



NxSAM RLCM — Quick Guide

Quick reference guide for the RLCM 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

RLCM

- RLCM — Regulatory & Line Compliance Management
- Configuring risk in RLCM
- RLCM: every screen, column and action
- RLCM: find the right screen

Reference

- Glossary

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

RLCM

RLCM — Regulatory & Line Compliance Management

RLCM is where compliance work lives. Where the security modules ask *what is wrong with our systems*, RLCM asks *can we demonstrate that we meet our obligations* — to a regulator, a standard, or an internal policy.

The building blocks

	What it is
Control	A single thing you must do — "access is reviewed quarterly". The atom of compliance.
Template	A reusable set of controls, typically representing a standard or a regulation.
Audit	One assessment against a template, at a point in time.
Assessment	The act of going through an audit's controls and recording how you fare on each.
Finding	A control that is not adequately met.
Risk register	Risks arising from those gaps, tracked over time.
Framework	An external standard or regulation broken into its own requirements, each mapped to the controls that satisfy it.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

The relationship: a **template** defines controls; an **audit** applies a template to a part of your organisation; an **assessment** records the answers; **findings** capture the gaps; the **risk register** tracks what those gaps mean.

Why templates matter

Most organisations answer to several frameworks at once, and those frameworks overlap heavily. Templates let a control be defined once and reused, so evidence gathered for one obligation can serve another.

Master controls are maintained centrally, and templates draw on them. Improving a control definition improves every template using it.

Frameworks: answering many standards with one set of controls

Most organisations are held to several standards at once, and the standards overlap heavily — access review, incident response and change control appear in nearly all of them under different numbering. Assessing each standard separately means answering the same question several times and keeping several sets of evidence.

The **Common Control Framework** screens exist to avoid that. A framework is loaded as its own list of **requirements** — the clauses of the standard, with the standard's own reference codes — and each requirement is **mapped** to the controls in your library that satisfy it. You then assess the controls once, and every framework mapped to them reads the result.

Three things follow, and each has a screen:

- **Frameworks** — which standards you hold yourself to, their version, who issued them, how many requirements each has, and what proportion of those requirements are mapped to at least one control. That proportion is the framework's **Compliance %**.
- **Requirements** — the clauses of one framework, by section, each showing how many controls it is mapped to. A requirement mapped to nothing is a **gap**: a clause you are bound by and have no control for.
- **Control map** — for one requirement, the controls already mapped and the ones not yet mapped, with **Map** and **Unmap** between them.

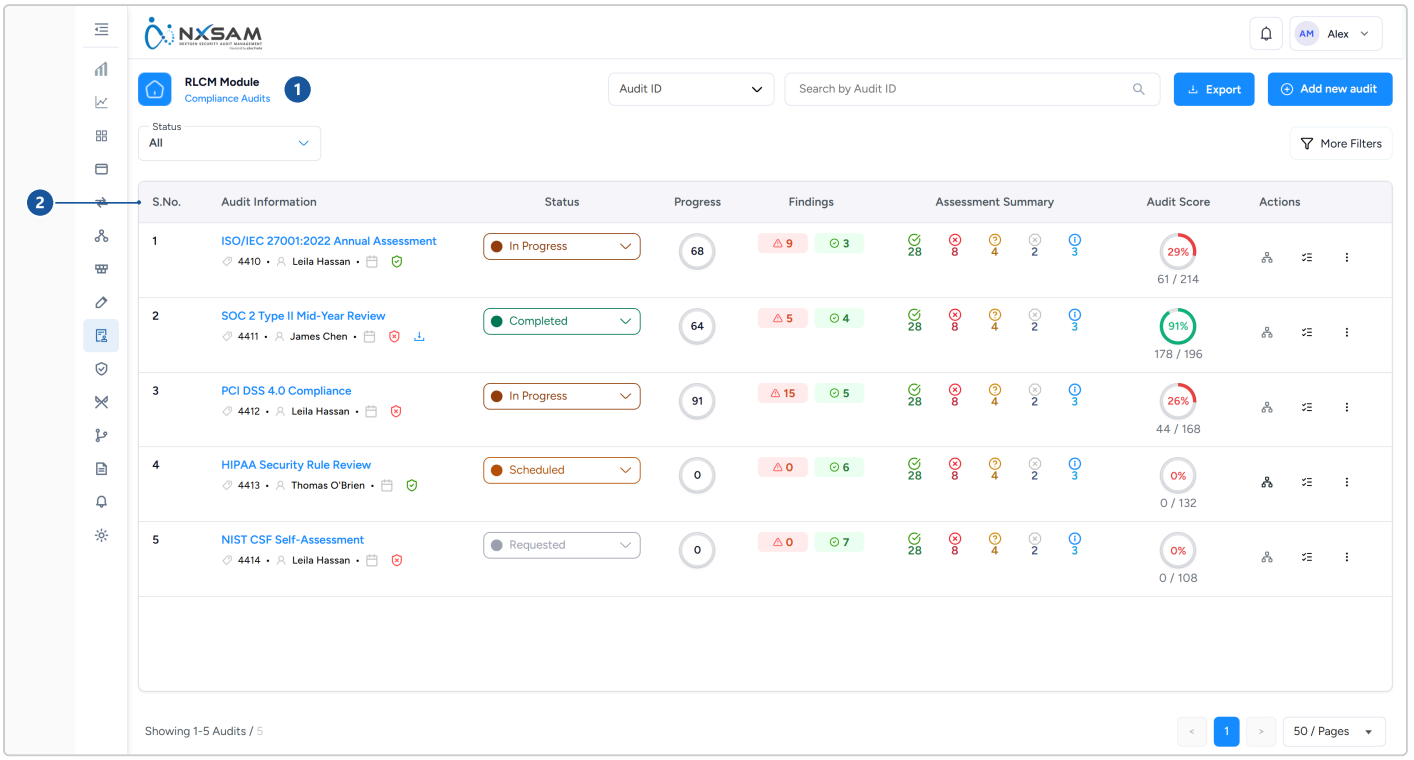
Requirements can be typed in one at a time or uploaded as a CSV — the upload screen offers a sample file in the exact layout it accepts, and keeps a log of every upload with what it accepted and rejected.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Compliance % measures mapping, not passing

A framework at 100 % has a control for every requirement. It says nothing about whether those controls are met — that is what the assessments say. A framework can be fully mapped and badly failed, or thinly mapped and passing everything it covers. Read the two figures together.

How an audit runs



Compliance audits against a framework.

1 where you are · 2 audit and framework

1. **Create the audit** from a template, scoped to whatever you are assessing.
2. **Assess each control** — met, not met, partially met, or not applicable — with evidence and commentary.
3. **Raise findings** where controls are not adequately met.
4. **Track remediation** against those findings.
5. **Close the audit** when the assessment is complete.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Audits recur. Last year's audit stays as the record of that point in time; this year's is a new audit against the same template, which is what makes trend and improvement visible.

Findings here are not vulnerabilities

An RLCM finding is a **control gap** — something you cannot yet demonstrate. It is not a technical weakness in a system, and it is tracked separately from the security modules.

The two are related in practice: a control requiring timely patching is demonstrated by the SLA performance the security modules record. But they are separate objects with separate lifecycles, and conflating them causes confusion in reporting.

Risk register

Where a control gap represents ongoing exposure, it is recorded as a risk: rated, owned, and tracked until treated. This is the bridge between "we do not meet this control" and "here is what that means for the business and who is dealing with it".

Getting started

If you are new to RLCM, the useful order is: look at an existing **template** to see how controls are structured, then open a completed **audit** to see how those controls were assessed and what findings resulted. The structure is much clearer from a worked example than from the configuration screens.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Configuring risk in RLCM

RLCM scores compliance risk rather than technical severity, so it has its own scoring model — separate from the CVSS-derived severity used elsewhere in NxSAM. These screens define that model.

Why it is separate

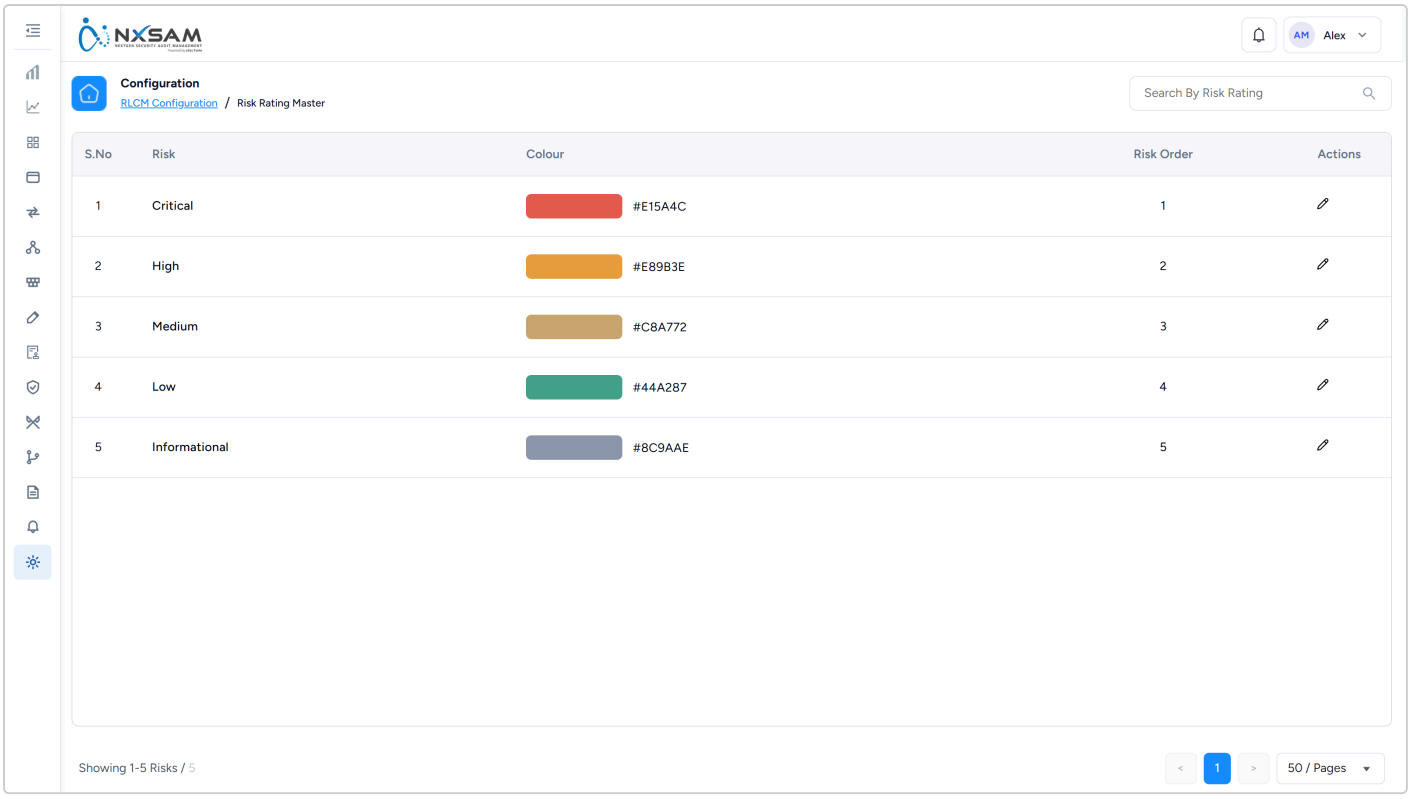
A missing control is not a vulnerability. It has no CVSS score, no exploit, and often no technical impact at all — its significance is regulatory. Scoring it on the same scale as a remote code execution would be meaningless in both directions.

So RLCM keeps its own rating scale, its own status values, and its own weighting.

The pieces

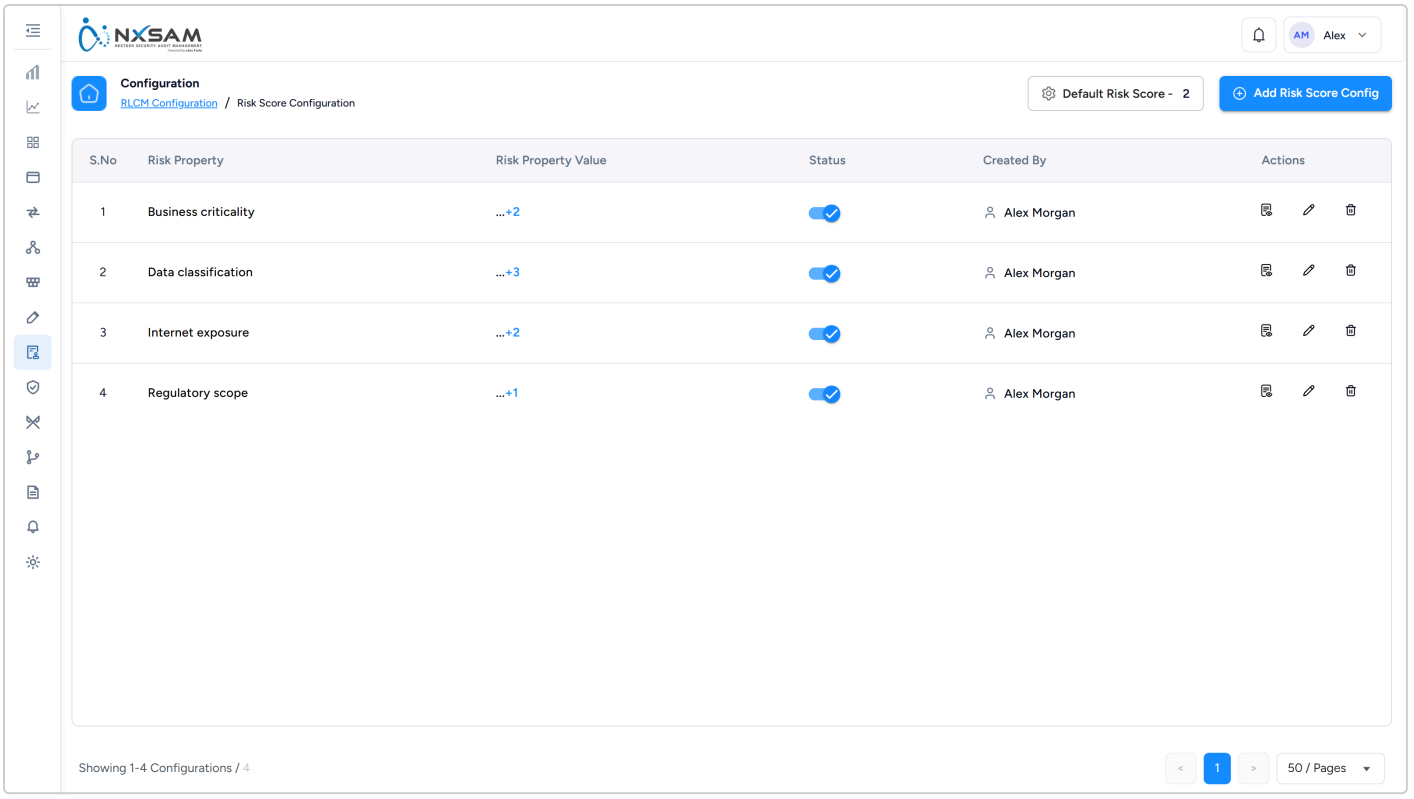
Screen	What it sets
Risk rating master	The scale itself — the levels a compliance risk can be rated at
Risk master status	The states a risk moves through as it is treated
Risk configuration	How ratings are assigned to findings
Risk score configuration	How individual ratings combine into an overall score
Risk property master	Additional attributes to record against a risk
Weight configuration	The relative weight of controls, sections or domains

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



Configurations → RLCM Configuration → Risk Rating Master — the scale a compliance risk is rated on

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



RLCM → Risk Score Configuration — how individual ratings combine into one score

Weighting is what makes a score meaningful

Without weights, every control counts equally, and an audit is scored on the proportion of controls passed. That reads well and says little: failing a core access-control requirement counts the same as failing a documentation one.

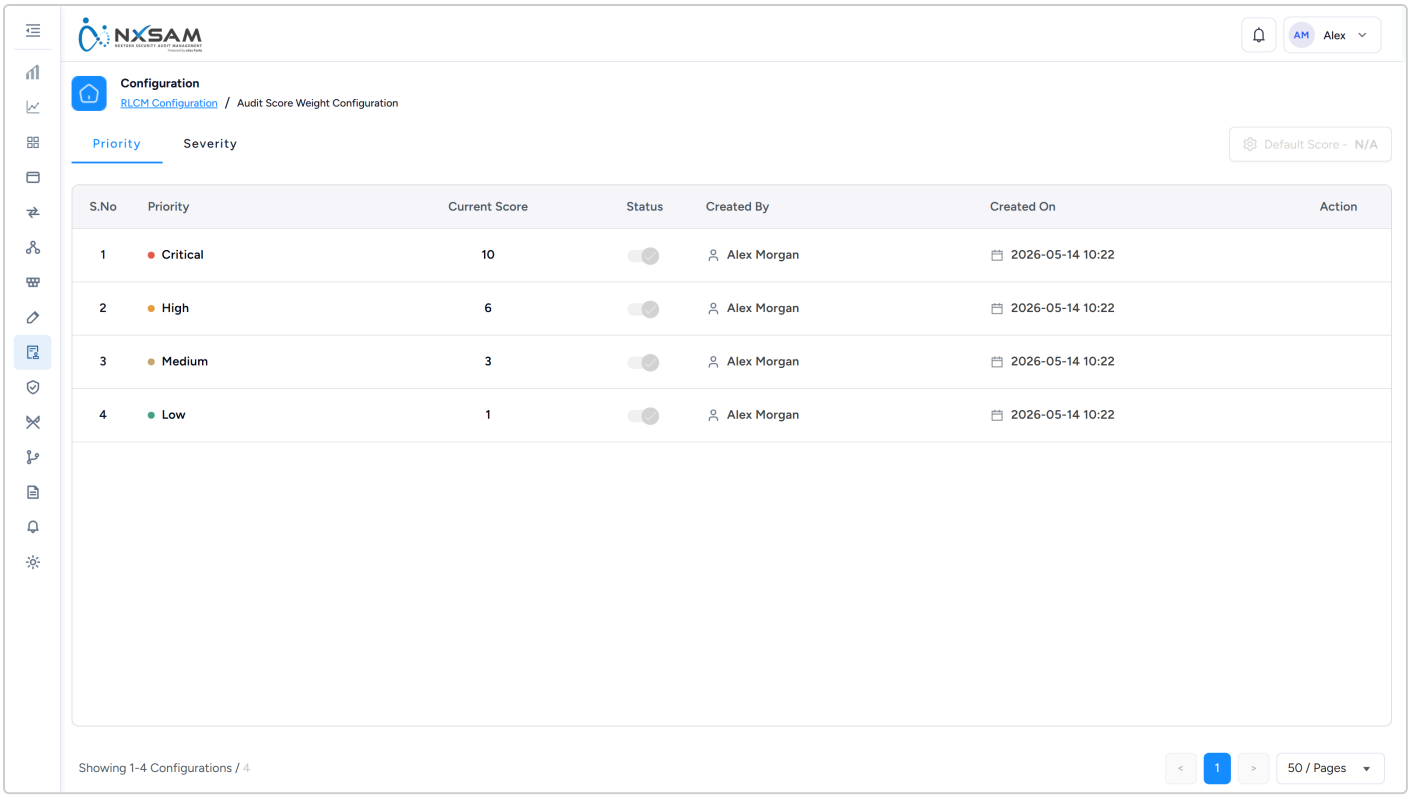
Weighting lets a framework's own emphasis be reflected — so the score moves most when the things that matter most are failing. It is the difference between a score that tracks compliance posture and one that tracks paperwork volume.

Re-weighting changes historical scores

Scores are computed from the current configuration. Change the weights and previously completed audits will score differently when their score is next displayed.

