



NxSAM Third-Party Risk (TPRM) — Quick Guide

Quick reference guide for the Third-Party Risk (TPRM) module

Product release	**NxSAM 2026.09**
Verified against code on	**2026-09-10**
Document revision	**b441b08-dirty**
Audience	**End users**
Document owner	**eSec Forte Technologies — Product Documentation**

Screenshots are taken from a demonstration data set. Figures are illustrative.

eSec Forte Technologies

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Table of Contents

Third-Party Risk (TPRM)

- Overview
- Third-Party Risk: every screen, column and action
- Third-Party Risk (TPRM): find the right screen

Reference

- Glossary

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Third-Party Risk (TPRM)

Third-Party Risk (TPRM)

TPRM assesses the security of organisations you depend on — suppliers, partners, service providers. The questions are the same as for your own systems, but you cannot scan a third party's infrastructure, so the evidence comes from them.

What makes it different

Three things shape how TPRM works:

1. **The vendor supplies the answers.** You send a questionnaire; they respond with evidence. You are assessing their claims, not observing their systems.
2. **Vendors log in themselves.** Vendor users get restricted access — they see only their own assessments and nothing else in your NxSAM.
3. **Effort should match exposure.** A supplier handling customer data warrants far more scrutiny than one supplying stationery.

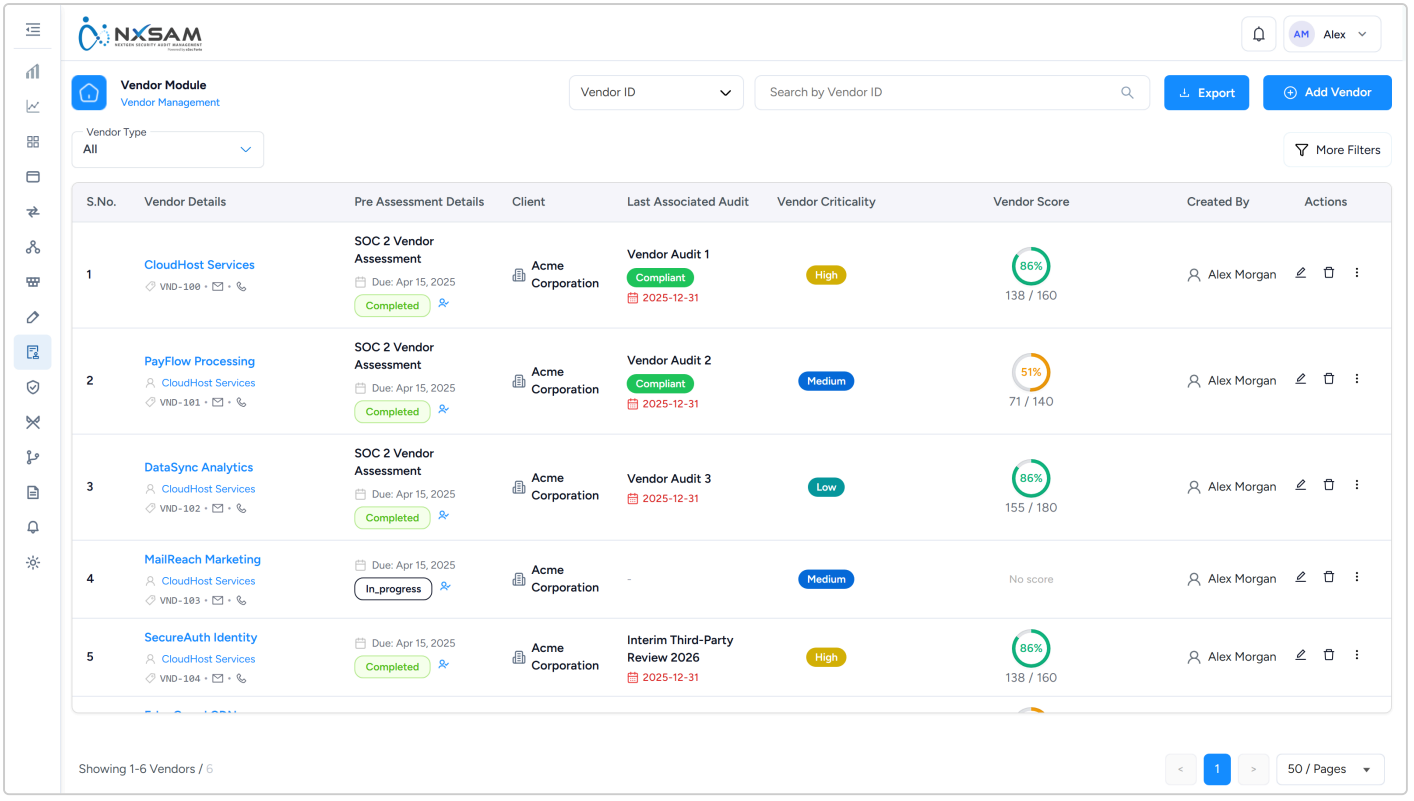
Pre-assessment: deciding how much scrutiny

Rather than sending every vendor the same long questionnaire, a short **pre-assessment** establishes what the relationship actually involves — what data they touch, what access they have, how critical they are.

That produces a tier, and the tier determines the depth of the full assessment. It keeps effort proportionate on both sides, and means a low-risk supplier is not asked to complete a two-hundred-question review.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

The full assessment



The vendor register, with criticality and assessment state per supplier.

1. **Create the audit** from a template appropriate to the vendor's tier.
2. **Invite the vendor.** Their users receive access to their assessment only.
3. **The vendor responds**, answering controls and attaching evidence.
4. **You review** the responses — accepting, challenging, or asking for more.
5. **Findings** are raised where responses are inadequate.
6. **Risks** are recorded where gaps represent ongoing exposure.

Vendor users

Vendor users are external people with deliberately narrow access. They see their own assessments and nothing else — not your assets, not your findings, not other vendors.

