



NxSAM Deviations & Risk Acceptance — Quick Guide

Quick reference guide for the Deviations & Risk Acceptance 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

Deviations & Risk Acceptance

- Overview
- Request a deviation
- Deviations: every screen, column and action
- Deviations & Risk Acceptance: find the right screen

Reference

- Glossary

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Deviations & Risk Acceptance

Deviations & Risk Acceptance

Sometimes a vulnerability cannot be fixed within its SLA. The fix may need a vendor release, a change freeze may be in force, or the cost of fixing may genuinely outweigh the risk. A **deviation** records that decision formally — who asked, who approved, on what grounds, and until when.

The purpose is that accepting risk is a dated, reviewable decision with a name attached, rather than a finding quietly ageing out of sight.

The shape of a deviation

Requested by	The person asking to defer the fix
Justification	Why it cannot be fixed now, and what compensates for it
Approver	Determined by the approval configuration, usually by severity
Valid until	The date the acceptance stops being valid

How one moves through the system

1. **Raised** against a specific vulnerability, with a justification and a proposed end date.
2. **Routed** to an approver. Who that is depends on your approval configuration — more severe findings usually require more senior sign-off.
3. **Approved or rejected.** Rejection returns the vulnerability to normal tracking.
4. **Active** until its end date.
5. **Expired** once that date passes.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

What expiry means

When a deviation expires, the vulnerability returns to normal tracking. It does not re-open — it was never closed — but it stops being covered by an accepted-risk decision and appears again in the expired list for attention.

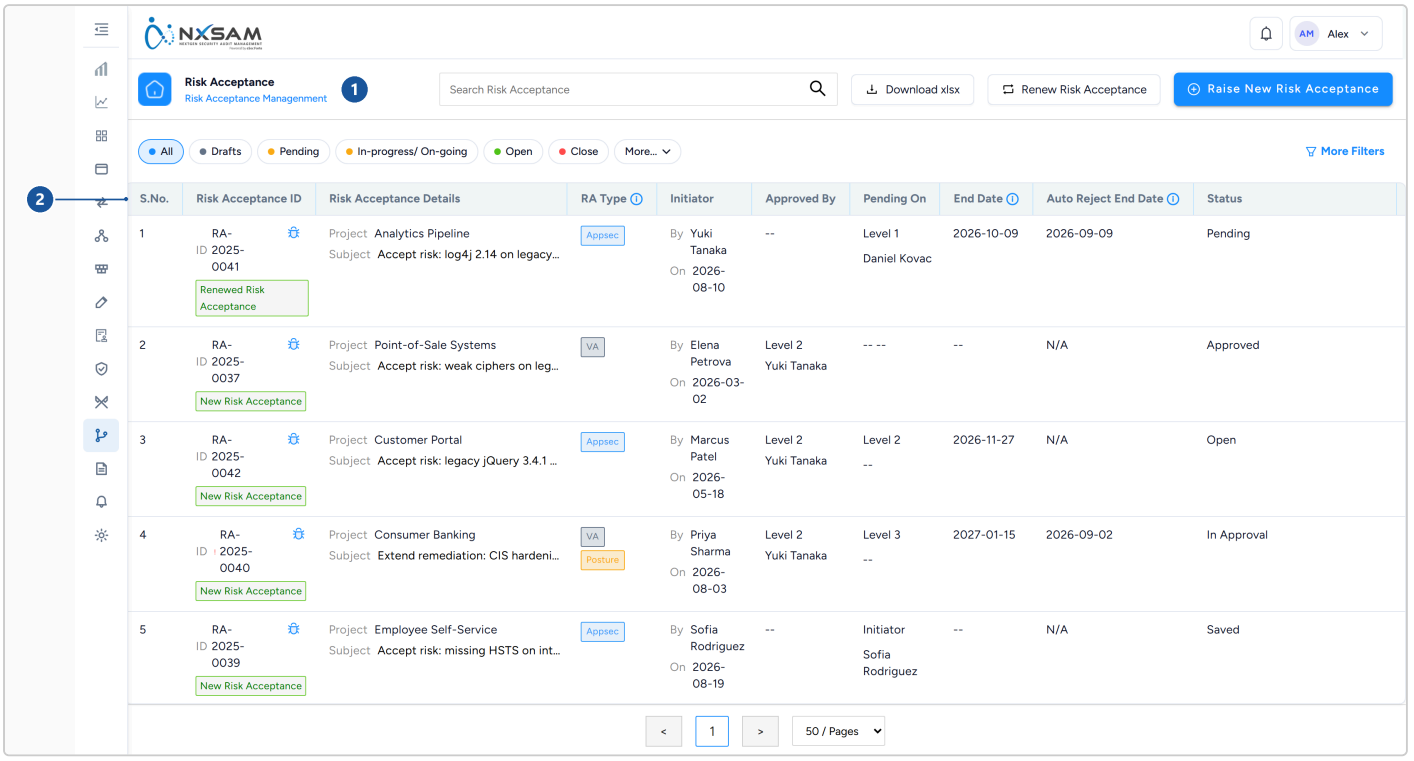
Expired deviations can be **renewed** if the situation genuinely has not changed. Renewal is a fresh decision with a fresh end date, not an extension of the old one, so it goes through approval again.

