IONITY GLOBAL

(Pty) Ltd · AEDI · Building Tomorrow, Today

IT SYSTEMS AUDIT

Final Report & Recommendations

Phase 1 — Assessment & Advisory

PREPARED FOR **Shout-It-Now NPC**

PREPARED BY **Ionity Global (Pty) Ltd**

Engagement: Q021-SN01-AD1-26D · QTE-2026-002

Document: DOC-2026-07-021 · Version 1.0 FINAL

Date: 20 July 2026 (SAST)

Classification: **CONFIDENTIAL — CLIENT**

Governance: Policy 986 AED · AED 900 · TM²

www.ionity.today | ai@ionity.today | +27 646 999 877

"Anything is Possible with God."

Contents

1. Executive Summary

Shout-It-Now NPC delivers front-line HIV, TB, STI, PrEP and gender-based-violence (GBV) services to South African youth — more than **1.2 million people have learned their HIV status** through its programmes. Its technology estate has grown organically around the **SMART 2.0** clinical hub across 21 systems and two clouds. Ionity Global was engaged to perform an independent Phase 1 IT Systems Audit, Assessment & Advisory: baseline the estate, risk-rank the findings against POPIA and ISO/IEC 27001, and set a costed remediation path.

1.1 Overall posture verdict

Mission-critical delivery works — mobile clinics run on SMART 2.0 daily. But the estate's security and governance maturity is **"Initial"**: the forensic scan returned a posture score of **33.7/100 (Grade F)**. The estate is capable but is paying for its past — fragmented finance, dormant paid-for tools, an 18-month maintenance gap on the clinical core, an unguarded cloud perimeter, and identity sprawl. Encouragingly, the workloads are basic and scattered, which makes the recommended consolidation low-complexity.

1.2 Critical findings at a glance

The following RED items require action this quarter:

- **F-24 · No MFA on AWS —** the root account key has no MFA and all 6 IAM users are unprotected (0/6); four accounts are dormant yet enabled, including an external vendor idle 1,012 days.
- **F-23 · No logging —** AWS CloudTrail is disabled across all 18 regions; no Config, no GuardDuty. A breach would go unseen and POPIA §22 notification could not be met.
- **F-06 · Unmaintained clinical core —** SMART 2.0 has had no patch cadence for ~18 months on a runtime reported end-of-life.
- **F-04 · Email-security gap —** email protection covers ~40 of ~200 mailboxes; live phishing exposure observed.
- **F-28 · Azure Entra sprawl —** 1,000+ directory identities against ~200 mailboxes — a 5:1 ratio, unMFA'd, licence- and POPIA-exposed.
- **F-29 · CHOMI on Botpress —** GBV survivor conversations (special personal information) cross the border twice — to Botpress cloud and to an offshore LLM — with no operator agreements.
- **F-07 · AWS cost cliff —** the AWS commitment expires September 2026; the ~R9k/month rate can rise to R60–70k/month if it lapses.

> **Data residency (F-17) was CONFIRMED RESOLVED.** The AWS configuration scan (30 Jun 2026) verified the SMART 2.0 clinical database is hosted in-country (af-south-1) — the previously drafted cross-border concern is closed GREEN. Residual checks: the SNowl 2 data store and an eLearning test instance in eu-west-1.

1.3 Headline recommendations

- **Exit AWS entirely** and re-home the clinical workloads onto Ionity Private Intranet hosting — sovereign micro-computing nodes on SA soil (addresses F-06, F-07, F-23–F-27).
- **Retain and right-size Azure / Microsoft 365** as the identity and productivity backbone; reconcile the Entra directory (F-28); Ionity absorbs Azure-bound migration cost up to R25,000.
- **Consolidate the finance stack** — evaluate Dynamics 365 (NGO ~60% discount) against a Sage upgrade; retain S-Cube; 3/6/9-month staged hand-over (F-05, F-09, F-10).
- **Harden identity now** — enforce MFA, disable dormant/vendor accounts, rotate stale keys, wire HR→Entra joiner/mover/leaver (F-24, F-03).

- **Rebuild CHOMI as a local AI + RAG bot** on the Ionity edge, so survivor data never leaves the country (F-16, F-29).

