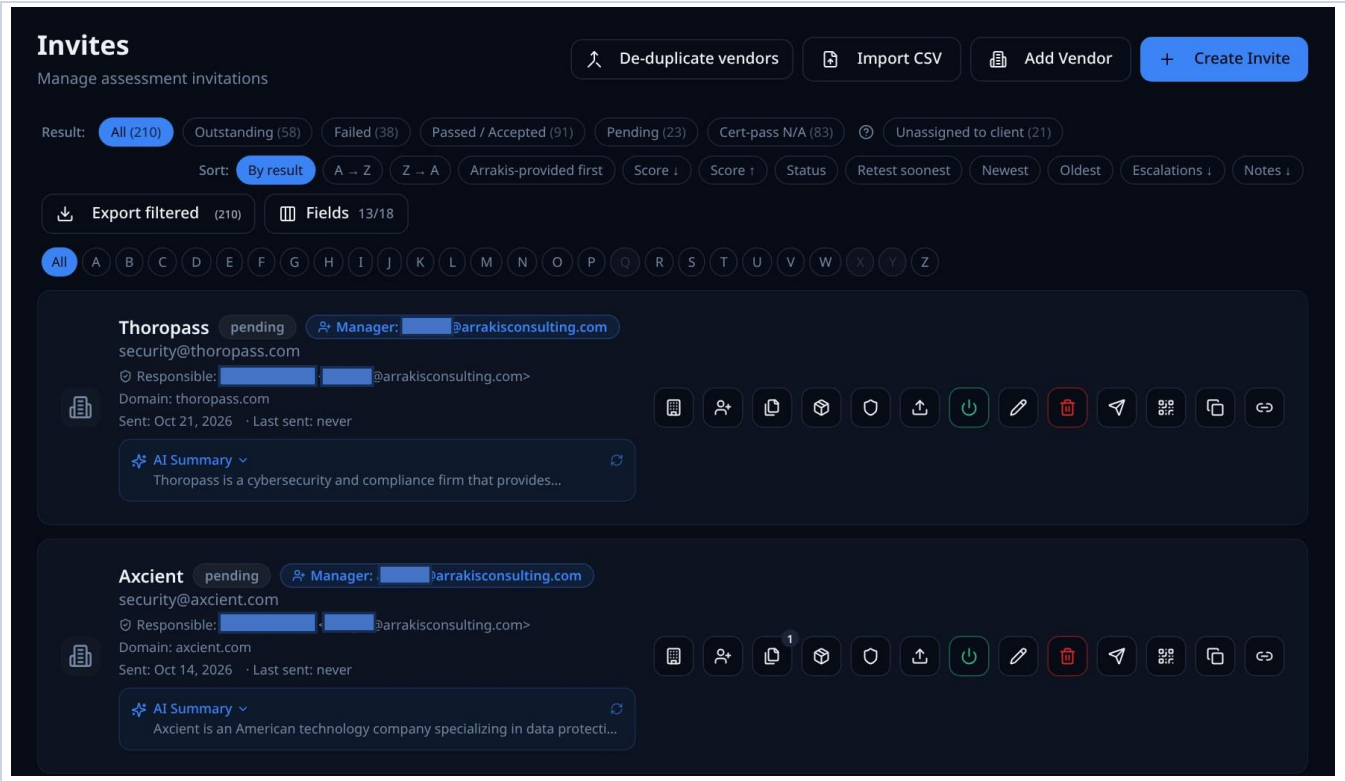
Category management: weights, descriptions and question counts in one view.

> **Certification-aware scoring**
> Vendors holding a valid SOC 2 or ISO 27001 can upload it as evidence and be accepted via certification — saving them time while keeping your record complete.

VENDOR ONBOARDING

Secure invitations, effortless for vendors.

Getting vendors to respond is often the hardest part. Prosikon makes it fast for them and secure for you.



