Audit and Comply

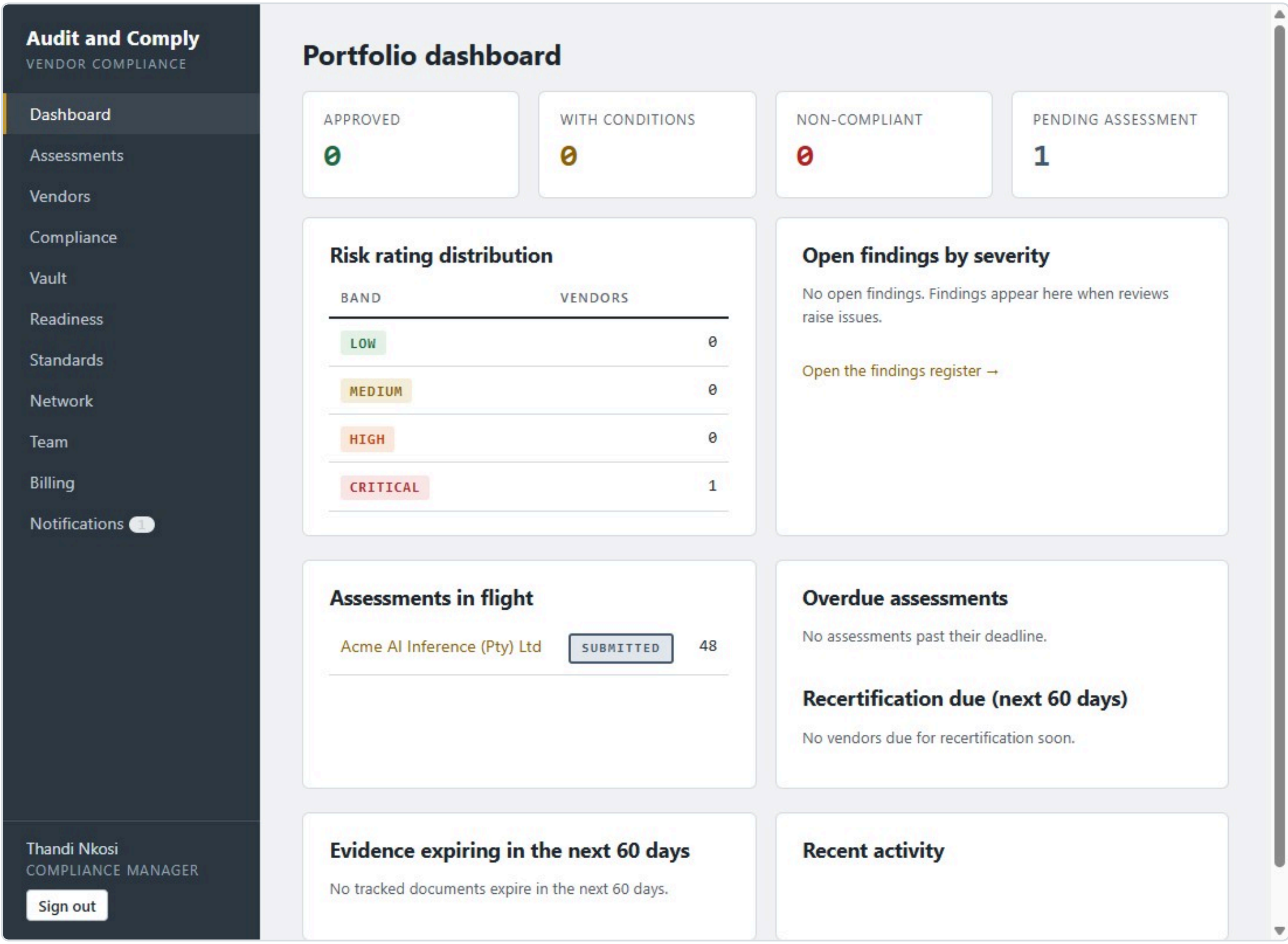
TRAINING GUIDE 2 OF 5

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.

