Audit and Comply

TRAINING GUIDE 5 OF 5

The Readiness Journey: From Gap Check to Genuinely Ready

For: every company — gap check free, actions on Pro · auditandcomply.com · July 2026

> **Who this guide is for:** companies that want to get up to standard *before* a customer or regulator asks — or that just received their first questionnaire and want a structured way to close the gaps. The **gap check is free** for every account; acting on gaps is Pro.

1. Why readiness, even unaudited

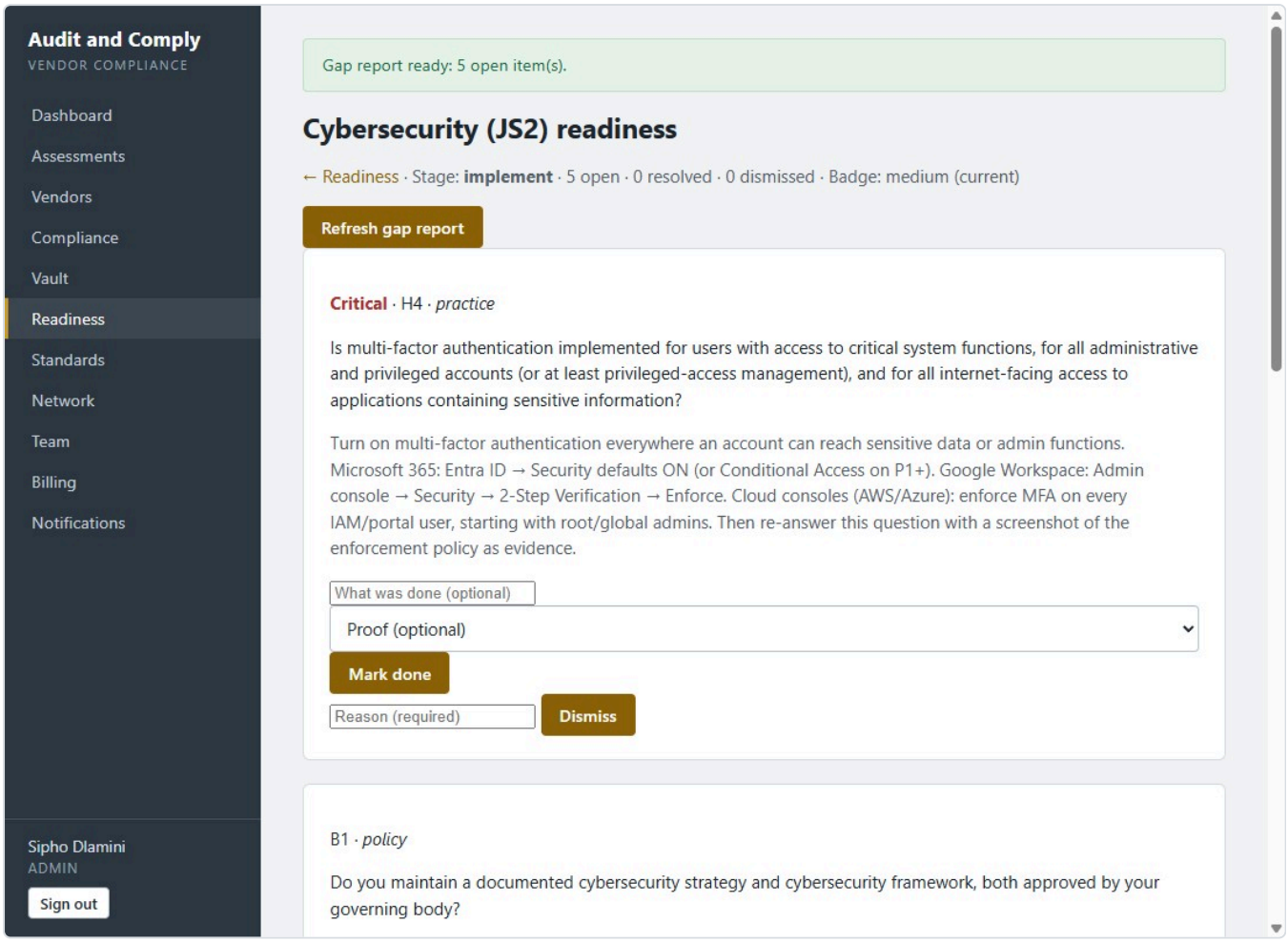
An incident response plan is the difference between a bad day and a business-ending one — whether or not anyone ever audits you. And in South African financial services the questionnaire always arrives eventually: insurers now assess every provider under Joint Standards 1 and 2. The readiness journey turns "we should get compliant sometime" into a worked plan.

2. Programmes: one per standard

Open **Readiness** in the navigation and pick a standard — Cybersecurity (JS2), POPIA, Information Security, or Insurance Outsourcing. Each programme walks five stages, and you can always revisit earlier ones:

Stage	What happens
Profile	Fill in the company profile once — it grounds every generated policy and the gap guidance.
Assess	Run the standard's lite self-assessment. Answer honestly — the gap report is only as good as the answers. Already completed one? It's adopted automatically.
Plan	Build the gap report: every failing control, classified into the action that fixes it.
Implement	Work the cards until the open count is zero.
Maintain	Reviews and obligations keep it alive; renew the assessment to refresh your badge — a renewal that fails a control re-opens its gap.

3. The gap report: every gap knows its fix



Gap cards, critical first. Each shows the failing requirement and the kind of fix: a policy to generate, a practice to change, a recurring duty to install, or evidence to attach.

Gaps come from your own answers: a "no" or "partially", a tripped mandatory question (pinned as **CRITICAL**), or a "yes" with no evidence behind it. Each card is classified:

Kind	Meaning	The action on the card
Policy	A document is missing (e.g. incident response plan).	*Generate this policy* — one click into Policy Studio, pre-linked so the gap tracks the document to approval, then attach it back onto the failing answer.
Practice	No document fixes it (e.g. MFA not enforced).	Concrete how-to guidance for your systems (Microsoft 365 / Google / AWS steps); mark done, optionally attach proof.
Obligation	A recurring duty is missing (e.g. annual pen test).	*Install the obligation* — pre-configured onto its governing policy, reminders included.
Evidence	The claim is fine; the proof is missing.	Attach a current library document — it files onto the original answer and closes the gap.

> **Dismissing a gap requires a written reason** — it stays on the record. Honest risk decisions are fine; silent ones aren't.

4. Free vs Pro on this journey

- **Free (the gap check):** start programmes, complete the profile, run the lite self-assessment, and see the *full* gap report — real requirements, real classifications, plus an outline preview of each policy the platform would write (its table of contents and the obligations it would install).
- **Pro:** everything above plus the fixes — generate the policies, follow the guides, install the obligations, attach evidence, dismiss with reasons — and completed core assessments earn the shareable badge.

5. Maintain: the standing dashboard

When the last gap closes, the programme flips to **Maintain**: your generated policies with their review states, active obligations with due dates, and your badge status with a renewal prompt when it nears expiry. Compliance stops being a project and becomes a rhythm — the reminders do the remembering.

6. A realistic first week

1. 1 Monday: company profile (5 minutes) + start the JS2 programme.
2. 2 Tuesday: lite self-assessment with the person who knows your IT (30–45 minutes). Build the gap report.
3. 3 Wednesday: fix the criticals — usually MFA (the guidance walks you through it) and generate the missing incident response plan.
4. 4 Thursday: review and approve the generated policies; install their obligations.
5. 5 Friday: attach evidence, close the remaining cards, and look at a Maintain dashboard you didn't have on Monday.
