





# NxSAM Reports — Quick Guide

Quick reference guide for the Reports 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

Reports

- Overview
- Build a report template
- Generate a report
- How a report is produced
- Reports: every screen, column and action
- Reports: find the right screen

Reference

- Glossary

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Reports

# Reports

Reports turn what NxSAM holds into something you can send to someone who does not use NxSAM — a board, an auditor, a customer, a regulator.

## The kinds of report

| | Use it for |
|---|---|
| **Assessment reports** | The findings of one audit, written up for the team that owns the application or infrastructure. |
| **Overall vulnerabilities** | Everything currently open across the estate, for management reporting. |
| **Report templates** | Reusable layouts so every report of a given kind looks the same. |
| **Custom report templates** | Your own structure, when the supplied layouts do not fit. |
| **Report search** | Finding a report generated earlier. |

## How generating one works

1. Choose the report and its scope — which audit, which assets, which period.
2. Submit it. Generation happens in the background.
3. The report appears in Reports Management when it is ready.
4. Download it.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

**Reports are generated, not rendered on demand**

A report is produced once and stored. It is a snapshot of the data at the moment it ran, which is what makes it valid to send to an auditor — it does not change after you have shared it.

The corollary is that a report does not update. If the data has moved on, generate a new one rather than expecting the old file to reflect it.

## Why a report can differ from the screen

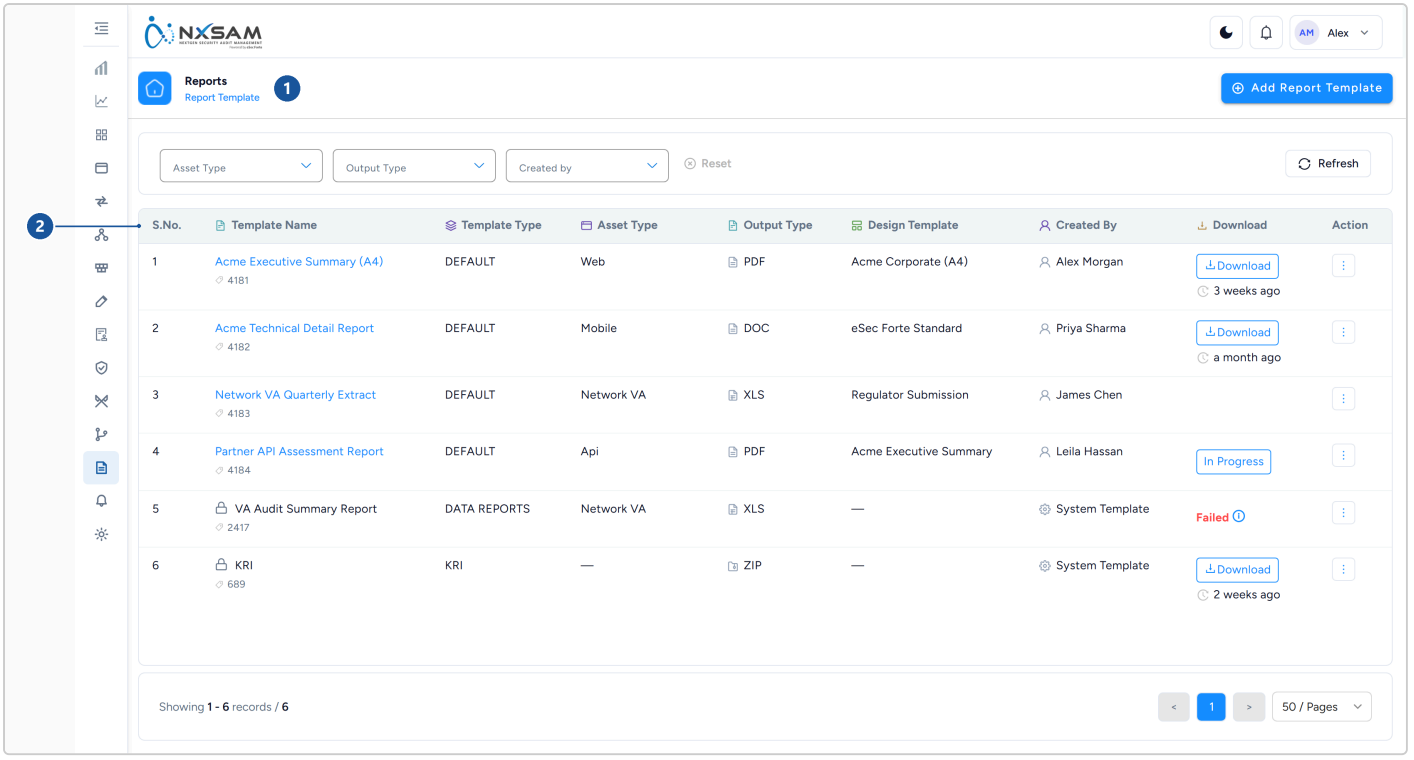
The single most common question about reports. Usually one of:

- **Time.** The report was generated earlier; the screen is live. SLA states in particular change as dates pass, with no data edit at all.
- **Scope.** The report covered one audit or one asset group; the screen is showing more, or less.
- **Inclusion rules.** Reports may exclude findings the screen includes — those awaiting approval, for instance.

Check the report's generation timestamp and scope before treating a difference as an error. Regenerating is the quickest way to confirm.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

# Templates




Report templates fix structure so reports are consistent whoever produces them.

1 where you are · 2 the template list

Templates control structure and appearance so reports are consistent regardless of who produced them. A template fixes which sections appear, in what order, and how findings are grouped and presented.

Editing a template affects **future** reports. Reports already generated are files, and files do not change.

# Scheduled and emailed reports

Where configured, reports can be produced on a schedule and emailed to a defined list. The practical benefit is that recipients who never sign in still receive the picture.

Two things to keep in mind:

- The recipient list is part of the schedule's configuration, so people who join or leave a team need it updated.

