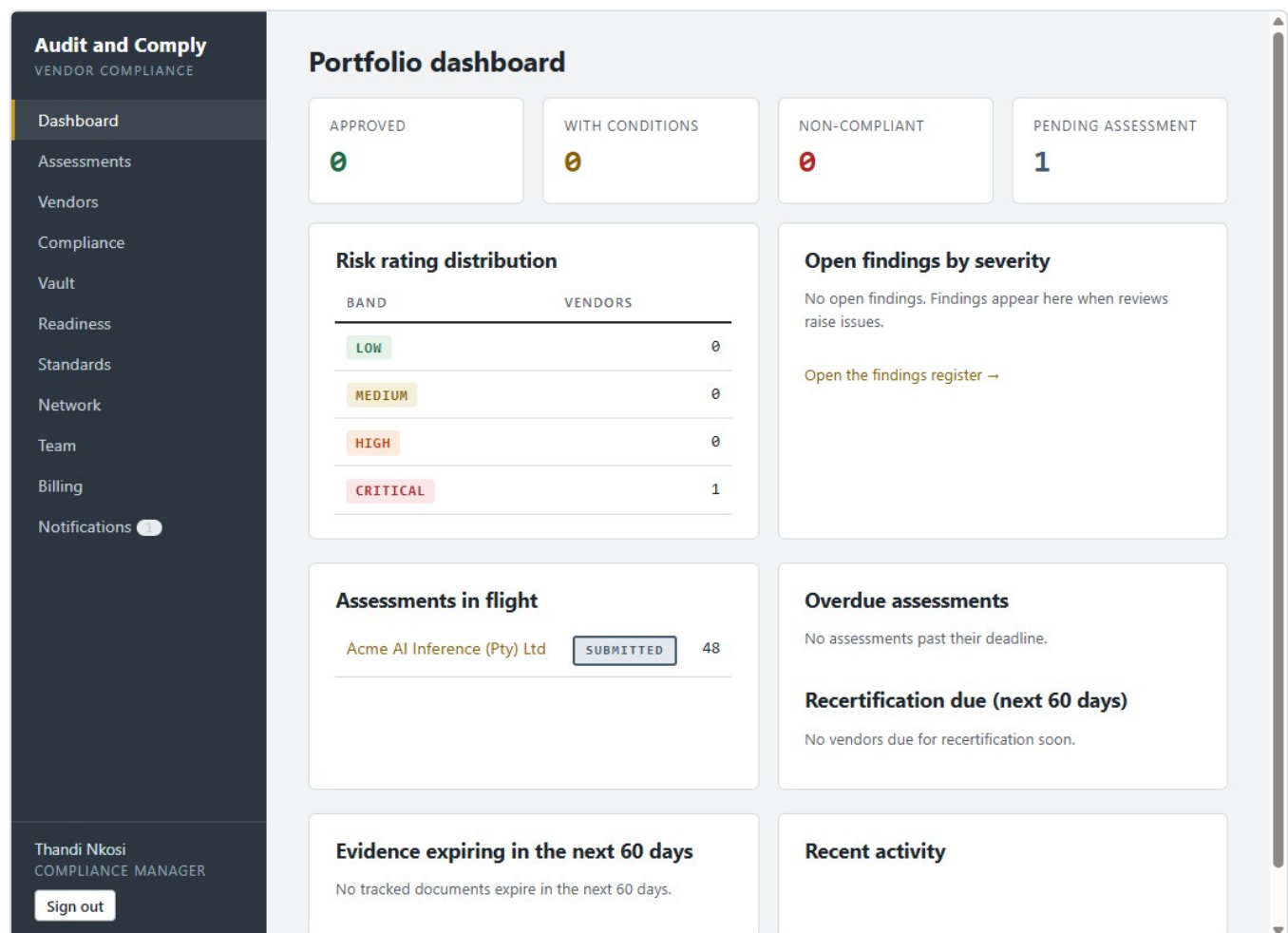


The Assessor Guide: Vendors, Assessments & Review

For: compliance managers & reviewers (Premium plan) • auditandcomply.com • July 2026

Who this guide is for: **Compliance managers** who run vendor due diligence end-to-end, and **Reviewers** who verify evidence on submitted assessments. Requires the Premium plan.

1. The dashboard: your daily starting point



The dashboard surfaces what needs attention: assessments awaiting review, non-compliant results, overdue items, expiring evidence and upcoming recertifications.

Everything on the dashboard is a link — click through to the vendor, assessment or finding it refers to. A red **NON-COMPLIANT** banner means a kill question failed somewhere: a vendor gave an answer the questionnaire defines as disqualifying (for example refusing to sign a data-processing agreement). That verdict is immediate and survives any score.