Because they are external, their access needs managing as relationships change. A vendor user whose engagement has ended should be deactivated.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Reusing work across vendors

Vendors answering similar questionnaires give similar answers, and standards overlap heavily. TPRM includes support for identifying where a control in one framework matches a control in another, so an answer already given can be reused rather than re-collected.

This matters most when a vendor is assessed against several frameworks, or reassessed year after year — a great deal of what they told you last time remains true.

What good looks like

- **Tier first, then assess.** Pre-assessment before the full questionnaire keeps effort proportionate.
- **Findings need owners on your side.** A vendor gap is your exposure; someone internal has to decide what to do about it.
- **Reassess on a cycle.** A vendor assessed once three years ago is effectively unassessed.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Third-Party Risk: every screen, column and action

TPRM assesses organisations rather than systems, and the people answering are outside yours — which shapes every screen in the module.

The vendor register

Column	What it holds
Vendor Details	Name, identifier, and the parent vendor where one exists
Pre Assessment Details	The triage result that decided how much scrutiny this vendor gets
Client	Which of your organisations engages them
Last Associated Audit	The most recent assessment
Max Expiry Date	When the current assessment stops being valid
Vendor Criticality	How much your business depends on them
Vendor Score	The assessment result
Created By	Who onboarded them

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Max Expiry Date is the register's working column

A vendor assessment has a validity period. **Max Expiry Date** is the latest date the current assessment remains acceptable, and a register sorted by it is a work queue — everything approaching that date needs reassessment.

A vendor past it is not "overdue on a task"; they are a supplier you can no longer evidence having assessed, which is a different conversation with an auditor.

Vendor Criticality against Vendor Score is the pair that matters. A low score on a low-criticality supplier is tolerable. The same score on a critical one is the finding.

Parent and child vendors exist because large suppliers are engaged through subsidiaries — assessing the parent once and inheriting to the children avoids assessing the same organisation repeatedly.

Vendor Email on the onboarding form is optional, and it does two things when given. If it matches an existing user, that user is linked as the vendor's default user; if it does not, a new user is created with it. Left blank, no user is created and one can be added later from Vendor users. Give it when you know who at the vendor will answer the assessment; leave it blank when you do not, rather than inventing a contact.

Pre-assessment

A short questionnaire that decides how much assessment a vendor warrants.

Column	What it holds
Vendor	Who is being triaged
Scorecard	Which scoring model was applied
Submitted	Whether the vendor has responded
Scope	What the engagement covers
Computed Tier	The tier the scorecard calculated
Final Tier	The tier actually applied

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Column	What it holds
Status	Where the pre-assessment is

> ⚠ **Computed Tier and Final Tier are separate on purpose**
>
> The scorecard computes a tier from the answers. A human can override it, and the override is recorded separately rather than replacing the computation.
>
> When they differ, someone made a judgement — and that is exactly what an auditor asks about. The two columns exist so the question has an answer.

The detail and summary screens follow the RLCM shape: `Sections`, `Control Details`, `Current Level`, `User Input` for the detail; `Section`, `Control`, `Current Level`, `POC Input`, `Rev Input` for the summary; and `Sections`, `Control details`, `Status`, `POC`, `Reviewer` for management.

Note there is no auditor column in pre-assessment. Triage is an internal judgement about how much work to do, not an assessment in its own right.

The scorecard configuration

Defines how pre-assessment answers become a score and a tier. Changing it re-tiers future pre-assessments; it does not re-tier vendors already triaged, so a register can hold vendors tiered under two different models.

Vendor users

External people who sign in to complete assessments.

Column	What it holds
Vendor Details	Which vendor they belong to
User Details	Name and contact
Role	What they can do

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Column	What it holds
User Type	The kind of account
Allowed Audit Type	Which assessments they may see
OTP Login	Whether one-time-password sign-in is enforced for them
User Status	Active or not

> ⚠ **These are accounts outside your organisation**
>
> **Allowed Audit Type** is an access control, not a convenience filter. A vendor user who can see assessments beyond their own engagement can see how you assess their competitors.
>
> **OTP Login** matters more here than for internal users: you do not control these people's password hygiene, their device, or what happens to their account when they change jobs. Enforcing OTP is the only lever you have.
>
> **User Status** is what you set when an engagement ends. Deleting the user loses the audit trail of who answered what.

Which fields the vendor user form shows is a setting, not a property of the form. Configurations → RLCM Configuration → Vendor User Form Setting has a **Form Type** of **Basic** — *only the core fields, for quick onboarding* — or **Advanced**, which adds **User type**, **Roles**, **User status**, **Landing page**, **IP group** and **Allowed audit type**, and a separate switch for **OTP Login**. A vendor user created under Basic gets the defaults for everything Advanced would have asked; check them there if a vendor user can see more or less than intended.

Vendor properties

`Property Name`, `Property Type`, `Order`, `Required`, `Created By` — custom fields on a vendor record. **Required** blocks vendor creation until filled, which is how an organisation enforces that, say, a contract reference is always captured.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

TPRM audits and findings

Findings share the RLCM shape — `Audit & Finding Info`, `Control Details`, `Risk & Observations`, `Status` — with **Add Risk** and **Map Existing Risk**.

The distinction that matters: a TPRM risk belongs to *your* register, not the vendor's. You are recording a risk your organisation carries because of a supplier, which is why these findings feed the same register as internal ones.

Control similarity

Matches a vendor's questionnaire against controls already assessed elsewhere, so a vendor who has answered an equivalent question for another framework is not asked again. **Broad Match** finds the same requirement worded differently; **Precision Match** finds close textual correspondence.