If a trend line moves without any audit activity, a weighting change is the first thing to check.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

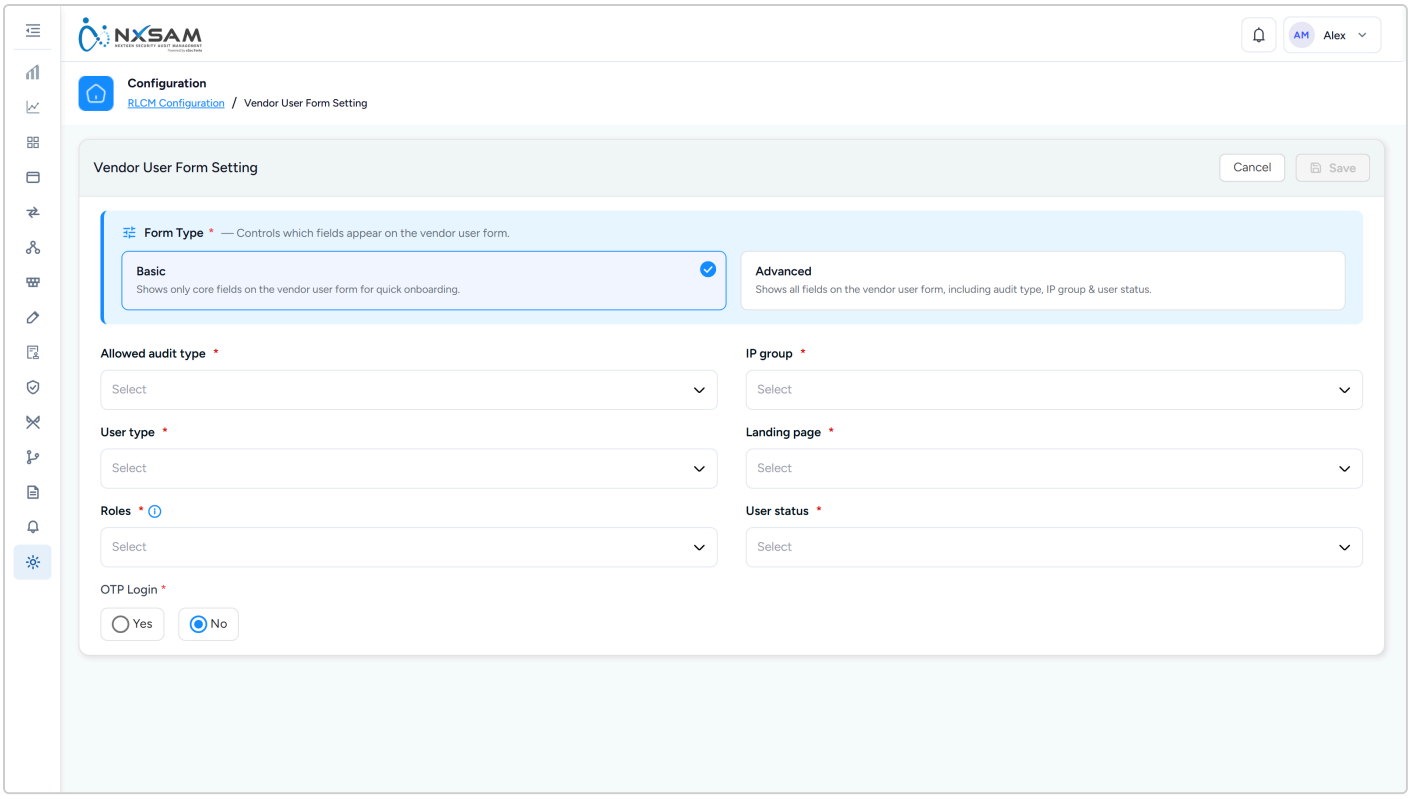


RLCM → Weight Configuration — the relative weight of each domain and control

Vendor user form setting

Controls what an external vendor user sees and can fill in when responding to a TPRM assessment. Vendor users are outside your organisation, so this is a disclosure decision as much as a usability one — anything exposed here is visible to a third party.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



Configurations → RLCM Configuration → Vendor User Form Setting — what an external vendor user is shown

Recurring assessments

Schedules assessments to be raised automatically — annually, half-yearly or quarterly — against a template and category, for a vendor or for the organisation itself. When the date arrives the audit is created with its default POC, reviewer and auditor already assigned, and appears in the audit list like any other.

This is what turns "we assess our critical suppliers every year" from an intention into something that happens without anyone remembering. **Pending First Cycle** is how you tell the difference between the two: a configuration that is active but has never run has not proved anything yet.

The panel is titled *Purging Configurations*

Nothing on this screen deletes data. Every control on it creates or schedules an assessment; the heading is misleading rather than a hidden behaviour.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

RLCM: every screen, column and action

The module has a three-role review model that nothing else in the product uses, and most of its screens are shaped around it.

POC, Reviewer, Auditor — the three inputs

A control is answered three times, by three roles, and all three answers are kept:

Role	Provides
POC	The point of contact for the control — the person who owns the process being assessed
Reviewer	An internal check of that answer
Auditor	The independent conclusion

The control screens carry a column per role: `POC Input`, `Rev Input`, `Auditor Input`, and a **Control status details** view showing `POC`, `REVIEWER`, `AUDITOR` side by side.

Disagreement between the three is the point, not a fault

A control where the POC says compliant and the auditor says not is exactly what the model is for. The three columns preserve that disagreement rather than overwriting it, which is what makes the assessment defensible later.

`NA` on the control-management table marks a control the POC has declared not applicable — which the reviewer and auditor can still disagree with.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Assessments

Screen	Columns
Assessment list	`Audit ID`, `Audit Details`, `Status`, `Last Status Update`, `Control Status`
Assessment detail	`Sections`, `Control Details`, `POC response`, `Control Status`
Assessment detail (v2)	`Sections`, `Control Details`, `Current Level`, `User Input`, and the **AI Evidence Analysis Status** with its **AI Score** where AI evidence analysis is switched on
Audited controls	`Section`, `Control`, `Current Level`, `POC Input`, `Rev Input`, `Auditor Input`
Control management	`Sections`, `Control Details`, `Status`, `POC`, `Reviewer`, `Auditor`, `NA`

Current Level is the maturity or compliance level currently claimed for the control, as distinct from pass/fail — RLCM assesses degree rather than a binary.

Row action: **View Audit Finding**.

Control Details carries what used to be two columns — the control's reference ID and its name — in one cell, reference first. Sorting and searching still work on either part.

AI evidence analysis

Where an administrator has enabled it, the assessment detail carries two extra cells per control: **AI Evidence Analysis Status** and **AI Score**. The platform reads the evidence uploaded against a control and suggests a compliance finding with a confidence score out of 100. The status is *pending* until that run completes, and shows *failed* — with the reason on hover — if the evidence could not be read.

Clicking the status opens the **AI Evaluation**: the **AI Confidence Score**, an **AI Summary** of what the evidence shows, and the **AI Finding** it suggests. The auditor's own form shows the same panel beside the answer, so the suggestion is read alongside the evidence rather than instead of it.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

> ⚠ **The AI evaluation is a suggestion to the auditor, not an answer**
>
> Nothing here records a result. The auditor's input is still the auditor's — the evaluation is there to make reading a large evidence pack faster, and a confidence score is a statement about how clearly the evidence supports the finding, not about whether the control is met. An auditor who disagrees with it should simply answer differently; the disagreement is preserved like every other disagreement in this module.
>
> Evidence analysis runs on a schedule and within a per-audit spending cap that the administrator sets. A control that stays *pending* for a long time has usually run into that cap — see System: AI configuration.

Save response against Submit response

The assessment screen offers both, and they are not the same action:

Button	Effect
Save response	Records the answer and leaves the control where it is
Submit response	Records it *and* advances the control to the next person
Reject	Sends the control back for rework, with the reason

Saving is how a long questionnaire is worked over several sittings. Nothing moves, nobody is notified, and the answer is not visible as complete.

> ⚠ **A saved response has not been submitted**
>
> This is the most common reason an assessment appears stalled with every control apparently answered. The answers exist; they were never submitted, so the control is still pending on the person who wrote them.
>
> **Pending On** is the column that settles it — it still names the author rather than the next reviewer.

Where a screen offers a bulk submit, it applies the same advance to every selected control at once. Use it after working through a section; it does not save unsaved edits for you.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Audits

Column	What it holds
Audit Information	The assessment
Status	Where it is
Progress	How much has been answered
Findings	How many failures it produced
Assessment Summary	The rolled-up result
Audit Score	The weighted score

Progress and Audit Score answer different questions. Progress is how much of the work is done; score is how well it went. An assessment at 40% progress has a score computed from 40% of the controls, and it will move as the rest are answered — which is why an in-flight score should not be reported.

Findings and the risk register

Both share a shape:

Column	What it holds
Finding ID / **Audit & Finding Info**	Identity and provenance
Control Details	Which control failed
Risk & Observations	What the failure means and what was observed
Status	Where the finding has got to

Actions: **Add Risk**, **Map Existing Risk**, **Status History**, **View Audit Finding History**.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Add Risk and Map Existing Risk are the module's central decision

A control failure is not itself a risk — it becomes one when someone decides it matters. **Add Risk** creates a new entry in the register. **Map Existing Risk** attaches the failure to a risk already recorded.

Mapping is nearly always the right answer when the same weakness has been found before: one risk with six contributing findings is a register an executive can read, where six separate risks saying the same thing is not.

The control library

Screen	Columns
Controls	`Control Details`, `Answer & Comments`, `Process Groups / Standards`, `Priority`
Master library	`Control Details`, `Process Groups / Standards`, `Justification & Evidence`
Library map	`Control Details`, `Process Groups / Standards`
Assessed controls	`Name`, `Type`, `No. of Controls Mapped`, `Passed Controls`, `Failed Controls`, `Failed Control Severity Wise`

Justification & Evidence on the master library is what makes a control reusable. The evidence recorded once against the master answers the same control wherever it appears — which is the whole economics of the unified control framework.

Standards, sections and templates

Screen	Columns
Standards	`Standard Name`, `Created By`

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Screen	Columns
Sections	`Reference ID`, `Section Name`, `Section Description`, `Total Controls`, `Total Sub Sections`, `Sequence`
Section controls	`Control Details`, `Answer & Comments`, `Process Groups / Standards`, `Skip Rule`, `Sequence`
Templates	`Template Details`, `Category Name`, `Total Controls`, `Total Sections`, `Organization`, `Created By`
Audit categories	`Category Name`, `Template Count`, `Audit Type`, `Created By`
Domains	`Domain Name`, `Created By`
Process groups	`Process Name`, `Created By`
UCF	`UCF`, `Control Count`, `Created By`

Template actions: **View Template Details**, **Edit Template Details**, **Clone Template**, **Export Template**, **Delete Template**.

Clone Template is how a standard gets tailored without losing the original. An organisation adapting ISO 27001 to its own scope clones the template and edits the copy; editing the original changes every assessment that uses it.

Sequence on sections and controls sets reading order in the assessment and the report. It is not cosmetic — an assessment presented out of order is materially harder to review.

Template Details and **Control Details** each fold a reference ID and a name into one cell. **Answer & Comments** on a section's controls shows what kind of answer the control demands and whether a comment is mandatory; **Process Groups / Standards** shows what the control is tagged with, collapsing to a count when there are many. **Skip Rule** marks a control that a skip rule can hide from an assessment — either because the rule is defined on this control, or because this control is one the rule hides — so a control that is "missing" from an assessment can be checked here before anyone assumes it was deleted.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Common control framework (CCF)

Three screens, reached in sequence: a framework, its requirements, and the control map for one requirement. Their purpose is explained in the overview; this is what is on them.

Frameworks

Column	What it holds
Framework	The standard's name and your reference ID for it
Ver.	Which edition or year
Type	The kind of standard
Authority	Who issues it — ISO, NIST, a regulator
Req.	How many requirements it has
Compliance %	The proportion of requirements mapped to at least one control
Status	Active or inactive
Actions	**View** the requirements, **Edit**, **Delete**

Add Framework asks for the framework name, a reference ID, the authority, type, version, a description, an **Initial status**, and two periods: the **Validity period** in months (12 by default) and the **Warning period** in days before expiry (30 by default). The reference ID accepts letters, numbers and `. _ -` only.

Frameworks marked as a **System Framework** ship with the product and cannot be edited or deleted; their requirements are likewise marked **System Requirement**. Everything you add yourself can be.

Requirements

One framework's clauses. The header cards give the framework's shape at a glance: **Total requirements**, **Mapped to controls**, **Unmapped (gaps)** and **Avg controls / req.**

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Column	What it holds
Ref. Code	The standard's own numbering for the clause
Section	Which part of the standard it sits in
Requirement	The clause, with its full description on the detail
Mapped Controls	How many controls satisfy it
Coverage	Whether it is mapped at all
Actions	Open the **control map**, **Edit**, **Delete**

Add Requirement takes the reference ID (the standard's own code, such as a clause number), a requirement name, its section, a group, and the description. **Upload CSV** loads many at once — **Download Sample** gives the accepted layout, and the upload keeps **Requirement Upload Logs** recording what each run accepted and rejected. **Export Requirements** downloads the list.

Unmapped (gaps) is the number to work down. Every requirement in it is a clause you are held to and have no control for. It is also the number an external assessor will ask about first, because it is the one that cannot be argued.

Control map

Two lists for one requirement: **Mapped Controls** and **Unmapped Controls**, with **Map** and **Unmap** to move a control between them and **Select All** for bulk moves. The unmapped list can be filtered by the control's priority and domain, so a requirement about access control can be mapped from the access-control controls without scrolling the whole library.

Mapping is reversible and does not touch the control or any assessment of it. What it changes is the framework's **Compliance %** and the requirement's **Coverage**, both of which update as soon as the map is saved.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Risk configuration

Screen	Columns
Risk master	`Risk Details`, `Status`, `Likelihood`, `Impact`, `Risk Level`, `Risk Score`, `Created By`
Risk levels	`Risk`, `Min Risk Score`, `Max Risk Score`, `Created By`
Risk rules	`Risk`, `Priority`, `Audit Property`, `Status`, `Created By`
Risk score config	`Risk Property`, `Risk Property Value`, `Status`, `Created By`
Risk properties	`Property Name`, `Property Type`, `Order`, `Required`, `Created By`
Risk rating master	`Risk`, `Colour`, `Risk Order`
Risk master status	`Risk Master Status`, `Colour`, `Status Order`, `Comment Required`, `Evidence Required`, `Closed Type`
Score weighting	`level`, `Current Score`, `Status`, `Created By`, `Created On`

Likelihood × Impact produces Risk Score, and Risk Levels turn that score into a band. Changing the band boundaries re-rates every existing risk immediately, with no assessment activity — the same trap as the CVSS mapping elsewhere in the product.

> ⚠ **Evidence Required is enforced, and is the one that blocks people**
>
> A risk status flagged **Evidence Required** cannot be selected without an attachment. A user reporting that a status "does nothing" when clicked is usually hitting this, because the requirement is not stated until the save is attempted.
>
> **Comment Required** behaves the same way, and **Closed Type** decides which statuses stop a risk counting as open.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

The configuration viewers show the rules as they will evaluate: `Audit Property`, `Condition`, `Value` for risk rules, and `Value`, `Risk Score` for scoring.

History and evidence

Screen	Columns
Risk history	`Auditor`, `Update On`, `Status`
Risk master status history	`Auditor`, `Status`, `Comments and Attachments`
Closure document	`Auditor`, `Status`, `Comments and Attachments`
Finding summary	`Status`, `Count`

Comments and Attachments is the audit trail an assessor is judged on. A risk closed with no attachment has no evidence that it was closed for a reason, and that is precisely what an external auditor samples.

Reporting from an assessment

Download Xls Report exports the assessment as a spreadsheet — the form compliance teams work in, because they annotate it and send it back to control owners.

Request New PDF queues a fresh PDF. It is a request rather than a download because the document is rendered in the background: the existing PDF stays available while the new one builds, and a report that "has not updated" is usually one whose regeneration has not finished.

Recurring assessments

`Configuration`, `Client`, `Default Assignees (POC, Reviewer, Auditor)`, `Frequency`, `Starts From`, `Next Audit`, `Status`, and a history of `Raised On`, `Audit`, `Raise Result`, `Audit Status`.

Each row is a standing instruction to **raise an assessment automatically** on a frequency — annually, half-yearly or quarterly — against a chosen template and category, for a vendor or for the organisation itself. When the date arrives the audit is created with the default POC, reviewer and auditor already assigned, and appears in the audit list like any other.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

The four figures across the top answer whether the schedule is actually working:

Figure	What it tells you
Active Configurations	How many schedules are switched on, out of the total defined
Next Scheduled Audit	The date and configuration that will fire next
Last Auto-Created Audit	The most recent audit this screen produced
Pending First Cycle	Active configurations that have never yet run — the ones worth checking
Vendors Configured	How many of the vendors you can see have a schedule at all

Raise Result in the history is the one to read after a date passes: a configuration can be active, reach its date, and still fail to raise — a deleted template or an assignee who has left will do it — and nothing else on the screen shows that.

> **The panel is titled *Purging Configurations***
>
> It does not purge anything. Nothing on this screen deletes data — every control on it creates or schedules an assessment. The heading is misleading rather than a hidden behaviour, but it is alarming enough to be worth saying plainly.

Control similarity

`Control Name`, `Broad Match`, `Precision Match`, with a sync state showing when the index was last refreshed.

Compares a new questionnaire against controls already assessed. **Broad Match** catches controls covering the same ground in different words; **Precision Match** is a close textual correspondence. A high broad match with a low precision match usually means the same requirement worded for a different framework — reusable evidence, different phrasing.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

The **Needs sync** state means the index has not been rebuilt since controls changed, so matches will be stale.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

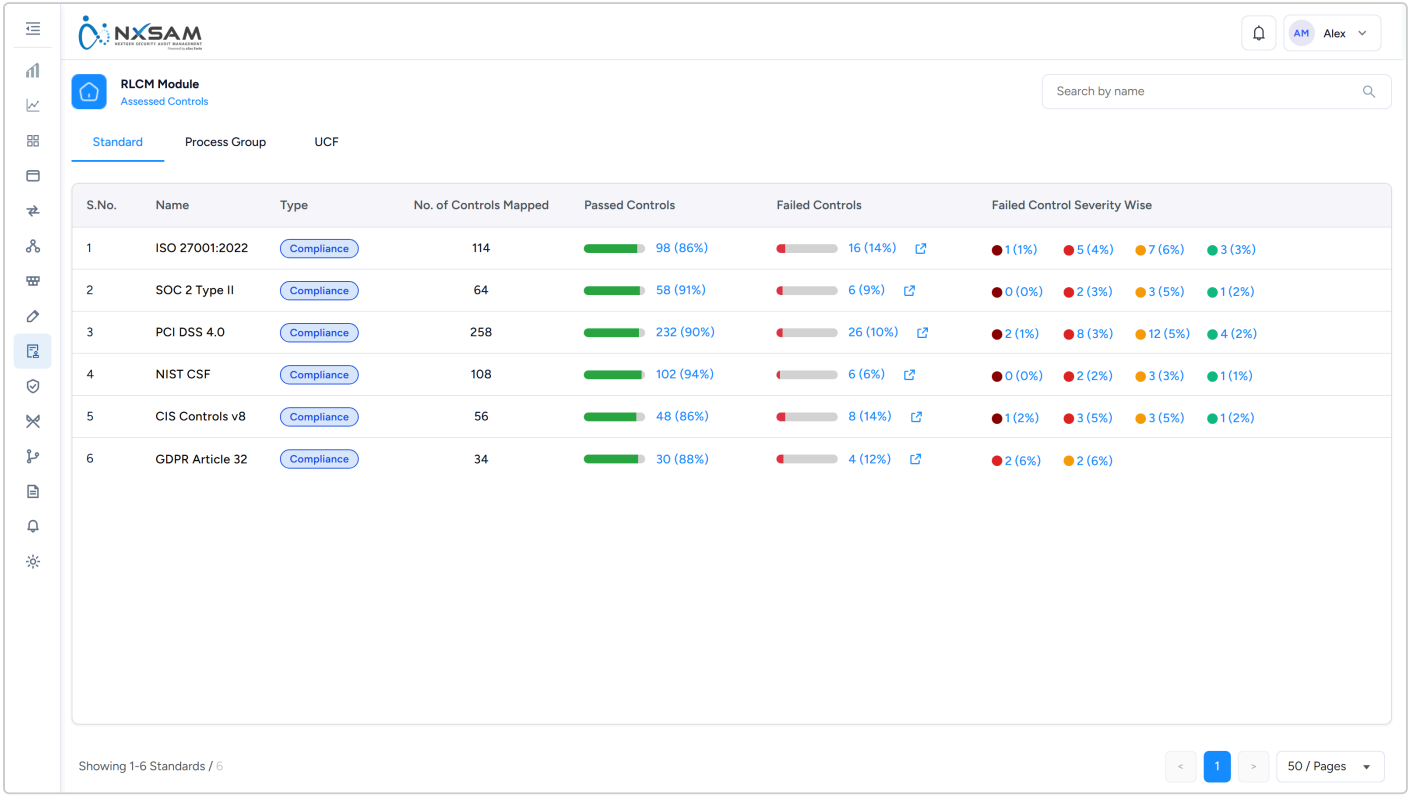
RLCM: find the right screen

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.