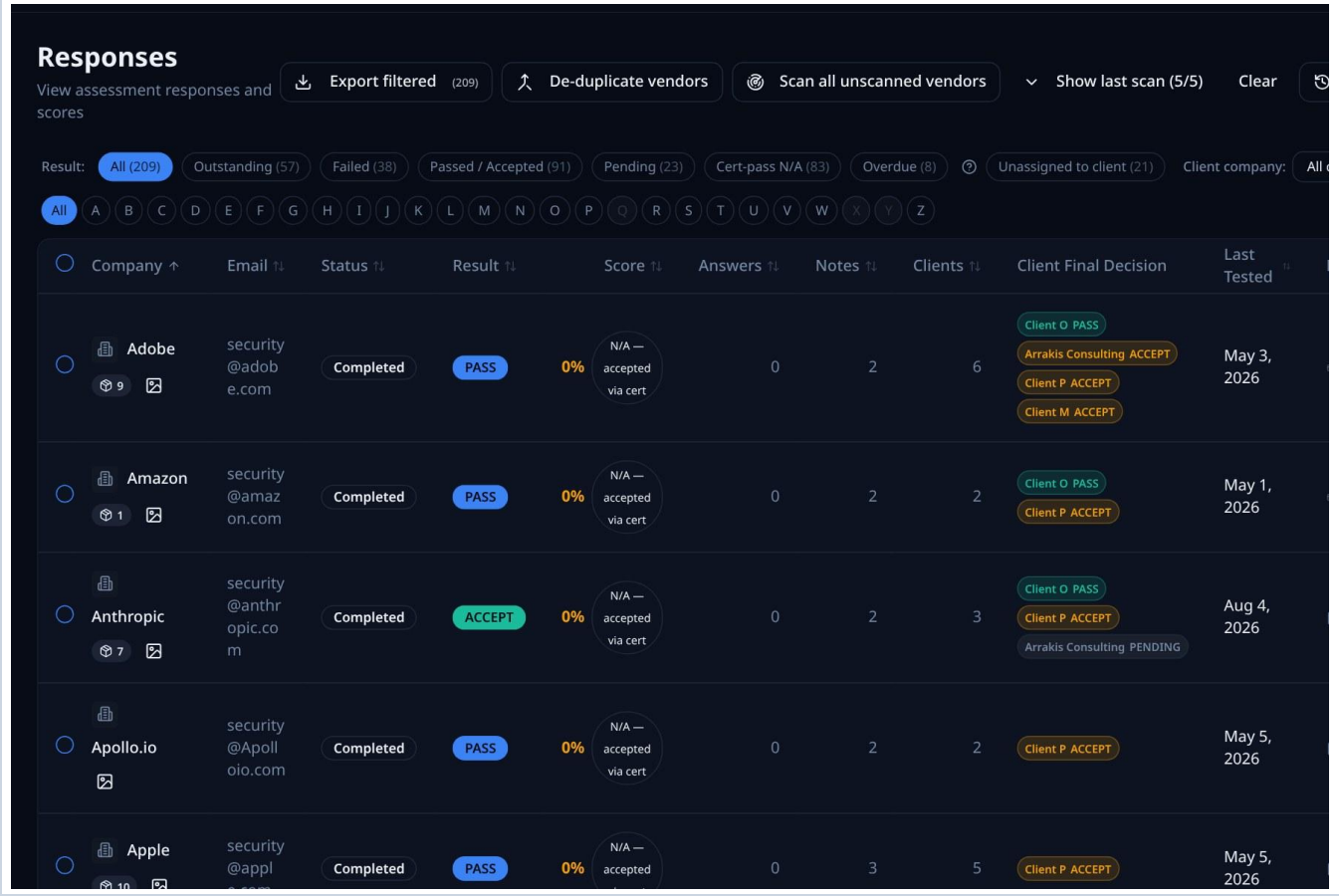
Invites: filter, sort and manage every vendor invitation, with AI-generated company summaries.

- **Invite-only access** — each vendor receives a unique assessment link and QR code plus a security code in the invitation email.
- **Easy sign-in** — respondents sign in with a one-time magic link or their Microsoft account — no passwords to manage.
- **Bulk onboarding** — import vendors from CSV, de-duplicate records and assign vendor managers and client companies in bulk.
- **Resend in one click** — resend the security code and QR code at any time; admins can view the link and QR directly.
- **Protected evidence** — uploads are limited to PDF, JPG and PNG. Files can be marked protected so only the uploader and authorized staff can open them.
- **Conversion tracking** — see when invites are opened, sign-ins completed and assessments started.