This is the difference between a fifty-question assessment and a two-hundred-question one, and vendors notice.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

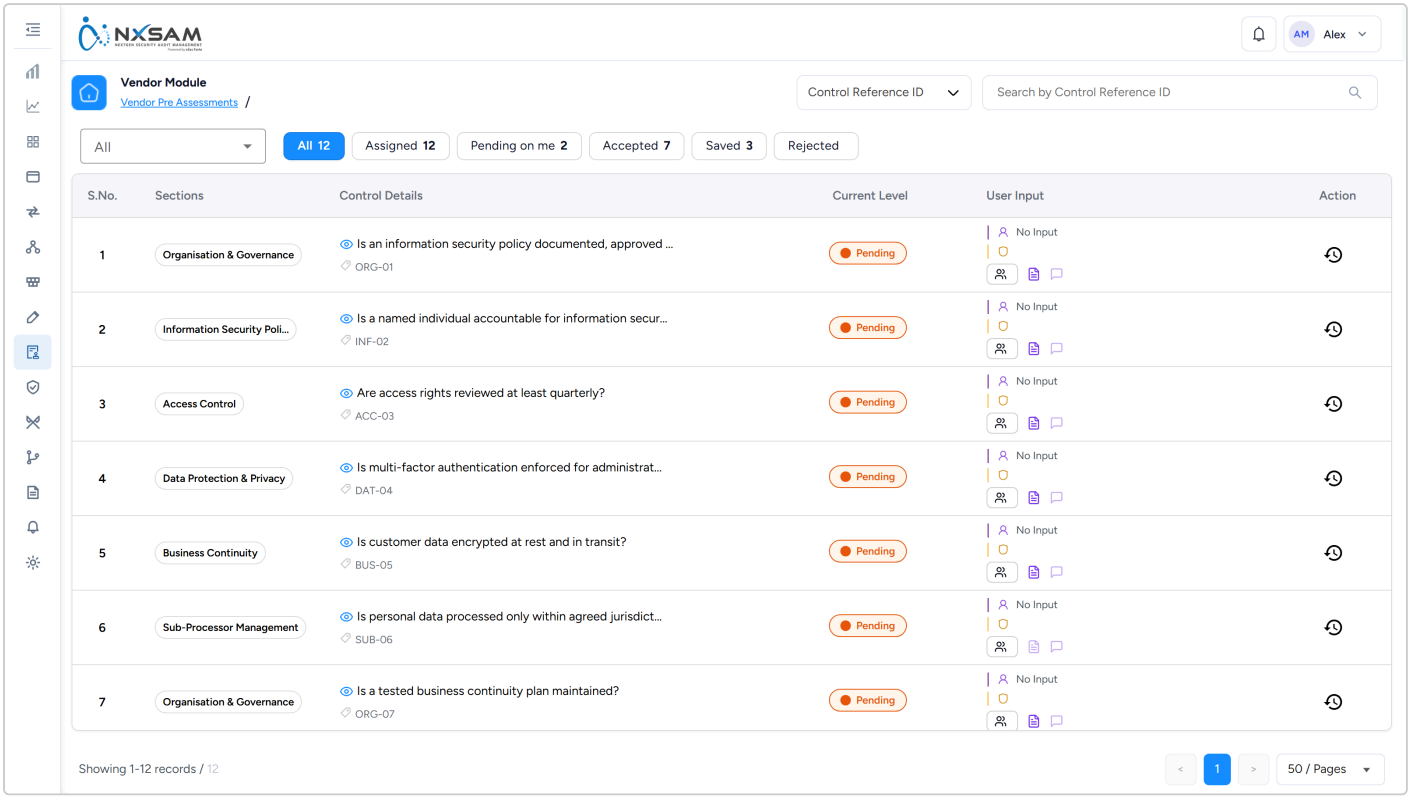
Third-Party Risk (TPRM): find the right screen

Every screen in this module, what each one is for, and where it lives. Use it to find the right screen quickly, and to confirm you are on the one a colleague means — several screens in this product have similar names and different jobs.

Screenshots come from a demonstration data set, so the figures are illustrative. Click any screenshot to open it at full resolution.

Pre-Assessment Detail

One vendor's pre-assessment responses in full.