⚠ A deviation does not close the vulnerability

This is the most common misunderstanding. A finding under an approved deviation is still an open finding. It still appears in open counts, and depending on your configuration it may still age.

A deviation documents *why nothing is being done yet*. It does not assert the weakness is gone. Only validation of an actual fix does that.

Where to find things



Risk acceptances and their approval state.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

1 where you are · 2 approval state and expiry

Screen	Shows
Deviation Management	All deviations and their current state
Validated Vulnerabilities	Findings with an approved, still-valid deviation
Expired Vulnerabilities	Findings whose deviation has lapsed and now need attention

The Expired list is the one worth reviewing on a schedule. Items land there without anyone doing anything — the date simply passes — so nothing prompts you unless you look.

Configuration

Two settings shape how deviations behave:

- **Approval configuration** — who must approve, usually by severity.
- **Designation configuration** — which roles may request and which may approve.

Both are administrative settings. Changing them affects future requests, not decisions already made.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Request a deviation

Use this when a vulnerability genuinely cannot be fixed within its SLA — the fix needs a vendor release, a change freeze is in force, or the remediation carries more risk than the finding does.

Before you raise one

Be able to answer three questions. An approver will ask all of them.

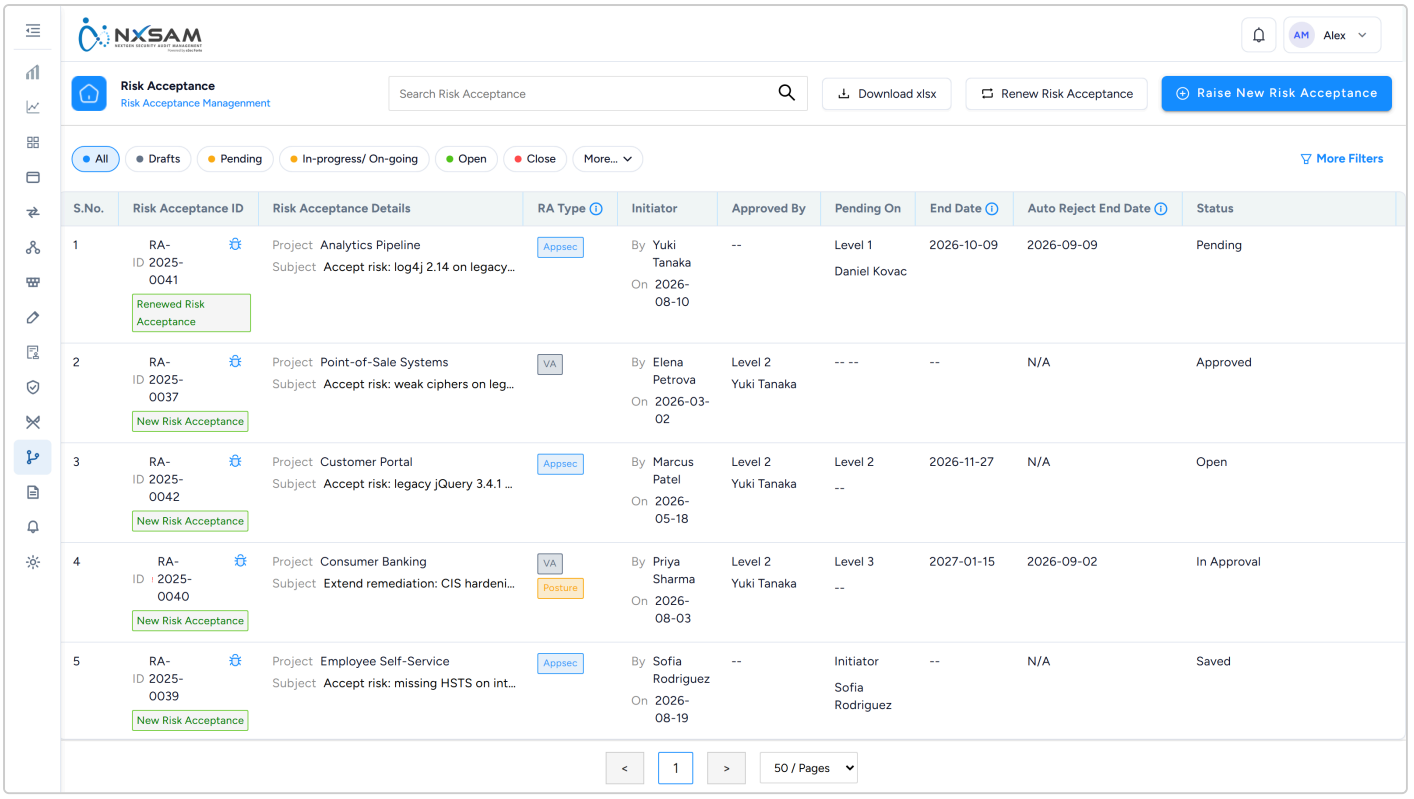
1. **Why can it not be fixed now?** A specific reason, not "no capacity".
2. **What reduces the risk meanwhile?** Compensating controls — restricted access, additional monitoring, network segmentation.
3. **When will it be fixed?** A date you can defend, not an open-ended extension.