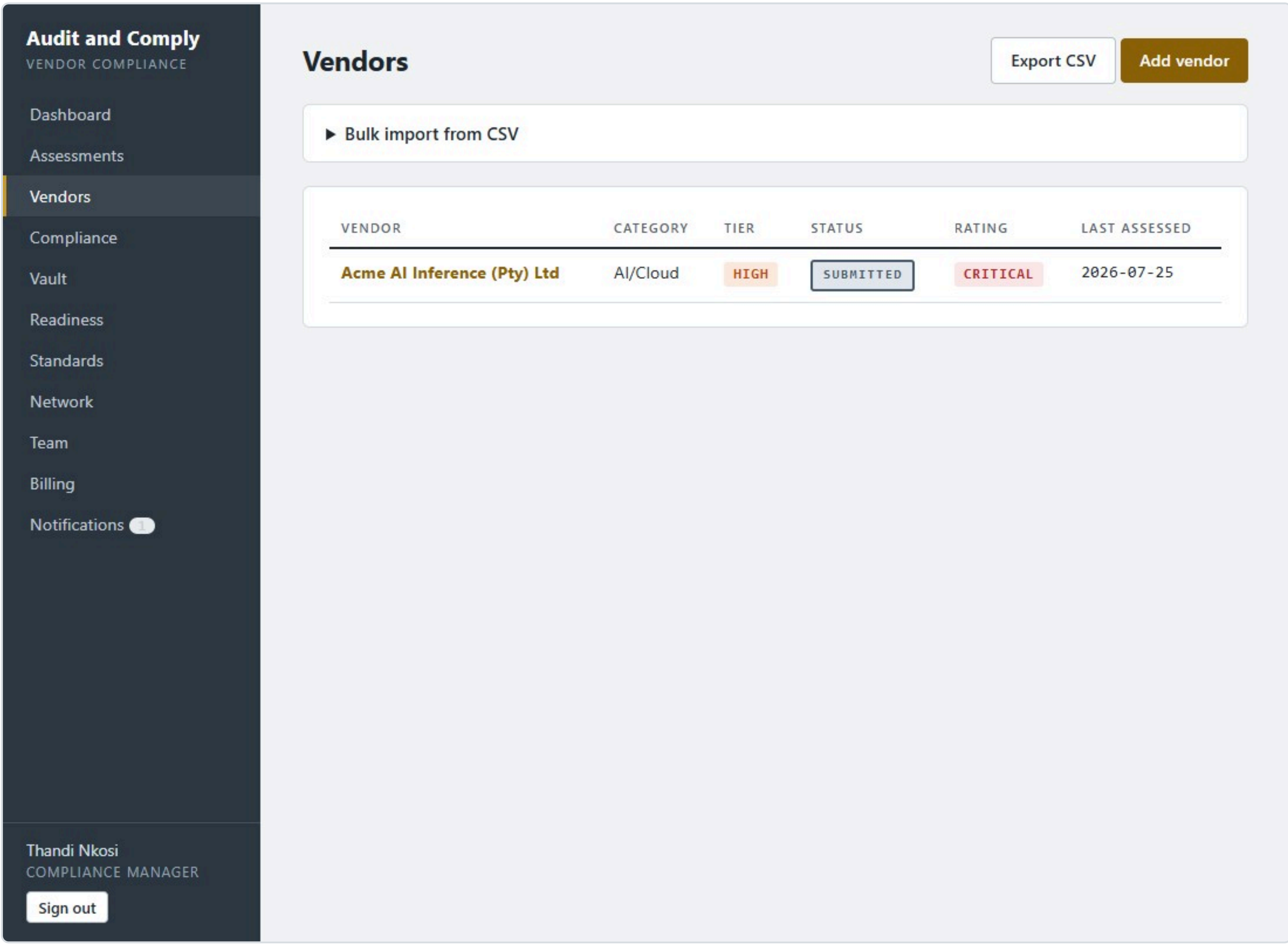
1. The dashboard: your daily starting point