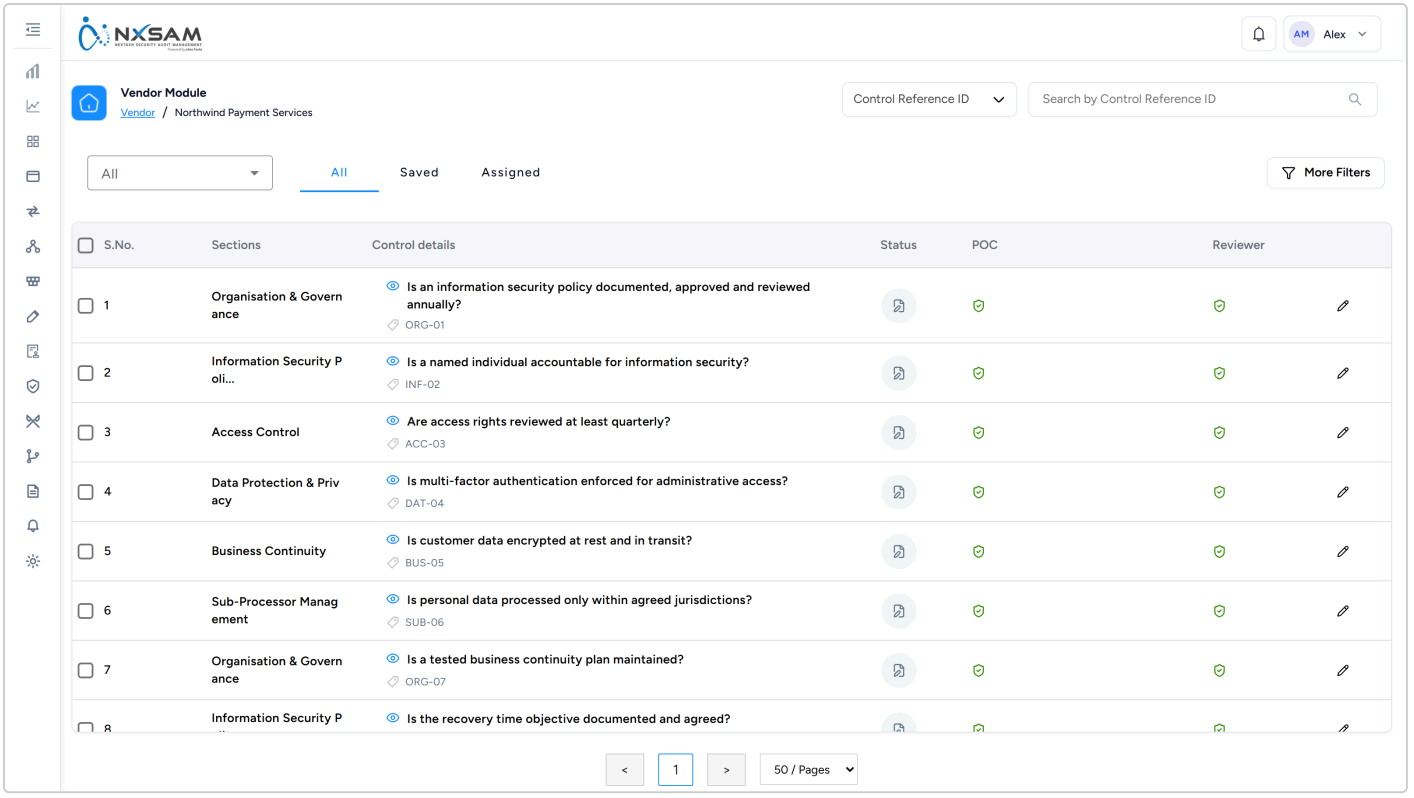


Vendor → Pre-Assessment Detail

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Pre-Assessment Management

Pre-assessments in flight and their outcomes.

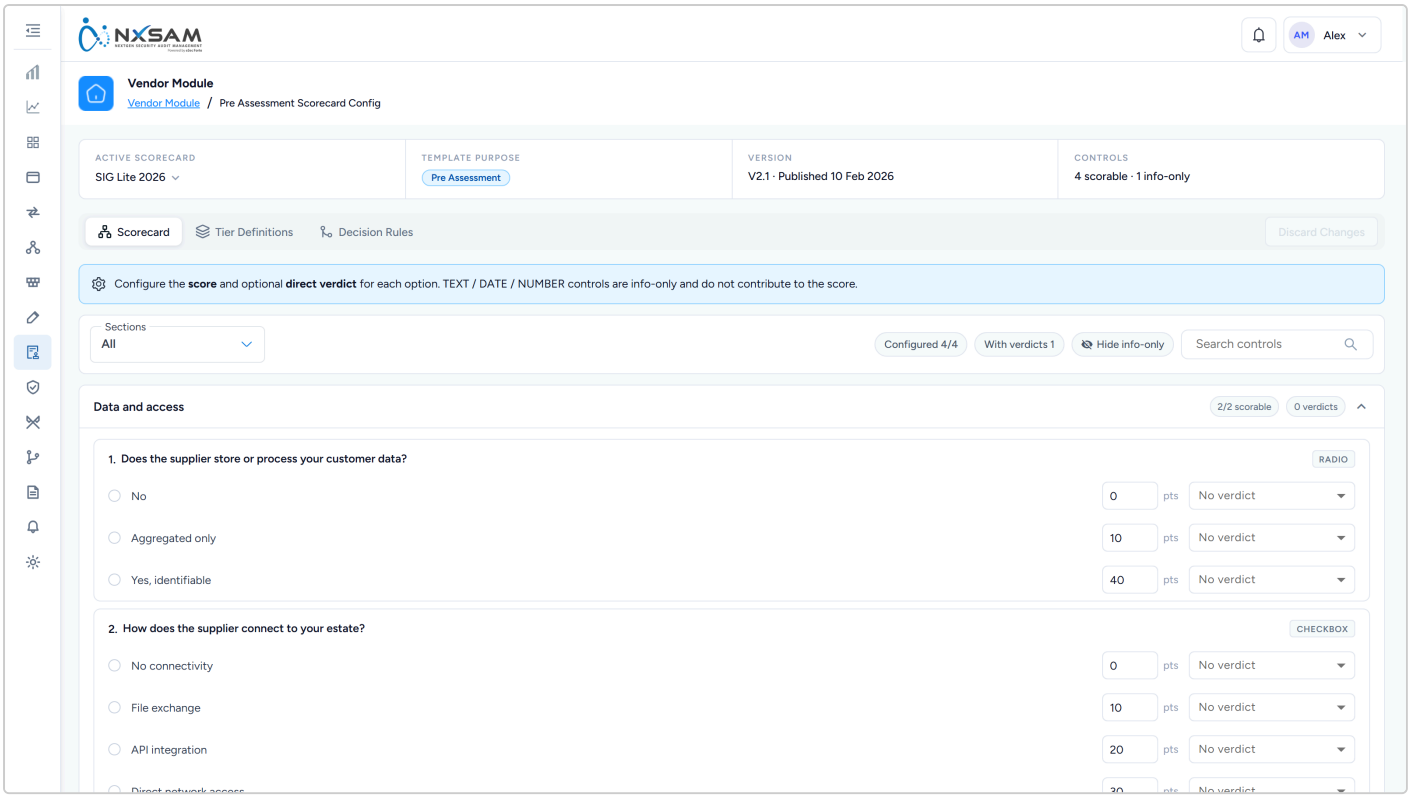


Vendor → Pre Assessment → Pre-Assessment Management

Pre-Assessment Scorecard

How pre-assessment answers turn into a score and a tier.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