1.4 Financial summary

The total annual IT run-rate is approximately **R1.2 million** (summed system costs, finance view). Of this, roughly **R620,000** was flagged as poor value — fragmented, duplicated and dormant spend. The audit isolates **≈ R335,000 per year of recurring gains**, lands the estate near a **R865,000 run-rate**, and removes an AWS renewal cliff worth up to R630,000/year in exposure. The Ionity Private Intranet cluster costs R118,500 once-off plus R7,950/month, with payback of approximately **12 months** against today's AWS run-rate. The cost model is now console-verified: the SMART 2.0 AWS account bills US$529.38/month on average (US$3,176.26 over Jan–Jun 2026).

2. Engagement Background & Scope

2.1 Client context

Shout-It-Now is a South African Non-Profit Company (NPC). SMART 2.0 is its custom electronic clinical management hub, running a POPIA-relevant central database for HIV/TB/STI/PrEP workflows, dispensing and social-work case management. Every mobile clinic depends on it.

2.2 Objectives

By the end of the engagement the client has: a documented baseline of the IT estate expressed as a maturity score; a risk-ranked findings register (5×5 likelihood × severity, RYG-rated); a gap analysis against POPIA and ISO/IEC 27001; quick-win actions inside 30 days; and a prioritised, costed remediation roadmap with software recommendations.

2.3 Scope — 21 systems across two tracks

Internal operational: Sage Evolution · Fusion (Neurasoft) · CaseWare · S-Cube / BioSyn · SSRS · Salesforce · Consumate · ASQ / Eduvoss / Baseline.

External / client-facing: SMART 2.0 · SNowI 2 · CHOMI / AIMEE · iShout / ShoutLink · MojaMind · eLearning · Microsoft 365 · Azure · AWS · Snipe-IT · WhatsApp · FreshService · Fetch / Self Cav.

2.4 Out of scope

Implementation of the recommendations. Phase 1 identifies possibilities and options; where several options exist, all are listed and the client decides the direction. Implementation and support fall to a subsequent phase.

2.5 Phase model

Phase	Focus	Status
1	Discovery, assessment & advisory (this report)	Complete
2	DOME consolidation, migration, QMS & Chomi v2	Next
3	Rationalise, decommission & finance cut-over	Then

2.6 Stakeholders & interviews

- **Lilian Monji** — Corporate Services / Commercial

- **Neetin Daya** — IT Operations (client single point of contact)
- **Pierre van Papendorp** — Finance
- **Ionity delivery** — Johan van Antwerp (Managing Director), Ian Raven (assessment & integration)

3. Methodology & Assessment Framework

The audit followed an optimise-and-consolidate-before-replace principle: assess the estate against a consistent framework, secure continuity and compliance evidence first, then sequence rationalisation. Findings are stated as "we observed…", or "requires confirmation" where evidence was incomplete.

3.1 Five General Foundations

Baseline domains assessed for every system: (1) asset inventory; (2) security & access controls; (3) backup & disaster recovery; (4) network performance & capacity; (5) compliance & policy enforcement.

3.2 Ten Specific Pillars

Depth coverage for custom-build, multi-cloud, AI and sensitive-data environments: integrations & data flows; vendor & source-code custody; cloud configuration posture; logging, monitoring & IR readiness; identity lifecycle; patch & change management; data classification, retention & destruction; AI & model governance; architectural single points of failure; and cost & licence rationalisation.

3.3 Rating scheme & risk matrix

RYG: RED = material risk / non-compliance, act now; AMBER = weakness to remediate on a timeline; GREEN = adequate. Risk score = Likelihood × Severity on a 5×5 matrix (RED ≥ 15, AMBER 8–14, GREEN ≤ 7).

3.4 Evidence base

Stakeholder interviews; the April-2026 system assessment workbook; AWS, Azure and Microsoft 365 configuration scans; the IA·MCP forensic audit engine (20 tools, 100 controls, frameworks CIS v8 / ISO 27001 / SOC 2 / NIST 800-53 / POPIA); and live console captures on 20 July 2026 (AWS Cost Explorer, IAM, EC2 regions, and the CHOMI Botpress analytics). Evidence index in Appendix C.

4. System Landscape & Data Flows

4.1 SMART 2.0 as the central hub

SMART 2.0 is the anchor system. SNowI 2, ShoutLink, iShout, eLearning and a MojaMind data share all reference its AWS environment. Its supplier concentration and hosting drive several of the highest-priority findings — and mean one coordinated migration moves five systems at once.