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

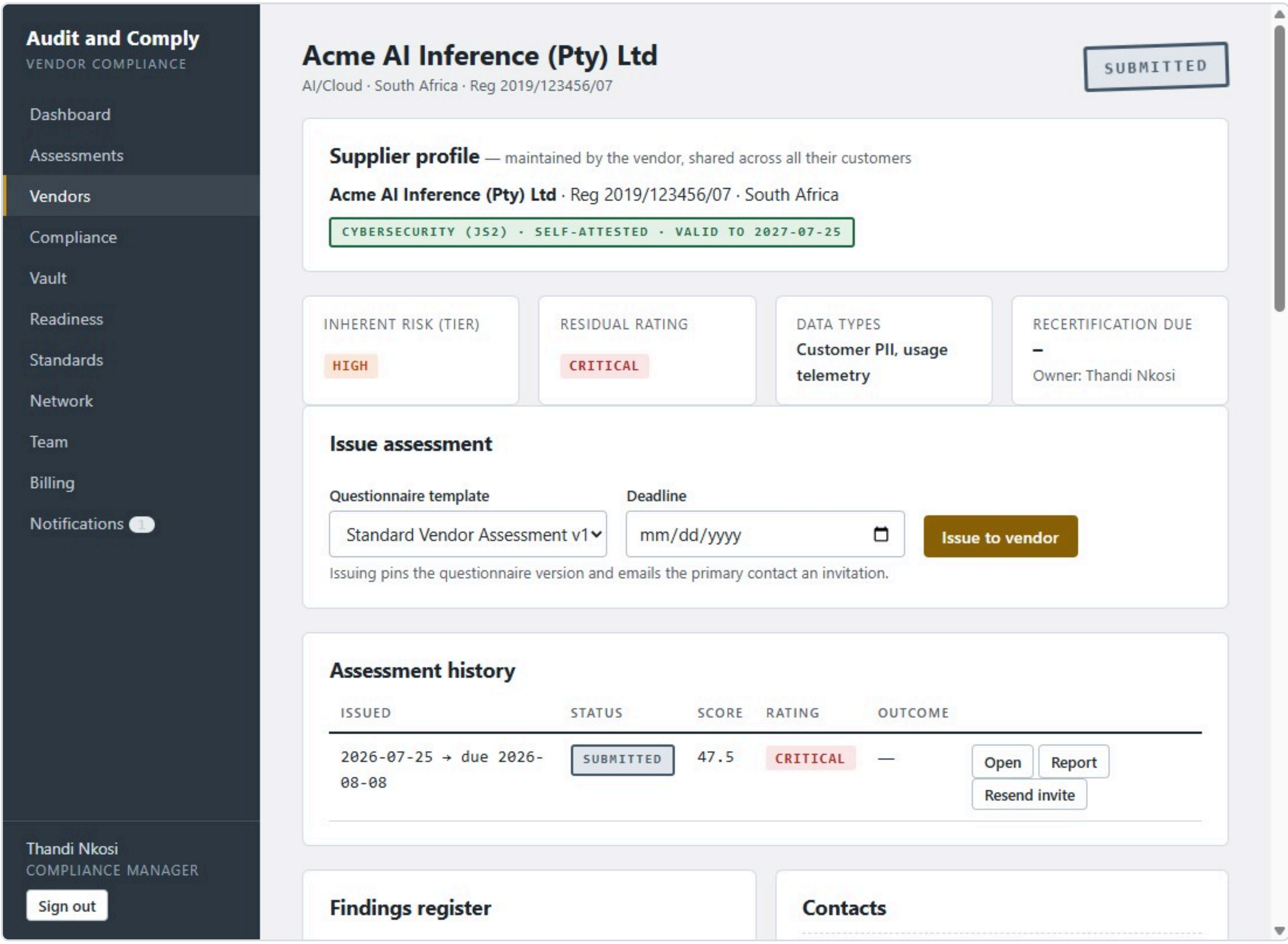


The vendor book: status, risk tier, current assessments, and CSV import/export.