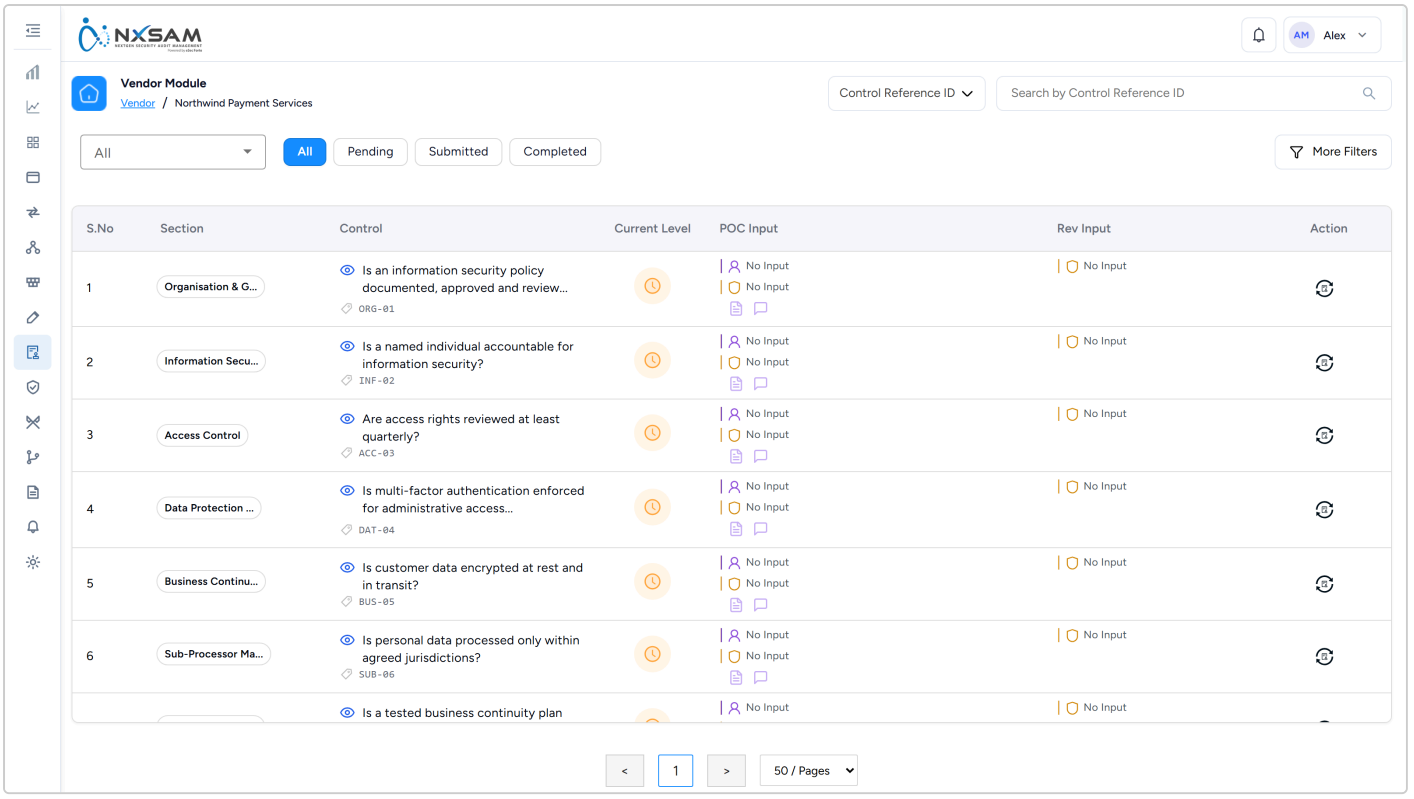


Vendor → Pre-Assessment Scorecard

Pre-Assessment Summary

The resulting tier and score, and what it means for the assessment that follows.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