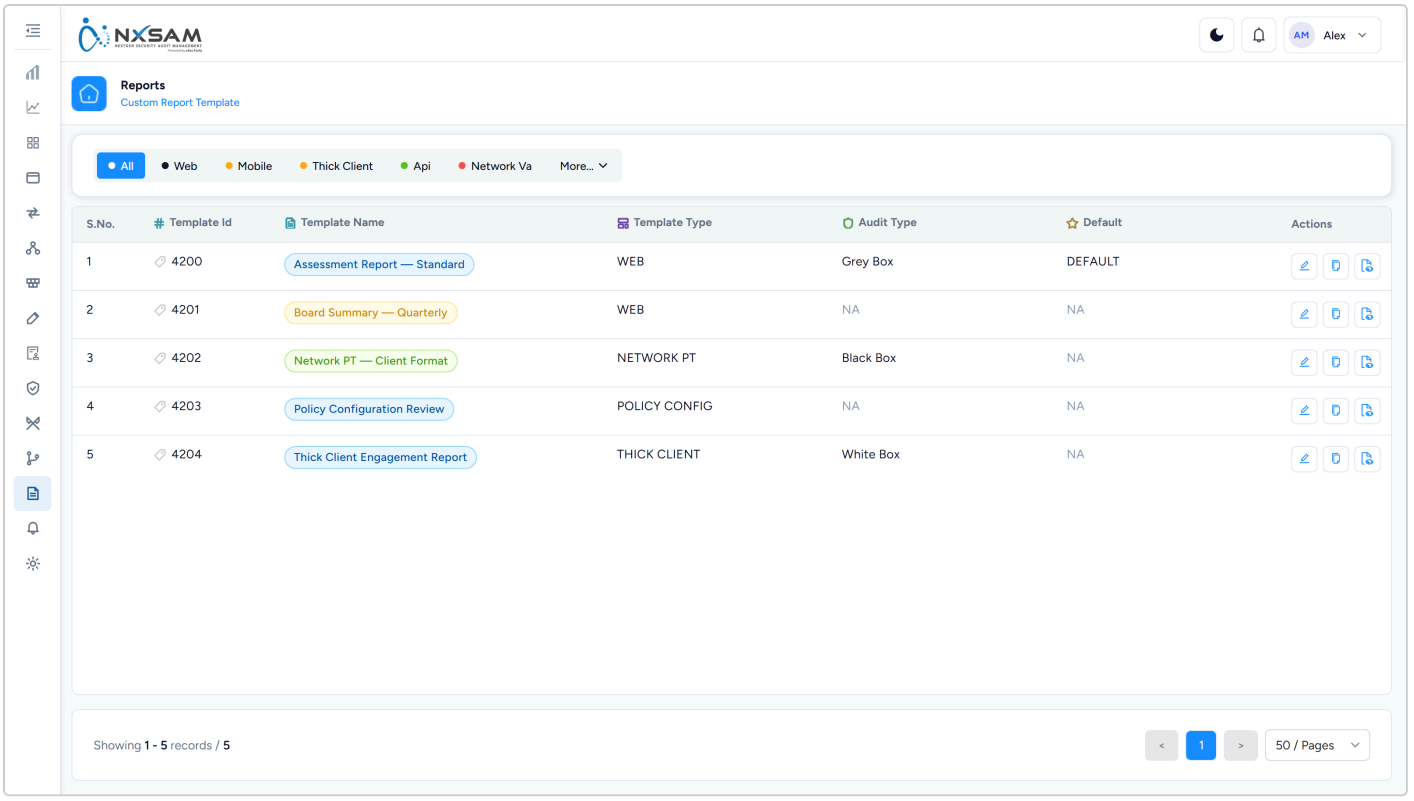
Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

- A scheduled report reflects the data at the moment it ran, which is normally overnight. A recipient comparing it against the live screen later in the day will see differences, and those differences are expected.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

# Build a report template

A report template decides what a generated report contains and in what order. Templates are yours to define: the supplied ones are a starting point, not a limit, and most organisations end up with several — one for an internal technical audience, one for a customer or regulator, one for the board.




Reports → Custom Report Templates

## 1. Create the template

**Add Template** asks for the frame the document sits in:

| Field | What it decides |
|---|---|
| **Template Name** | How it appears when someone generates a report |