REVIEW AND DECIDE

Every response, every decision, on record.

Review answers question by question, then record a decision your auditors can trace back to its justification.



Responses: A–Z navigation, result filters, scores and client final decisions per vendor.

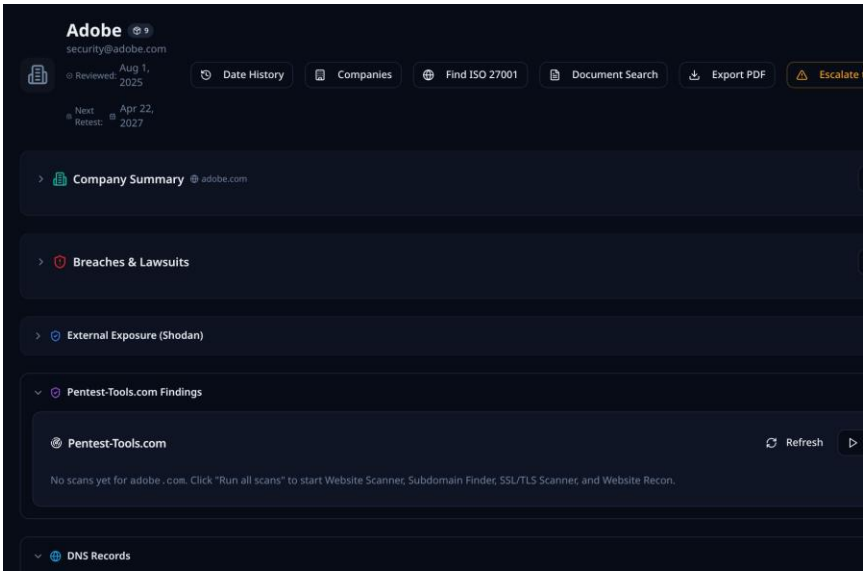
- **Fast navigation** — jump by letter, filter by Outstanding, Failed, Passed, Pending, Overdue or Unassigned, and export exactly what you see.
- **Grouped by category** — responses are organized by category with conditional questions nested beneath their parent.
- **Vendor manager suggestion** — suggest an outcome with a reason — including SPRS Self Attest and C3PAO Passing Assessment for defense contractors.
- **Client final decision** — Pass, Fail, Accept, Pending or Exempt, with written justification required for Accept and Exempt.
- **Protected justifications** — justifications are visible only to authorized users, and every view is logged.
- **Bulk edit** — assign many vendors to client companies and vendor managers in a single action.

VENDOR INTELLIGENCE

Trust, but verify.

Self-attestation only tells part of the story. Prosikon checks each vendor's real-world internet footprint so you can corroborate what they tell you.





Vendor profile: company summary, breaches and lawsuits, external exposure, Pentest-Tools findings and DNS records.

External exposure (Shodan)
Discover open ports, services and known vulnerabilities on the vendor's internet-facing systems.

Pentest-Tools.com scans
Website Scanner, Subdomain Finder, SSL/TLS Scanner and Website Recon — run from the vendor profile.

DNS records
Pull DNS records via DNSDumpster to map the vendor's domains and hosting.

Breaches and lawsuits
AI-assisted research summarizing public breach and litigation history.

Certification finder
Locate published ISO 27001 certificates and security documents for the vendor.