Assessed Controls

Controls that have been evaluated, with the evidence and the conclusion reached.

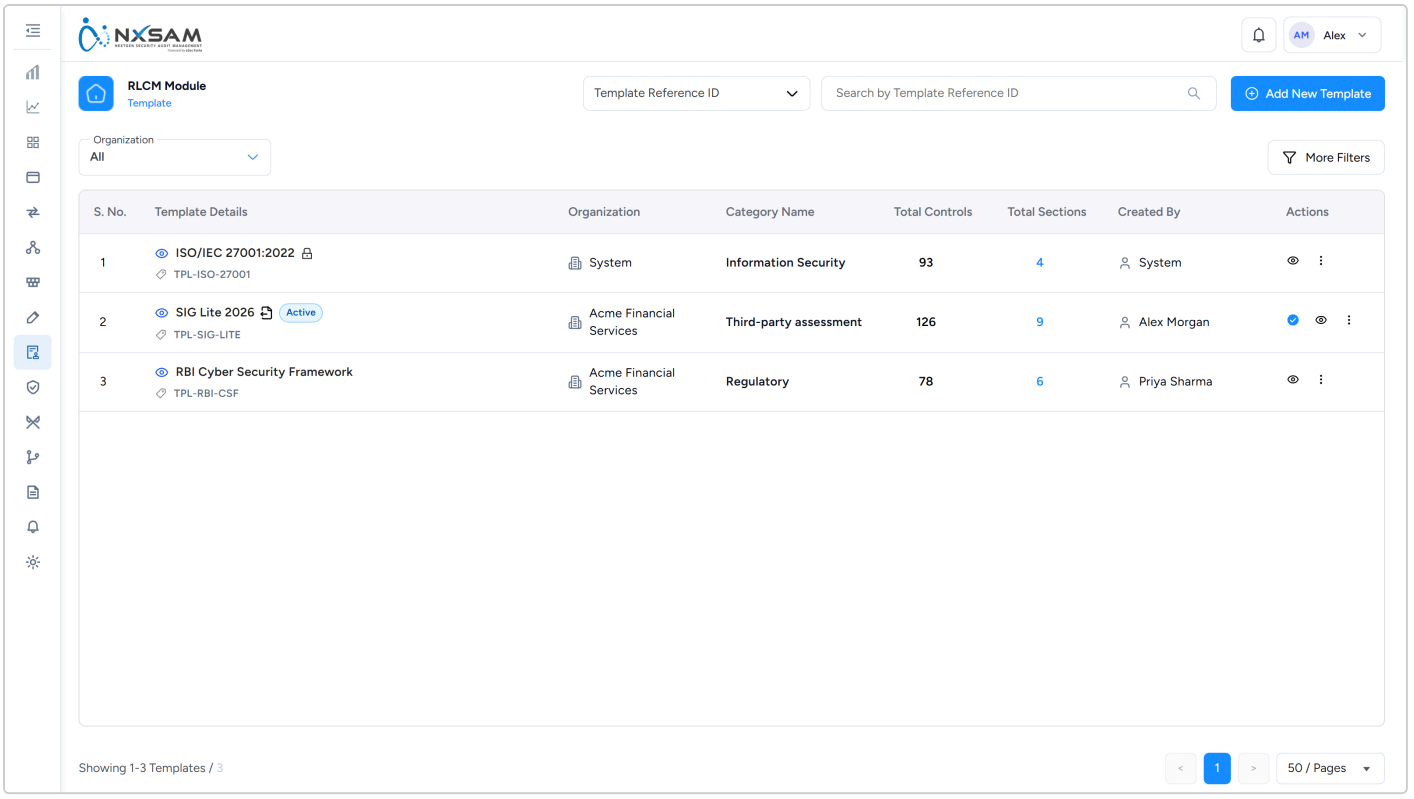


RLCM → Assessed Control

Assessment Templates

A reusable set of controls and questions, so two assessments of the same kind cover the same ground.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

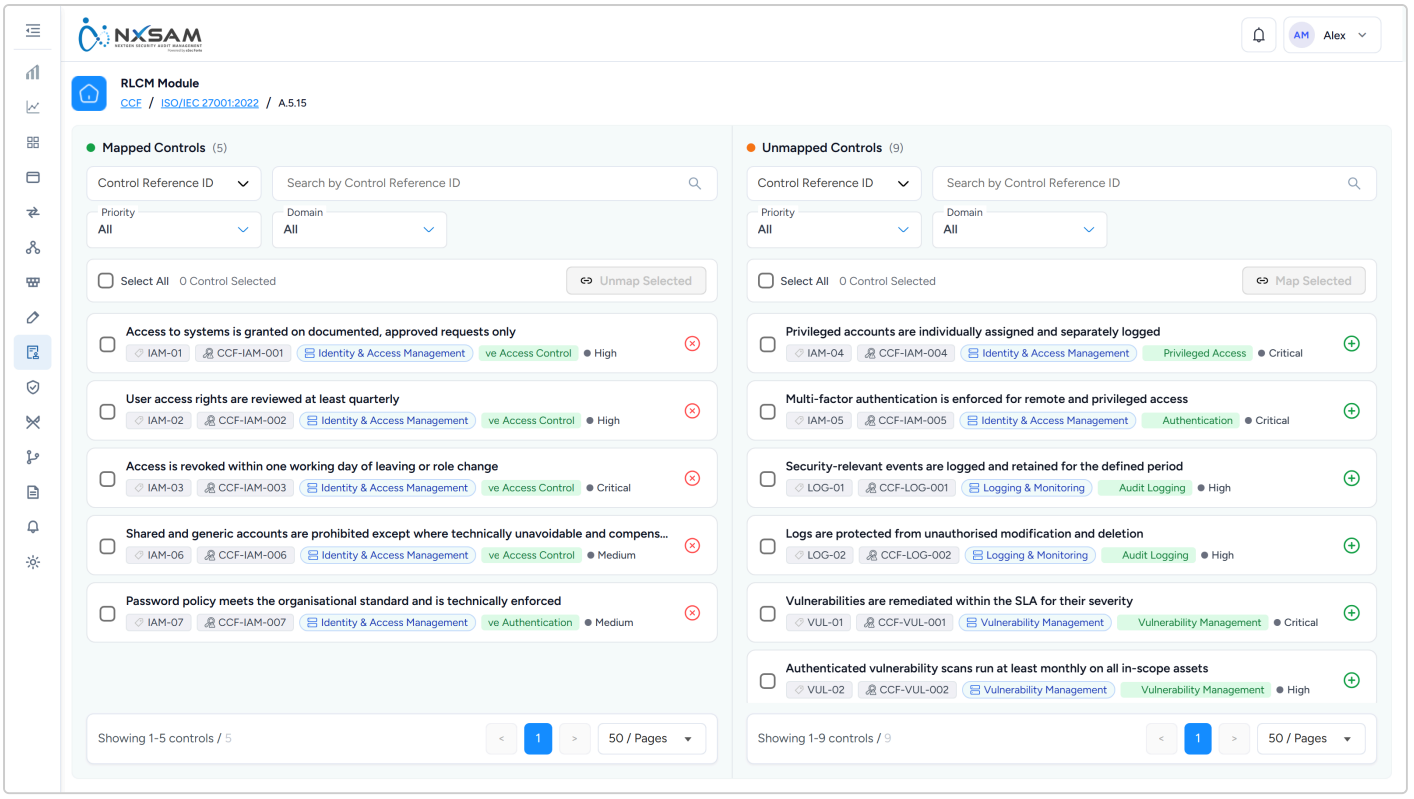


RLCM → Assessment Templates

CCF Control Map

For one requirement, the controls already mapped and the ones not yet mapped, with Map and Unmap between them. Mapping changes coverage; it touches no assessment.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

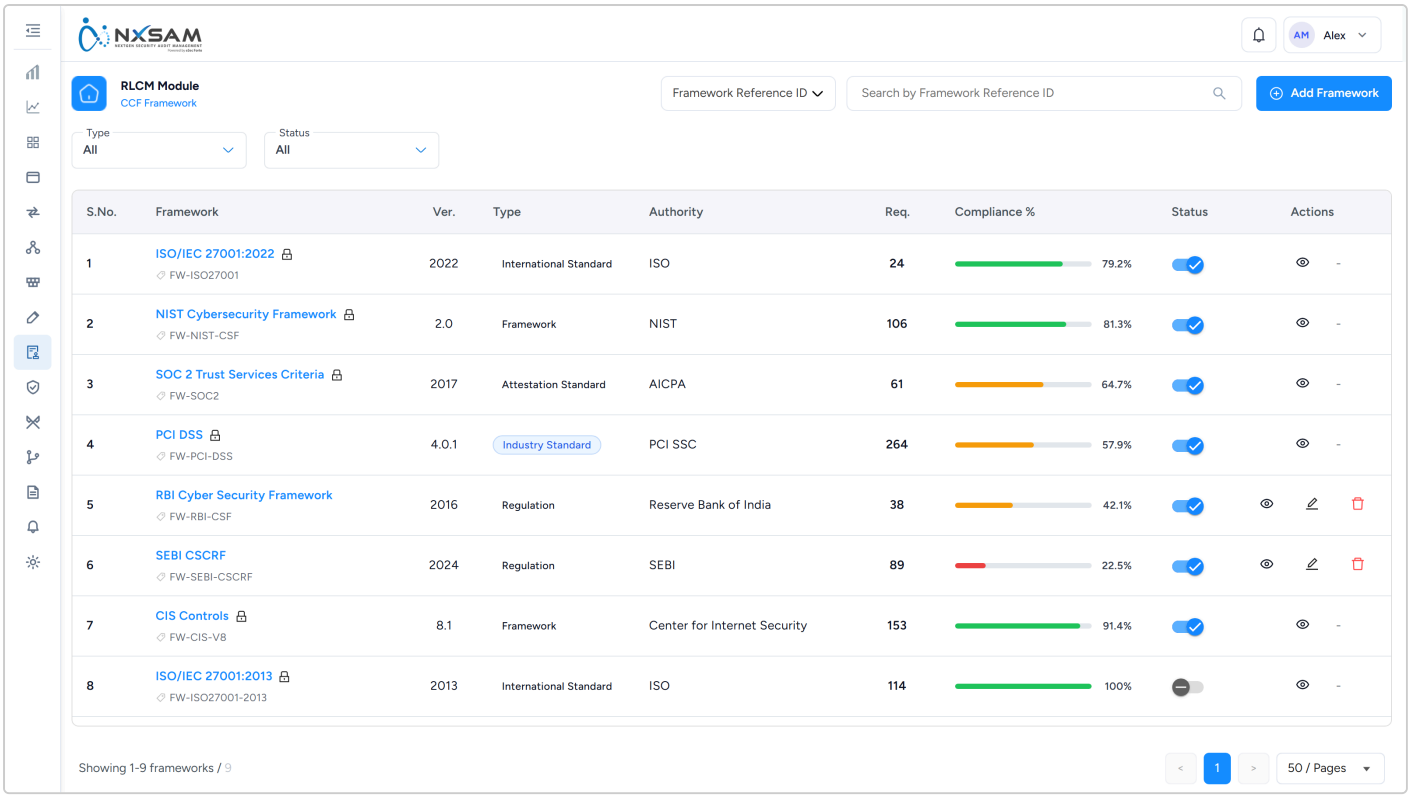


RLCM → CCF → Requirement → CCF Control Map

CCF Frameworks

The external standards you hold yourself to, each with its requirement count and the proportion of requirements mapped to at least one control. Compliance % here measures mapping, not passing.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

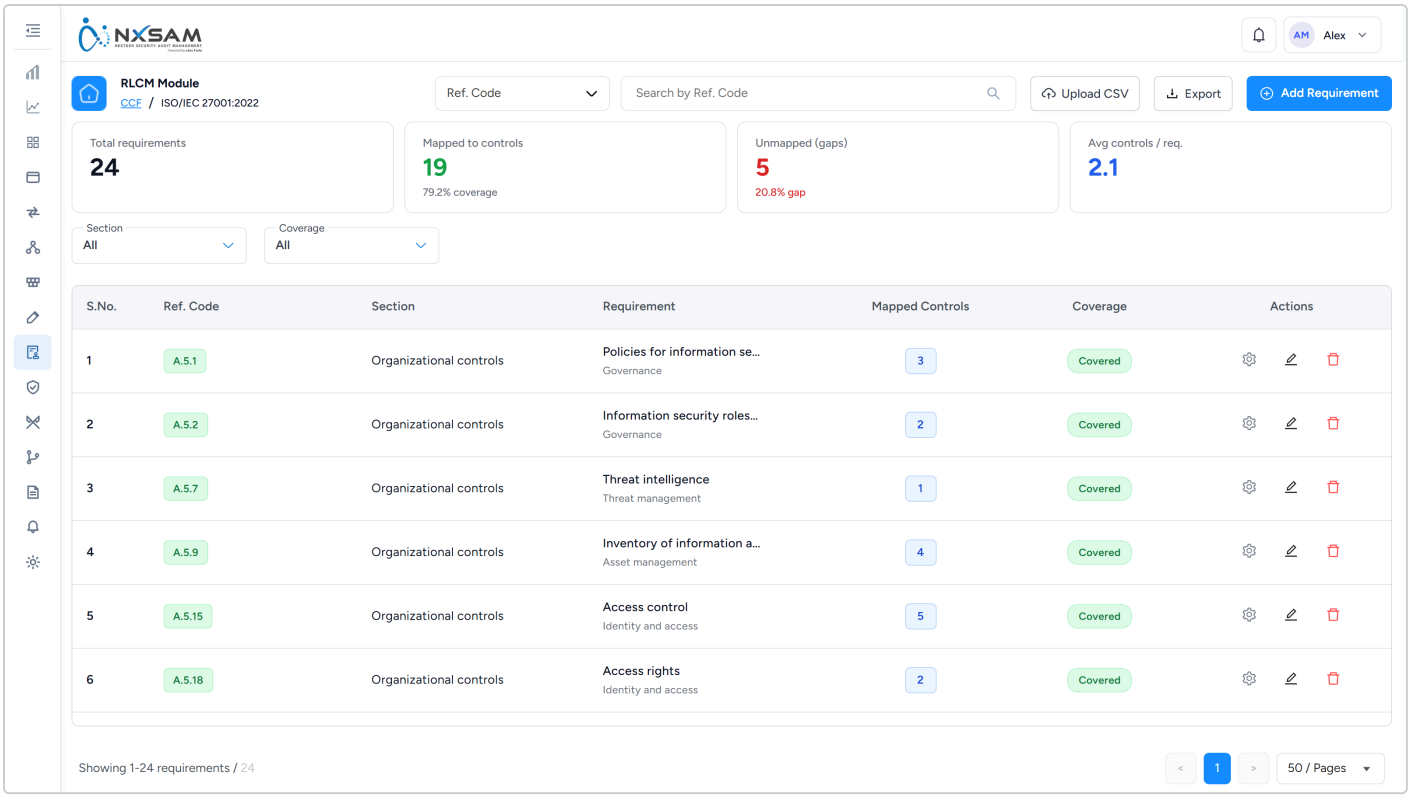


RLCM → CCF

CCF Requirements

One framework's clauses by section, each showing how many controls satisfy it. Unmapped (gaps) is the number to work down — every one is a clause you are held to and have no control for.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

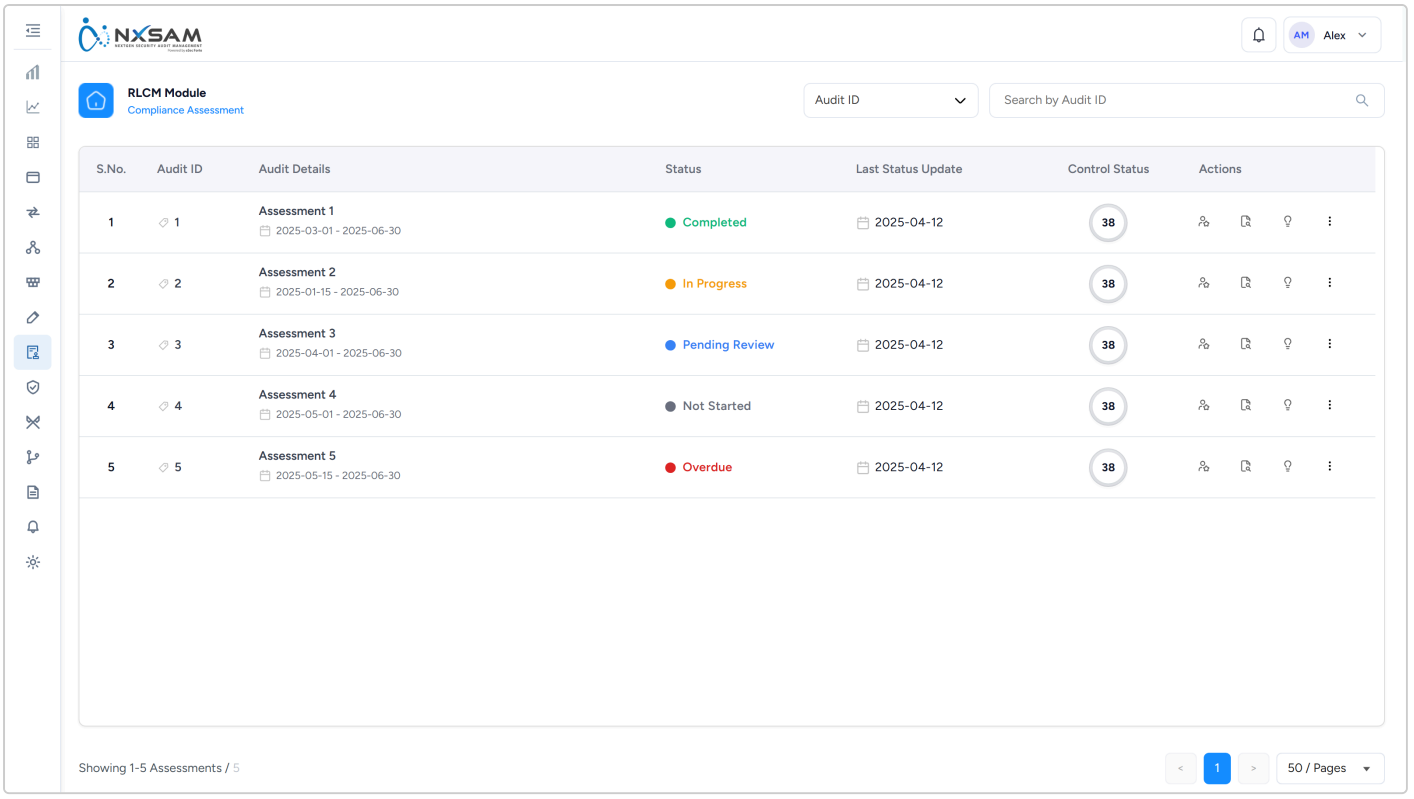


RLCM → CCF → CCF Requirements

Compliance Assessments

Assessments in progress and completed, with their control status and review state.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