2. Registering vendors

Audit and Comply
VENDOR COMPLIANCE

Dashboard
Assessments
Vendors
Compliance
Vault
Readiness
Standards
Network
Team
Billing
Notifications ☐

Thandi Nkosi
COMPLIANCE MANAGER
[Sign out](#)

Vendors

[Export CSV](#) [Add vendor](#)

► Bulk import from CSV

VENDOR	CATEGORY	TIER	STATUS	RATING	LAST ASSESSED
Acme AI Inference (Pty) Ltd	AI/Cloud	HIGH	SUBMITTED	CRITICAL	2026-07-25

The vendor book: status, risk tier, current assessments, and CSV import/export.

Register vendors one by one (**Vendors** → **New**) or import your whole book from CSV using the columns shown in the import panel. Each vendor carries:

- **Criticality tier** (low / medium / high) — drives which template is suggested, recertification frequency, and whether outcomes need a second approval.
- **Category and data types** — what the vendor touches; useful in filtering and reporting.
- **A primary contact** — the person who receives the assessment invitation. If that email already serves another company on the platform, the existing account is linked rather than duplicated: the contact sees both companies clearly separated after one sign-in.

3. Issuing an assessment

Audit and Comply

VENDOR COMPLIANCE

Dashboard

Assessments

Vendors

Compliance

Vault

Readiness

Standards

Network

Team

Billing

Notifications

Thandi Nkosi

COMPLIANCE MANAGER

Sign out

Acme AI Inference (Pty) Ltd

AI/Cloud · South Africa · Reg 2019/123456/07

SUBMITTED

Supplier profile

— maintained by the vendor, shared across all their customers

Acme AI Inference (Pty) Ltd · Reg 2019/123456/07 · South Africa

CYBERSECURITY (JS2) · SELF-ATTESTED · VALID TO 2027-07-25

INHERENT RISK (TIER)

HIGH

RESIDUAL RATING

CRITICAL

DATA TYPES

Customer PII, usage telemetry

RECERTIFICATION DUE

—

Owner: Thandi Nkosi

Issue assessment

Questionnaire template

Standard Vendor Assessment v1

Deadline

mm/dd/yyyy

Issue to vendor

Issuing pins the questionnaire version and emails the primary contact an invitation.

Assessment history

ISSUED	STATUS	SCORE	RATING	OUTCOME
2026-07-25 → due 2026-08-08	SUBMITTED	47.5	CRITICAL	—

Open

Report

Resend invite

Findings register

Contacts

The vendor record: issue an assessment (choose template + deadline), see the supplier-maintained profile, shared standard assessments, evidence and history.

From the vendor record, pick a questionnaire and a deadline. The dropdown offers **platform templates** (the built-in Standard Vendor Assessment plus the standard framework packs — Joint Standard 1, JS2 Cybersecurity, POPIA, InfoSec, B-BBEE) and **your own published templates**. Another organisation's templates never appear.

The vendor's contact receives an email invitation; reminders chase them automatically at 7 and 1 days before the deadline, then weekly once overdue — every send is logged. If they never respond you can close the assessment as **unresponsive**: the vendor is rated non-compliant and the audit entry cites the documented attempts.

Accept instead of re-asking. If the supplier has shared a completed standard assessment with you (the "assess once, share many" flow), the vendor record shows it — you can review it live and *accept it in lieu* of issuing your own questionnaire. An immutable snapshot of exactly what you relied on is kept on the vendor record forever.

4. Custom templates & AI import

Audit and Comply

VENDOR COMPLIANCE

Dashboard

Assessments

Vendors

Compliance

Vault

Readiness

Standards

Network

Team

Billing

Notifications

Thandi Nkosi

COMPLIANCE MANAGER

Sign out

Questionnaire templates

Templates define the questions vendors answer. Platform templates are maintained by Audit and Comply and always available; duplicate one to make it your own, or start from scratch. Published templates are locked — issued assessments depend on them — so to change one, duplicate it, edit the draft and publish the new version.

Your templates

You haven't created any templates yet. Duplicate a platform template below, or create a blank one.

Create a blank template

Generate from a document (AI)

Platform templates

Read-only. Duplicate one to customise it for your organisation.