Raising the request

1. Open the vulnerability.
2. Choose the option to request a deviation or risk acceptance.
3. Complete:
   - **Justification** — the answers to the three questions above.
   - **Valid until** — the date the acceptance should lapse.
   - **Compensating controls** — what is in place meanwhile.
4. Submit.

The request routes to an approver automatically, based on severity. More severe findings require more senior approval.

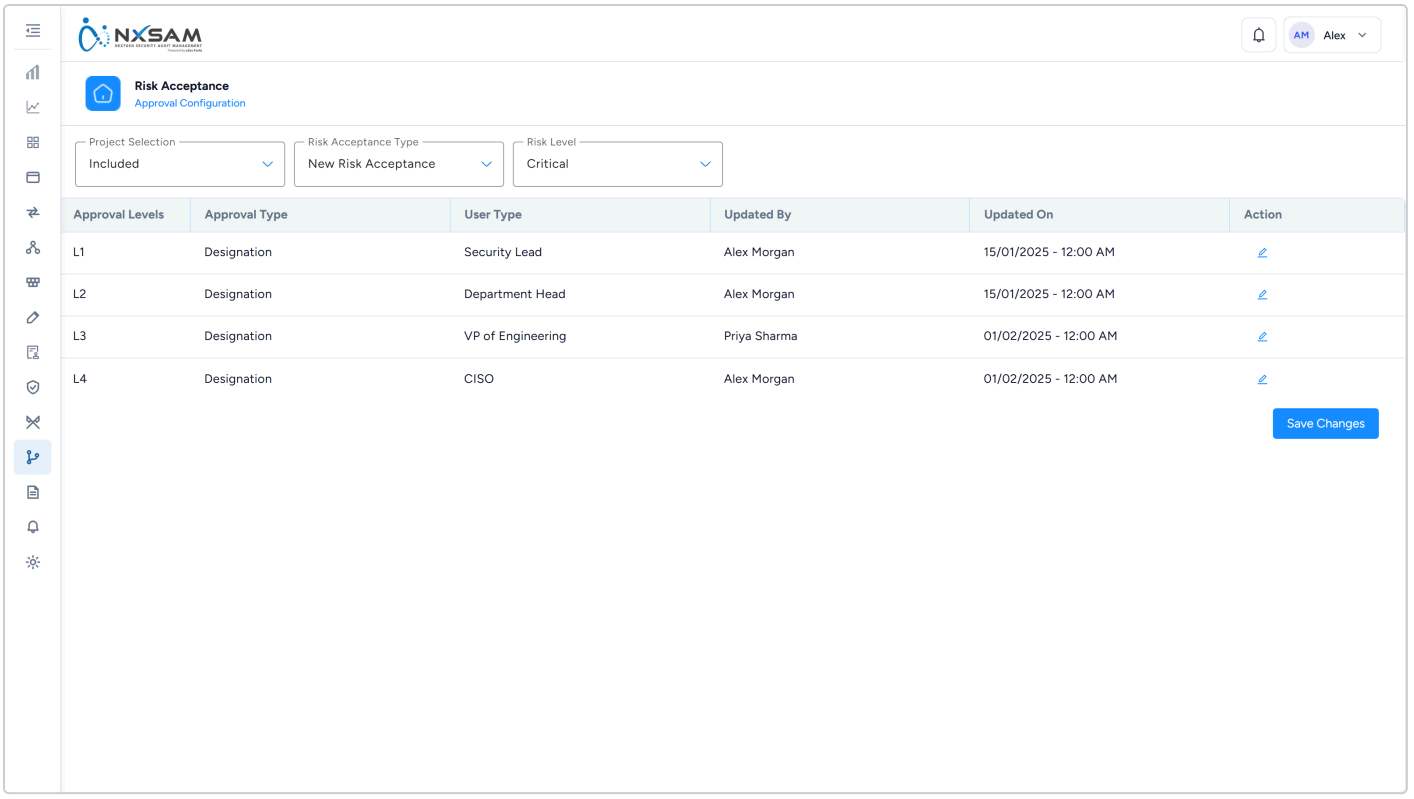
Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



