

The Supplier Guide: Responding to Assessments

For: vendor contacts & contributors (free forever) • auditandcomply.com • July 2026

Who this guide is for: anyone whose customer sent them a compliance assessment. Responding is **free forever** — no plan required. The primary contact submits; contributors help answer.

1. Your portal

Audit and Comply

VENDOR COMPLIANCE

Dashboard

Assessments

Vendors

Compliance

Vault

Readiness

Standards

Network

Team

Billing

Notifications

Sipho Dlamini

ADMIN

Sign out

My compliance assessments

Assessments issued to **Acme AI Inference (Pty) Ltd** by **Audit and Comply Platform**.

QUESTIONNAIRE	FROM	ISSUED	DEADLINE	STATUS	
Standard Vendor Assessment	Audit and Comply Platform	2026-07-25	2026-08-08	IN PROGRESS	Continue

"My assessments" lists everything you've been asked to complete, who asked, the deadline, and your progress. One account serves every customer that assesses you — each assessment is clearly labelled with the company it came from.

You arrive by invitation: a customer registered you as their vendor and the platform emailed you a secure link to set a password. If several companies assess you, they all appear here after one sign-in — you never juggle multiple accounts.

2. Answering an assessment

Audit and Comply
VENDOR COMPLIANCE

[Dashboard](#)
[Assessments](#)
[Vendors](#)
[Compliance](#)
[Vault](#)
[Readiness](#)
[Standards](#)
[Network](#)
[Team](#)
[Billing](#)
[Notifications](#)

Sipho Dlamini
ADMIN

Sign out

Standard Vendor Assessment

From Audit and Comply Platform · Issued 2026-07-25 · due 2026-08-08

35 of 35 questions answered

A

B

C

D

E

F

G

I

Section A — Corporate and accountability

A1

Provide your registered company name, registration number, country of incorporation, and physical address.
Attach your company registration document as evidence.

Your answer

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

Evidence required: Company registration document

Upload Company registration document

Issue date

Expiry date (if time-limited)

Choose File

No file chosen

mm/dd/yyyy

mm/dd/yyyy

Issuing body

Notes

Upload evidence

Your answers on this section are saved automatically when you upload.

...or attach a document from your library

ISO 27001 Certificate v1 (Certification, expires 2027-06)

Attach existing

Answer section by section. Each question shows plain-language help; [E] questions require an attached document before you can submit. Save as you go — nothing is final until you submit.

- **Answer honestly, use "Partially" and "N/A" properly.** Both require a short written justification — a truthful "partially, because..." reads far better in review than an unsupported "yes".
- **Attach evidence where marked.** Upload the document at the question, or attach a current version straight from your library (see §3). Certificates carry expiry dates — the platform reminds you before they lapse.
- **Watch for the policy shortcut.** Where a question asks for a policy you don't have, a link offers to *generate* it for your business — see Guide 4 (Policy Studio).
- **Mind the mandatory questions.** Some answers are defined as disqualifying by your customer (e.g. refusing breach notification). The help text warns you.

Audit and Comply
VENDOR COMPLIANCE

Dashboard
Assessments
Vendors
Compliance
Vault
Readiness
Standards
Network
Team
Billing
Notifications

Sipho Dlamini
ADMIN

Sign out

Submission blocked — 18 item(s) still incomplete.

Standard Vendor Assessment

From Audit and Comply Platform · Issued 2026-07-25 · due 2026-08-08

IN PROGRESS

35 of 35 questions answered

A

B

C

D

E

F

G

I

Submission blocked — 18 item(s) incomplete:

- A1 — Mandatory evidence required (Company registration document)
- A2 — Mandatory evidence required (Information Regulator registration / authorisation assessment)
- A3 — Mandatory evidence required (Policy index or programme charter)
- A5 — Mandatory evidence required (Cyber-insurance certificate)
- B1 — Mandatory evidence required (Operator/data-processing agreement)
- B3 — Mandatory evidence required (Sub-processor register)
- C2 — Mandatory evidence required (Cross-border transfer mechanism documentation)
- C4 — Mandatory evidence required (DR summary)
- D1 — Mandatory evidence required (Contractual clause / provider terms)
- D3 — Mandatory evidence required (Provider retention terms)
- D4 — Mandatory evidence required (Architecture summary)
- D5 — Mandatory evidence required (Contractual clause / provider terms)
- E1 — Mandatory evidence required (ISO 27001 certificate / SOC 2 Type II report)
- E5 — Mandatory evidence required (Penetration-test attestation)
- F1 — Mandatory evidence required (Incident-response plan or summary)
- F2 — Mandatory evidence required (Incident-response plan or summary)
- G2 — Mandatory evidence required (Retention and destruction schedule)
- I1 — Mandatory evidence required (SLA document)

Section A — Corporate and accountability

A1

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

Attach your company registration document as evidence.