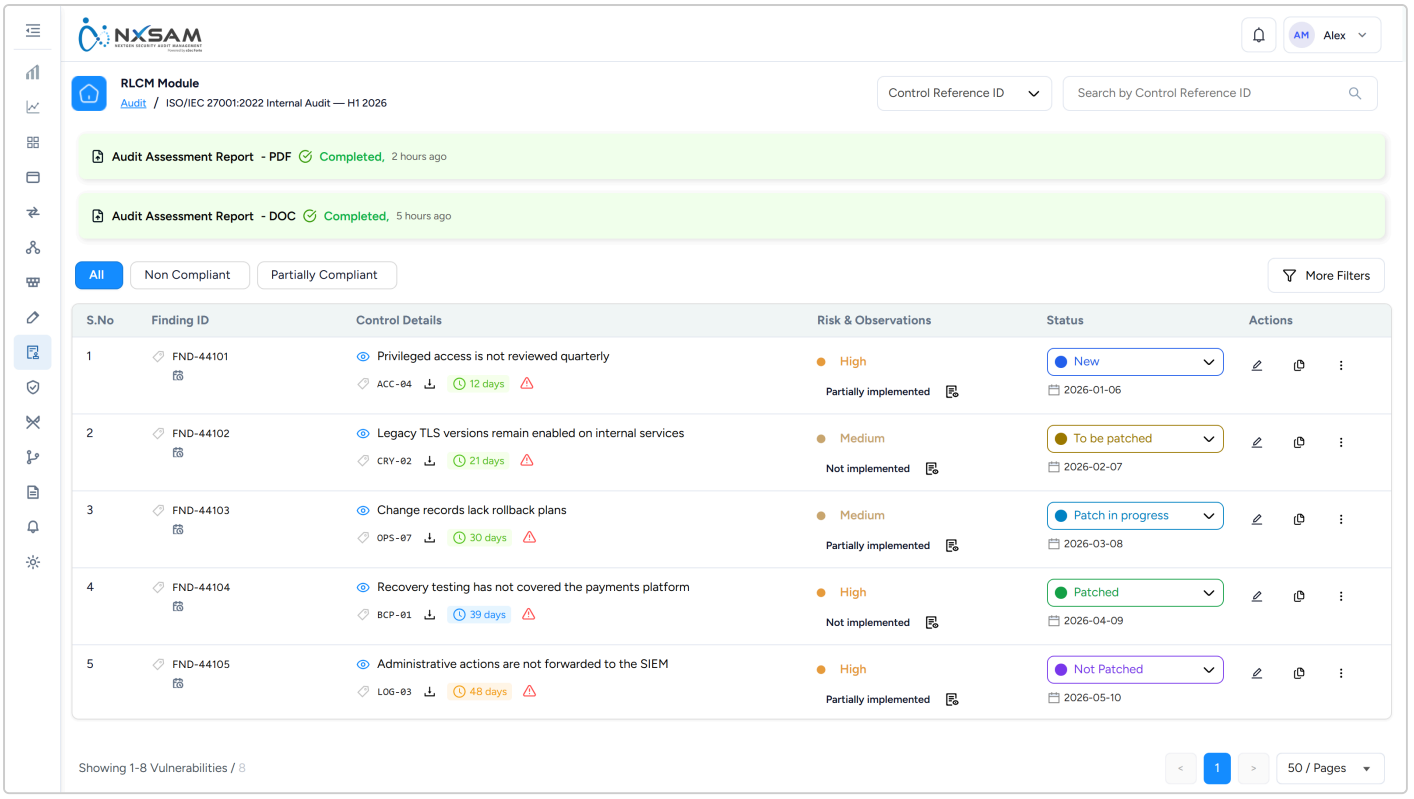


RLCM → Compliance Assessments

Compliance Risks

Risks raised from control failures, tracked and treated separately from technical vulnerabilities.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

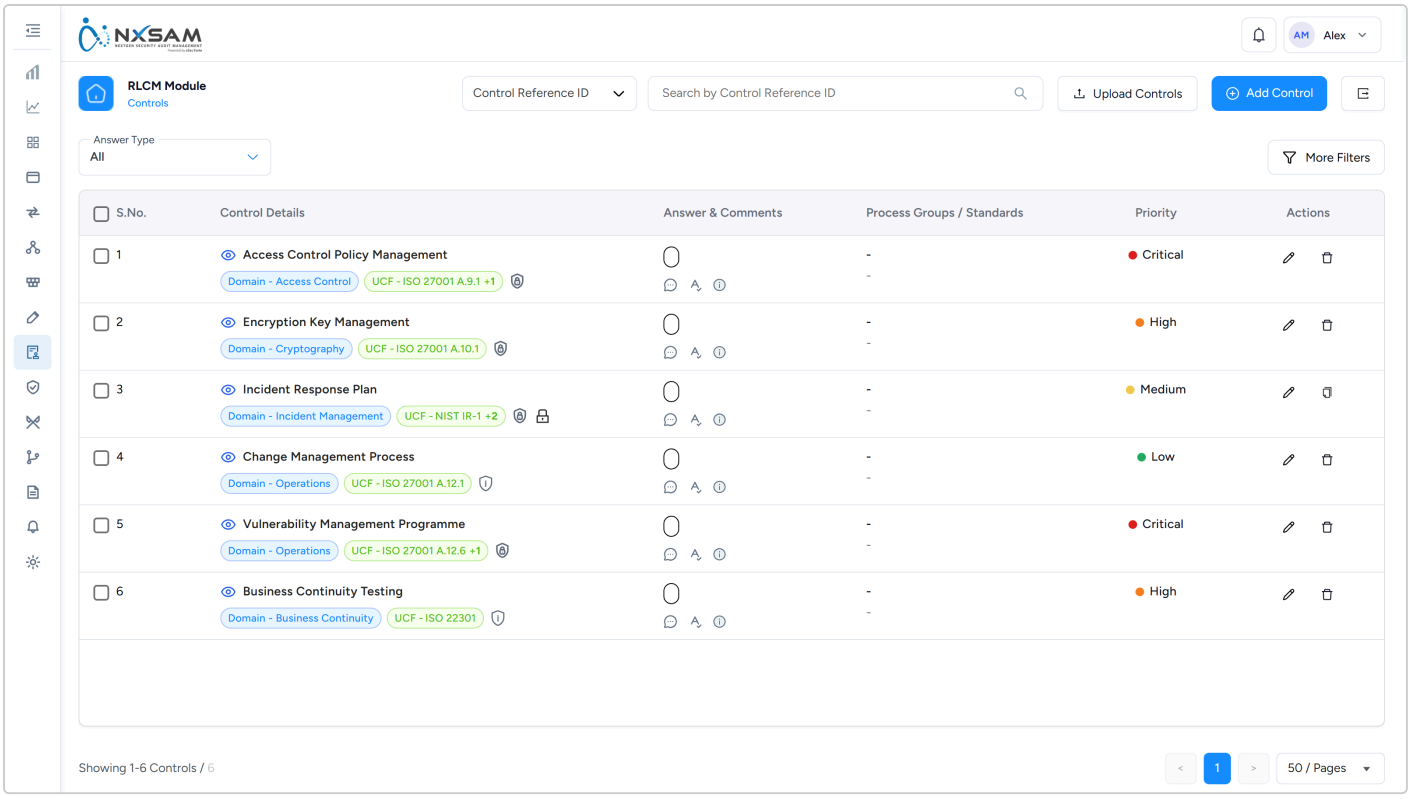


RLCM → Compliance Risks

Control Library

Every control available to assess against, across all frameworks.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

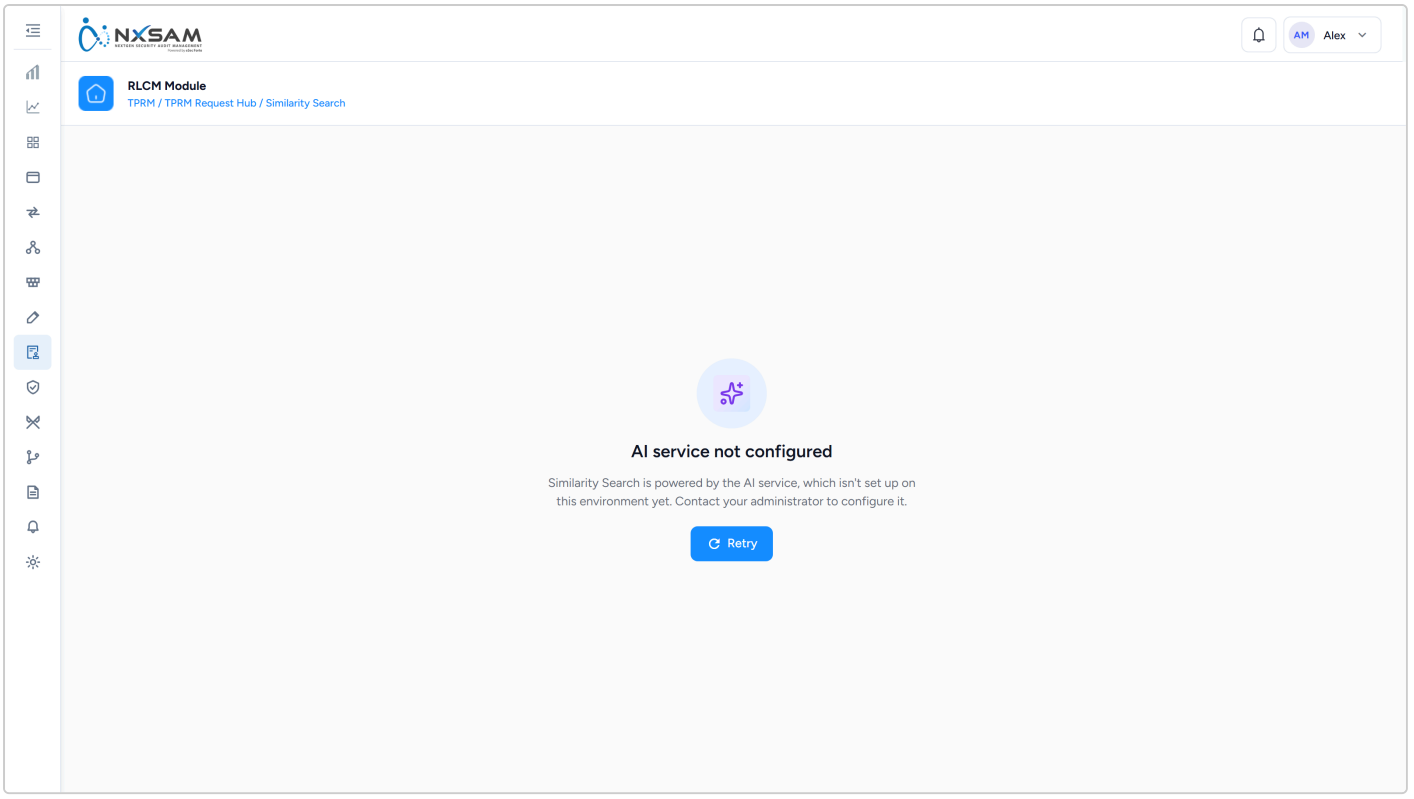


RLCM → Master

Control Similarity

Matches a vendor questionnaire against controls already assessed, so overlapping questions are not asked twice.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

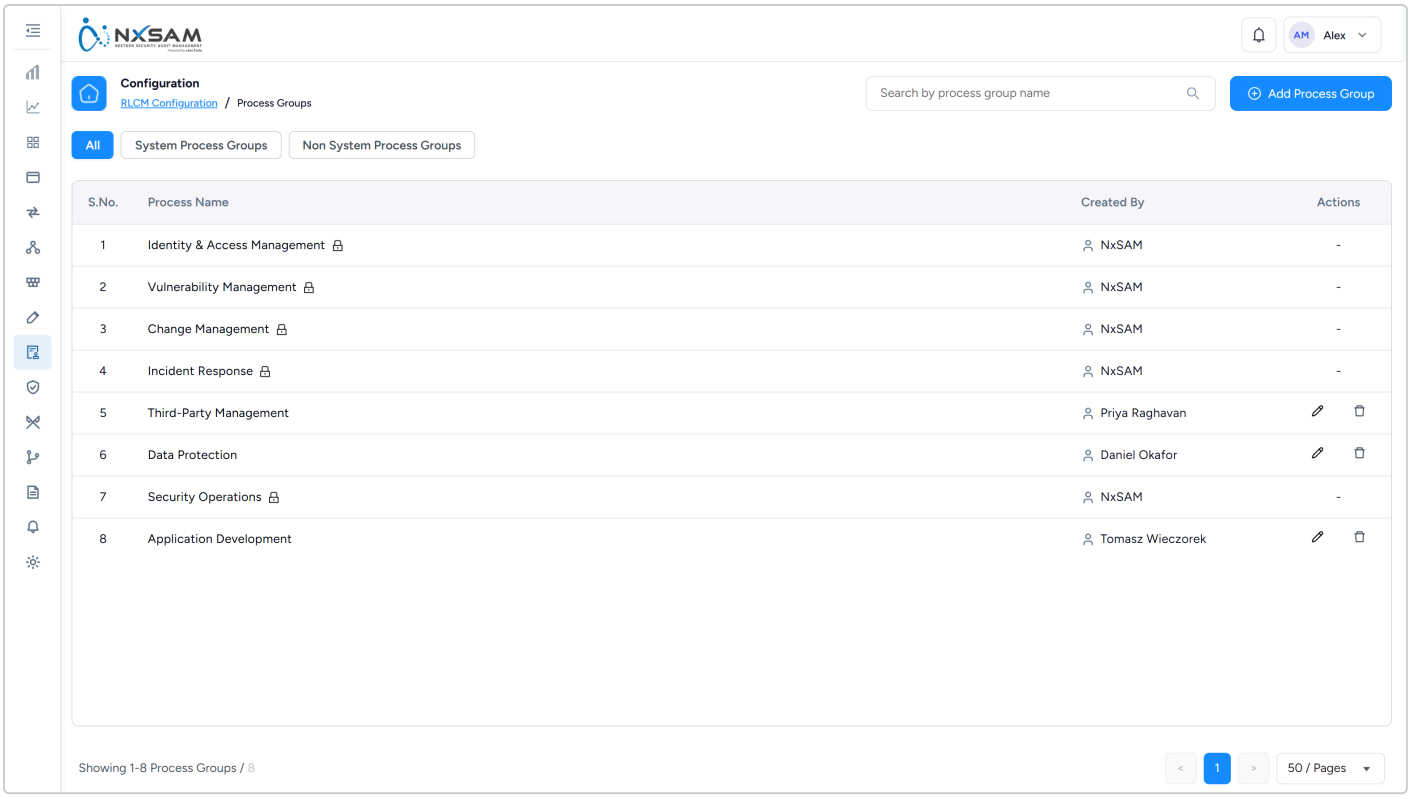


RLCM → TPRM → Control Similarity

Process Groups

Business processes controls are grouped against, so a failure can be reported by function rather than by clause.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

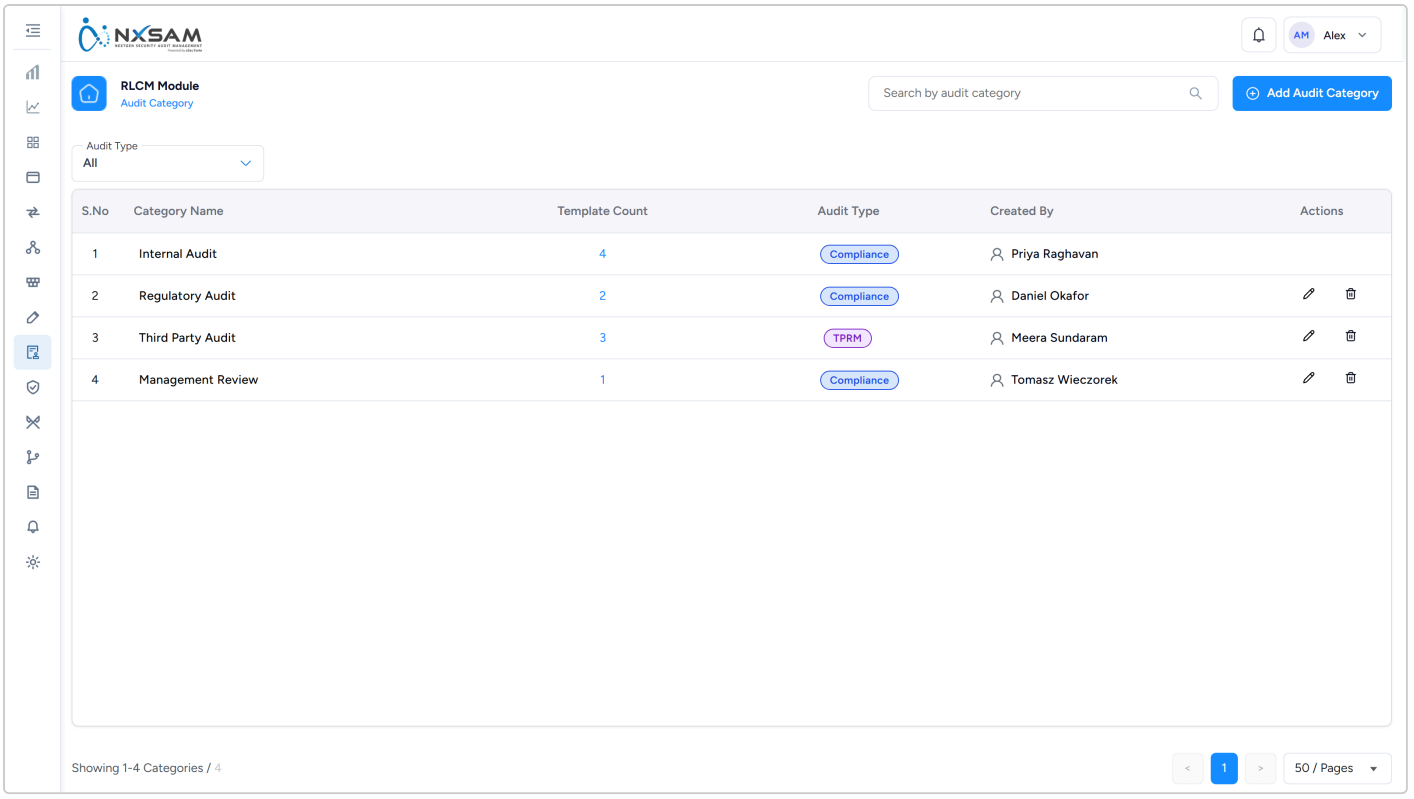


RLCM → Process Groups

RLCM Audit Categories

How compliance audits are classified for reporting.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

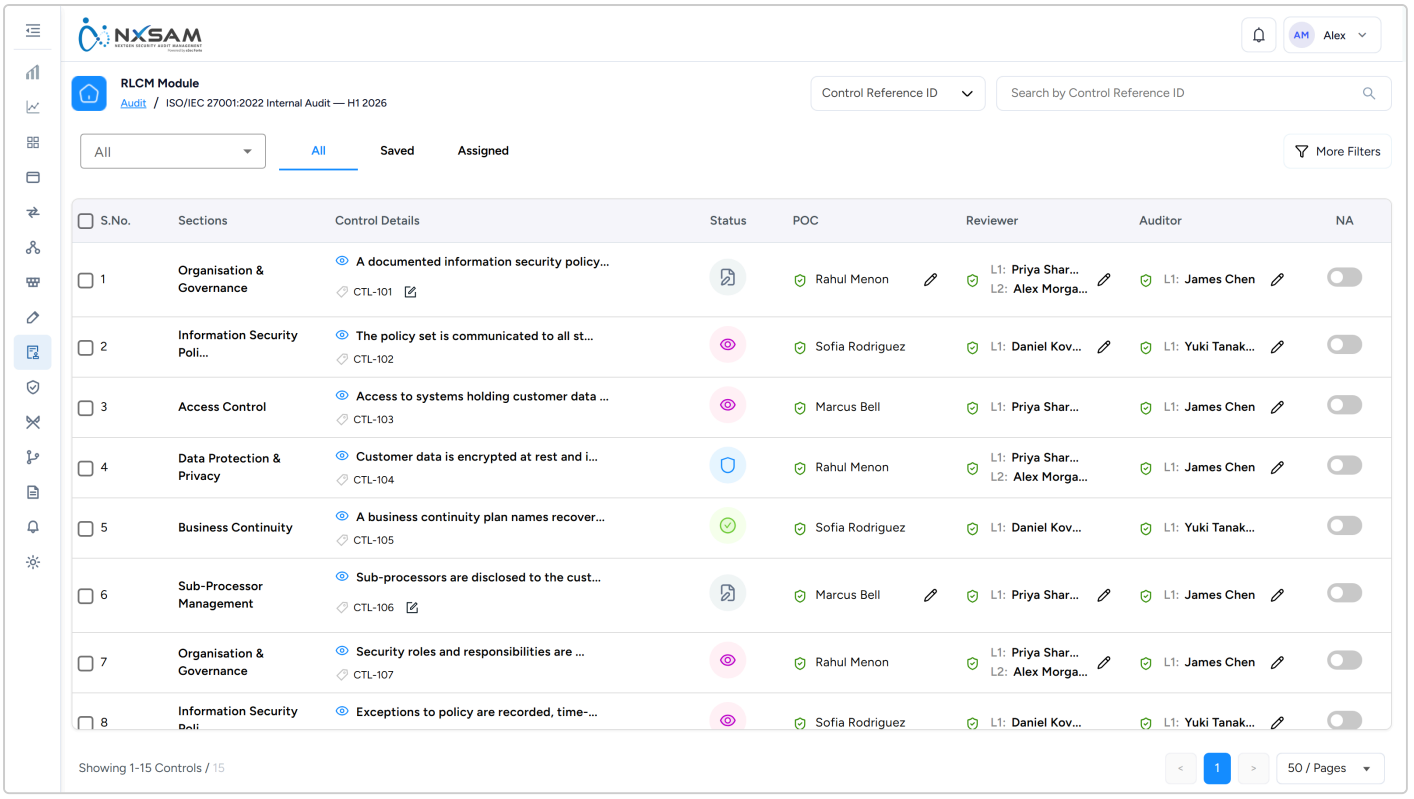


RLCM → Compliance → RLCM Audit Categories

RLCM Audit Management

Create and administer compliance audits, including scope and assigned assessors.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