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

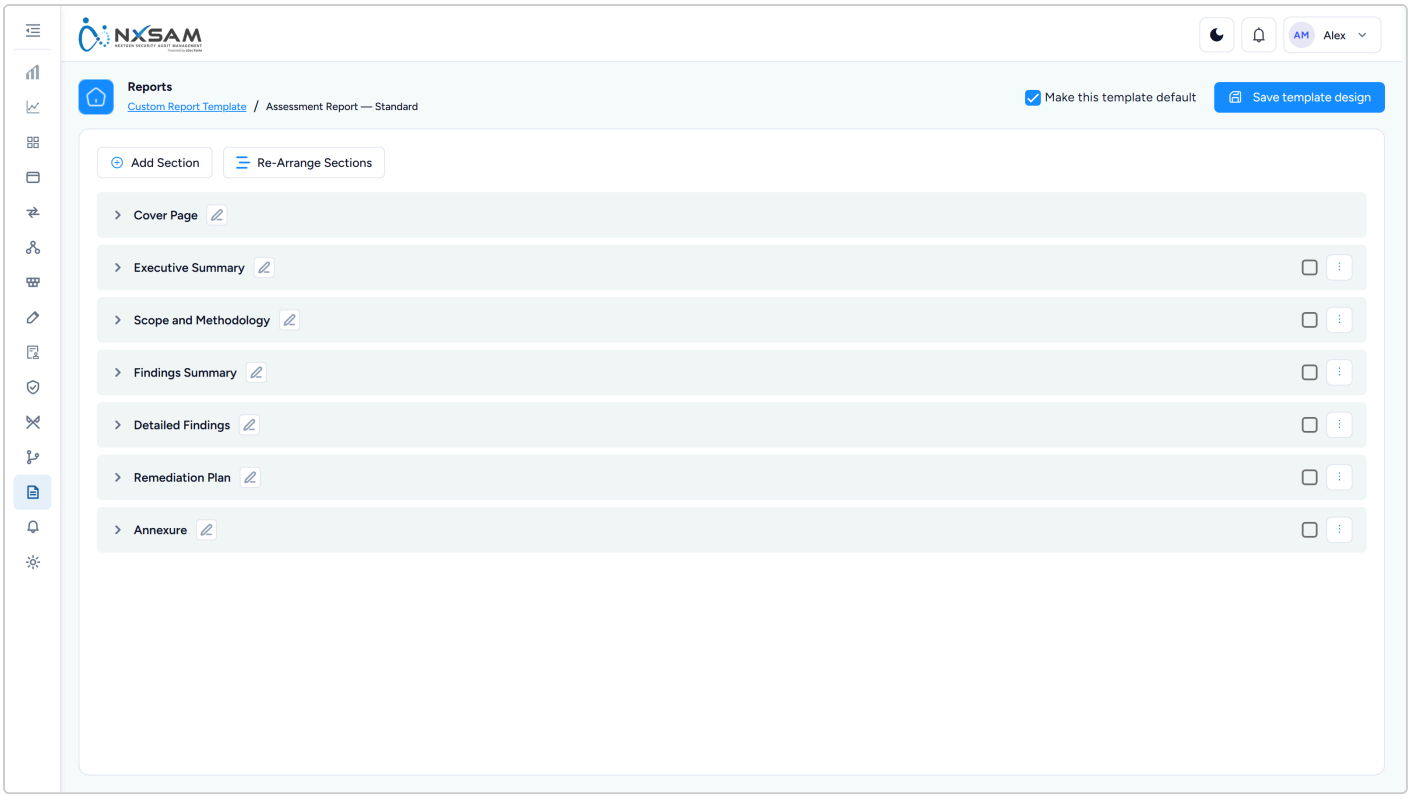
| Field | What it decides |
|---|---|
| **Report Type** | Which kind of report this template can produce — it decides which content blocks are available later |
| **Asset Type** | Which assets it applies to |
| **Report Format** | The output the template targets |
| **Design Template** | The visual design the document is rendered with |
| **Document Version**, **Author**, **Approved By** | Printed on the cover, and the fields an auditor looks for first |
| **Organization**, **Address**, **Contact Details**, **Email**, **Phone Number** | The issuing party's details on the cover |

Nothing here is the *content* of the report — that comes next, and it is where the work is.

## 2. Add sections

Open the template's **Sections**. A section is a chapter of the document.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.




Reports → Custom Report Templates → Sections

Each section carries three actions:

| Action | What it does |
|---|---|
| **Edit Section Name** | Rename it. Names are unique within a template and capped at 50 characters |
| **Add Sub-Section** | Adds a block of content inside the section |
| **Re-Arrange Sub-Sections** | Changes the order within the section |

**Section Position** decides where a new section lands. Order is part of the deliverable: a report whose executive summary follows the technical appendix is a different document to its reader, and no amount of correct content fixes that.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

## 3. Fill the sections

A sub-section holds either content you write or content the platform generates.

**Written content** is edited directly — headings, paragraphs, tables, and an image you upload for a diagram, an architecture sketch or a signature block. This is where scope statements, methodology, disclaimers and conclusions live: the parts that are the same in every report and should not be retyped.

**Generated content** is a block the platform fills at generation time from the audit the report covers. The blocks available depend on the report type, and include:

| Block | What it renders |
|---|---|
| **Assets in Scope** | What was assessed — affected IP, URL or application, asset group, classification |
| **Application / Audit Details** | The audit's own particulars, owner and phase |
| **Asset-Wise Vulnerability Statistics** | Counts per asset |
| **Findings by Severity / Status / Category** | The three standard breakdowns |
| **Closed Vulnerability List** | What was fixed, for a re-test or closure report |
| **CVE / CWE references** | The identifiers a technical reader cross-references |
| **Confirmatory rounds** | Separate columns per re-test round, so a report can show a finding's history across up to six confirmatory audits |

The point of the split is that written content is stable and generated content is current: you write the methodology once, and every report produced from the template carries this month's findings under it.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

## 4. Set the default

**Default** marks the template used when someone generates a report without choosing one. Changing which template is default changes what everyone who does not think about it produces — worth announcing rather than doing quietly.

## Sharing a template

| Action | What it does | When |
|---|---|---|
| **Share View** | One template, one owner. Your later edits reach everyone using it | A standard the organisation should follow |
| **Share Copy** | An independent copy that will drift from yours | A starting point someone will adapt |
| **Manage Config** | Which properties the template includes | Tuning what a shared template shows |

The choice matters more than it looks. Share View keeps a house style consistent and means a correction reaches every user; Share Copy hands over ownership and accepts divergence.