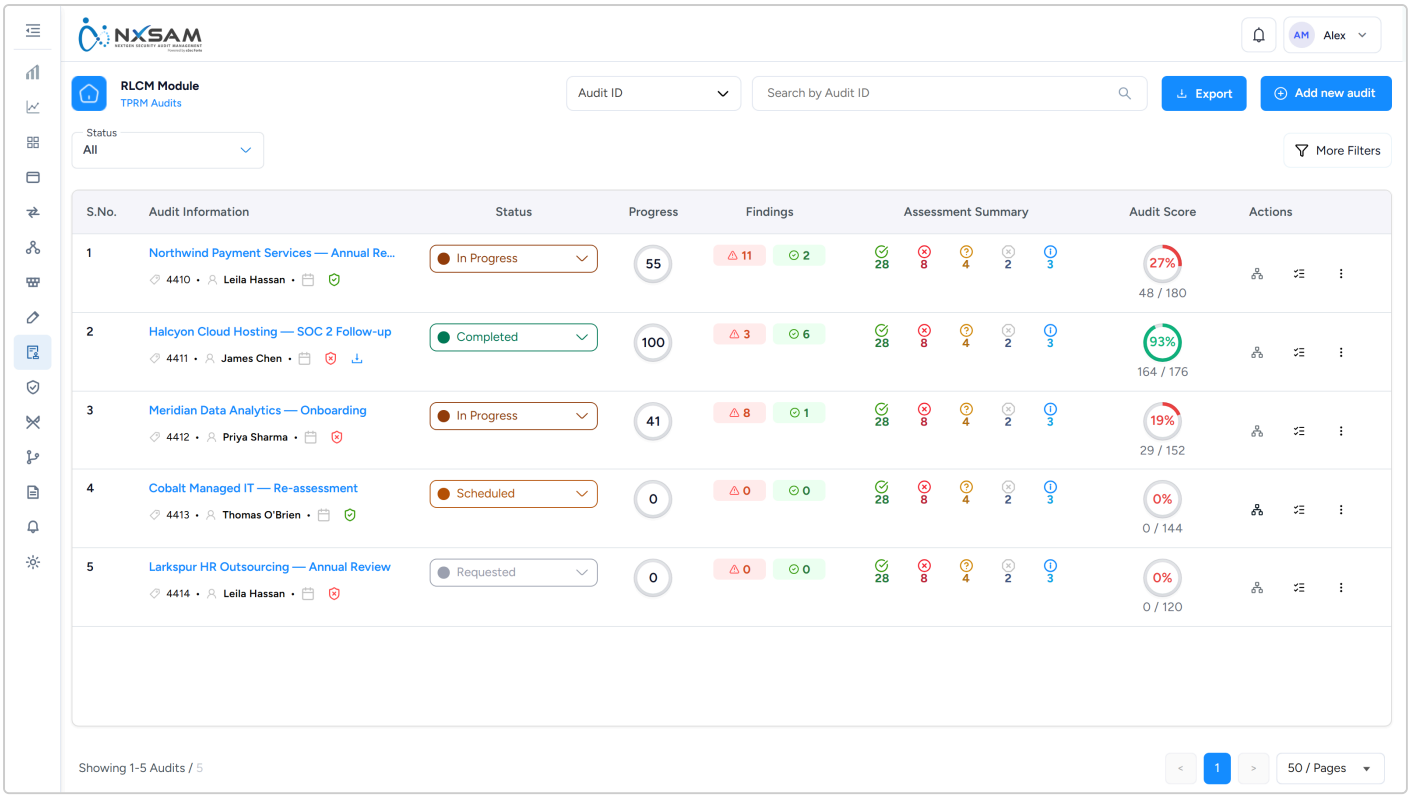


Vendor → Pre-Assessment Summary

TPRM Audits

Vendor assessments run as audits, with findings against the vendor rather than an asset.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

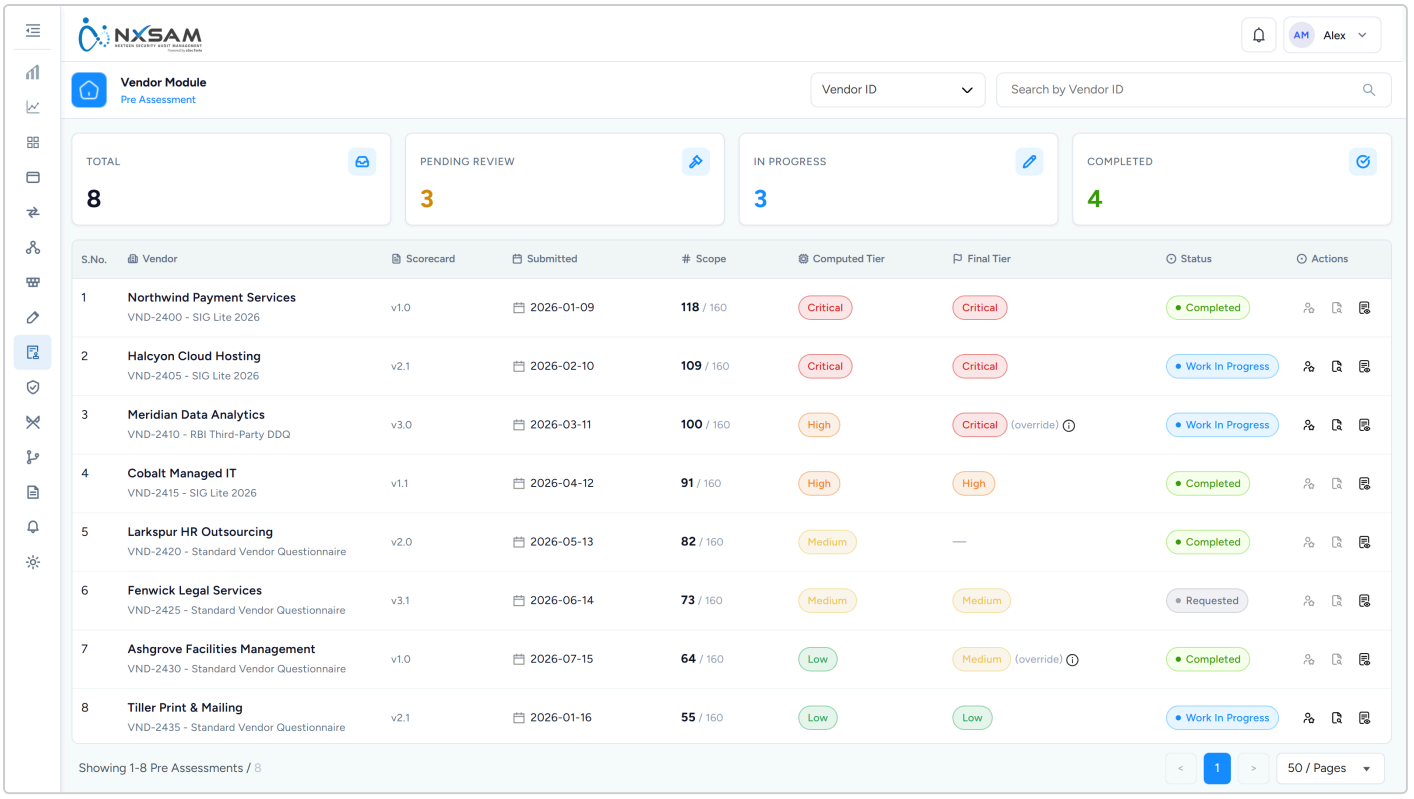


RLCM → TPRM

Vendor Pre-Assessment

A short questionnaire that decides how much scrutiny a vendor warrants before the full assessment.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