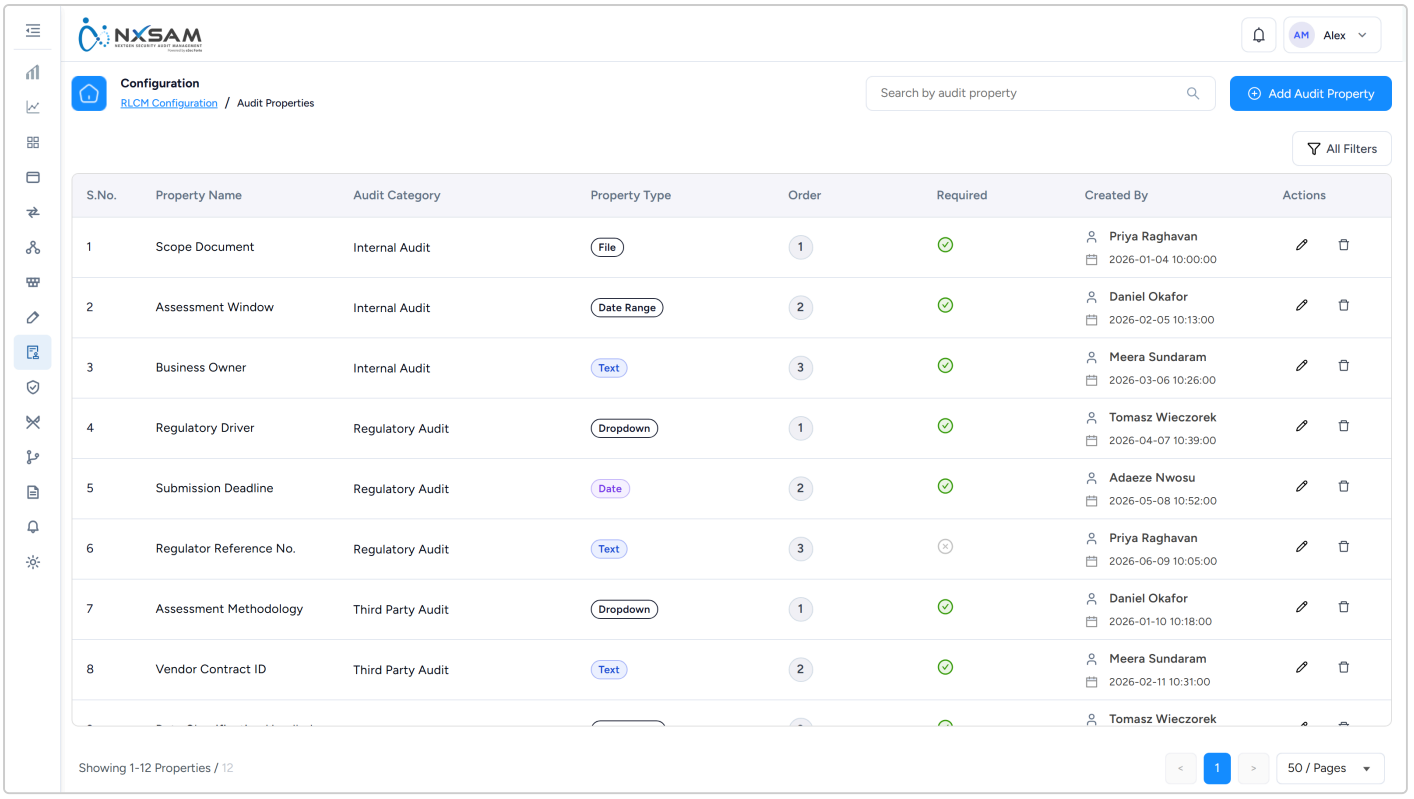


RLCM → Compliance → RLCM Audit Management

RLCM Audit Properties

Additional fields recorded against a compliance audit.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

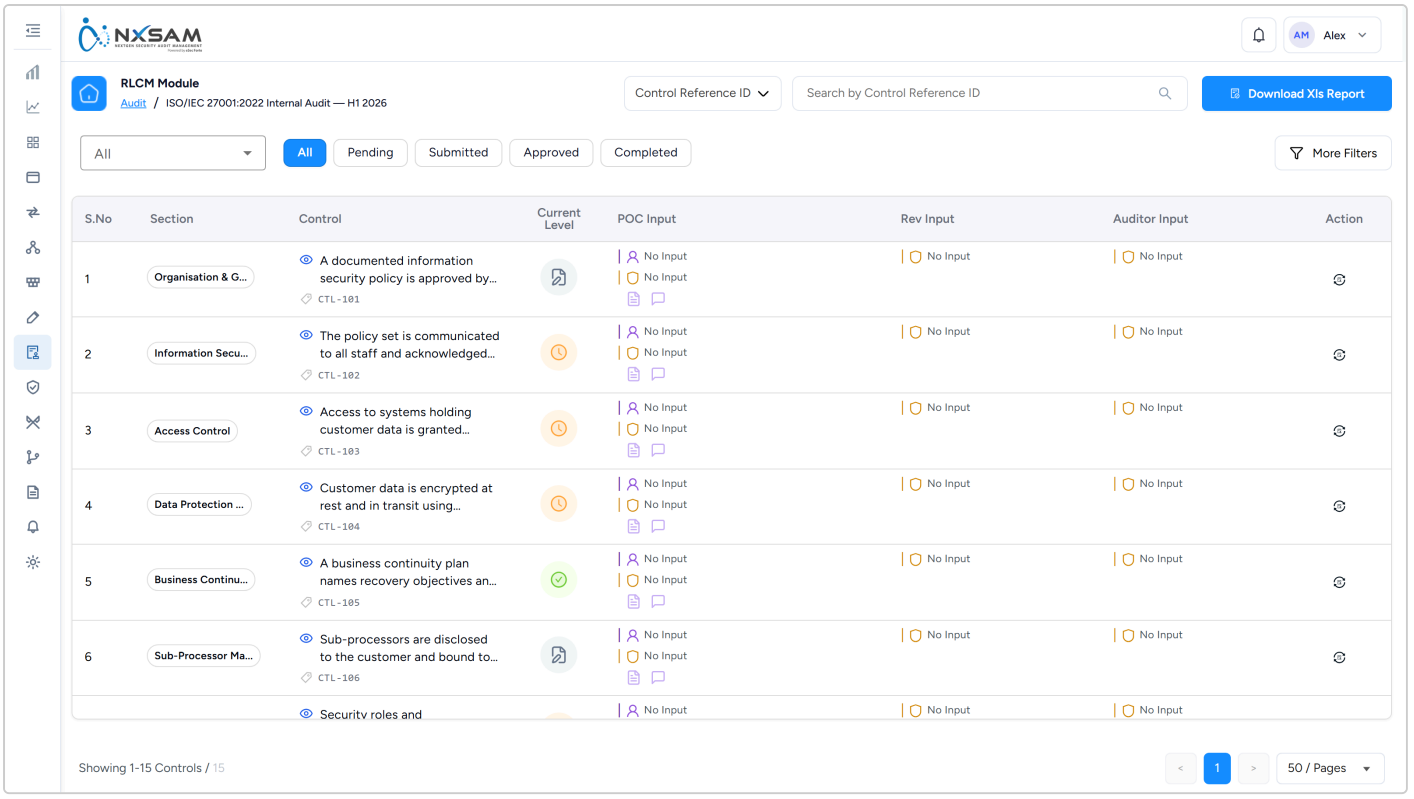


RLCM → RLCM Audit Properties

RLCM Audit Statuses

The states a compliance audit moves through, and the permitted transitions.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



RLCM → Compliance → RLCM Audit Statuses

RLCM Dashboard

Compliance posture — findings by audit type, control age, and the top failing process groups and standards.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

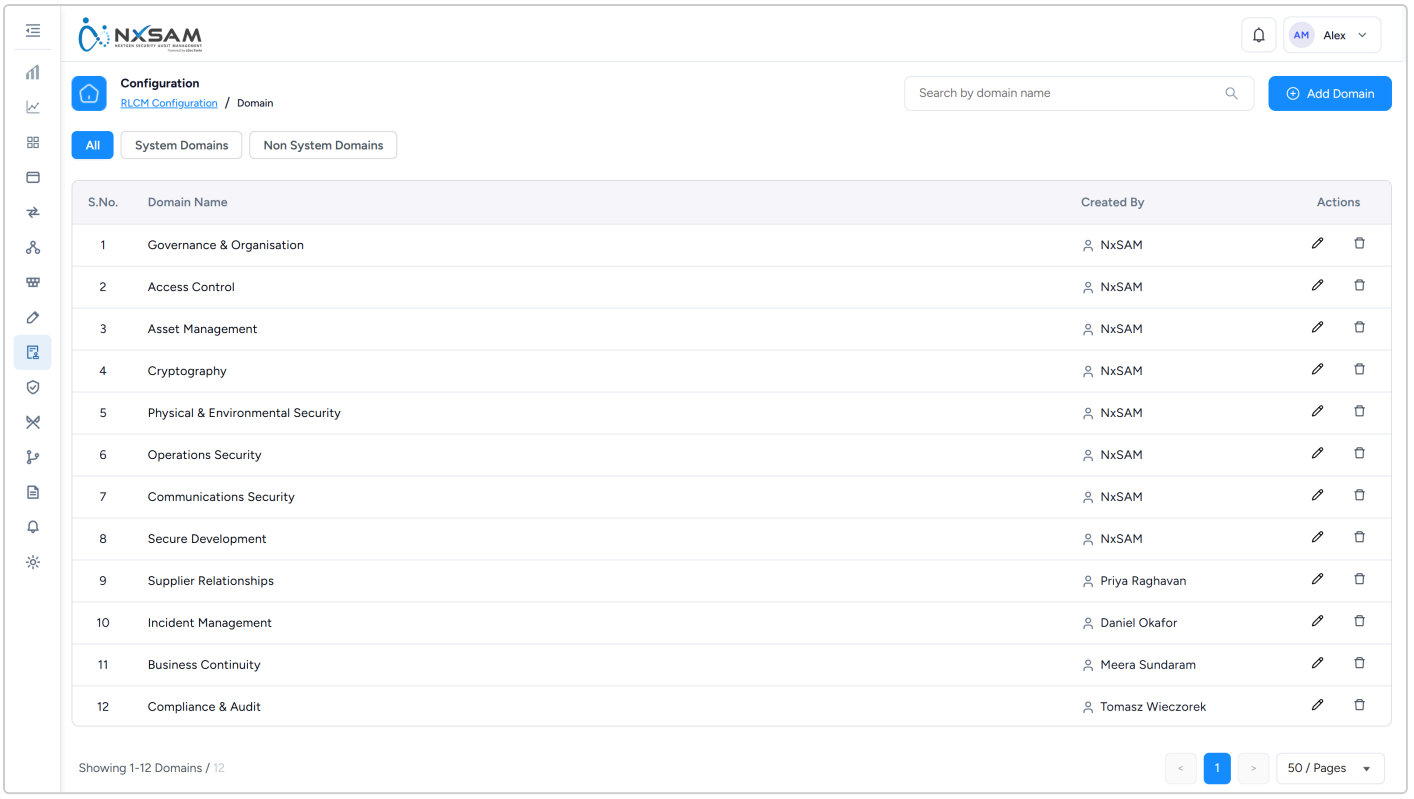


RLCM → Dashboards

RLCM Domains

The top-level grouping above process groups.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

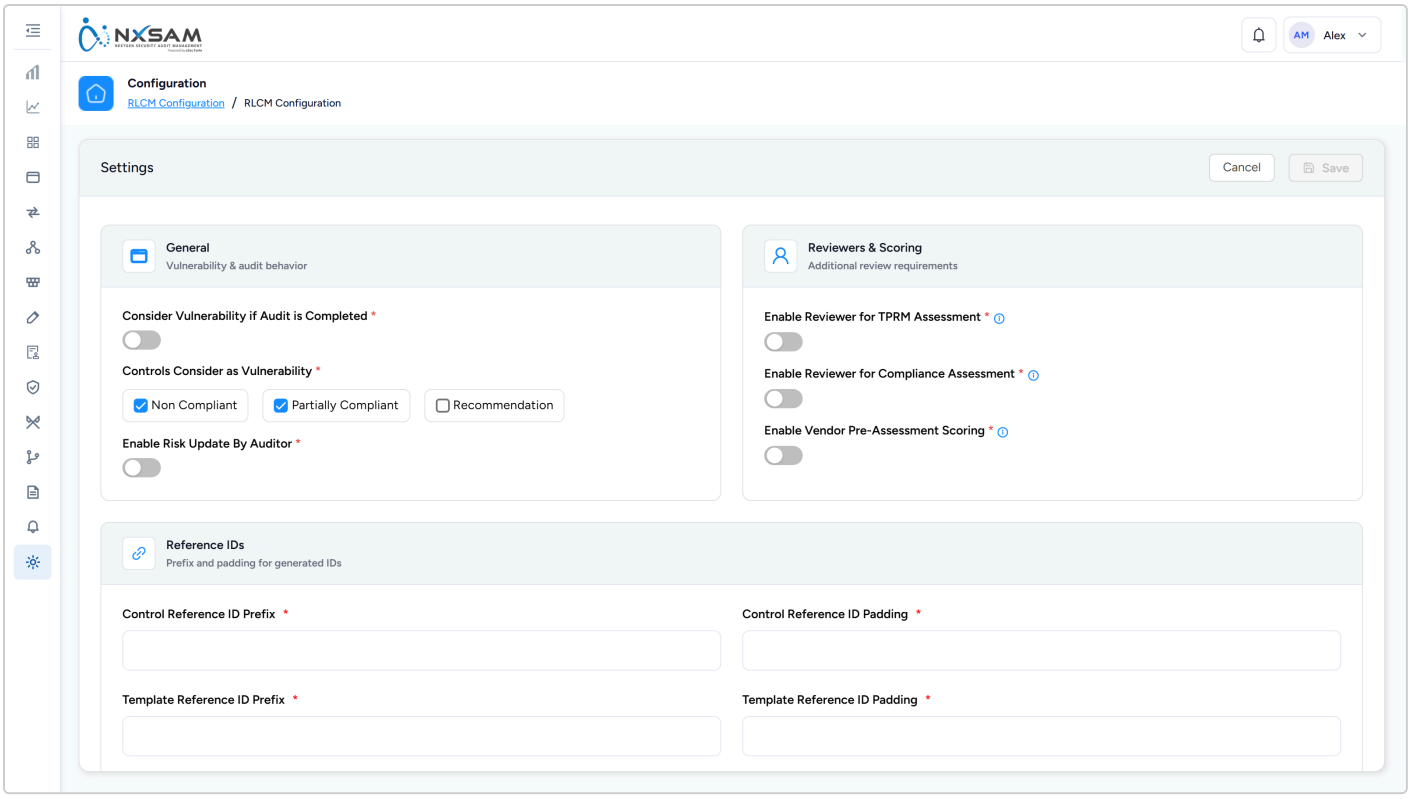


RLCM → RLCM Domains

RLCM General Configuration

Module-wide settings for compliance management.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

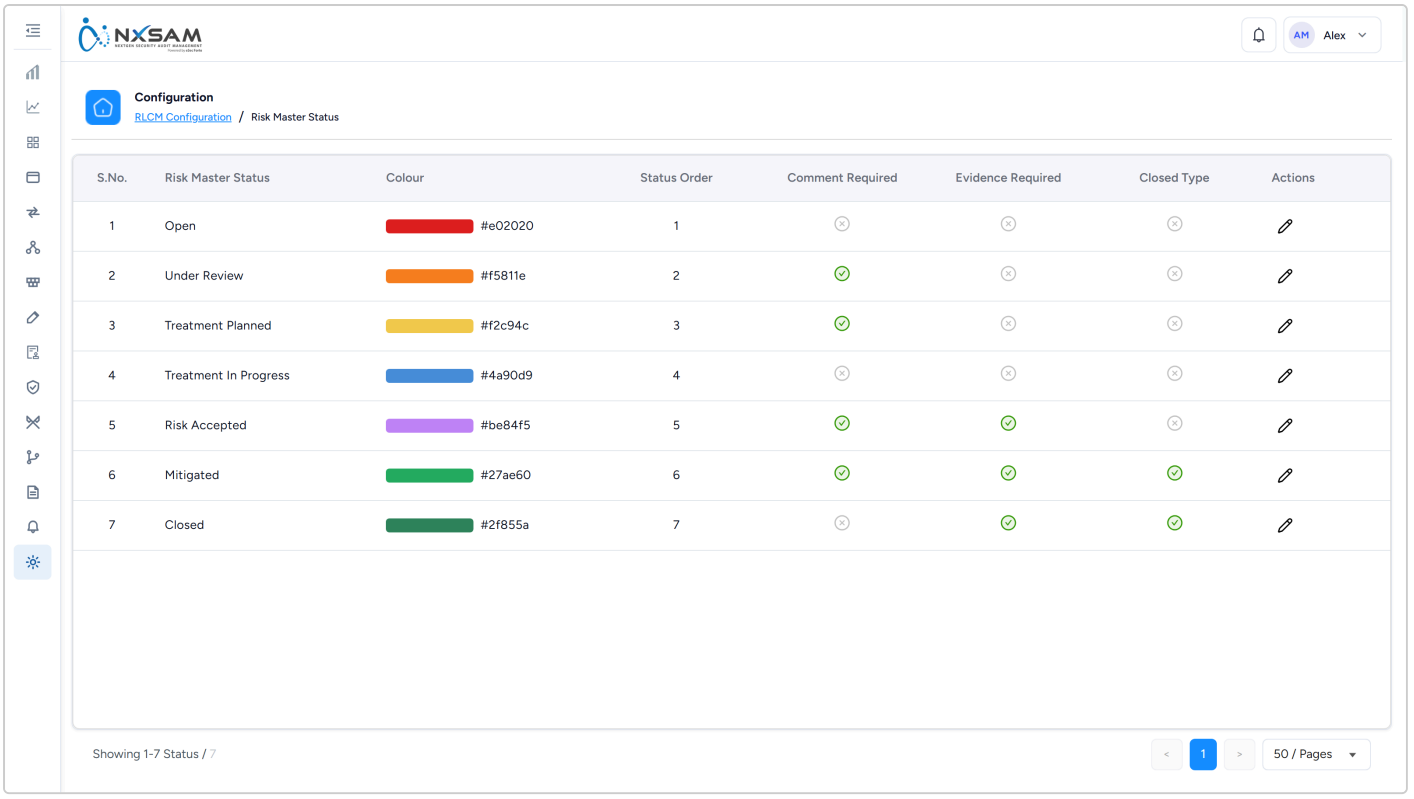


Setting → RLCM Configuration → RLCM General Configuration

RLCM Risk Statuses

The states a compliance risk moves through as it is treated.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