**Test a template before it is used in anger**

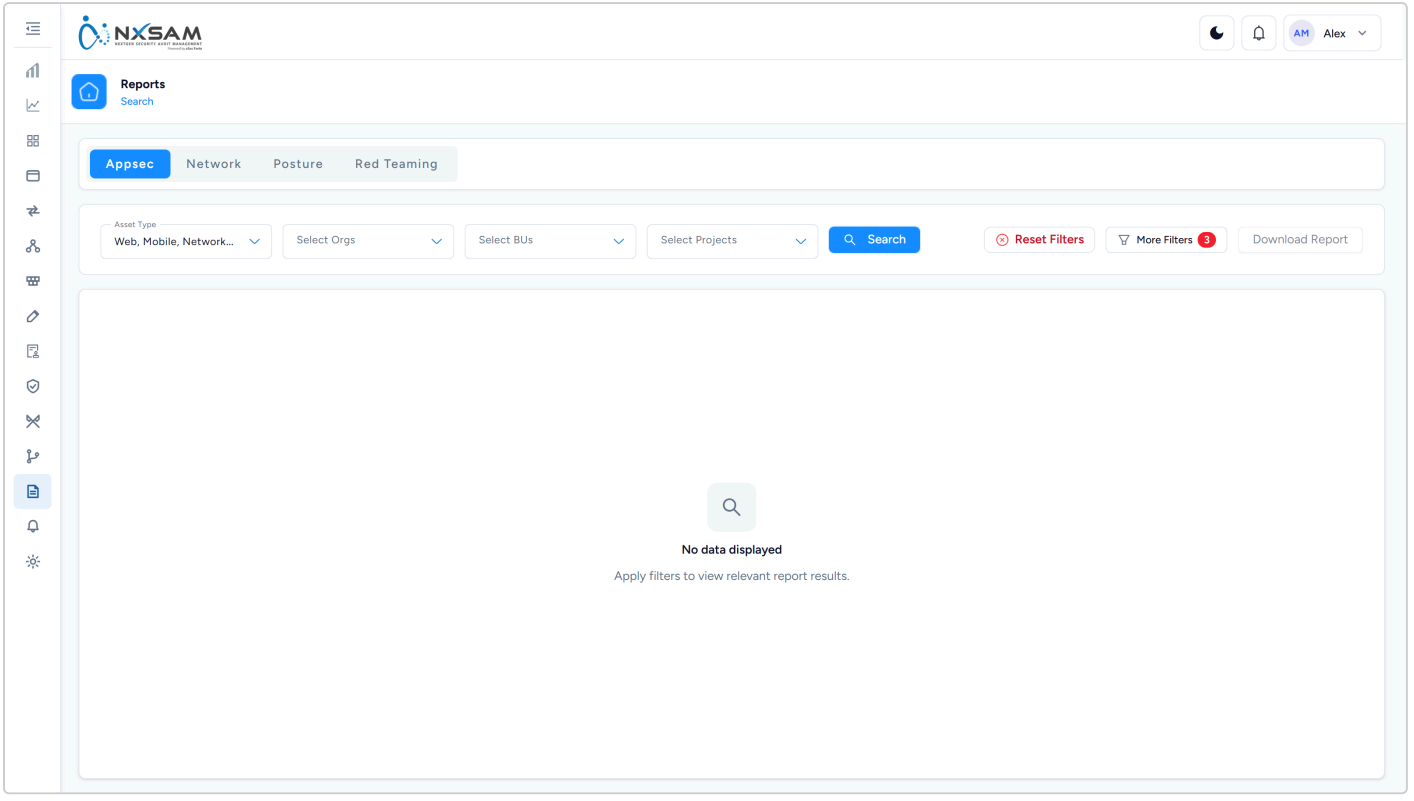
Generate one report from a new template against a real audit and read it end to end. Section order, an empty generated block, or a placeholder left in written content are all obvious in the output and nearly invisible in the builder.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

# Generate a report

## Steps

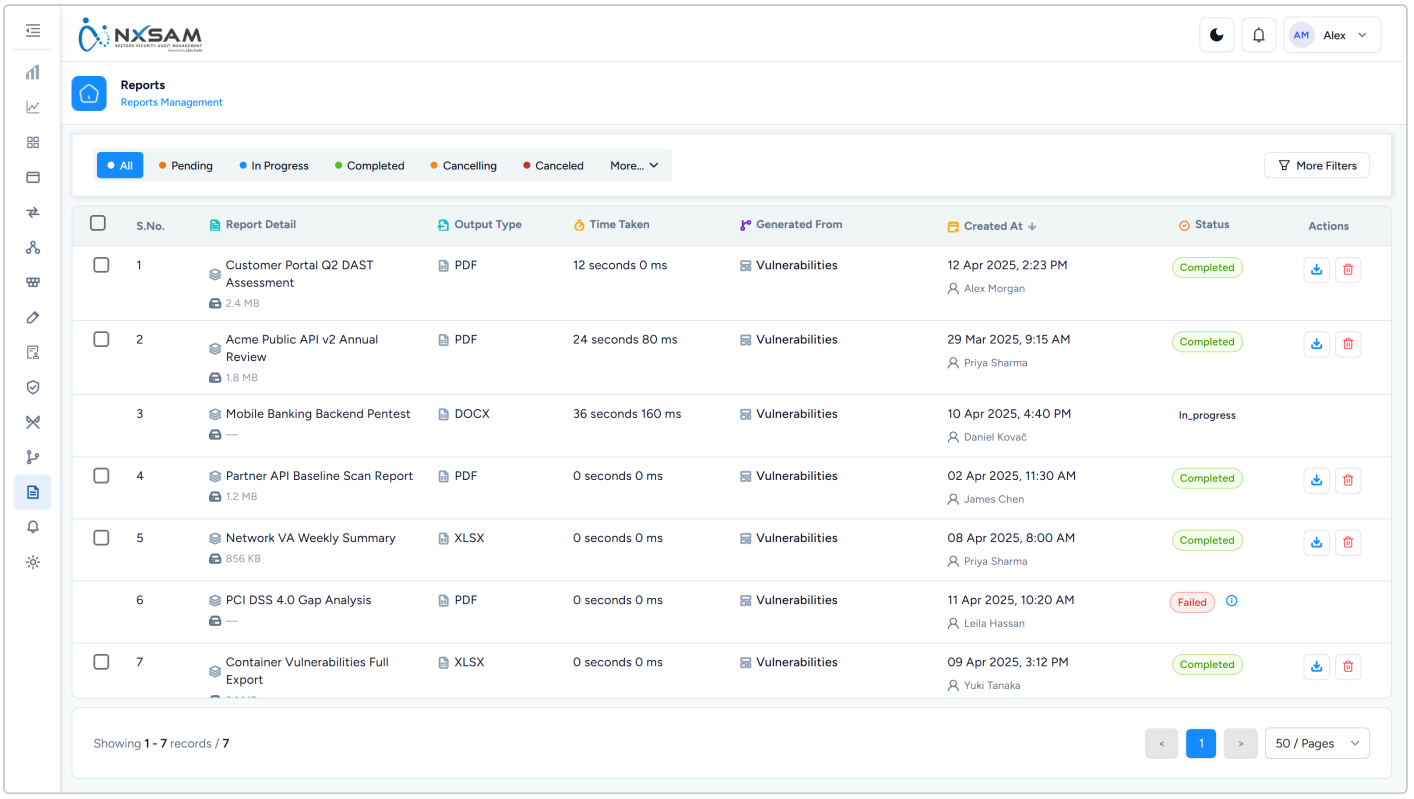
1. Go to **Reports** and choose the kind you need:
   - **Assessment report** — the findings of one audit
   - **Overall vulnerabilities** — everything currently open, across the estate
2. Set the scope — which audit, assets, or period.
3. Choose a template if more than one is available.
4. Submit.