4.2 Dual-cloud posture

The estate is split: clinical workloads on AWS (af-south-1, confirmed in-country), operational/identity on Azure and Microsoft 365. The split leaves identity in Azure, clinical data in AWS, and monitoring in neither — a harmonisation and visibility gap the plan closes.

4.3 Criticality summary

System	Function	Criticality
SMART 2.0	Clinical hub — HIV/TB/STI/PrEP	**Critical**
SNowI 2	Follow-up case-management CRM	**Critical**
CHOMI / AIMEE	WhatsApp GBV chatbot (Botpress)	**Critical**
S-Cube / BioSyn	Payroll & time-and-attendance	**Critical**
iShout · MojaMind · eLearning	AGYW app · e-art MH · courses	High
M365 · Azure · AWS	Productivity, identity & cloud infra	High
Sage · Fusion · SSRS	Finance & reporting	High
Snipe-IT · Data Warehouse · Salesforce	Assets · integration · leads	Low–Med

5. Findings

Each finding: context → observation → risk (RYG + score) → recommendation. Findings F-01 to F-27 follow the consolidated Phase 1 v3 register; F-28 and F-29 were added from the 20 July 2026 console review.

5.1 Cloud security & identity

F-24 No MFA & root-key exposure on AWS

Rating: RED **Risk:** P1 **POPIA:** C7

Observation. The AWS root account uses an access key with no MFA. All six IAM users are console-enabled with no MFA (0/6). Four are dormant yet still enabled — pierre.vanpapendorp (1,515 days), takudzwa.mabande (1,322 days), gareth.chandler@int32.co.za (external vendor, 1,012 days) and gino.janari (292 days). Active access keys are 1,374–1,633 days old; two have never been used. Console-confirmed 20 Jul 2026.

Recommendation. Enforce MFA on all users starting with the active admin; disable the four dormant accounts and the external-vendor account; delete the three unused/ancient keys; retire the root key; then wire HR→Entra joiner/mover/leaver so access cannot re-accumulate. Zero cost, one week.

F-23 No audit logging — CloudTrail disabled in all regions

Rating: RED **Risk:** P1 **POPIA:** C7 · §22

Observation. AWS CloudTrail management-event logging is disabled in all 18 enabled regions; AWS Config and GuardDuty are not enabled (Trusted Advisor, 30 Jun 2026). There is no record of API activity across the clinical estate — nobody would see a breach.

Recommendation. Enable a multi-region CloudTrail trail plus Config and GuardDuty as a quick win. Route logs to the monitoring node in the target architecture so POPIA §22 notification timelines can be met.

F-25 Internet-open security groups

Rating: RED **Risk:** P1 **POPIA:** C7

Observation. Security groups expose 0.0.0.0/0 on the sync and enrolment tiers of the clinical estate.

Recommendation. Close the groups to known sources; front all access with the WireGuard-only edge gateway in the target architecture.

F-26 Publicly accessible S3 bucket

Rating: AMBER **Risk:** P2 **POPIA:** C7

Observation. The S3 bucket “shoutitnow-hosted-content” is publicly accessible via bucket policy; a second bucket is not.

Recommendation. Restrict the bucket policy; audit contents for personal information; enable access logging.

F-27 Clinical database is Single-AZ

Rating: AMBER **Risk:** P2 **POPIA:** C7

Observation. The clinical RDS instance (sn-sql-db-01, af-south-1) is Single-AZ with no standby for automatic failover — and the estate has already taken two separate two-day outages.

Recommendation. Answer with the HA database pair (primary + hot standby, auto-failover) in the Ionity cluster; evidence restore drills monthly.

F-28 Azure Entra ID user sprawl

Rating: RED **Risk:** P1 **POPIA:** C7 · C8

Observation. Azure Entra ID shows over 1,000 user objects against roughly 200 real mailboxes — a 5:1 ratio. Likely stale leavers, guests, duplicates, service and bulk-imported records. On an estate with no MFA and no logging, most are invisible. Exact count to confirm on export.

Recommendation. Export and classify every identity (active/leaver/guest/service/client-record); disable then delete the dead; reclaim licences; enforce MFA and Conditional Access; make Entra the clean identity spine.

F-17 POPIA cross-border transfer (§72) — RESOLVED

Rating: GREEN **Risk:** — **POPIA:** §72

Observation. The AWS configuration scan confirmed the SMART 2.0 clinical database and primary compute are hosted in af-south-1 (Cape Town). Data residency for the primary clinical dataset is in-country; the previously drafted cross-border concern is closed.