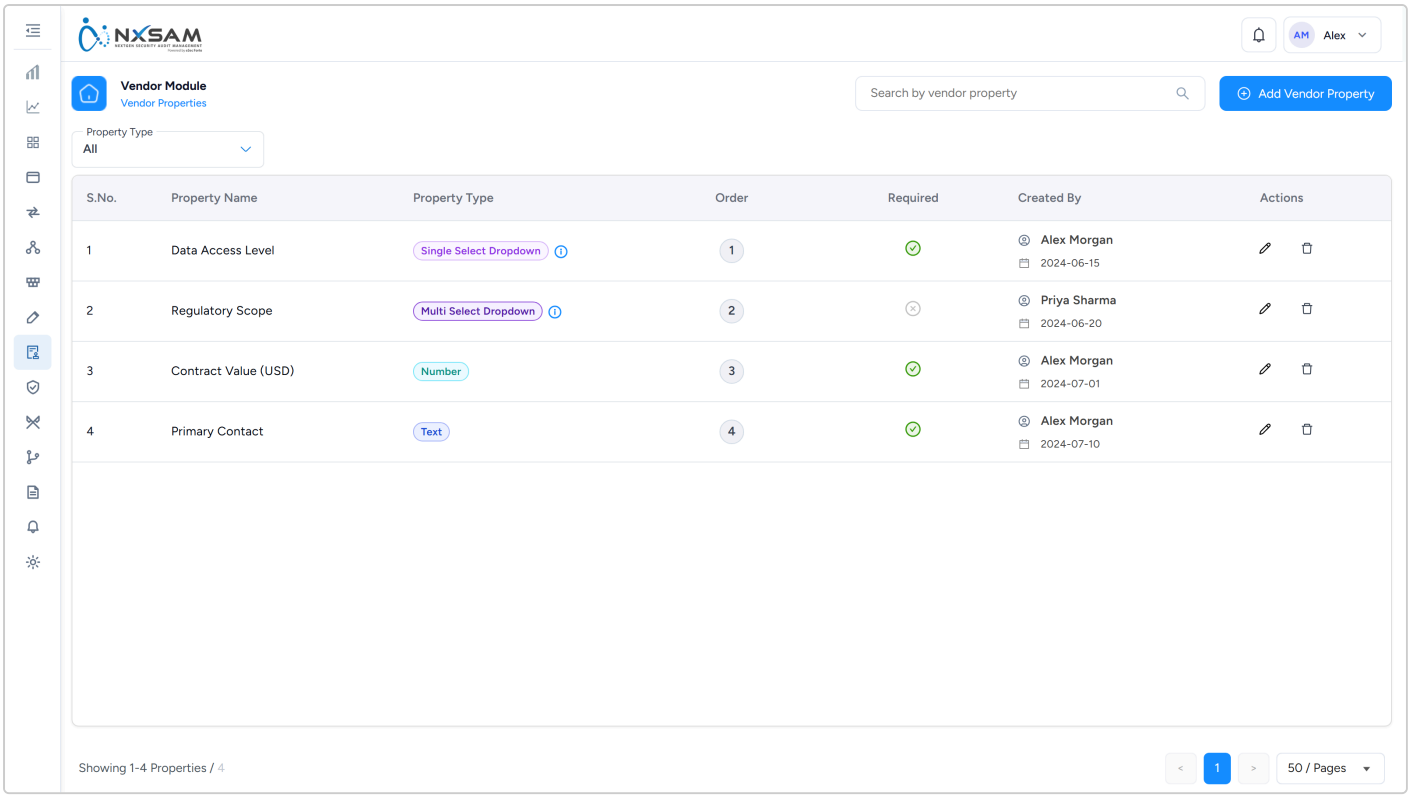


Vendor → Vendor Pre-Assessment

Vendor Properties

Custom fields recorded against a vendor.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