Deviation Management → Deviations — every request, its state and the finding behind it

Which approver a request reaches is not decided per request: it follows the designation and approval-level configuration held under Deviation Management.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



Deviation Management → Approval Configuration — which designation approves which severity

After submitting

Outcome	What happens
Approved	The finding is covered until the end date
Rejected	It returns to normal tracking; remediate it
Expired	The end date has passed; it appears in the Expired list

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

⚠ The vulnerability stays open throughout

A deviation does not close a finding or remove it from open counts. It records *why nothing is being done yet*. The weakness is still there, and NxSAM still reports it as an exposure.

This surprises people who expect an approved deviation to clear the number. It does not, deliberately.

When it expires

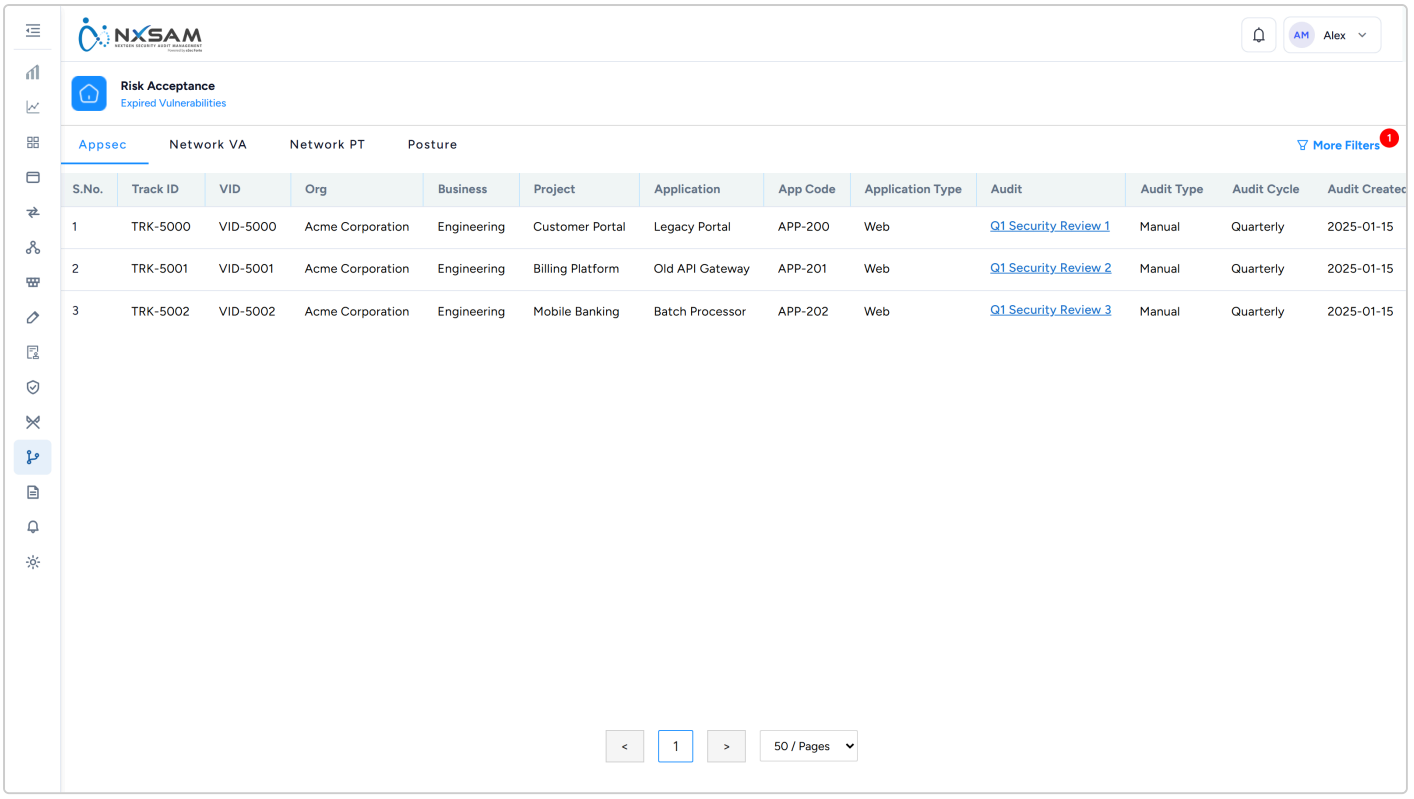
Nothing prompts you. The date passes and the finding appears in **Expired Vulnerabilities**.