Reports → Reports — choosing what a report covers before generating it

Generation happens in the background. The report appears in Reports Management when it is ready, and you download it from there.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.




Reports → Reports Management — generated reports, their state, and the download

### It is queued, not instant

A large report takes time. If it has not appeared, it is usually still being prepared rather than failed.

## Choosing the right scope

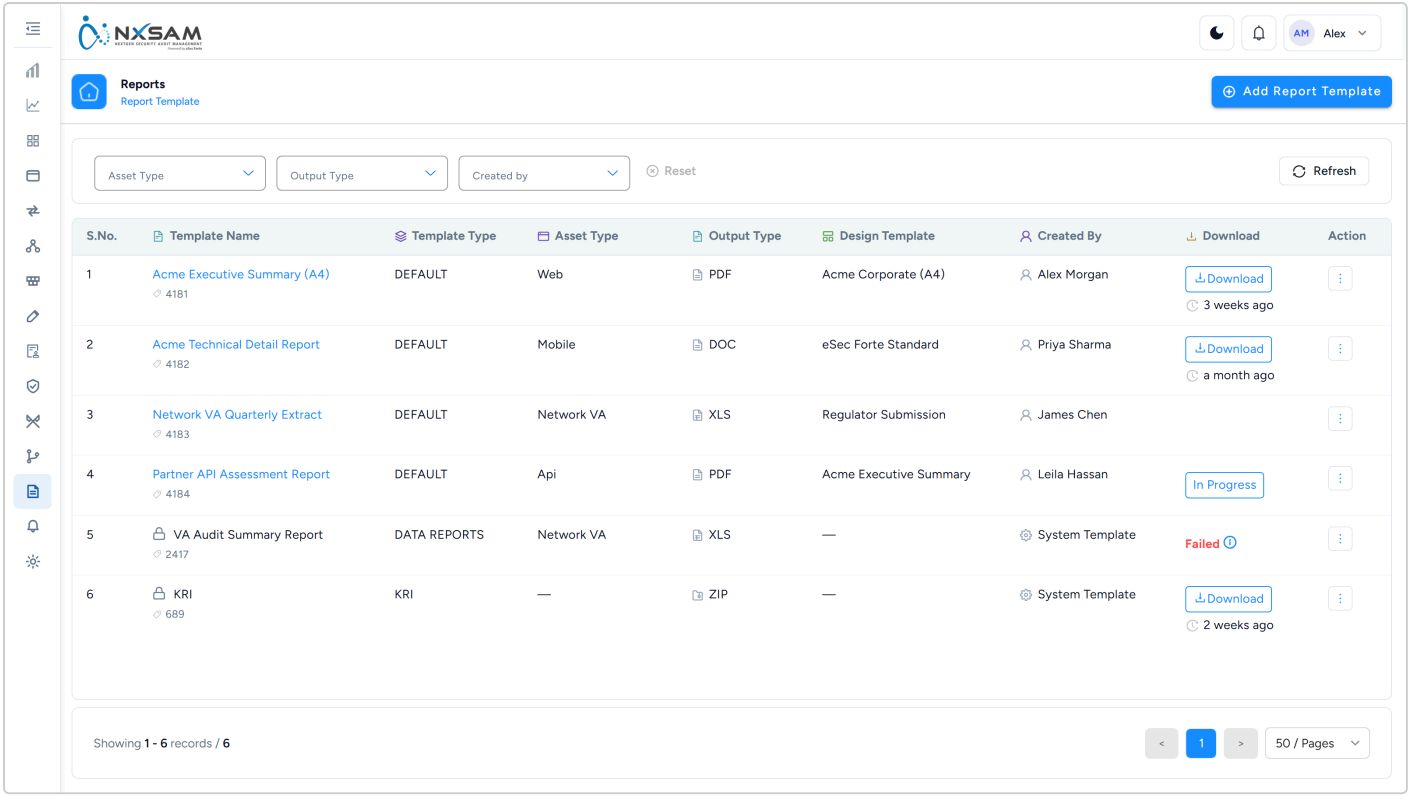
The most common cause of a report being wrong is scope rather than data.

| You want | Scope to |
|---|---|
| What we found in this assessment | The specific audit |
| Everything open right now | The whole estate, no audit filter |
| One team's position | Their business unit or project |

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

| You want | Scope to |
| --- | --- |
| One application's history | The asset, across audits |

Which template you pick decides the sections and the cover, not the data — two templates over the same scope contain the same findings.




Reports → Report Templates — the templates available when generating

## What the report contains

A report is a **snapshot**, produced once and stored. That is what makes it valid to send to an auditor — it does not change after you have shared it.

It also means the report will not update. If the data has moved on, generate a new one.

## Why a report can differ from the screen

Almost always one of three things:

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

1. **Time.** The report was generated earlier; the screen is live. SLA states change as dates pass, with no data edit at all.
2. **Scope.** The report covered a narrower or wider set than the screen is showing.
3. **Inclusion rules.** Reports may exclude findings the screen includes — those awaiting approval, for instance.