Recommendation. Clear the residuals — verify the SNowI 2 data store and confirm no live personal information sits on the eLearning/Moodle test instance in eu-west-1; then terminate or re-home that instance.

5.2 Cost, commitment & finance

F-07 AWS commitment expiring September 2026

Rating: AMBER **Risk:** P1 **POPIA:** —

Observation. The AWS commitment (type unconfirmed — Savings Plan / Reserved Instance / EDP) expires around September 2026. The committed rate of ~R9,000/month can rise to R60,000–70,000/month on-demand — a 7–8× step, billed in USD. Console-verified account spend averages US$529.38/month (US$3,176.26 Jan–Jun 2026), of which ~70% is overhead (support plan, load balancing, NAT, volumes, VAT) and CloudWatch is US$0.00.

Recommendation. Do not renew into another cycle. Exit AWS to the Ionity Private Intranet before the window closes, turning the September date into leverage rather than a deadline.

F-05 / F-09 / F-10 Fragmented finance stack & Sage EOL

Rating: AMBER **Risk:** P2 **POPIA:** —

Observation. Finance runs across Sage Evolution V9, Fusion, CaseWare, S-Cube and a BioSyn build with manual hand-offs; each is a reconciliation point and audit/SARS/grant-reporting risk. Sage Evolution V9 is end-of-life.

Recommendation. Consolidate to one backbone: evaluate Dynamics 365 (NGO ~60% discount, ~R20k/yr for 4 users) against a Sage 300/Intacct upgrade; retain S-Cube for payroll & T&A; phase legacy out over 3/6/9 months with no interruption to payroll or funder reporting.

F-08 Azure billing anomaly

Rating: AMBER **Risk:** P2 **POPIA:** —

Observation. After a payment disruption and a Microsoft write-off, Azure invoices read zero — an unquantified liability and continuity risk on the platform being retained.

Recommendation. Regularise the true billing position with Microsoft before migrating anything into Azure; move the tenant onto a clean subscription.

F-11 / F-12 Dormant paid-for systems

Rating: AMBER **Risk:** P2 **POPIA:** —

Observation. Snipe-IT (Azure, R72,000/yr) is licensed but not used — no database access, register kept in a manual spreadsheet. The Data Warehouse (Azure, R60,000/yr) never reached production; supplier GCT is reported bankrupt.

Recommendation. Migrate the asset register into the finance system and decommission Snipe-IT; retire the Data Warehouse and point Power BI directly at source databases (DOME inherits the role in Phase 2). ~R132,000/yr reclaimed.

5.3 Vendor custody, availability & data quality

F-02 Supplier / developer concentration

Rating: AMBER **Risk:** P1 **POPIA:** C7

Observation. The clinical core depends on one external developer (Garrett) at ~R350,000/yr all-in with no completed handover; SNowl's builder has left; iShout's handover is incomplete; the Data Warehouse supplier collapsed. Active knowledge loss is underway.

Recommendation. Progress code review → source escrow → clean handover; treat dependency reduction as a formal work-stream with maintenance under a contracted cadence.

F-01 / F-13 System sprawl & retirement candidates

Rating: AMBER **Risk:** P2 **POPIA:** —

Observation. Weak integration across 21 systems; ShoutLink unused ~1 year; Salesforce used only for lead capture.

Recommendation. Fold ShoutLink functions into SMART 2.0 web; replace/replicate Salesforce internally; no net-new sprawl.

F-03 HR → IT identity lifecycle gap

Rating: AMBER **Risk:** P2 **POPIA:** C7

Observation. No automated joiner/mover/leaver flow; orphaned accounts and delayed deprovisioning — evidenced directly by F-24 and F-28.

Recommendation. Automate lifecycle through Entra; recertify access quarterly.

F-15 iShout DataFree disabled

Rating: AMBER **Risk:** P2 **POPIA:** —

Observation. iShout's zero-rated ("DataFree") access is disabled, so AGYW users must fund their own data — undercutting reach and equity for the intended low-income audience.

Recommendation. Confirm the cause (cost/contract/technical) and restore DataFree in the action plan.