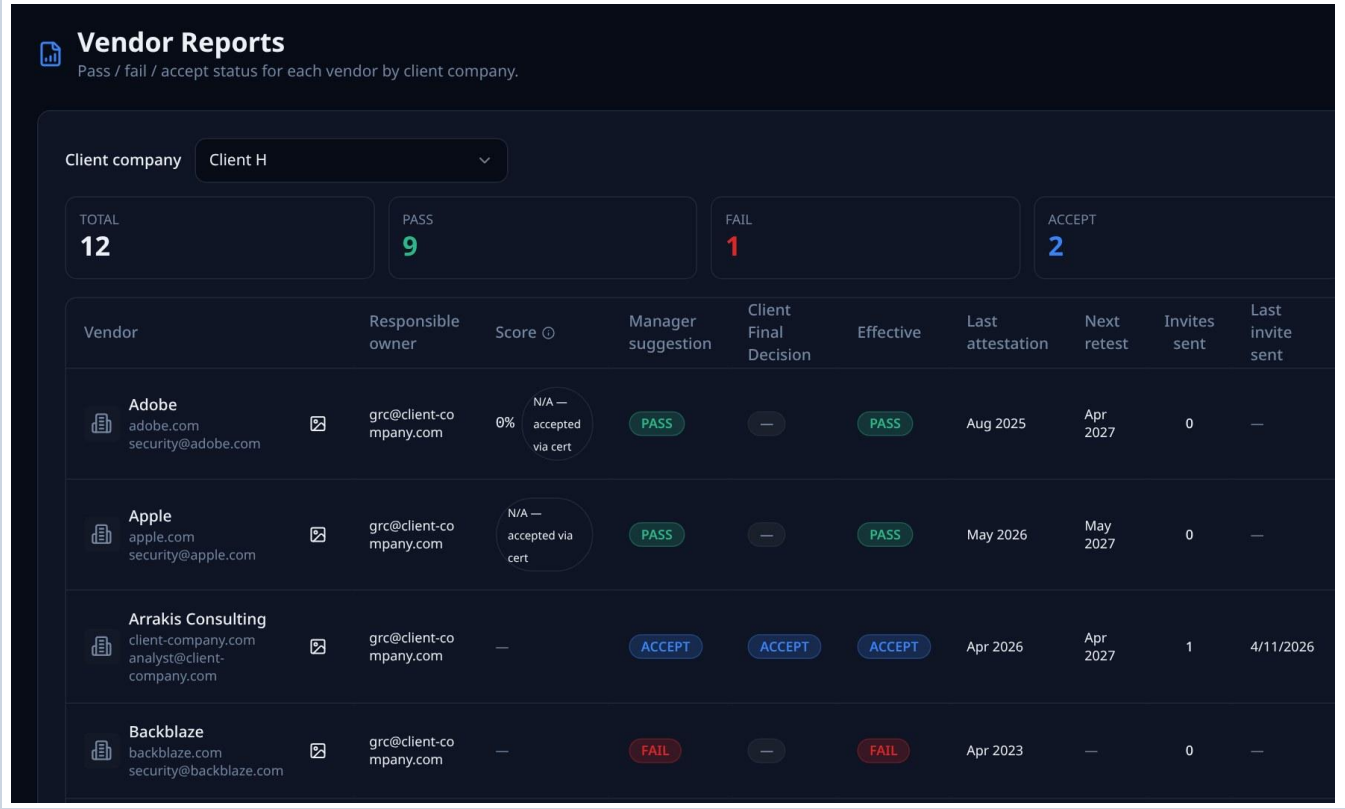
Escalate and export
Escalate concerns to the client company or export the full vendor profile as a PDF.

Public

REPORTING AND SCHEDULING

Reports that send themselves.

Give every stakeholder the view they need — on demand or on a schedule — without ever sending data to the wrong inbox.