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



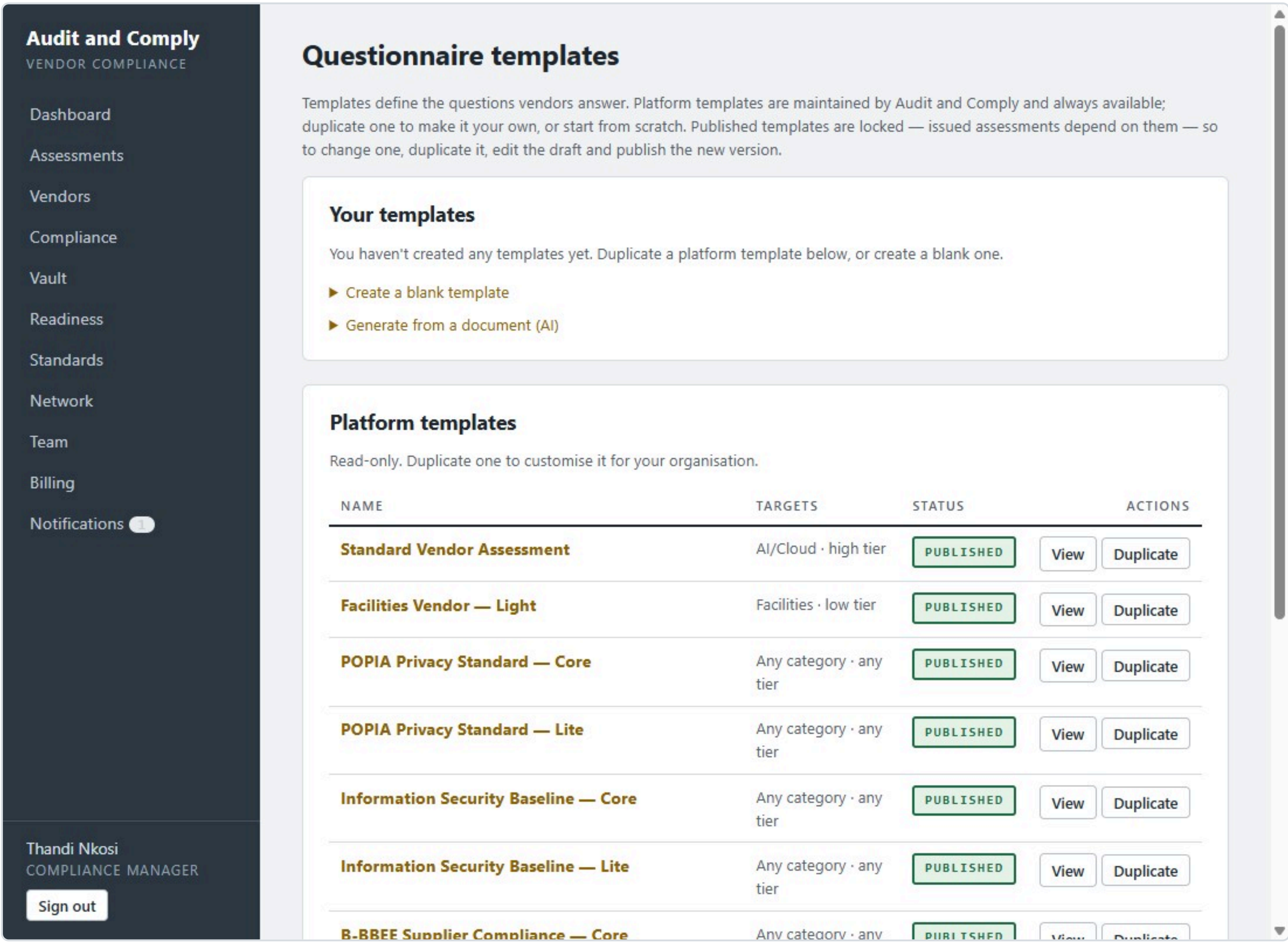
The vendor record: issue an assessment (choose template + deadline), see the supplier-maintained profile, shared standard assessments, evidence and history.