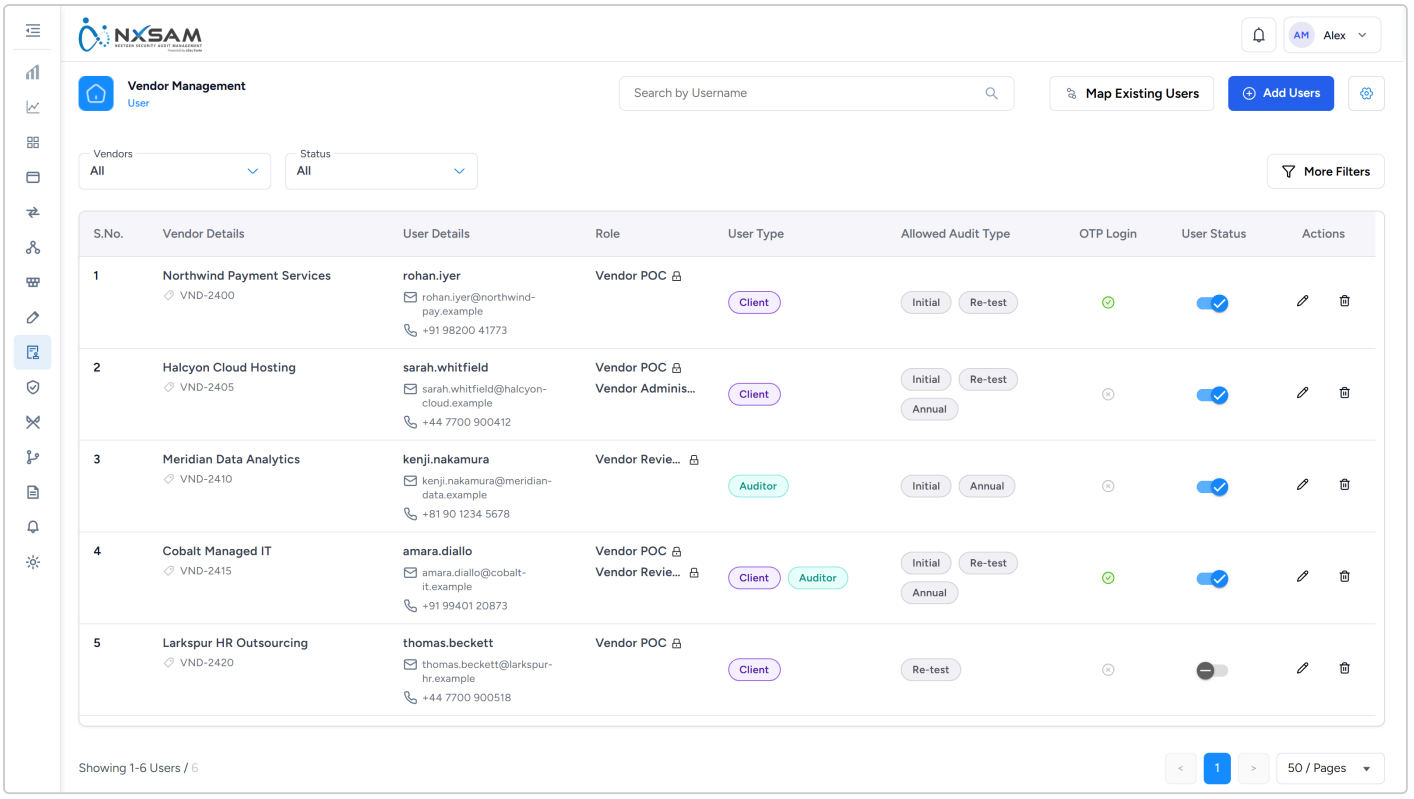


Vendor → Vendor Properties

Vendor Users

External contacts who can sign in to complete assessments. They see only what the vendor form settings allow.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



Vendor → Vendor Users

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Reference

Glossary

Terms as NxSAM uses them. Several are ordinary security words with a narrower meaning here, and those are the ones worth reading even if the term is familiar.

Assets and scope

Asset — anything that can hold a vulnerability: a web or mobile application, an API, a network host, a thick client, or a container image. Each type is a separate inventory with its own columns and its own licensed limit.

Asset property — an attribute recorded against an asset, such as criticality or whether it is internet-facing. Properties are more than description: they narrow SLA durations and feed the contextual risk score.

Bifurcation — splitting one application into separately assessed parts, so a large system can be tested module by module rather than as one unit.

Collection — a grouping of container images that comes from the scanning platform rather than from NxSAM, and is not editable here.

Scope — what an assessment covers. For applications this is the application; for compliance it is a host list, which is why compliance scope disputes are settled with an exported list of addresses.

Assessments

Audit — one assessment of one asset. It has a type, a category, a cycle, a scope, and a status of its own, separate from any finding's status.

Audit cycle — which round of a recurring programme an audit belongs to.

Confirmatory audit — a re-test created against a parent audit to verify that fixes hold. It is evidence about the original rather than an independent assessment, so the two should not be counted as two rounds of testing.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Considered — the marker deciding whether an audit contributes to aggregate figures. Normally the latest audit per asset that reached a final state. An audit that is *not* considered still shows its findings on the module screen while contributing to no dashboard or report.

Initial audit — a first assessment, as opposed to a confirmatory one.

Findings

Vulnerability (also *finding*, *issue*) — one weakness on one asset, found by one assessment.

Vulnerability master — the catalogue entry (title, description, remediation) inherited by every occurrence of that vulnerability everywhere. Editing the master changes all of them.

Posture — Policy Compliance's unit: one control checked against one host. Every check produces a posture whether it passed or failed, which is why this module's volumes dwarf the others.

Artifact — the evidence attached to a finding: the steps, description and images that let someone else reproduce it.

Instance — which occurrence, where the same control or finding applies more than once to the same asset.

Status

Validation status — whether a finding has been confirmed. Nothing is counted anywhere until this reaches *Approved*, which is also when **Discovered On** is populated.

Client status (also *current status*) — what is being done about the finding. Of its values, only two close it.

Closed type — the flag deciding whether a status stops something counting as open. It is configuration rather than a fixed rule, so a deployment can change what "closed" means.

Posture status — what a compliance check returned: pass, fail or **error**. Error means the check could not run — a scanner or credentials problem rather than a compliance result.

Sub status — the qualifier beneath a main status: which kind of acceptance, or which stage of an approval.

Time and SLA

SLA duration — how long a finding of a given severity on a given asset type may remain open. Configurable, and narrowable by asset property.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

SLA expiry — the resulting deadline. Changing an SLA duration re-derives expiry dates, which can make a batch of findings overdue with no data change at all.

Discovered On — when a finding was first observed. Blank until the finding is approved.

Last observed — the most recent sighting, which is how a finding is known still to exist.

Overdue — past SLA expiry and not closed.

Decisions

Deviation (also *risk acceptance*, *RA*) — a recorded decision not to fix something, with an approval chain and an expiry. It does **not** close the finding: the exposure is still live and still counts as open.

Exception — a status marking an agreed exception rather than a resolution. Reporting that conflates the two overstates remediation.

Auto reject end date — when a temporary acceptance lapses on its own.

Integrations and processing

Integration — a connection to a scanning tool, either pulling from its API or parsing an uploaded report.

Vulnerability key — the columns deciding whether an incoming finding is one already seen. Changing it redefines "the same finding" and splits history.

Queue — asynchronous work: imports, syncs, report generation. A screen that seems not to have updated usually has a queue entry that explains it.

Data process — how far a tool-fed audit has got through the import pipeline; the difference between "the upload finished" and "the data is ready".

Beat — a scheduled job maintaining derived data, such as recalculating SLA states as dates pass. A stopped beat produces figures wrong by a fixed interval and raises no error.

Governance

RLCM — Red Line Compliance Management: assessment of controls against frameworks, rather than of systems for weaknesses.

TPRM — Third-Party Risk Management: the same control assessment applied to suppliers. It shares screens with RLCM and differs by the audit's type.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

UCF — Unified Control Framework: the mapping that lets one control satisfy several frameworks at once, so answering it once covers each of them.

Control — a requirement being assessed, as opposed to a weakness being found.

Standard — the framework a control belongs to, such as ISO/IEC 27001 or PCI DSS.

Reporting

Considered audit filter — the switch on Report Search that reproduces either the dashboard's numbers or the module screens'. Comparing the two settles most disagreements about counts.

Design template — the layout a report renders through, separate from the template that decides its content.

Share view against share copy — sharing a template as a view keeps one definition that your edits reach; sharing a copy creates an independent template that will drift.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.