Check the generation timestamp and scope before treating a difference as an error.

## Sharing

Reports download as files. Consider before sending:

- **Sensitivity.** A vulnerability report is a map of your weaknesses. Treat it accordingly.
- **Age.** Include the generation date when you share, so the recipient knows what it reflects.
- **Audience.** An assessment report suits the team that owns the system; an overall report suits management.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

# How a report is produced

Report tickets divide almost evenly between "it never arrived" and "the numbers are wrong", and the two have completely different causes.

## It is a queued job, not a download

Requesting a report publishes a message. A separate rendering service consumes it, builds the document, and stores the file. Only then does it appear in Reports Management.

```
request → queued → renderer consumes → document built → stored → downloadable
```

Nothing about that is instant, and a large report legitimately takes minutes. The request returning successfully means the job was accepted, not that the report exists.

## "The report never arrived"

Check in this order:

1. **Is the job queued or failed?** Process Manager distinguishes the two immediately. `PENDING` means nothing consumed it; `FAILED` means the renderer ran and errored.
2. **Are other queued things also stalled?** Reports, imports and outbound email share the same broker. If all three are stuck, the report is a symptom, not the problem.
3. **Was it scheduled rather than requested?** A scheduled report runs on its own timetable — usually overnight — and did not run because it was not yet due.
4. **Was it emailed to a list you are not on?** Scheduled reports go to a recipient list configured on the schedule, which is maintained separately from user accounts. People who join or leave a team do not get added or removed automatically.

A report that failed for one scope and succeeds for a narrower one is usually a size problem: a report covering the entire estate over a long period can exceed what the renderer will complete.

## "The numbers are wrong"

Nearly always one of four things, and only the last is a defect.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

**The report is older than the screen.** A report is a snapshot at the moment it ran. SLA states in particular change with the passage of time alone — a finding that was approaching expiry when the report ran is overdue today, with no data edit involved. Check the generation timestamp first; it resolves this immediately.

**The scope differs.** The report covered one audit, one asset group or one period. The screen is showing something wider or narrower. This is the most common cause of a disagreement in absolute counts.

**Inclusion rules differ.** Reports may exclude findings awaiting approval, or audits not marked as considered — the same rules that make dashboards disagree with module screens. See the two-status-fields workflow.

**The template selects different fields.** A custom template that groups by a different property will legitimately produce different subtotals from the same data.

> **Regenerating is the fastest diagnostic**
>
> If a regenerated report matches the screen, the original was simply old, and nothing is wrong. That single step resolves a large share of these tickets before any investigation.

## Templates apply going forward

Editing a template changes future reports. Documents already produced are files on disk and do not change retrospectively — which is the point, since a report already sent to an auditor must not silently alter afterwards.

If someone needs the old report in the new format, it has to be regenerated, and it will then also pick up any data changes since the original run.

## What to collect before escalating

- The report type and the template used
- The generation timestamp and the scope it was run for
- The queue status, if it never arrived
- Whether a regeneration reproduces the discrepancy

The last one matters most: a discrepancy that disappears on regeneration was a timing artefact, and one that survives it is worth investigating.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

# Reports: every screen, column and action

Complements How a report is produced. This page covers the screens — the template library, the search views and the very wide export tables behind them.

## Reports Management

| Column | What it holds |
|---|---|
| **Report Detail** | What was generated |
| **Output Type** | PDF, XLSX, DOCX, CSV |
| **Time Taken** | How long generation took |
| **Generated From** | Which template or screen produced it |
| **Created At** | When |
| **Status** | Queued, generating, complete or failed |

**Time Taken is the column to look at when reports start failing.** A report that normally takes two minutes and now takes twenty is heading for a timeout, and the trend is visible here before anyone reports a failure.

## Assessment reports

`Application Name`, `Report Details`, `Audit Name`, `Size (MB)`, `Created By`, `Created On`, `Updated On`.

**Size (MB)** matters because assessment reports are emailed. A report past your mail gateway's attachment limit will generate successfully and never arrive, and this is the only place the size is visible before someone reports it missing.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

## Report templates

| Column | What it holds |
|---|---|
| **Template Id / Template Name** | Identity |
| **Template Type** | The kind of report |
| **Asset Type** | Which assets it applies to |
| **Output Type** | The format it produces |
| **Design Template** | The layout it renders through |
| **Created By** | Who defined it |
| **Download** | Retrieves the template itself |

### Row actions — seven

| Action | What it does |
|---|---|
| **View Template** | The template as defined |
| **Edit Template** | Change it |
| **Run Template** | Generate a report from it now |
| **Manage Config** | Which properties the template includes |
| **Share View Template** | Grants read access to another user |
| **Share Copy Template** | Gives another user their own copy |
| **Delete Template** | Removes it |

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

> **Share View and Share Copy are different commitments**
>
> **Share View** leaves one template with one owner — your later edits reach everyone using it. **Share Copy** creates an independent template that will drift from yours and never receive your corrections.
>
> Copy is right when another team needs to diverge. View is right when consistency matters, which for a report going to a regulator it usually does.

**Manage Config** carries `Property Name`, `Select Property`, `Check Linked Assets`. **Check Linked Assets** decides whether the report follows relationships — pulling in the hosts an application runs on, for instance — which changes both the content and how long generation takes.

**Run Template** opens a host selection of `Host IP`, `Host Name`, `Application Name`, `Application Code`, so a template can be run against a subset rather than everything it is scoped to.

## Custom report templates

`Template Id`, `Template Name`, `Template Type`, `Audit Type`, `Default`.

Section editing offers **Add Sub-Section**, **Edit Section Name** and **Re-Arrange Sub-Sections**. Order is part of the deliverable: a report whose executive summary appears after the technical appendix is a different document to its reader.

**Default** marks the template used when none is chosen. Changing which template is default changes what everyone generating a report without thinking about it produces.