You then either:

- **Remediate it** — the intended outcome, and the reason the deviation was time-limited.
- **Renew it** — if circumstances genuinely have not changed. Renewal is a *fresh* request with a fresh end date and fresh approval, not an extension.

Review the Expired list on a schedule. Items arrive there without anyone acting, so nothing draws attention to them.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



Deviation Management → Expired Vulnerabilities — acceptances whose end date has passed

Good practice

- **Keep periods short.** A three-month deviation reviewed on time is better governance than a two-year one nobody revisits.
- **Be specific in the justification.** It will be read by an auditor eventually, possibly long after everyone involved has forgotten the context.
- **Do not use deviations for false positives.** If the finding is not real, mark it a false positive. A deviation says "this is real and we accept it" — a materially different statement.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Deviations: every screen, column and action

A deviation is a decision not to fix something, recorded with an approval chain and an expiry. The module is mostly about who agreed and until when.

The deviation list

Column	What it holds
Risk Acceptance ID	The request identifier
Risk Acceptance Details	Subject and reason
RA Type	Which vulnerability types the acceptance covers — AppSec, VA, PT, Posture or RLCM
Initiator	Who raised it
Approved By	Who has approved so far
Pending On	Whose approval it is waiting for
End Date	When the acceptance expires

Row actions

View History, **Update Initiator**, **Delete Risk Acceptance**.

Update Initiator exists because acceptances outlive people. When the person who raised one leaves, the request would otherwise be pending on an account nobody uses — this reassigns it without restarting the approval chain.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

RA Type spans modules, which is why the module sits outside them

One acceptance can cover AppSec, VA, PT, Posture and RLCM findings together. That is deliberate: a decision to accept a risk is usually about a system, not about which scanner happened to find it.

It also means a finding can be under an acceptance raised from a module you are not looking at, which is the usual reason a finding shows as accepted with no visible acceptance in its own module.

Approval configuration

Screen	Columns
Approval levels	`Approval Levels`, `Approval Type`, `User Type`, `Updated By`, `Updated On`
Approver configuration	`Approval Levels`, `User Type`, `Approver Name`, `Status`, `Updated On`, `Comments`
Designations	`Designation Type`, `Users`, `Created By`, `Created On`

Approval is by **level**, and each level is satisfied by a **user type** or designation rather than by a named person. That is what lets the chain survive staff changes: a level requiring "Head of Infrastructure" is satisfied by whoever currently holds it.

Comments on the approver configuration record why a level was added or changed, which matters when an auditor asks who authorised the authorisation structure.

Deviation properties

`Property Name`, `Property Type`, `Mandatory`, `Info Hint`, `Sequence`, `Created By`.

Info Hint is the help text shown beside the field when someone raises a request. It is the cheapest place in the product to prevent bad requests — a mandatory "compensating control" field with a hint explaining what counts as one produces usable answers, and without the hint produces "N/A".

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Raising a deviation

The request form lists the findings being accepted:

Column	What it holds
vulVid	The finding's identifier
Observation	What was found
Recommendation	What was advised
Vulnerability Name and Status	The finding and **its status at the time the deviation was raised**
Audit Name	Where it came from
Asset Name	What it affects

> ⚠ **The status shown is historical, not current**
>
> The product states this on the screen itself: the status is the state of the vulnerability *when the deviation was raised*. A finding accepted while `New` still reads `New` on the acceptance months later, even if it has since moved.
>
> Read the finding's own screen for its current state. Reading the acceptance instead is the most common misinterpretation in this module.

Generate PDF Report produces the acceptance as a document — the artefact an auditor asks for, showing what was accepted, by whom, on what grounds and until when.

Bulk upload

Accepts **CSV** or **XLSX**, and covers **APPSEC / VA / PT / POSTURE** or **RLCM** — the two groups are uploaded separately because their identifiers differ.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

The queue reports `Status`, `Initiated By`, `Uploaded At`, **Download** and **Log File Download**. The log is the per-row outcome; a bulk upload that accepted fewer findings than expected explains itself there.