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

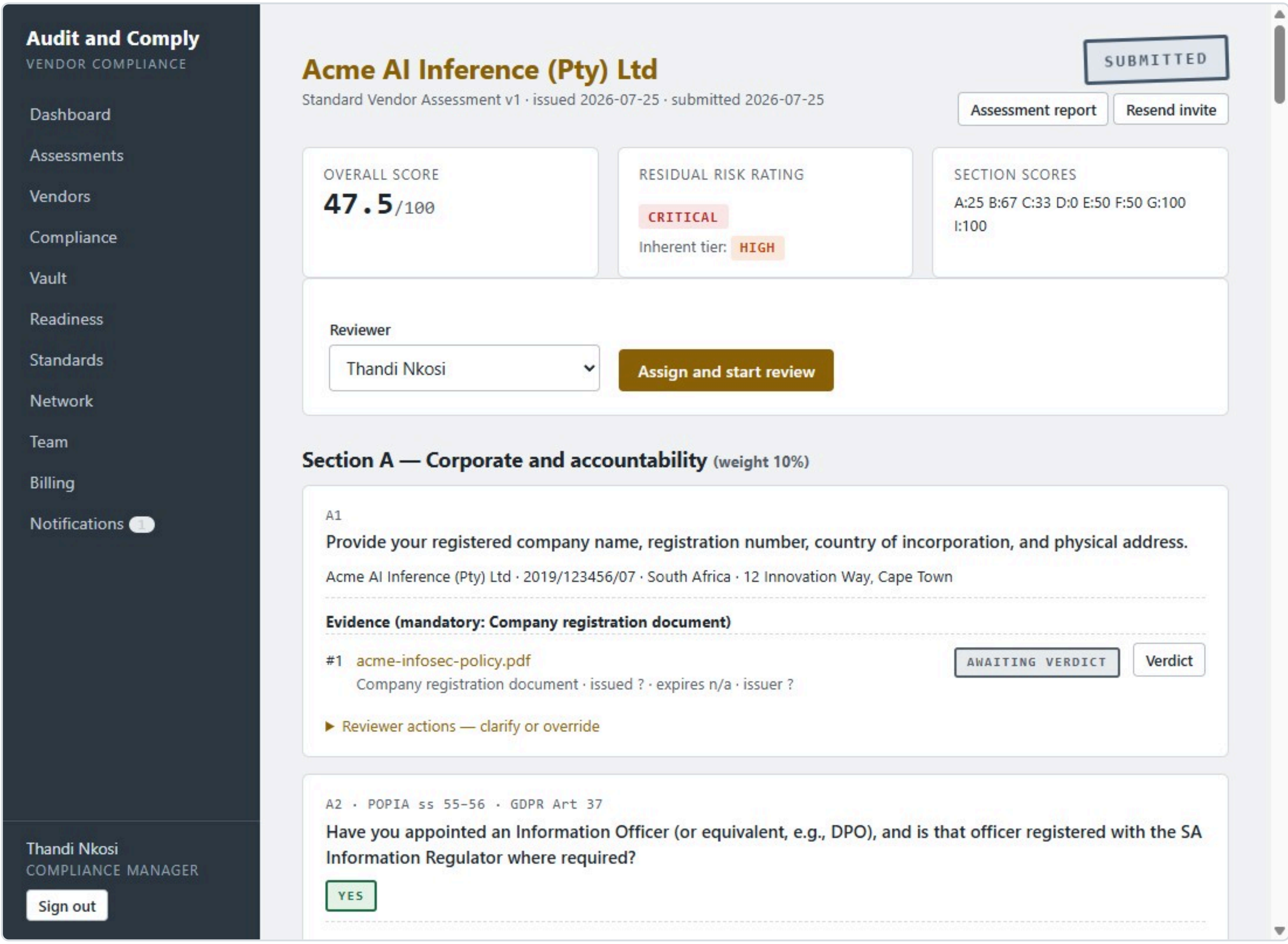


Templates: platform packs are read-only (duplicate to customise); your own templates support the full editor with kill questions, mandatory evidence, weights and conditional sections.

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



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.