NAME	TARGETS	STATUS	ACTIONS
Standard Vendor Assessment	AI/Cloud · high tier	PUBLISHED	View Duplicate
Facilities Vendor — Light	Facilities · low tier	PUBLISHED	View Duplicate
POPIA Privacy Standard — Core	Any category · any tier	PUBLISHED	View Duplicate
POPIA Privacy Standard — Lite	Any category · any tier	PUBLISHED	View Duplicate
Information Security Baseline — Core	Any category · any tier	PUBLISHED	View Duplicate
Information Security Baseline — Lite	Any category · any tier	PUBLISHED	View Duplicate
B-BBEE Supplier Compliance — Core	Any category · any	PUBLISHED	View Duplicate

Templates: platform packs are read-only (duplicate to customise); your own templates support the full editor with kill questions, mandatory evidence, weights and conditional sections.

Build questionnaires in the editor — sections, weights, answer types, **kill questions** (instant fail), **[E] mandatory evidence**, inverted scoring ("no" is the good answer), and conditional sections. The right-hand panel lists publish blockers live; a template must be published before it can be issued.

Already have a questionnaire in a document? Upload the Excel, PDF or scan on the Templates page and the AI reads it into a draft template in the background — every question preserved, kill/evidence flags inferred. The result is always a draft for your review; nothing publishes itself.

5. Reviewing a submission

Audit and Comply
VENDOR COMPLIANCE

Dashboard

Assessments

Vendors

Compliance

Vault

Readiness

Standards

Network

Team

Billing

Notifications

Thandi Nkosi

COMPLIANCE MANAGER

Sign out

Acme AI Inference (Pty) Ltd

Standard Vendor Assessment v1 · issued 2026-07-25 · submitted 2026-07-25

SUBMITTED

Assessment report

Resend invite

OVERALL SCORE

47.5/100

RESIDUAL RISK RATING

CRITICAL

Inherent tier: HIGH

SECTION SCORES

A:25 B:67 C:33 D:0 E:50 F:50 G:100 I:100

Reviewer

Thandi Nkosi

Assign and start review

Section A — Corporate and accountability (weight 10%)

A1

Provide your registered company name, registration number, country of incorporation, and physical address.

Acme AI Inference (Pty) Ltd · 2019/123456/07 · South Africa · 12 Innovation Way, Cape Town

Evidence (mandatory: Company registration document)

#1 [acme-infosec-policy.pdf](#)

Company registration document · issued ? · expires n/a · issuer ?

AWAITING VERDICT

Verdict

Reviewer actions — clarify or override

A2 · POPIA ss 55–56 · GDPR Art 37

Have you appointed an Information Officer (or equivalent, e.g., DPO), and is that officer registered with the SA Information Regulator where required?

YES

The review page: answers with evidence side by side. Record verdicts on each document, raise clarification threads, override question scores only with a written justification.

The moment a vendor submits, the assessment is scored: weighted sections, evidence-gated points, risk band from Low to Critical. Your job in review:

- 1 Verify evidence.** Open each document (view-only, watermark-free previews), record *accepted* or *rejected* with a reason. Points that depend on evidence only count when the evidence is accepted.
- 2 Ask, don't assume.** Clarification threads go straight to the vendor's portal; their replies attach to the question.
- 3 Override sparingly.** Any score override requires a written justification and lands in the audit trail.
- 4 Decide the outcome.** Approve, approve with conditions, or send back for remediation. High-tier vendors need a second compliance manager to confirm — the outcome stays "awaiting second approval" until they do.

6. Findings, remediation & risk acceptance

Every gap becomes a **finding** with a severity, owner and due date. Vendors respond with corrective evidence from their portal. You close findings, or **accept the risk** — which requires a named senior owner and an expiry date; when it expires, the finding reopens automatically. Expired mandatory evidence degrades an Approved vendor to "Approved with conditions" and raises a finding on its own.

7. The report & the audit trail

Audit and Comply

VENDOR COMPLIANCE

Dashboard

Assessments

Vendors

Compliance

Vault

Readiness

Standards

Network

Team

Billing

Notifications

Thandi Nkosi

COMPLIANCE MANAGER

Sign out

Print-ready report — use your browser's Print → Save as PDF for the regulator/auditor copy.