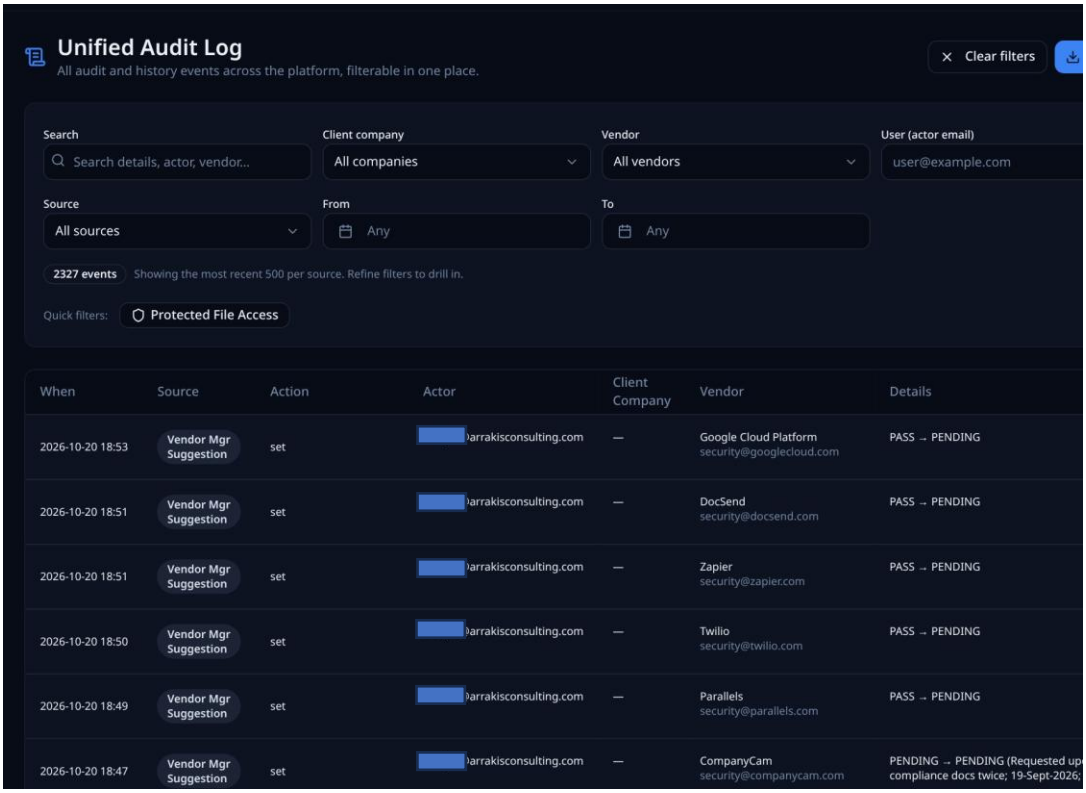
Vendor reports: pass, fail and accept status for each vendor by client company.

- **Client company reports** — pass / fail / accept status, scores, last attestation and next review date for every vendor.
- **Scheduled monthly reports** — vendor reports, passed-vendor reports and MSP portfolio reports delivered automatically.
- **Review calendar and reminders** — see upcoming and overdue reviews on a calendar and send reminders before assessments go stale.
- **Default recipients** — set To and CC recipients per client company so reports are addressed correctly every time.
- **Recipient safeguards** — reports can only go to the client's own email domain or authorized staff, and senders must confirm recipients before sending.
- **Confidentiality notice** — every emailed report carries an intended-recipients disclaimer.

AUDIT AND COMPLIANCE

An audit trail for everything.

When an auditor asks who saw what, who decided, and who received which report, the answer is one search away.



Unified audit log: every decision, report, email and file access in one searchable, filterable view.

- **Unified audit log** — decisions, report generation, emailed reports with their recipients, and administrative changes.
- **Protected file access audit** — every attempt to open a protected file is recorded, with quick filters.
- **Justification view audit** — see who viewed sensitive decision justifications and when.
- **Email log** — a complete record of what was sent, to whom, and whether it was delivered.

Align with the frameworks you report against

Map questions and evidence to the controls in the frameworks your organisation follows, so one assessment supports many compliance obligations.

SOC 2 · ISO 27001 · NIST CSF · GDPR · HIPAA · PCI DSS · FedRAMP

Framework logos indicate assessment alignment, not certification of Prosikon.

BUILT FOR EVERY STAKEHOLDER

The right view for every role.

Access is scoped by role and by client company, so each person sees exactly the vendors they are responsible for — and nothing more.

Role	What they can do in Prosikon
Super Admins and Admins	Configure categories, questions and frameworks; manage users and client companies; oversee every vendor, report, file and audit log.
Vendor Managers	Own a portfolio of vendors, review responses question by question, request evidence, add notes, tag colleagues, and suggest outcomes.
Client Companies	Record the final decision for vendors tied to their organisation, with justification captured for audit.
Approving Authorities	Automatically see every current and future vendor associated with their own client company, scoped by email domain.
MSPs and Consultancies	Invite their own client companies and assignees, assign vendors, and keep each client's vendors separate from everyone else's.
Read-only reviewers	View dashboards and reports without the ability to change data.
Vendor Respondents	Complete their own assessment and upload evidence — they never see another vendor's data.