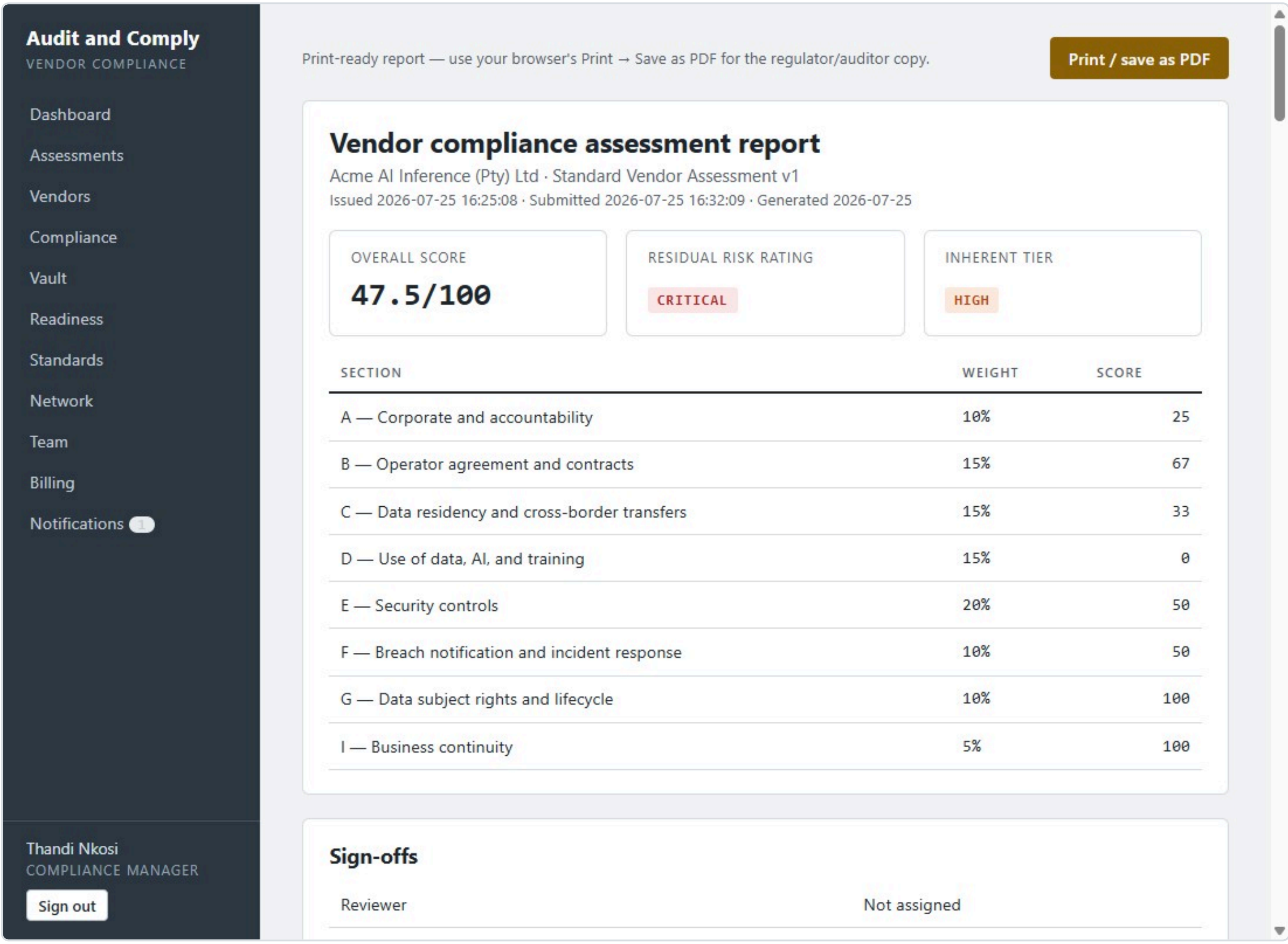
The moment a vendor submits, the assessment is scored: weighted sections, evidence-gated points, risk band from Low to Critical. Your job in review:

1. **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. **2** **Ask, don't assume.** Clarification threads go straight to the vendor's portal; their replies attach to the question.
3. **3** **Override sparingly.** Any score override requires a written justification and lands in the audit trail.
4. **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.