Validated and expired vulnerabilities

Both tables carry the full provenance of each finding:

`Track ID`, `VID`, `Org`, `Business`, `Project`, `Application`, `App Code`, `Application Type`, `Audit`, `Audit Type`, `Audit Cycle`, `Audit Created On`, `Audit Completed On`, `Audit First Reported On`, `Vulnerability Name`, `Severity`, `Risk Acceptance Expiry Date`, `Expired On`.

Risk Acceptance Expiry Date is the date the acceptance runs out — it was labelled *Risk Acceptance Date* in earlier releases, which read as the date it was granted. The value is unchanged; only the label is, and it now says what it always meant. Reports and the health-check rules that test it use the same wording.

Because an acceptance can cover findings from any module, the tables also carry the identifiers each module uses:

Column	Applies to
Tools	Which scanner reported the finding
QID / NEXPOSE ID / NESSUS ID	The scanner's own identifier — Qualys QID, Nexpose or Nessus id
Host, **Port**, **Protocol**	Network findings, where the acceptance is per service rather than per machine
Category	The finding's classification
Policy Name, **Control Name**	Policy Compliance findings, where the acceptance is against a control

The scanner identifier is what makes an acceptance verifiable. An auditor checking that an accepted finding is the one described will look it up by QID or plugin id in the scanner, not by the title — titles get rewritten, identifiers do not.

Audit First Reported On is the one that matters for an expiry dispute. It is when the finding was first raised, which may be several audits before the acceptance — so an acceptance expiring after six months can cover a finding that has been open for two years.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

The expired list is the module's most actionable screen: those acceptances have lapsed, so the findings are open again and, unless someone is watching this list, nobody has been told.

Vulnerability status history

`Audit ID`, `Audit Name`, `Severity`, `Vulnerability Status`, `Sub Status`, `Created On`, `Status Changed By`.

Sub Status carries the qualifier beneath the main status — which kind of acceptance, or which stage of an approval. Two findings both reading `Risk accepted` can differ in sub status, and that is what distinguishes a permanent acceptance from a temporary one.

Vulnerability summary

`Assets`, `Critical`, `High`, `Medium`, `Low`, `Info` — what an acceptance covers, at a glance, before approving it. An approver looking at a request for forty findings across twelve assets is being asked a different question from one looking at a single Low.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

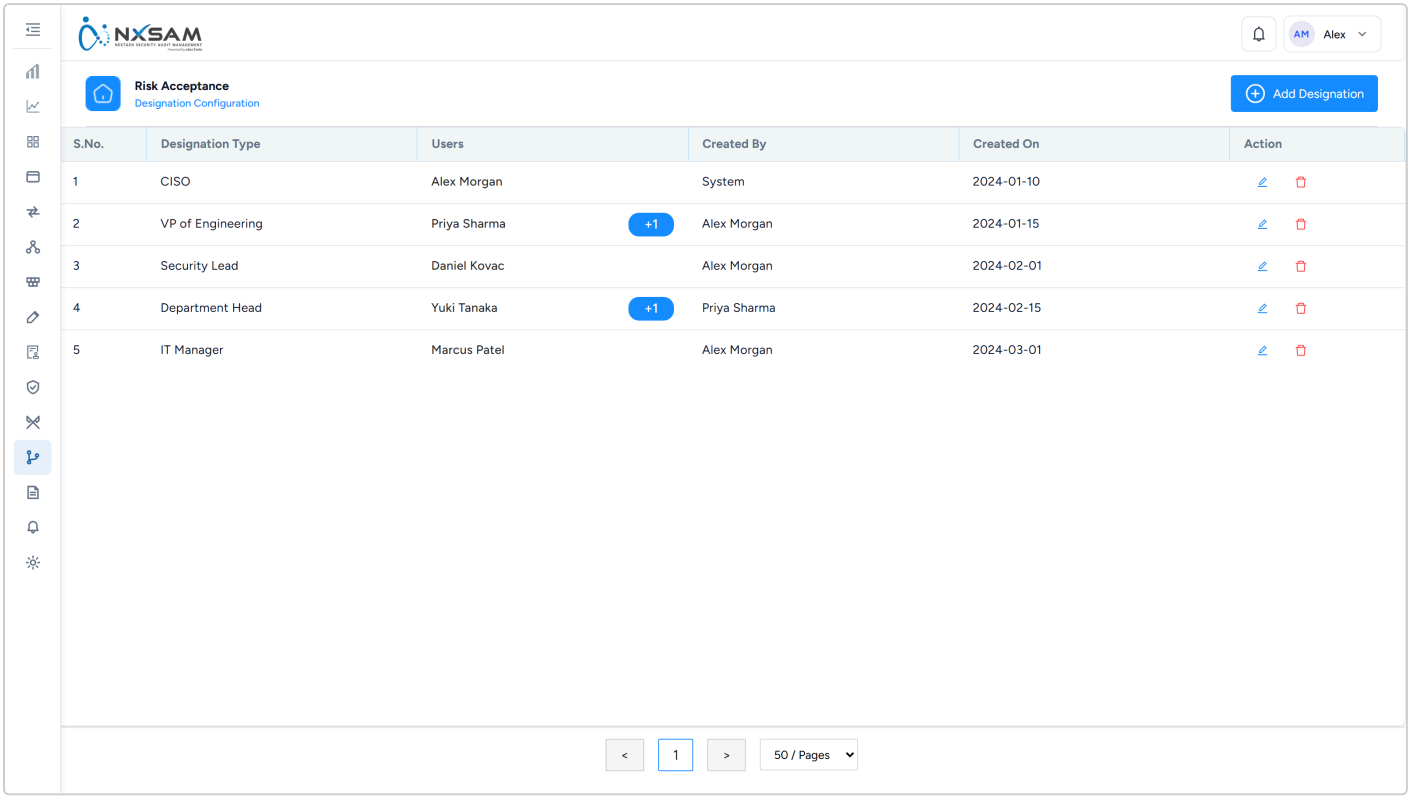
Deviations & Risk Acceptance: find the right screen