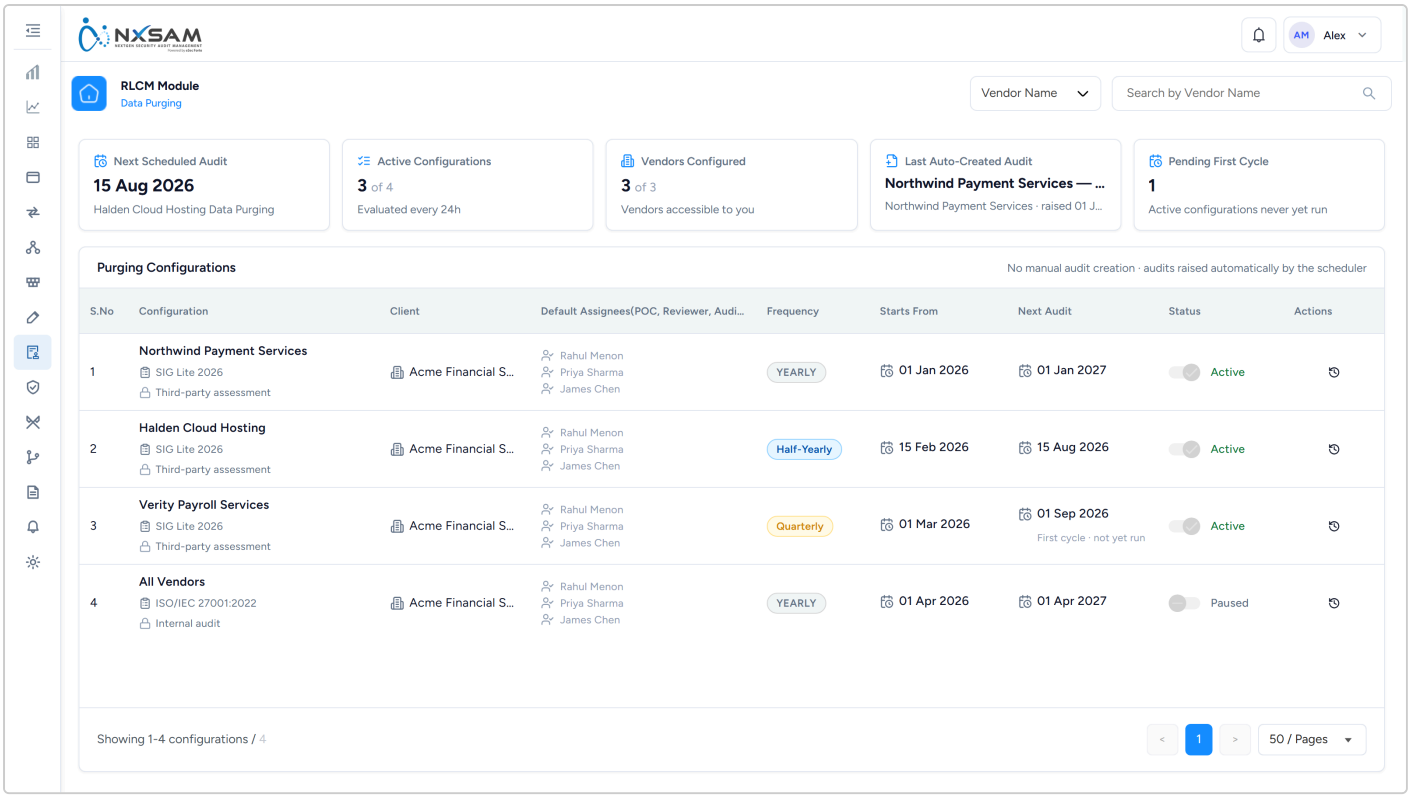


Setting → RLCM Configuration → RLCM Risk Statuses

Recurring Assessments

Standing instructions that raise an assessment automatically on a frequency, with its assignees already set. Titled "Purging Configurations" in the product; nothing on it deletes data.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

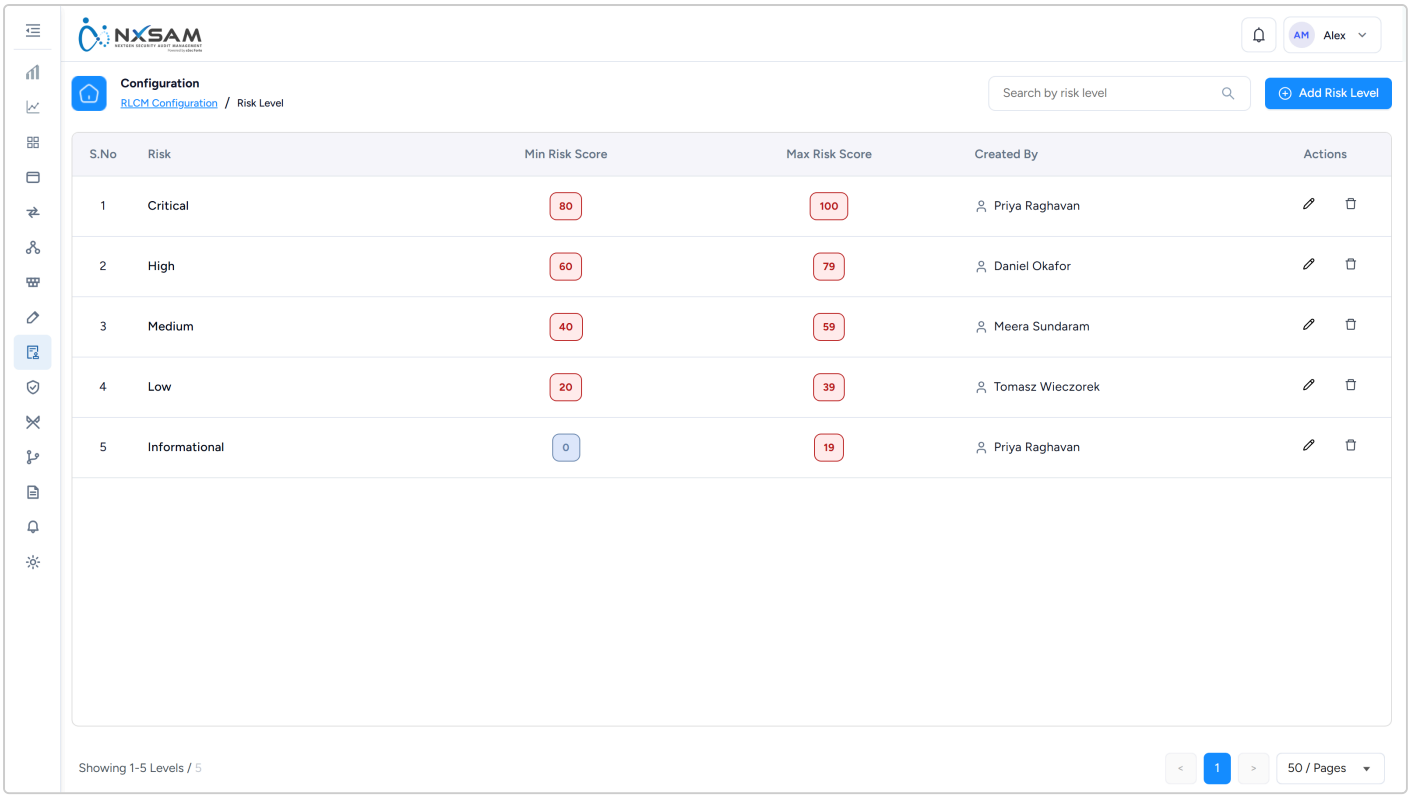


RLCM → Data → Recurring Assessments

Risk Levels

The rating scale used for compliance risk, separate from technical severity.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

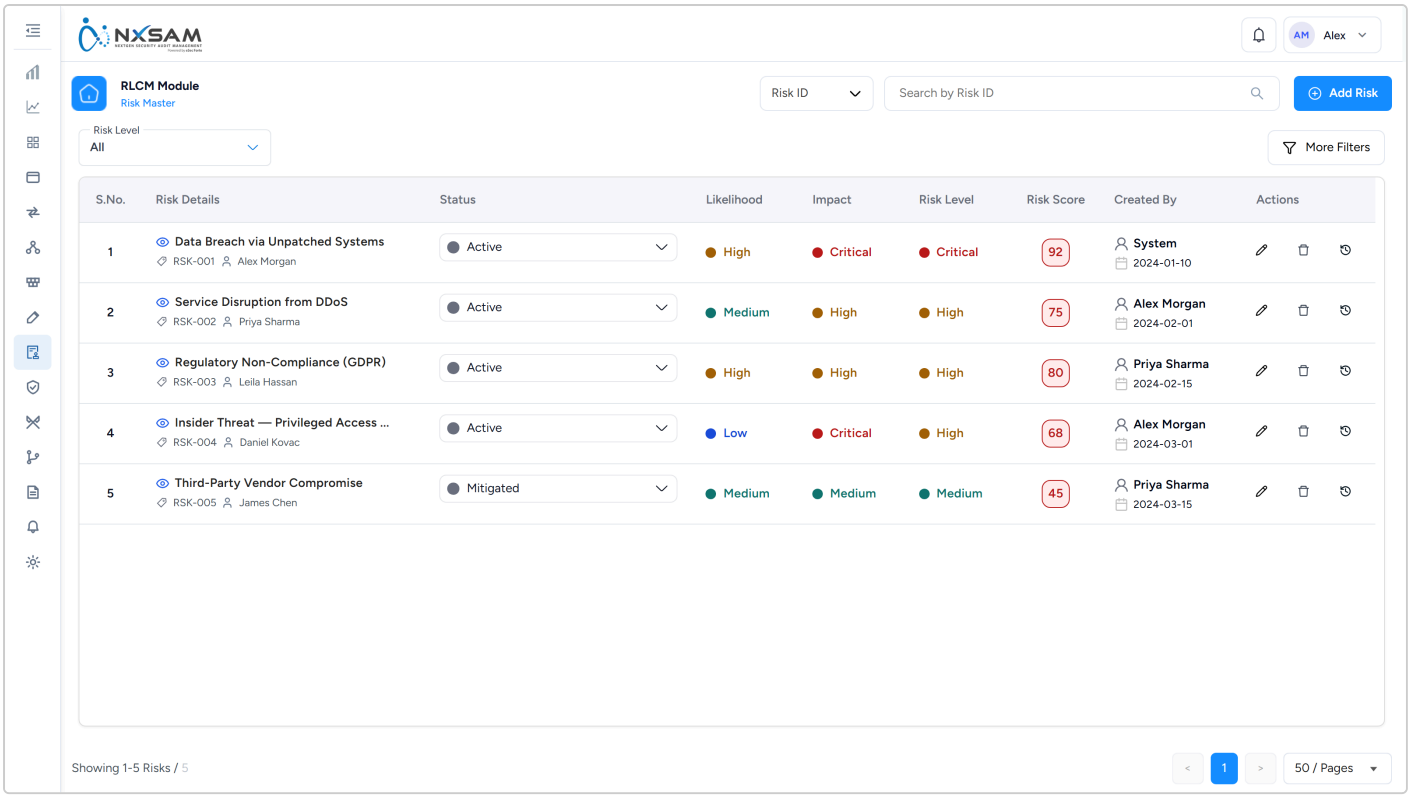


RLCM → Risk → Risk Levels

Risk Master

The catalogue of risks that can be raised, so wording stays consistent between assessments.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

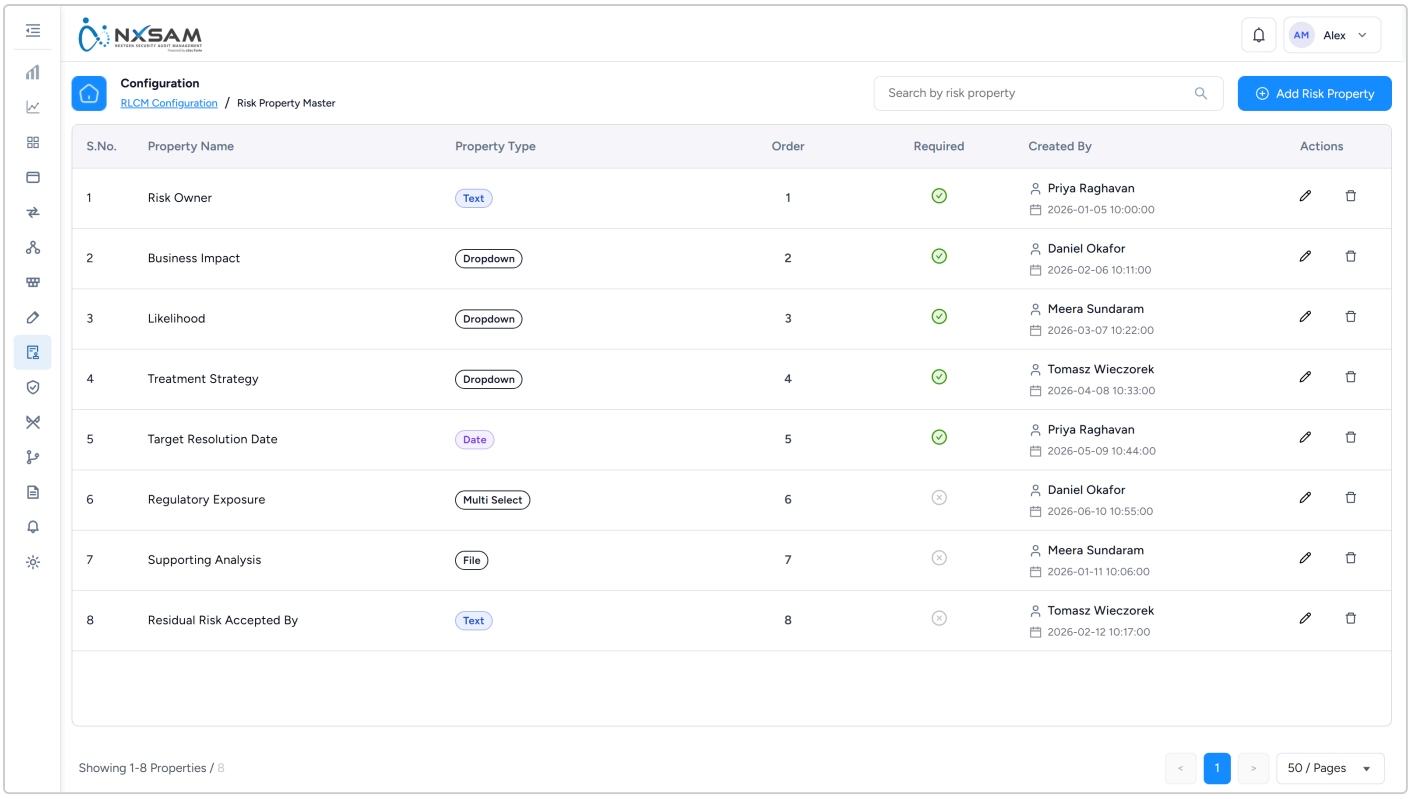


RLCM → Risk → Risk Master

Risk Properties

Additional attributes recorded against a compliance risk.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

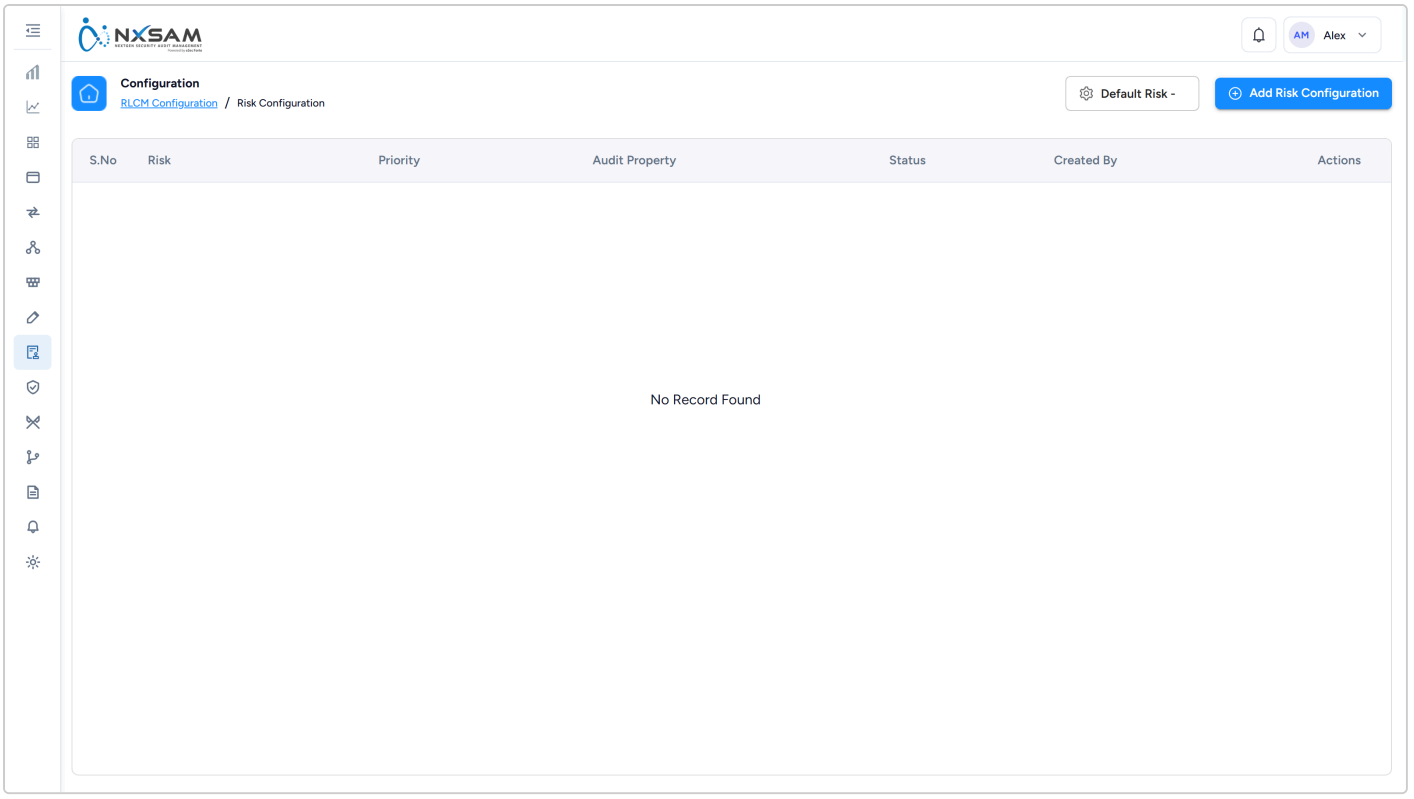


RLCM → Risk → Property → Risk Properties

Risk Rating Rules

How a control failure is turned into a risk rating.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

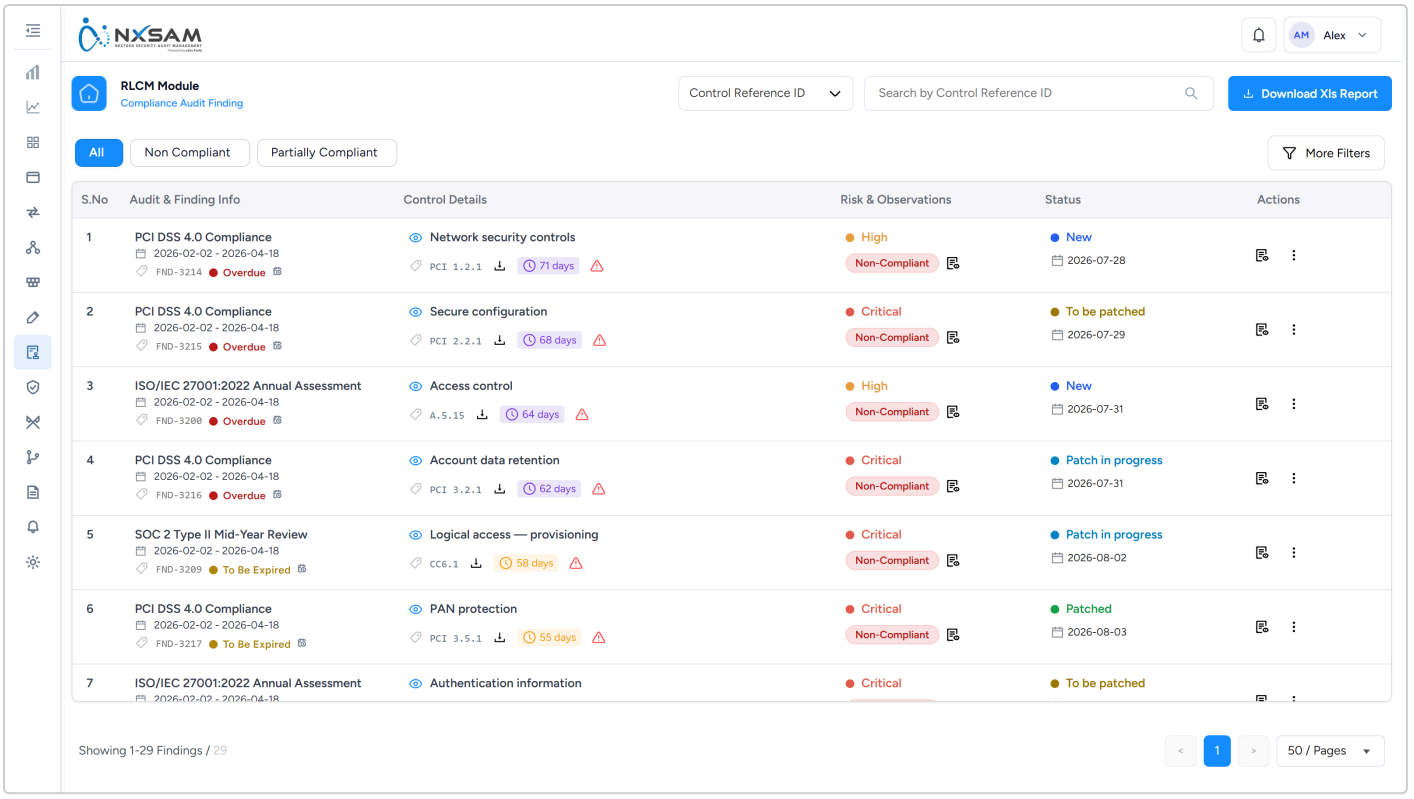


RLCM → Risk → Risk Rating Rules

Risk Register

The consolidated register — every open compliance risk with its rating, owner and treatment.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