5.4 Sensitive data, AI & compliance

F-29 CHOMI on Botpress — offshore special-PI processing

Rating: RED **Risk:** P1 **POPIA:** §72 · C7 · C8

Observation. CHOMI, the GBV support chatbot, runs on Botpress cloud (confirmed not Azure, not SA-hosted). Its analytics dashboard shows live LLM calls on real traffic — 191 users, 431 sessions, 2,988 bot and 1,334 user messages last month. Survivor conversations (special personal information) therefore leave the country twice: to Botpress and to an offshore LLM. The system snapshot labels CHOMI "anonymous / minimal PII", yet the compliance questionnaire classes GBV data as special PI, and the FreshService handoff carries name, cell and location.

Recommendation. Put operator agreements (POPIA §20–21) in place with Botpress and the LLM provider; reconcile the classification to special PI; set retention/destruction on conversation logs; rotate the departed-developer credentials; then execute the recorded direction — rebuild CHOMI as a local AI + RAG bot on the Ionity edge (local LLM) so survivor data never leaves SA.

F-16 AI & model governance

Rating: AMBER **Risk:** P2 **POPIA:** C7

Observation. AI touchpoints (CHOMI, AIMEE, Self Cav, the planned reporting agent) need a consistent governance frame.

Recommendation. Apply one frame to every AI touchpoint: model provenance & hosting jurisdiction; prompt-injection & PII-leakage controls; human-in-the-loop escalation; conversation logging with retention.

F-14 MojaMind — most sensitive data & migration

Rating: AMBER **Risk:** P2 **POPIA:** C7 · SU ethics

Observation. MojaMind (e-art mental health) combines HIV status, mental-health data and potential minors — the estate's most sensitive profile; go-live slipped; a new supplier is needed post-launch.

Recommendation. Gate go-live on POPIA basis, ethics clearance and crisis-path readiness; land it in the retained Azure estate (within the R25,000 absorption barrier); delay contractor handover until the intervention completes.

F-18 – F-22 Data classification, minors, HPCSA, operators, funders

Rating: AMBER **Risk:** P2 **POPIA:** C3 · C7 · C8

Observation. Cross-cutting: special-PI scope not fully classified; minors' data engages the Children's Act; HPCSA clinical-data obligations; operator/processor agreements incomplete; funder (PEPFAR / Global Fund) evidence mapping outstanding.

Recommendation. Run a compliance evidence sprint in Phase 2: classify special PI, set retention/destruction schedules, execute operator agreements, and assemble the funder evidence register.

6. Consolidated Findings Register

ID	Domain	Finding	RYG	Prio
F-01	Integration	System sprawl & weak integration	AMBER	P2
F-02	Vendor custody	Supplier / developer concentration	AMBER	P1
F-03	Identity	HR→IT joiner/mover/leaver gap	AMBER	P2
F-04	Email security	~40 of ~200 mailboxes protected; phishing	RED	P1
F-05	Finance	Value-for-money of technology spend	AMBER	P2
F-06	Patch/change	Clinical core unmaintained ~18 months	RED	P1
F-07	Cost/licence	AWS commitment expiring Sep-2026	AMBER	P1
F-08	Cost	Azure billing anomaly (reads zero)	AMBER	P2
F-09	Finance	Finance systems not integrated	AMBER	P2
F-10	Fit-for-purpose	Sage Evolution V9 end-of-life	AMBER	P2
F-11	Cost	Snipe-IT dormant (R72k/yr)	AMBER	P2
F-12	Cost	Data Warehouse never implemented (R60k/yr)	AMBER	P2
F-13	Rationalise	ShoutLink under retirement review	INFO	P3
F-14	Sensitive data	MojaMind sensitive domain & migration	AMBER	P2
F-15	Access/reach	iShout DataFree disabled	AMBER	P2
F-16	AI governance	Model provenance / guardrails / logging	AMBER	P2
F-17	Cloud/POPIA	Residency CONFIRMED af-south-1 (§72 closed)	GREEN	—
F-18	Data class.	Special-PI scope	AMBER	P2
F-19	Compliance	Minors & the Children's Act	AMBER	P2
F-20	Compliance	HPCSA clinical governance	AMBER	P2
F-21	Compliance	Operator / processor agreements	AMBER	P1
F-22	Funders	PEPFAR / Global Fund evidence mapping	AMBER	P2
F-23	Cloud logging	CloudTrail disabled 18/18 regions	RED	P1
F-24	IAM	Root key + 0/6 MFA; dormant/vendor accounts	RED	P1
F-25	Network	Internet-open security groups (0.0.0.0/0)	RED	P1
F-26	Data exposure	Public S3 bucket	AMBER	P2
F-27	Resilience	Clinical RDS Single-AZ; two 2-day outages	AMBER	P2
F-28	Identity/Azure	Entra 1,000+ users vs ~200 mailboxes	RED	P1
F-29	AI/POPIA	CHOMI Botpress + offshore LLM — special PI	RED	P1