**Build a report template** walks the whole sequence — the cover fields, sections and their order, the difference between written and generated content, and what Share View versus Share Copy commits you to.

## Report search

The widest table in the product. Every attribute a finding carries, so a report can be built by filtering rather than by writing a template:

`Vuln #`, `Issue Type`, `Issue #`, `Org`, `BU`, `Project`, `Application`, `Bifurcation Type`, `App code`, `Application Type`, `Application Facing`, `Audit`, `Audit Type`, `Audit Category`, `Audit Considered`, and the finding's own fields.

Row actions: **Vulnerability History**, **View SLA History**, **View Advisories**.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

**Audit Considered as a filterable column** is what makes this screen useful for reconciliation. Filtering to considered audits reproduces the dashboard's numbers; including everything reproduces the module screens. Comparing the two answers most "why do these disagree" questions directly.

## Findings across modules in one report

Because a report can span modules, the search and export tables carry each module's own identifiers alongside the shared ones:

| Column | Applies to |
|---|---|
| **VID** | The finding's own identifier |
| **CVE** | Network and container findings carrying an advisory |
| **Title** | The finding name as its source reported it |
| **Technology** | The stack the asset is built on |
| **Network Types** | The network classification of a host |
| **Policy Details** / **Posture Status** | Policy Compliance rows — which benchmark, and pass, fail or error |
| **Opened on Date** | When the finding was first opened |

A single export therefore mixes rows where some columns are empty by nature — a Policy Compliance row has no CVE, a container row has no policy. Empty cells in this table are a consequence of combining modules, not missing data.

## SLA history

`SLA Expiry Date`, `Audit ID`, `Audit Name`, `Updated By`, `Created At`.

An SLA expiry can change — because the severity changed, because the SLA configuration changed, or because someone adjusted it. This is the record of that, and it is what settles a dispute about whether a finding was overdue at a particular moment.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

# The overall vulnerability report

`Ticket ID`, `Key`, `Org`, `BU`, `Project`, `Audit Details`, `Vuln Details`, `Application Details`, `Asset Property`, `Host Details`, `Source Details`, `Port & Protocol`, `Group Details`, `Control ID`, `Plugin ID`.

Actions: **History**, **View Advisories**. The page offers **Overall report** and **Old overall report** — the current format and the previous one, kept because customers build their own tooling on the export and cannot always switch formats on your schedule.

## The detail tables behind it

**Vulnerability detail** — `Ticket ID`, `Risk Acceptance Expiry Date`, `Risk Acceptance Comment`, `First Reported On`, `Last Observed Date`, `Duration(In Days)`, `Score`, `SLA Expiry Date`, `Is Overdue`, `Vulnerability Status`, `Vulnerability Sub Status`.

**Duration (In Days)** is the age of the finding, and read against `First Reported On` it is the number that appears in board reporting. It counts from first report, not from the current audit — so a finding carried through four audits shows its true age.

**Audit detail** — `Audit Cycle`, `Audit Scope Length`, `Initial/Confirmatory`, `Audit Assigned On`, `Assigned Auditor Name`, `Audit Completed On`.

**Application detail** — `Org`, `BU`, `Project`.

## Applications with no findings

Two tables cover the assets a report found nothing on:

**No-vuln application detail** — `App Code`, `Asset Name`, `Internet Facing`, `Priority`, `Host Accessibility`, `Asset Type`, `OS`.

**No-vuln audit detail** — `Audit Cycle`, `Audit Created On`, `Audit Assigned On`, `Assigned Auditor Name`, `Audit Completed On`.

### A clean asset is evidence, and it needs the audit detail to be believable

"No findings" means nothing on its own — it could mean assessed and clean, or never assessed. The paired audit detail is what distinguishes them: an asset with a completed audit and no findings is evidence, and one with no audit is a coverage gap.

This is why the report carries both tables rather than simply omitting clean assets.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

## Vulnerability history

`Audit ID`, `Audit Name`, `Risk`, `Vulnerability Status`, `Sub Status`, `Discovered Date`, `Created On`, `Status Changed By` — the same shape as the module histories, so a finding traced from a report reads identically to one traced from its module.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