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.

Approver Designations

The roles that can approve, used to build the approval chain.

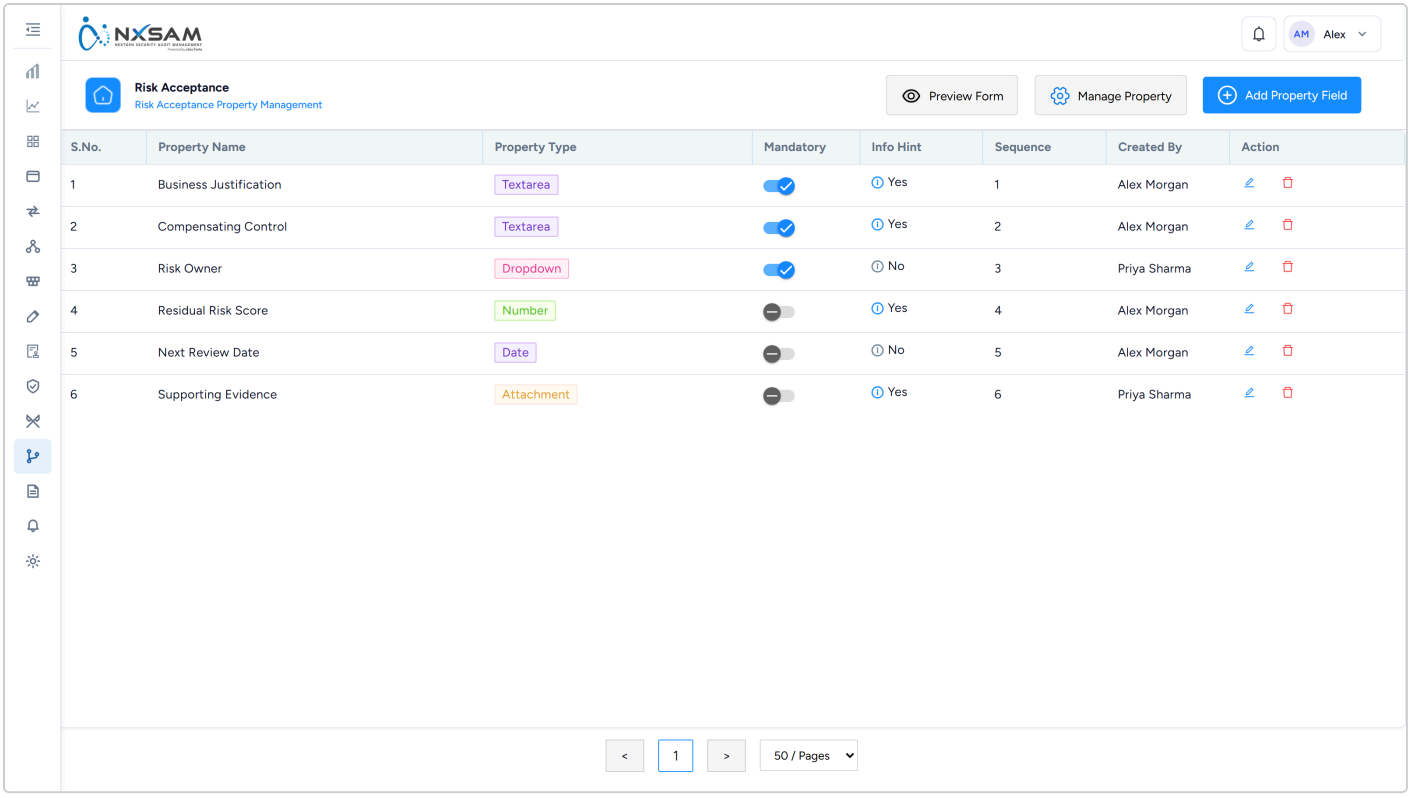


Risk Acceptance (RA) → Designation Configuration

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Deviation Properties

Additional fields captured on a deviation request, such as the compensating control.