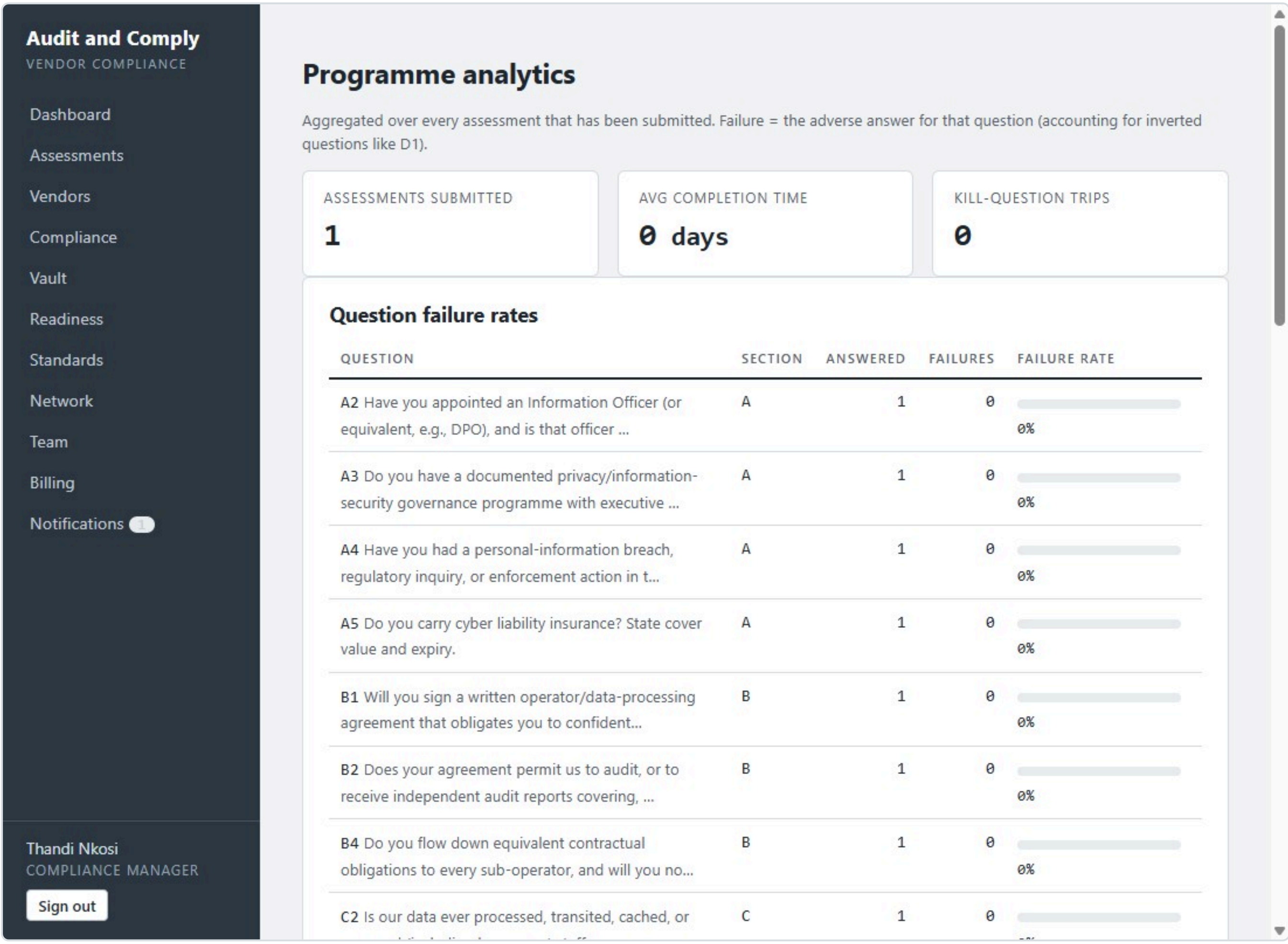
7. The report & the audit trail



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).