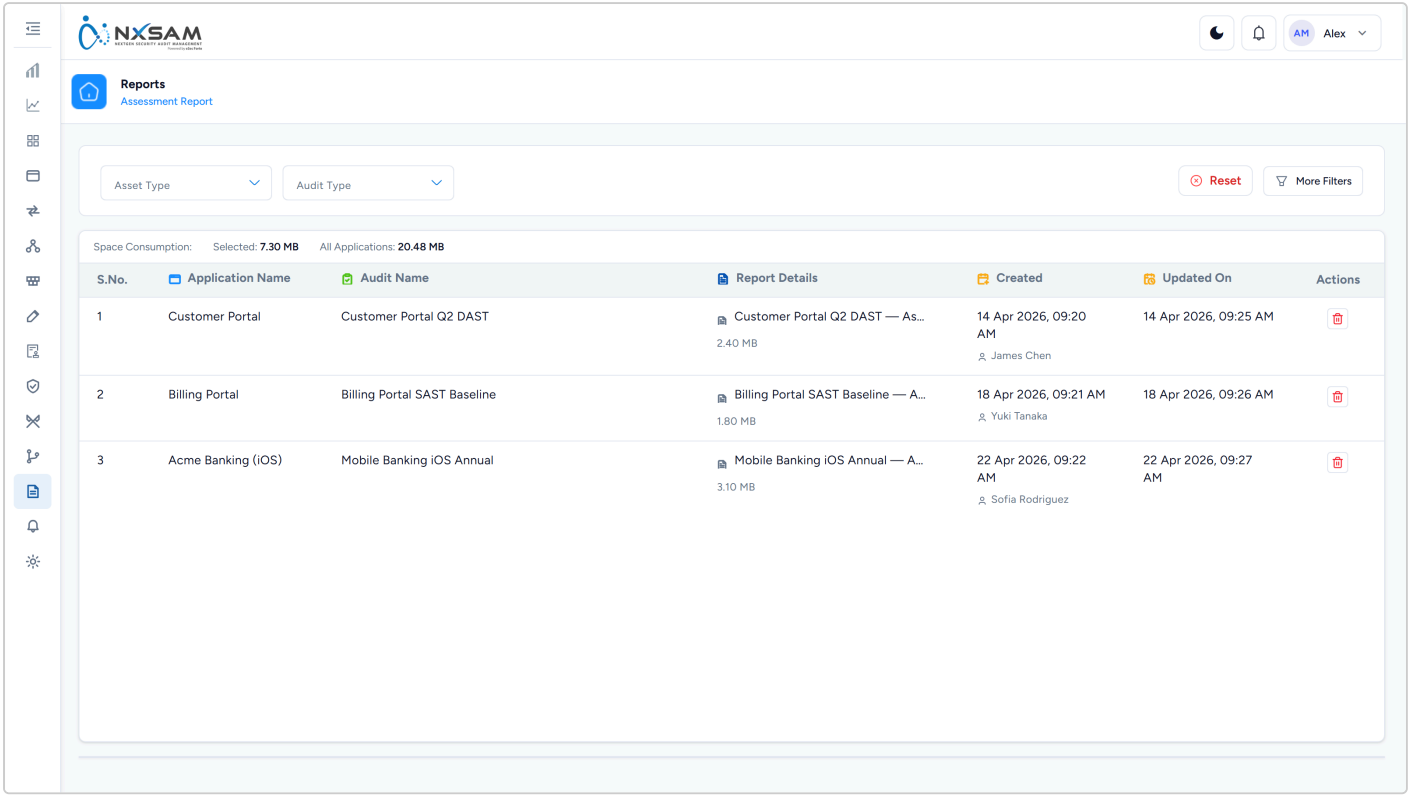
# Reports: find the right screen

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.

## Assessment Reports

Generated assessment documents, grouped by asset type, with the storage each consumes.

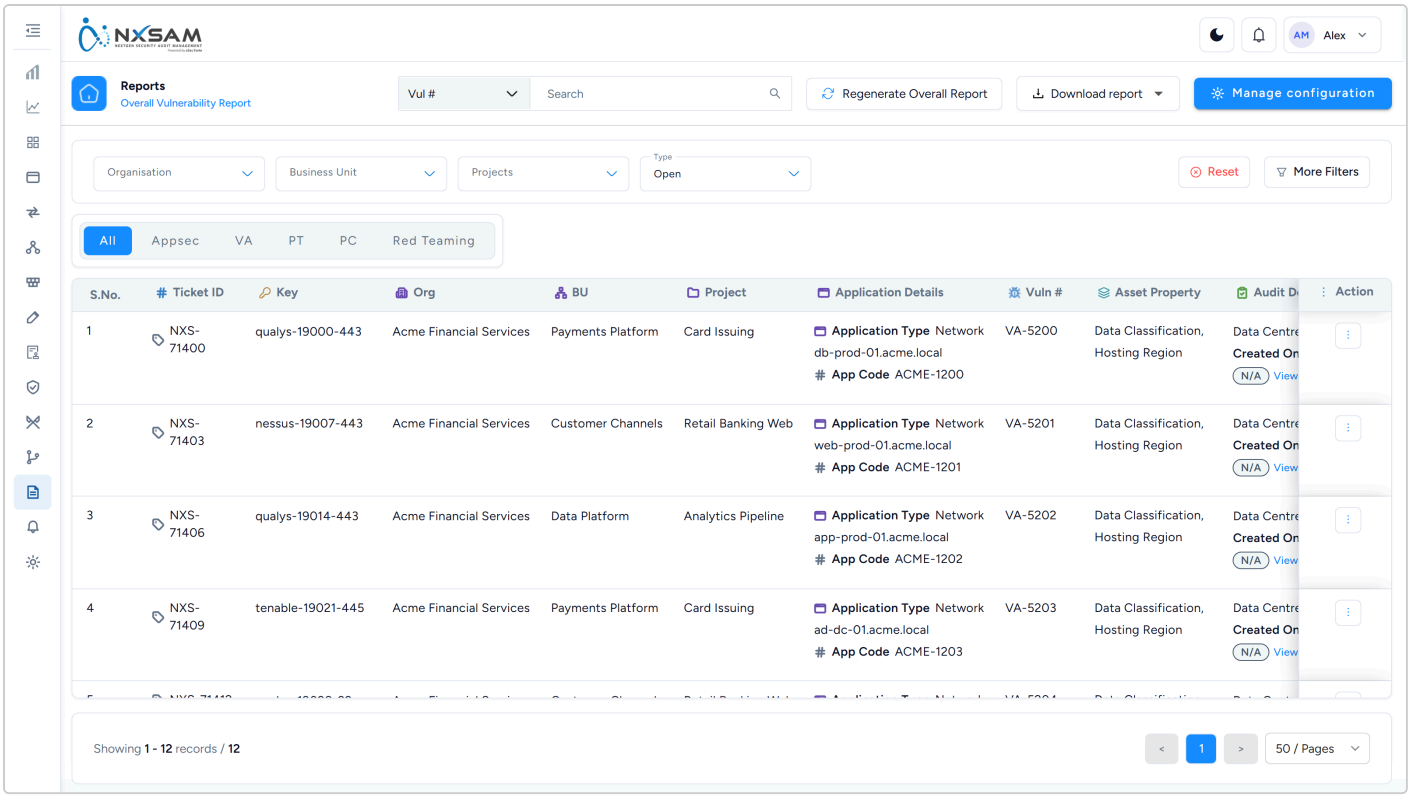



Reports → Assessment Reports

## Overall Vulnerabilities Report

One row per finding across every module, with the asset context an auditor asks for. The widest grid in the product — scope it before generating.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.




Reports → Overall Vulnerabilities Report

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.