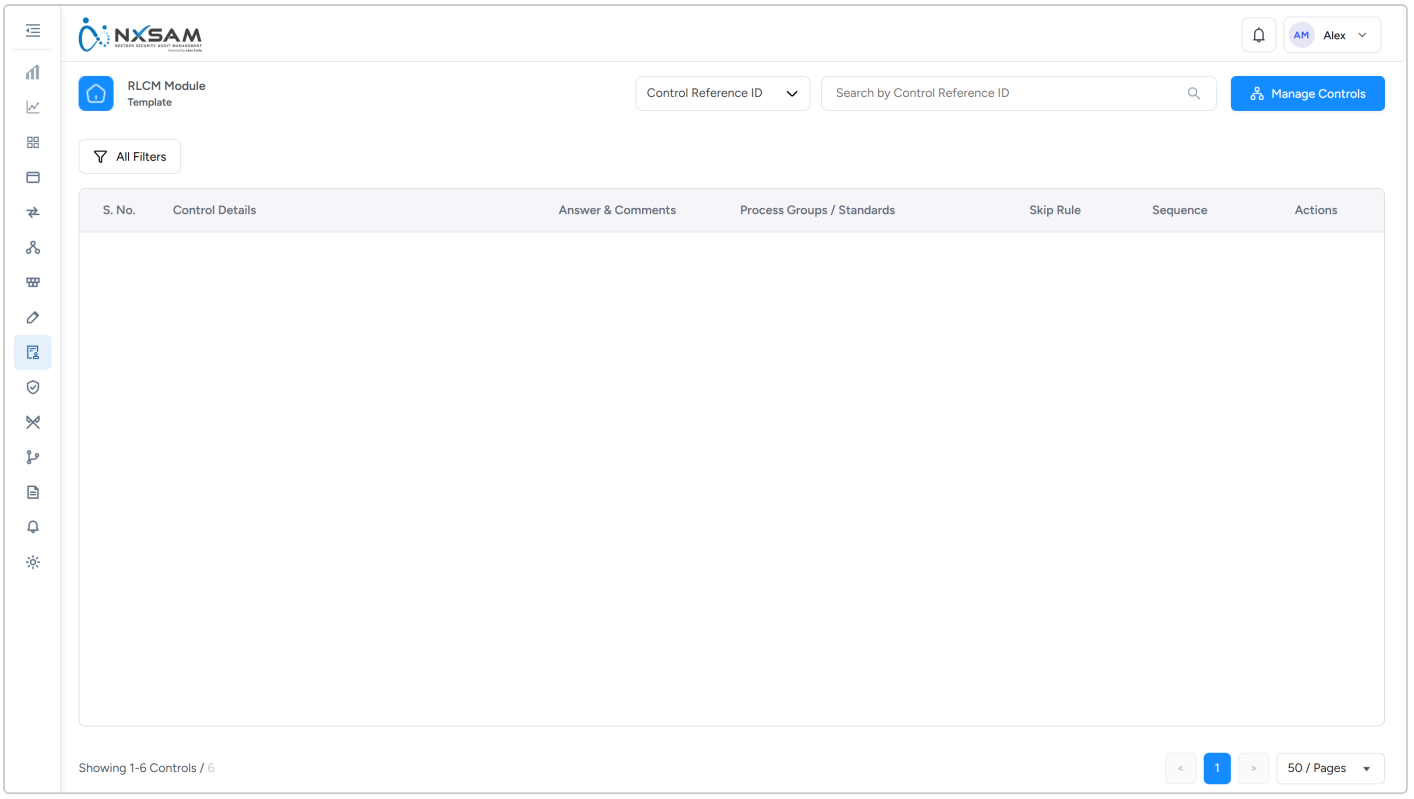


RLCM → Risk Register

Section Controls

Which controls belong to which section of a standard.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

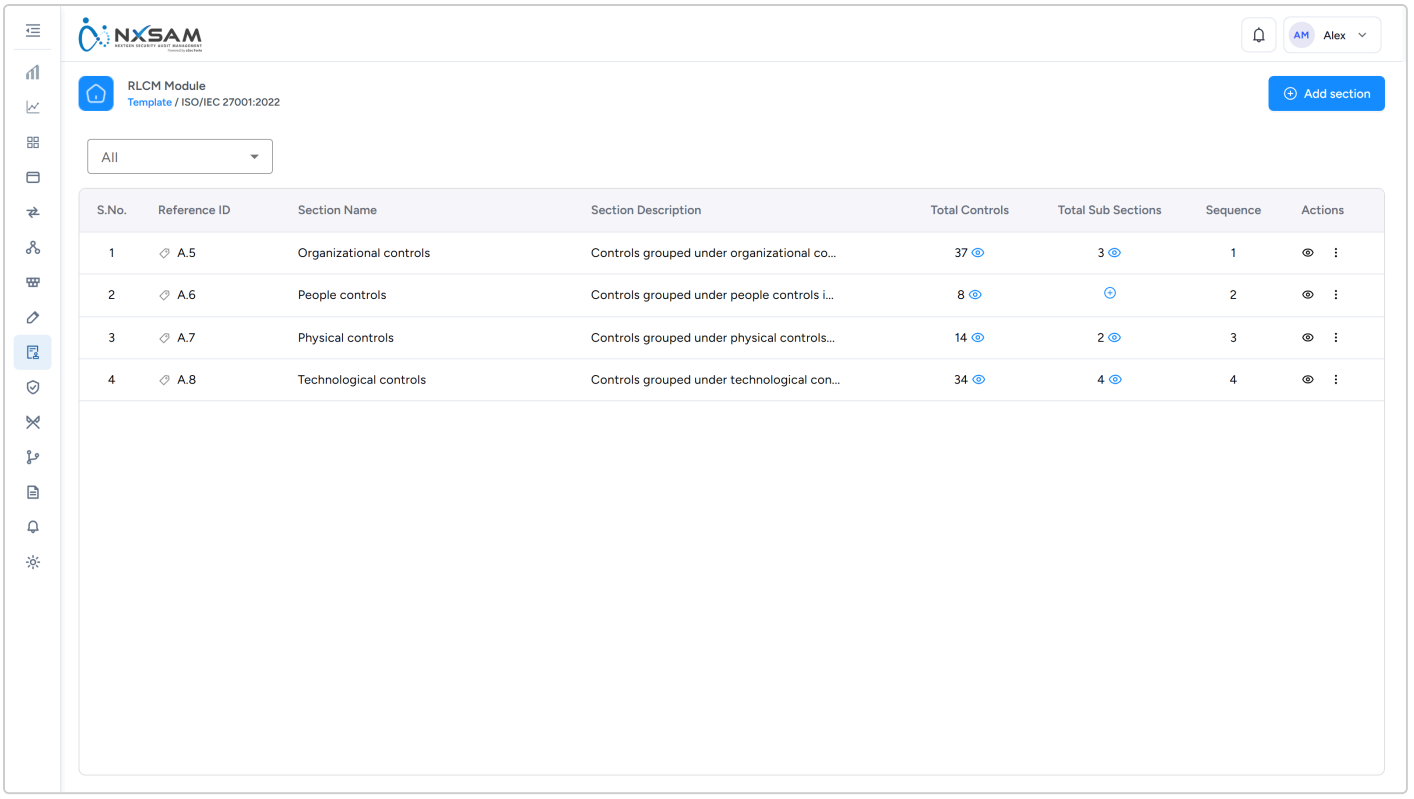


RLCM → Section → Section Controls

Standard Sections

How a standard divides into sections, used for scoring and reporting at section level.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

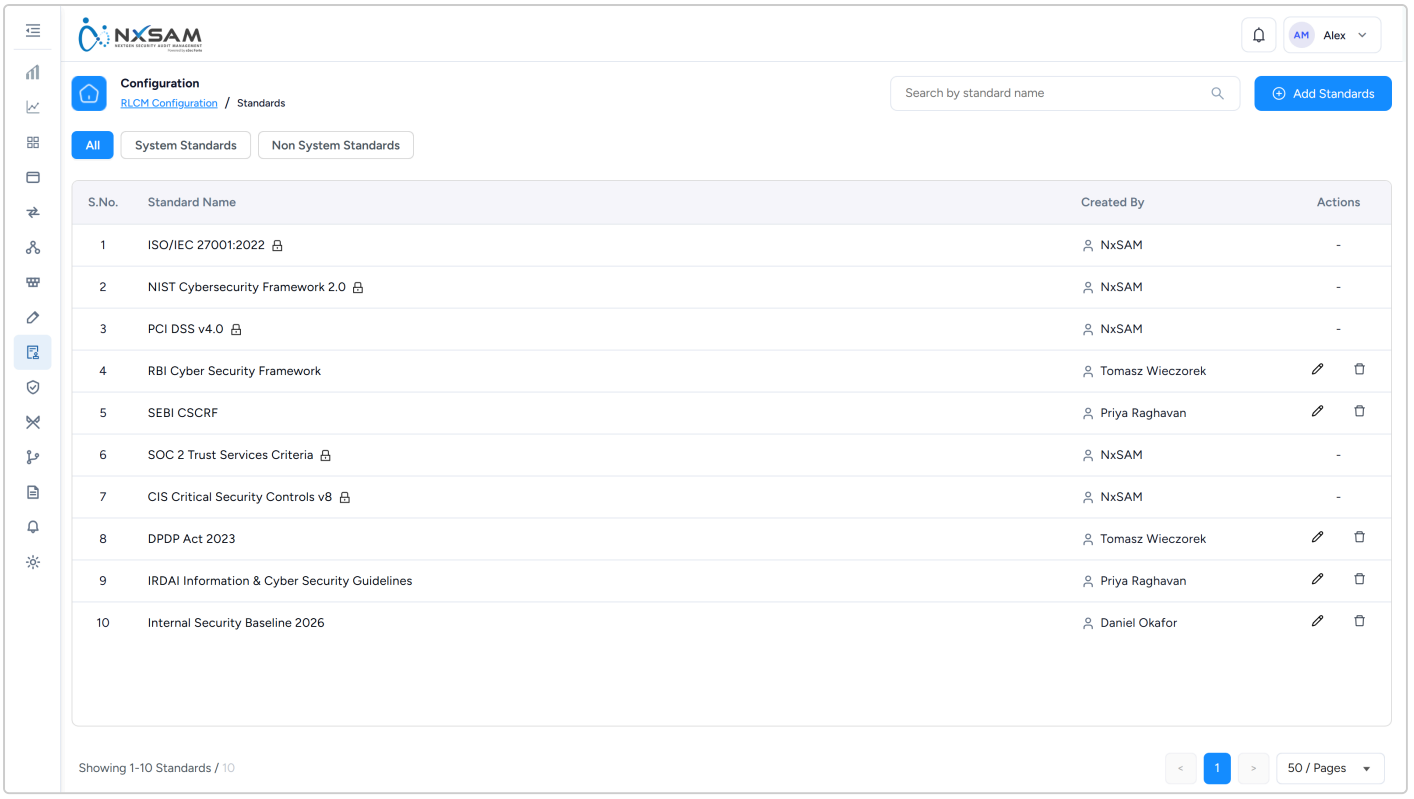


RLCM → Standard Sections

Standards

The frameworks in use — ISO 27001, PCI DSS, an internal baseline. Each carries its own controls.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

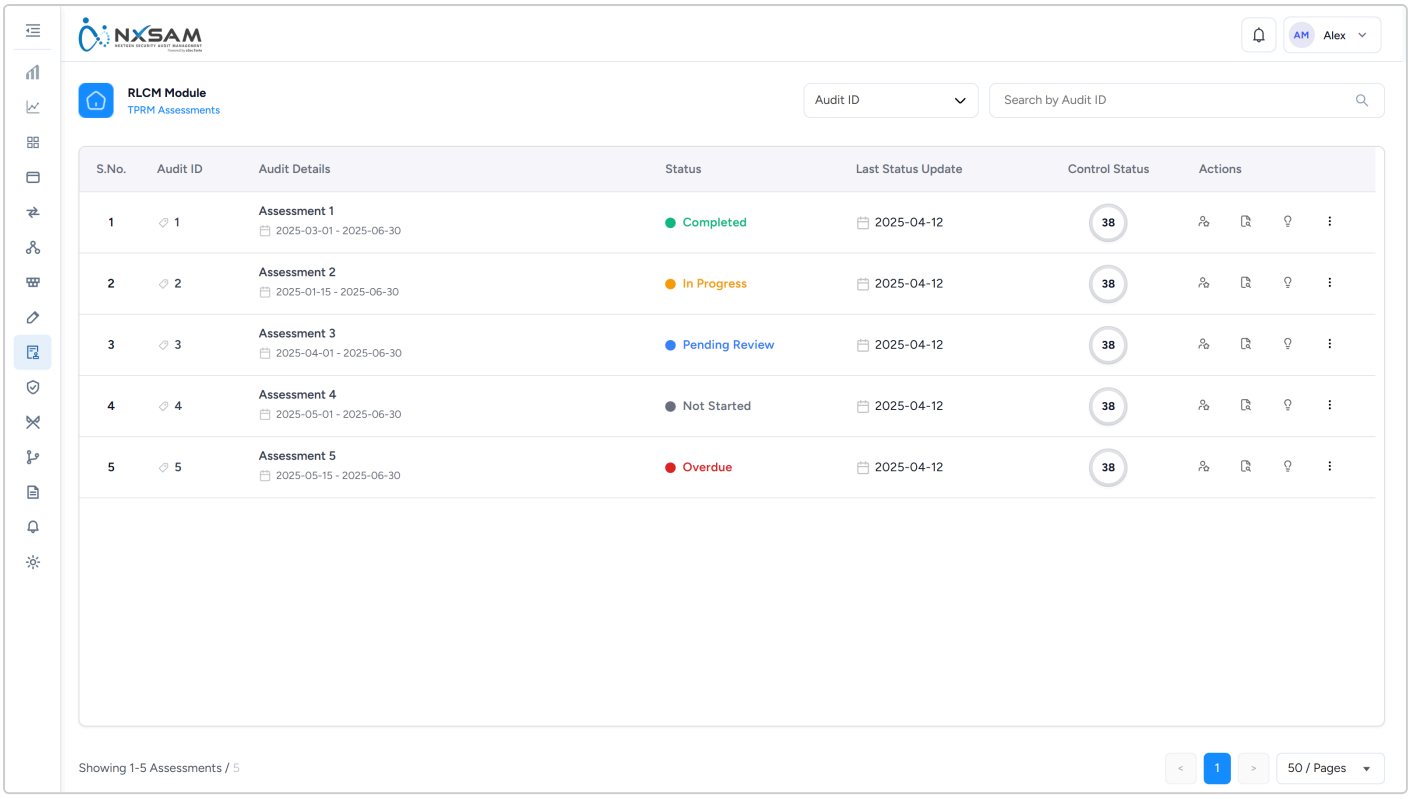


RLCM → Standards

TPRM Assessments

Assessments issued to vendors, and how far each has progressed.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

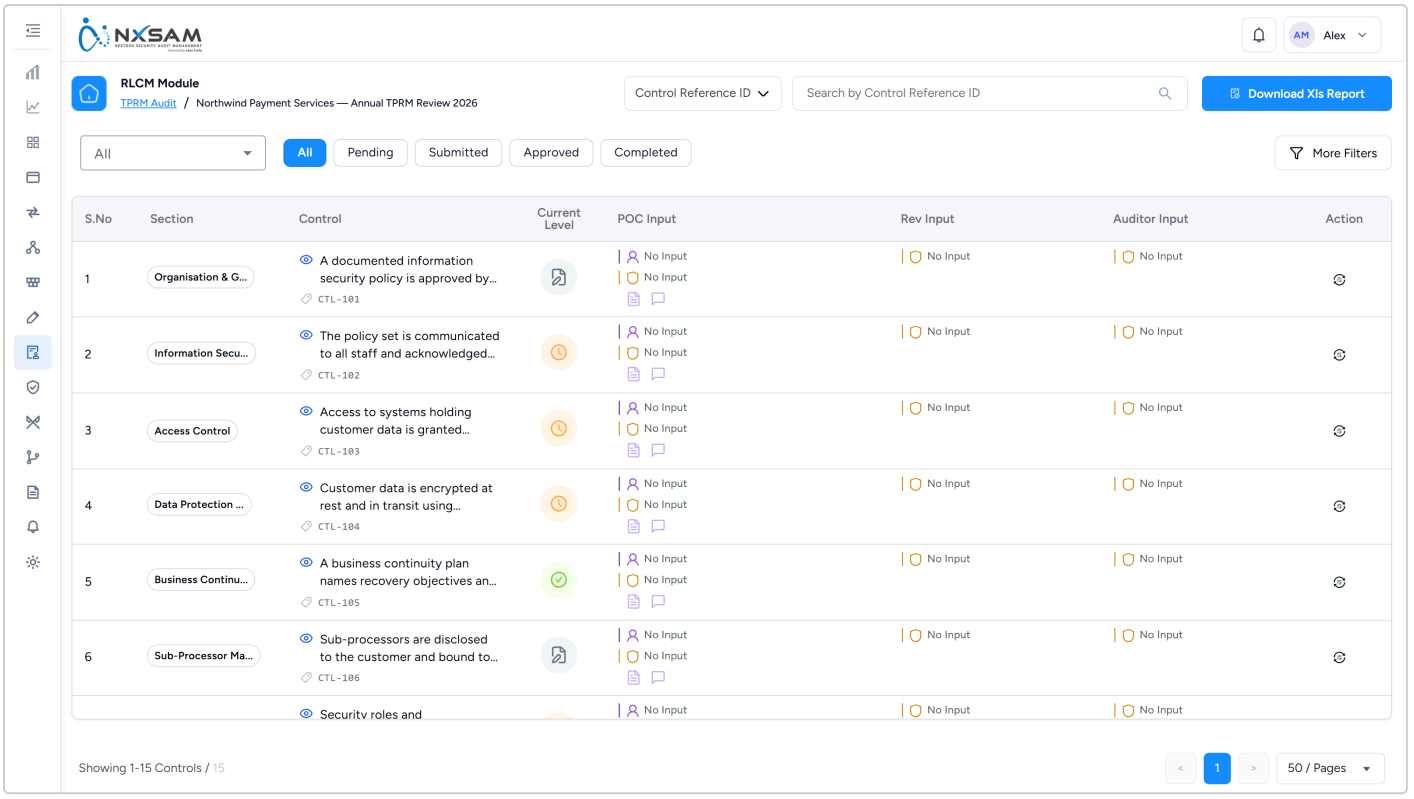


RLCM → TPRM → TPRM Assessments

TPRM Audit Statuses

The states a vendor assessment moves through.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

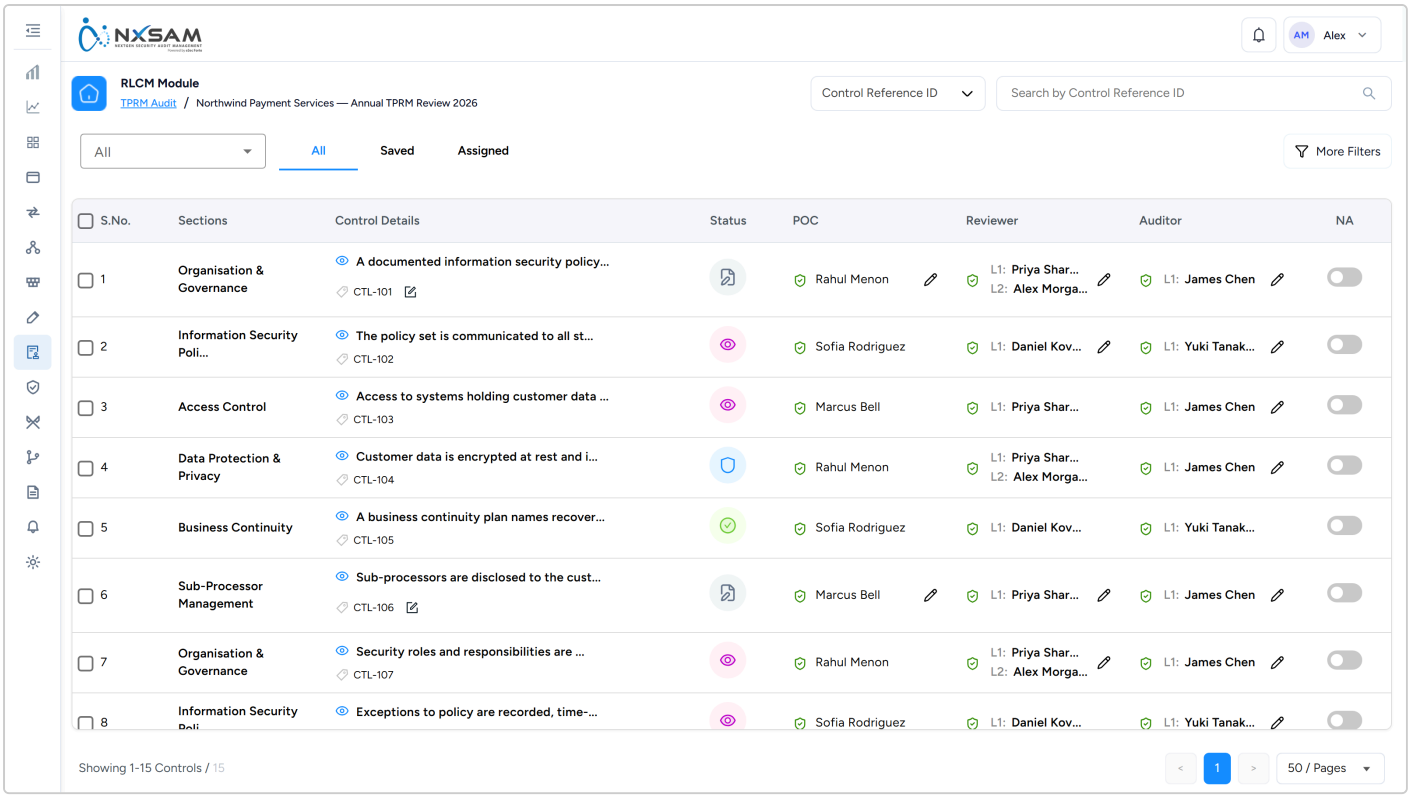


RLCM → TPRM → TPRM Audit Statuses

TPRM Control Management

A vendor assessment being worked: each control, who it is waiting on, and what they have done with it.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