7. Recommendations & Remediation Roadmap

7.1 Quick wins (0–30 days)

- Enforce MFA on all AWS/Entra users; disable dormant and external-vendor accounts; rotate/delete stale access keys (F-24, F-03).
- Enable multi-region CloudTrail + Config + GuardDuty; close 0.0.0.0/0 security groups; fix the public S3 bucket (F-23, F-25, F-26).
- True-up email security to all ~200 mailboxes; enforce MFA on mail (F-04).
- Decide the AWS exit before the September commitment window; regularise the Azure billing anomaly (F-07, F-08).
- Decommission dormant Snipe-IT and retire the Data Warehouse — ~R132,000/yr reclaimed (F-11, F-12).

7.2 Short term (1–3 months)

- Stand up the Ionity Private Intranet cluster and parallel-run migrate the AWS workloads with zero clinic downtime.
- Confirm the finance consolidation path (Dynamics 365 vs Sage) after a fresh NPO demo; begin the 3/6/9-month hand-over.
- Reconcile the Entra directory; make Entra the single identity spine (F-28).

7.3 Medium term (3–6 months)

- Rebuild CHOMI as a local AI + RAG bot on the Ionity edge; execute operator agreements and retention schedules (F-16, F-29, F-21).
- Run the compliance evidence sprint (POPIA Conditions, minors, HPCSA, funder mapping); begin the ISO/IEC 27001 readiness programme.

7.4 The AWS exit — Ionity Private Intranet hosting

This estate does not need a hyperscaler; it needs sovereignty, a patch cadence and a predictable rand-denominated bill. The recommendation is a cluster of micro-computing nodes installed on Shout-It-Now premises, owned by Shout-It-Now, operated under an Ionity managed-service cadence.

CLINICAL tier — recommended	Detail
Topology	8 nodes: edge gateway · 2× app · HA database pair · sync · reporting · backup · monitoring
Once-off (CAPEX)	R118,500 — installed, hardened, handed over; hardware owned by the client
Managed hosting	R7,950 / month flat (R95,400/yr) — patching, 24/7 monitoring, backups, IR runbook, refresh reserve
vs AWS today	≈ R213,000/yr AWS-linked baseline → −55%; payback ≈ 12 months
Data residency	100% in-country by architecture; §22-ready logging; HA failover (answers F-27)

Azure and Microsoft 365 are retained as the identity and productivity backbone. What fits moves there — MojaMind (per its own plan), the asset register, M&E datasets and the HR→Entra lifecycle — with Ionity absorbing migration cost up to R25,000. Alternatives were weighed: lift-into-Azure (viable, higher run-rate), stay-on-AWS-and-harden (renewal roulette continues), local VPS/colocation (recreates the ops gaps), and a SOVEREIGN dual-site hybrid (the Phase-2 end-state).

7.5 Cost-benefit & savings realisation

Gain	Source	Annual (ZAR)
Exit AWS → Ionity intranet (all AWS workloads)	F-06 · F-07 · F-23–F-27	+ R117,600
Decommission Snipe-IT; register into finance	F-11	+ R72,000
Retire Data Warehouse; direct Power BI links	F-12	+ R60,000
Finance consolidation (D365 vs Sage V9, net)	F-05 · F-09 · F-10	+ R50,000
SSRS folded into intranet reporting node	F-SSRS	+ R36,000
Identified recurring gains	**before Phase-3 vendor savings**	**≈ R335,600 / yr**

Plus risk avoided: the AWS cliff never fires — up to ≈ R630,000/yr of exposure removed. The estate run-rate trends from ≈ R1.2m to ≈ R865,000/yr, with the poor-value portion falling from R620,000 to ≈ R285,000.

8. Compliance & Standards Readiness

8.1 POPIA posture

Residency (§72) is now GREEN — confirmed in-country. The remaining exposure is Condition 7 (security safeguards): no MFA, no logging, open perimeter, and offshore GBV-data processing (F-23, F-24, F-25, F-29). Condition 3 (accuracy — duplicate client records) and Condition 8 (retention — no destruction schedules) require the evidence sprint. §22 breach-notification cannot currently be met without centralised logging — closed by the monitoring node.