Collaboration built in

Leave notes on any vendor, tag a colleague with @mention, and Prosikon emails them the note, what it is attached to, and who wrote it.

Public

SECURITY

Built on zero-trust principles.

A platform that holds your vendors' security evidence has to be secure itself. Security is the foundation of every layer of Prosikon.

Encrypted at rest
Data is encrypted at rest with AES-256, and sensitive fields are encrypted at the column level.

Row-level security
Every database table enforces access rules, so users only reach the records they are entitled to.

Multi-factor authentication
Authenticator-app MFA protects every staff account.

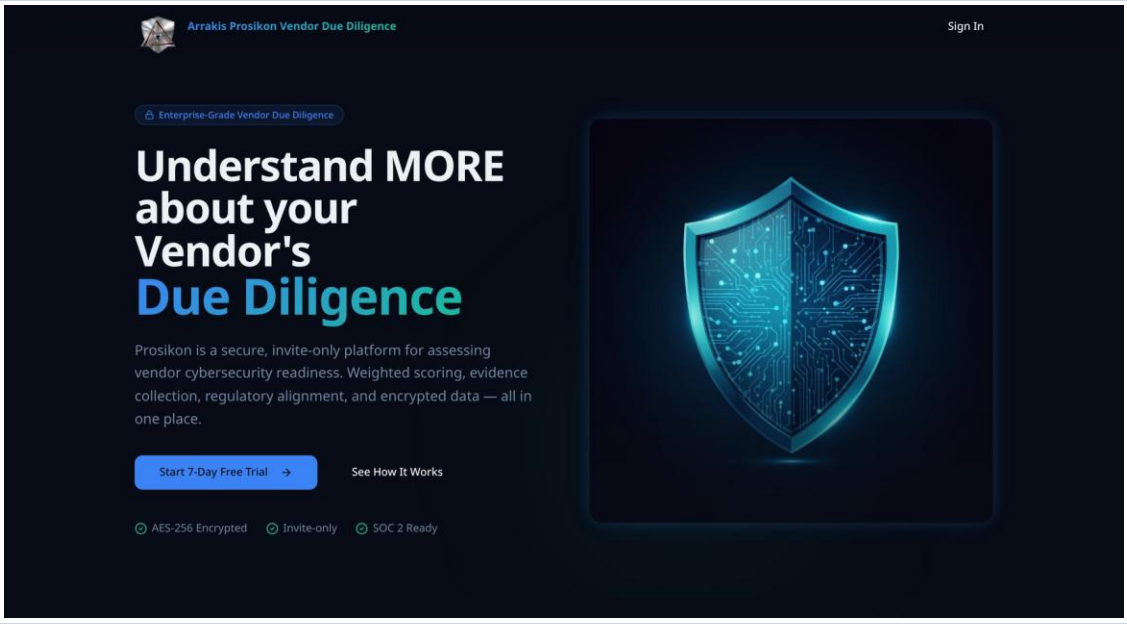
Invite-only access
No public sign-up. Vendors reach only their own assessment through a unique, coded invitation.

Isolated file storage
Evidence is stored per vendor, limited to PDF, JPG and PNG, with optional protected status.

Session protection
Inactivity timeouts sign idle users out automatically.

Full version history
Every response change is recorded for a complete audit trail.

No cross-vendor visibility
Vendors, clients and MSPs are strictly separated from one another.



prosikon.arrakisconsulting.com

GET STARTED

Why teams choose Prosikon.

- **One platform** — questionnaires, evidence, scoring, external scans, decisions, reports and audit trail together.
- **Faster vendor responses** — secure links, QR codes, magic-link sign-in and conditional questions keep questionnaires short.
- **Defensible decisions** — every outcome carries a justification and every access is logged.
- **Scales with you** — from a single security team to MSPs managing many client companies.
- **Backed by Arrakis Consulting** — a cybersecurity consultancy that uses Prosikon in its own vendor risk work.

Ready to strengthen your vendor risk program?

Start a 7-day free trial and run a full assessment cycle on your own vendors — questionnaire, evidence, scoring, external scan, decision and review date.

START YOUR FREE TRIAL

prosikon.arrakisconsulting.com/signup/trial

Questions? Talk to our team

support@arrakisconsulting.com

Public