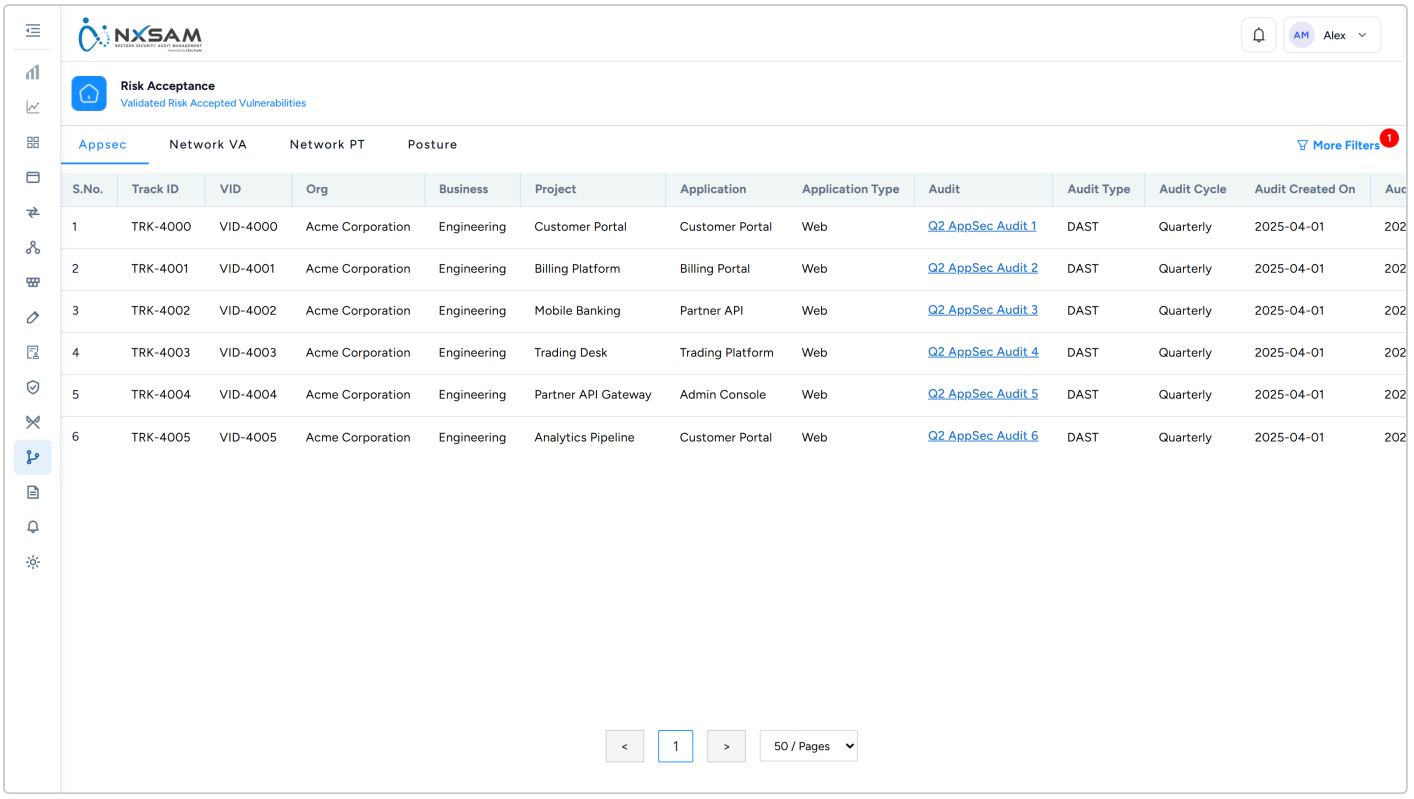


Risk Acceptance (RA) → RA Property Management

Validated Vulnerabilities

Findings covered by an accepted deviation, with the date that acceptance expires.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.



Risk Acceptance (RA) → RA Vulnerabilities

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.