Print / save as PDF

Vendor compliance assessment report

Acme AI Inference (Pty) Ltd · Standard Vendor Assessment v1

Issued 2026-07-25 16:25:08 · Submitted 2026-07-25 16:32:09 · Generated 2026-07-25

OVERALL SCORE

47.5/100

RESIDUAL RISK RATING

CRITICAL

INHERENT TIER

HIGH

SECTION	WEIGHT	SCORE
A — Corporate and accountability	10%	25
B — Operator agreement and contracts	15%	67
C — Data residency and cross-border transfers	15%	33
D — Use of data, AI, and training	15%	0
E — Security controls	20%	50
F — Breach notification and incident response	10%	50
G — Data subject rights and lifecycle	10%	100
I — Business continuity	5%	100

Sign-offs

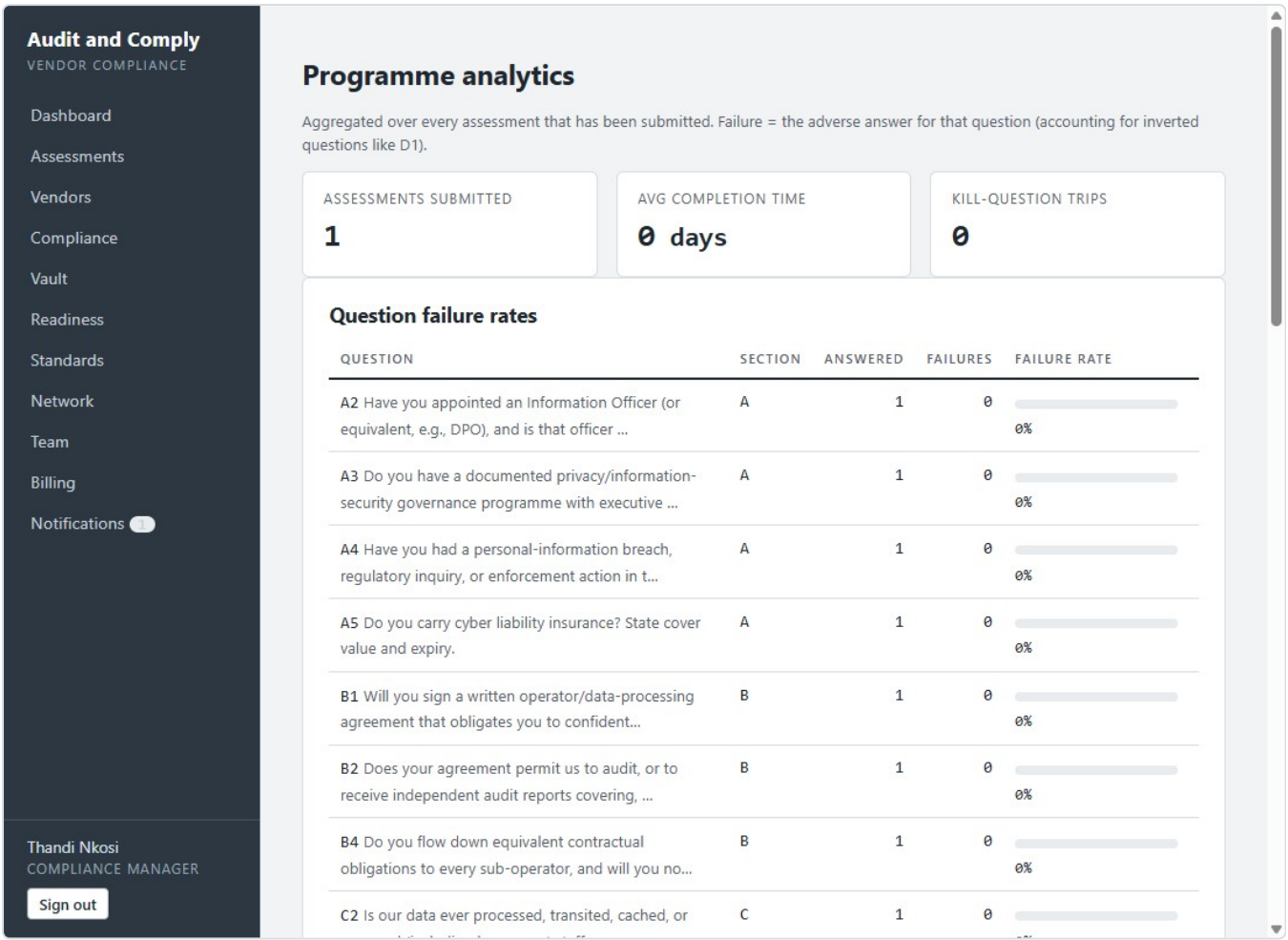
Reviewer

Not assigned

The assessment report: everything a regulator would ask for — answers, evidence verdicts, scores, overrides with justifications, outcome and approvals — exportable in one click.

Every answer, verdict, override and outcome is logged append-only. Nobody — administrators included — can edit history. Recertification is scheduled automatically by tier, and the dashboard reminds you when it's due.

8. Analytics



Failure rates by question and framework build up as assessments come in — see where your vendor base is weakest (and which requirements to lead with).