8.2 ISO/IEC 27001 readiness

Sequenced against Annex A: asset inventory (fixed by the register), access control (identity lifecycle + individual logins), operations security (patch cadence), supplier relationships (custody & escrow), and incident management (runbook + evidence). Phase-2 QMS documentation makes the readiness programme formal.

8.3 Funder & regulatory obligations

PEPFAR / Global Fund data-sovereignty and evidence requirements, and HPCSA clinical-data obligations, are answered by an evidence-first posture: restore drills, access logs, residency attestation and DR metrics become artefacts the client can hand over rather than claims it makes.

9. Forward Look & Conclusion

Phase 1 is complete. The estate is capable but under-governed, and paying for a fragmented past. The path forward is not “rip and replace” — it is exit the volatile, unguarded cloud; retain and harden what works; consolidate the sprawl; and re-home the most sensitive workloads onto sovereign, owned infrastructure. One architecture — the Ionity edge with local AI — answers both the clinical hub and the GBV chatbot.

Decisions required from the client: (D-1) approve the AWS exit before August 2026; (D-2) choose the finance backbone after the NPO demo; (D-3) mandate the quick-wins immediately; (D-4) sign off Phase-2 scope; (D-5) green-light the parallel FLOW and AI-reporting builds. The audit is self-funding — the fruit pays for the tree.

> **Bottom line.** ≈ R335,000/yr of recurring gains identified, an ≈ R630,000/yr cliff avoided, data residency confirmed, and a costed, zero-downtime route to a lean, sovereign, funder-ready estate.

Appendix A — Recorded system costs

System	Recorded annual cost	Direction
SMART 2.0 (all-in incl. vendor)	~R350,000	Exit AWS → Ionity intranet
iShout	R96,000	Exit → intranet; restore DataFree
MojaMind	~R84,000	Retained Azure (per plan)
Snipe-IT	R72,000	Decommission → finance system
Sage Evolution V9	~R70,000	Consolidate (D365 vs Sage)
Data Warehouse	R60,000	Retire → DOME (Phase 2)
CHOMI	R54,000	Rebuild as local RAG on edge
SSRS	R36,000	Fold into intranet reporting
Fusion	R24,000	Decide with Sage (coupled)
FreshService	R10,000	Retain (low lock-in)

Note. *Profiled systems total ≈ R856,000/yr; adding Microsoft 365 (~R132,000), payroll (S-Cube/BioSyn), Azure, Salesforce and connectivity brings the full IT run-rate to ≈ R1.2 million/yr. Figures are indicative, drawn from the system register (reviewed 27 Mar 2026) and console verification (20 Jul 2026); vendor confirmations at sign-off.*

Appendix B — Evidence index

- AWS Cost Explorer, account 334982276367, Jan–Jun 2026 — US$3,176.26 total, US$529.38/mo avg (console 20 Jul 2026).
- AWS IAM users — 6 users, 0/6 MFA, 4 dormant incl. external vendor; keys 1,374–1,633 days (console 20 Jul 2026).
- AWS EC2 regions — af-south-1 + eu-west-1 active; us-east-1 empty (console 20 Jul 2026).
- AWS Trusted Advisor — CloudTrail logging 18/18 regions RED (30 Jun 2026).
- CHOMI Botpress analytics — 191 users, 431 sessions, 2,988 bot + 1,334 user messages; live LLM activity/cost panels (20 Jul 2026).
- IA·MCP forensic engine — posture 33.7/100 Grade F; frameworks CIS/ISO 27001/SOC 2/NIST/POPIA.
- 14 system profiles; consolidated final report (Phase 1 v3); 158-document engagement repository.

Appendix C — Glossary

AGYW — Adolescent Girls & Young Women. CAPEX — capital expenditure. GBV — gender-based violence. HA — high availability. HPCSA — Health Professions Council of SA. IAM — identity & access management. IR — incident response. LLM — large language model. MFA — multi-factor authentication. NPC — Non-Profit Company. POPIA — Protection of Personal Information Act. PITR — point-in-time recovery. RAG — retrieval-augmented generation. RDS — AWS Relational Database Service. RTO/RPO — recovery time / point objective. SPOF — single point of failure. §72 — POPIA cross-border transfer condition.