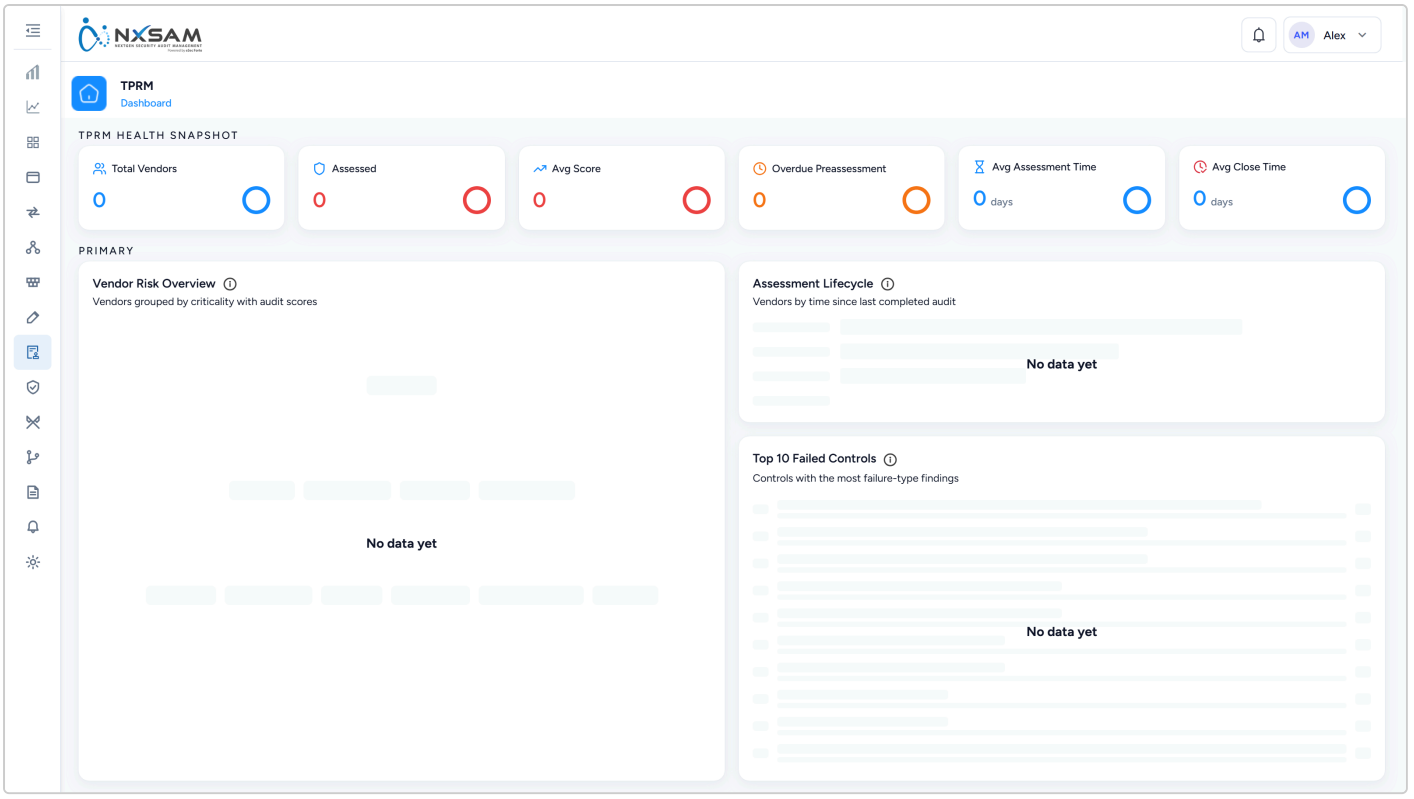


RLCM → TPRM → TPRM Control Management

TPRM Dashboard

Third-party risk posture across the vendor portfolio.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

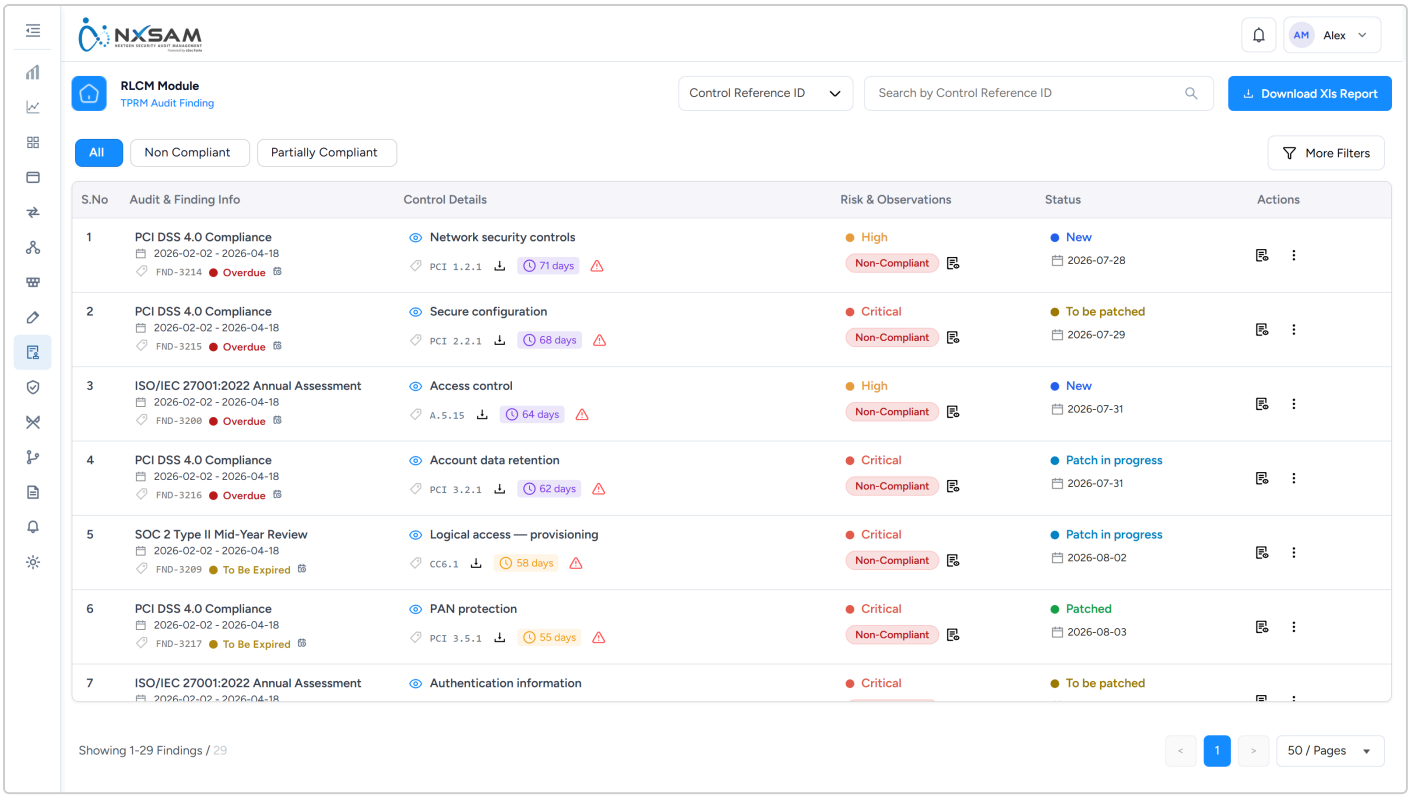


RLCM → TPRM → TPRM Dashboard

TPRM Findings

What a vendor assessment found, and what was asked of the vendor.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

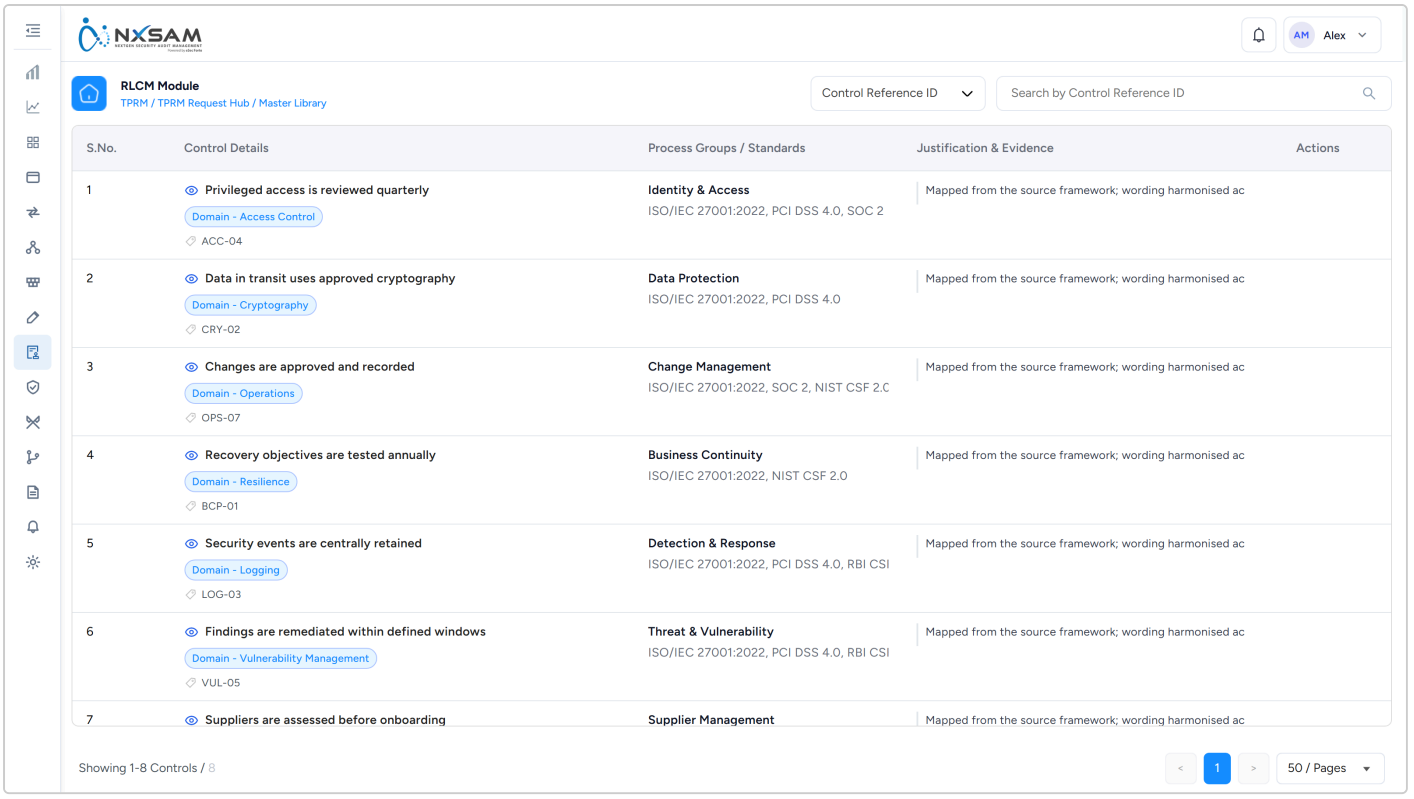


RLCM → TPRM → TPRM Findings

TPRM Question Library

Reusable questions for vendor assessments, so vendors are asked consistently.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

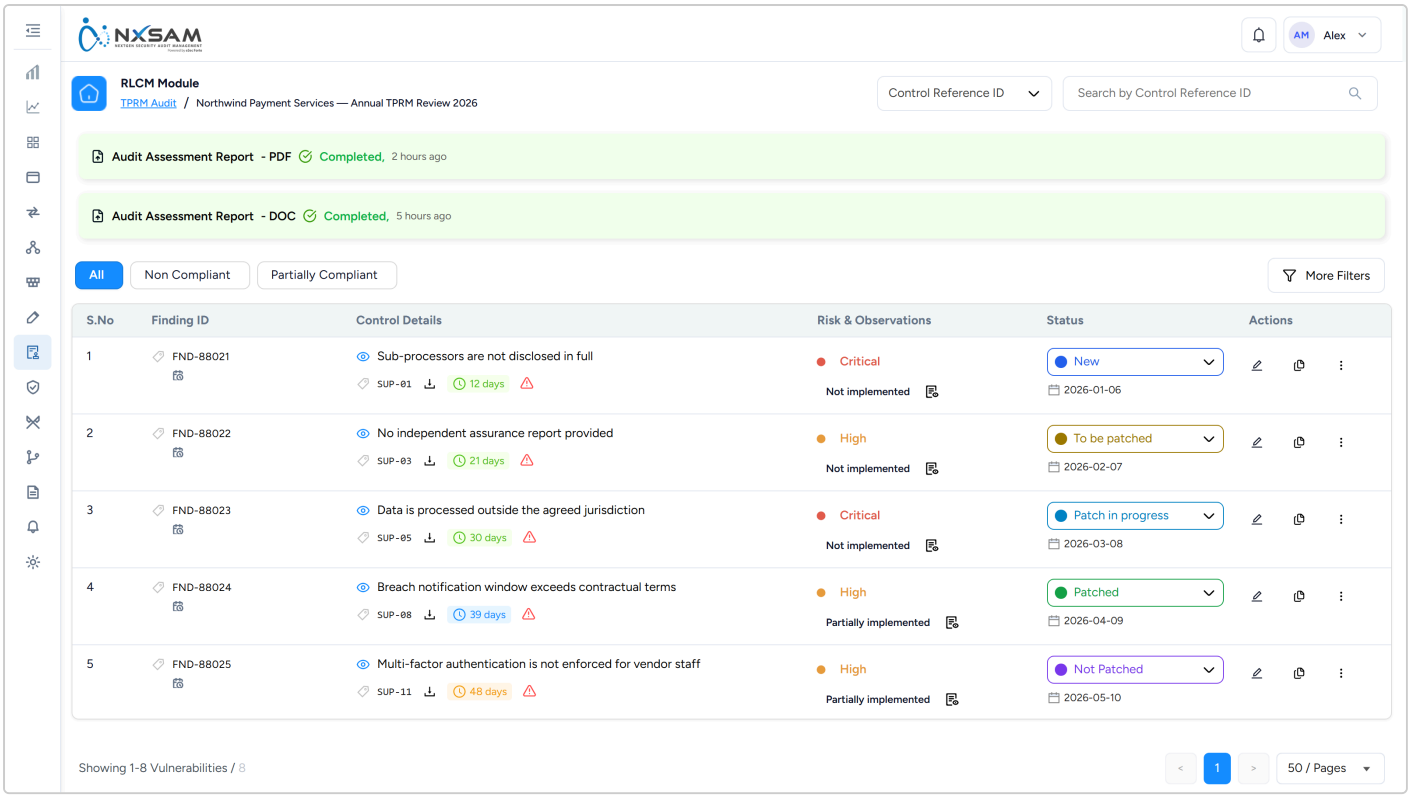


RLCM → TPRM → Master → TPRM Question Library

TPRM Risks

Risks arising from a vendor relationship rather than from your own estate.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

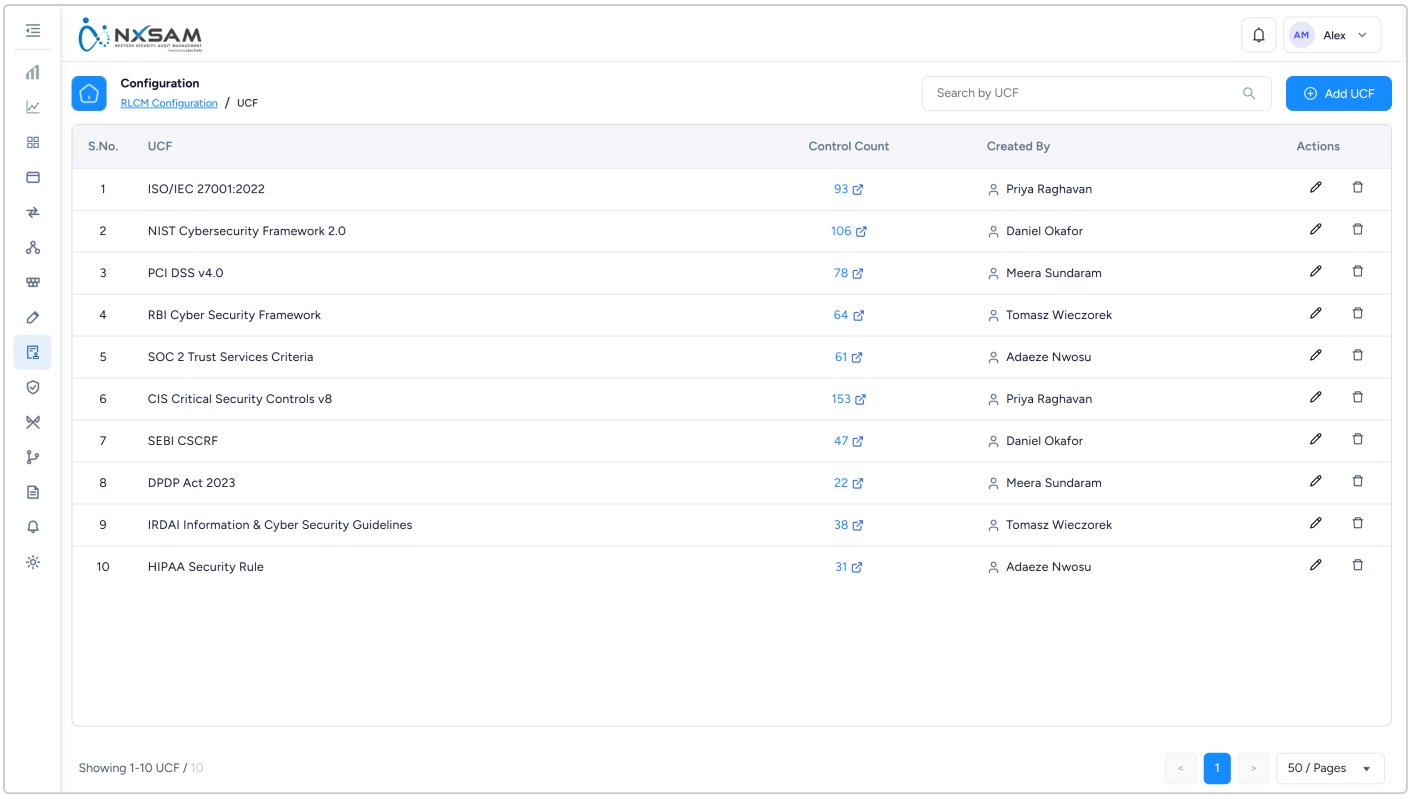


RLCM → TPRM → TPRM Risks

Unified Control Framework

One control mapped to the several frameworks that require it, so evidence is collected once and reused.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



RLCM → Unified Control Framework

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.