Submitting runs a completeness check first: unanswered questions, missing justifications and missing mandatory evidence are listed with links. Nothing embarrassing can slip through half-done.

Only the **primary contact** can submit. Submission is final — answers lock and scoring happens immediately. If the reviewer needs more, they'll open a clarification thread, which appears in your portal and email.

3. Your document library

Audit and Comply
VENDOR COMPLIANCE

[Dashboard](#)
[Assessments](#)
[Vendors](#)
[Compliance](#)
[Vault](#)
[Readiness](#)
[Standards](#)
[Network](#)
[Team](#)
[Billing](#)
[Notifications](#)

Sipho Dlamini
ADMIN

Sign out

Document library

Your company's compliance documents, shared across every assessment you complete. Upload a **new version** when a document is renewed: new and ongoing assessments offer the new version, while assessments that already carry the old one keep it — history is never rewritten.

ISO 27001 Certificate v1
Certification · acme-iso27001-cert.pdf · expires 2027-05-25

New version

Information Security Policy v3 v1
Policy · acme-infosec-policy.pdf

New version

Professional Indemnity Insurance v1
Insurance · acme-pi-insurance.pdf · expires 2027-02-25

New version

[► Add a document](#)

The library keeps every compliance document with version history. Attach the current version to any assessment; old assessments keep the exact version they were given, forever.

Upload certificates, policies and reports once, reuse them everywhere. "New version" keeps the chain: assessments you submitted earlier still show the file they were assessed on (the point-in-time guarantee), while new attachments get the latest. Documents you upload at questions register in the library automatically.

4. Complete once, share with every assessor

Audit and Comply
VENDOR COMPLIANCE

Dashboard

Assessments

Vendors

Compliance

Vault

Readiness

Standards

Network

Team

Billing

Notifications

Sipho Dlamini
ADMIN

Sign out

Standard assessments

Complete a standard framework pack **once**, then share it with the companies that assess you — they can accept it instead of sending you their own questionnaire. Badges from completed packs appear on your network listing.

Your badges

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

Framework packs

POPIA Privacy Standard

Protection of Personal Information Act, 4 of 2013 — the eight conditions for lawful processing plus operator, cross-border and direct-marketing duties.

Core ▼ Start

Information Security Baseline

A general-purpose security control baseline organised by domain: governance, people, access, data protection, operations, development, incidents, continuity and third parties.

Core ▼ Start

B-BBEE Supplier Compliance

Broad-Based Black Economic Empowerment status capture and integrity checks. Verification stays with SANAS-accredited agencies and sworn affidavits — this pack captures and validates existing artefacts; the platform never performs verification.

Core ▼ Start

Insurance Outsourcing Due Diligence

Due-diligence dimensions for service providers to insurers, structured on Joint Standard 1 of 2024 (Outsourcing by Insurers) section 7.5 and the recurring re-assessment duty in section 10.4.

Core ▼ Start

Cybersecurity & Cyber Resilience (Joint Standard 2)

Cybersecurity and cyber resilience requirements structured on Joint Standard 2 of 2024 (FSCA & Prudential Authority, effective 1 June 2025): governance, strategy and framework, the identify-protect-detect-respond-recover fundamentals, testing, cyber hygiene practices, and

Core ▼ Start renewal

Standard packs (JS1, JS2 Cybersecurity, POPIA, InfoSec, B-BBEE): complete one self-assessment per framework and share it with every company that assesses you. Completed packs earn a 12-month badge.

Tired of answering the same spreadsheet for every insurer? On Pro, complete a **standard framework pack** once and grant each assessing company access. They can accept it instead of sending their own questionnaire — and an immutable snapshot protects you both. Sharing is per company, per framework, and revocable (forward-only: what they already accepted stays theirs).

5. Findings & remediation

If review raises findings against you, they appear in your portal with severities and due dates. Respond with what you fixed and attach corrective evidence — the reviewer closes the finding or asks again. Everything is threaded and logged; nothing gets lost in email.

6. Your company profile

Under **Portal** → **Company profile**, the primary contact maintains a shared profile (registration details, industry, systems, data types). Your customers see it on their vendor record — saving you the same ten intro questions each time — and it powers the AI features in Guides 4 and 5.

