Teteza360 Potential-Client Demonstration Pack

From fragmented compliance activity to accountable readiness

23 August 2026

Executive summary

Teteza360 gives a Malawian organisation one governed place to understand its personal-data processing, assess gaps, assign corrective work, connect credible evidence and demonstrate readiness. It replaces a fragile chain of spreadsheets, documents, email follow-ups and disconnected point tools with traceable workflows and clear human accountability.

Teteza360 does not sell an automatic “compliant” badge. It preserves the source, version, input, reviewer, decision, evidence and remaining risk behind an organisation’s current position.

Contact **sales@itesmw.com** to arrange a tailored demonstration.

The customer problem and market gap

Privacy programmes are operational programmes, but many organisations manage them as periodic document exercises. The resulting gap is not only knowledge of a law; it is the ability to turn requirements into repeatable work across departments and prove what happened later.

Common approach	Operational consequence
Spreadsheets for inventories and actions	Conflicting versions, weak ownership and difficult evidence traceability
Shared drives for evidence and policies	Unclear validity, review state, source and approved controlled copy
Email for incidents, requests and vendor reviews	Deadlines, decisions and separation of requester/internal communication become hard to reconstruct
Generic task tools	Flexible tasks without privacy-specific state, source mappings, frozen decisions or disclosure safeguards
Standalone policy or assessment tools	Results remain disconnected from ROPA, actions, evidence, incidents and management assurance
Ungoverned AI assistants	Answers may lack approved sources, data boundaries, fixed contracts and accountable human review

Teteza360 fills that operating gap by linking the programme: organisation facts → governed assessments → findings → accountable actions → reviewed evidence → ongoing registers → point-in-time reports.

Value proposition

For leadership: see current readiness, unresolved risk and evidence coverage without commissioning a fresh spreadsheet consolidation.
For DPO/compliance teams: coordinate the full programme through purpose-built state transitions and review gates.
For departments: receive bounded tasks and contribute evidence without receiving unrestricted administrative access.
For IT/security/procurement: connect safeguards, tests, vendor due diligence, contracts and transfers to the same accountability record.
For reviewers: receive scoped, watermarked, expiring access to selected immutable report snapshots.

Evidence-based differentiators

1. **Malawi-oriented legal-content governance.** Legal source versions, sections, obligations and controls have independent review and explicit publication; candidate content is not treated as legal truth.
2. **Separation of duties by design.** High-impact assessment, evidence, incident, privacy, vendor, transfer, security and publication workflows require authorised independent review.
3. **Reproducible outcomes.** Deterministic rule/assessment/security/transfer results freeze their inputs, versions and contributions rather than presenting unexplained scores.
4. **Evidence as a lifecycle.** Private files start quarantined, retain SHA-256, classification and scan state, and require controlled review and validity.
5. **Operational breadth with a shared record.** ROPA, DPIA, incidents, rights, consent, vendors, transfers, DPO work, security, training, registration, policies, regulatory updates and reports connect through one tenant boundary.
6. **Controlled external collaboration.** Rights, consent, vendor and audit-room portals use email-bound, expiring/revocable access; production raw secrets are not stored.
7. **Governed innovation.** Malamulo, document intelligence and voice intake default off and fail closed without approved routes/prompts/sources/files and human review.
8. **Tenant access assurance.** Platform status alone grants no tenant access; support is tenant-approved, purpose-bound, capability-scoped, MFA-confirmed and time-limited.

Demonstration: MBank

MBank is a fictional demonstration organisation. A recommended 45-minute journey is:

1. Dashboard and organisation profile — frame scope and attention.
2. Assessment — show governed questions, reproducible score and cited findings.

3. Action plan and evidence — turn a gap into owned work and independently reviewed proof.
4. ROPA and DPIA — show relational processing facts and risk treatment.
5. Incident or rights request — demonstrate clocks, tasks, human decisions and protected output.
6. Executive report and audit room — freeze assurance and share only selected evidence.
7. Assurance ledger — show access review and short-lived support controls.

The presenter should say what is implemented, identify default-off tools, and avoid entering production personal data.

Suggested implementation approach

Phase 1 — Discover (one to two weeks)

Confirm scope, entities/departments, roles, priority processing, existing registers/evidence, incident/request procedures, security controls, reporting expectations, integrations, hosting, retention and success measures. Produce configuration and migration plan.

Phase 2 — Configure and pilot (two to four weeks)

Provision tenant and named administrators; configure structure and access; establish profile, baseline assessment, priority ROPA and evidence; validate workflows with a pilot group; complete security/access acceptance and administrator training.

Phase 3 — Roll out (two to six weeks)

Onboard remaining departments in waves; register material processing, vendors, transfers, policies and open actions; establish governance calendar, reporting and support procedures. Timing depends on source-data quality and customer availability.

Phase 4 — Operate and improve

Run monthly attention reviews, quarterly access/management assurance and annual/material-change programme refresh. Track adoption, overdue actions, accepted evidence coverage, processing-review status, request/incident timeliness and exception attention—without converting metrics into an unconditional compliance claim.

Indicative pricing framework — non-binding

The following framework is for discovery and budgeting only. It is **not a quotation**, excludes applicable taxes and third-party costs, and must be replaced by an ITES-approved proposal.

Component	Indicative basis	Illustrative range (USD equivalent)
Foundation subscription	One tenant, core workspaces, standard support	350–750/month
Professional subscription	Expanded users/workflows, enhanced reporting/support	800–1,800/month
Enterprise programme	Multiple entities or complex assurance, tailored service	From $2,000/month
Implementation	Discovery, configuration, pilot, training	2, 500–12,000 one-time
Data preparation/migration	Based on volume, quality and mapping	Scoped after discovery
Optional governed-tool enablement	AI/document/voice governance and private runtime work	Scoped separately
Bespoke integration/development	Approved change request	Time-and-materials or fixed milestone

Final price should consider active users, organisations, data volume, service hours, recovery targets, hosting model, migration effort, training, integrations, bespoke controls and contract term. Quote in the agreed currency and address exchange-rate handling.

Draft service-level schedule — non-binding

This draft is subject to technical validation and contract. Availability excludes agreed maintenance, customer systems, internet/provider events outside the contracted boundary, force majeure and customer misuse.

Measure	Draft target
Service hours	24×7 platform availability; support handling per purchased tier
Monthly application availability	99.5% standard; enhanced target subject to architecture and price
P1 initial response	1 hour, 24×7 for enhanced support; 4 business hours standard
P2 initial response	4 business hours
P3 initial response	1 business day
Planned maintenance notice	5 business days where practicable
Backup recovery point / time	Deployment-specific and contractually tested; no default promise
Security incident notice	Without undue delay under agreed incident terms after confirmed relevant impact
Service reporting	Monthly on request/tier; incident report for material events

Service credits, measurement source, exclusions, escalation contacts, data processing terms, vulnerability handling, support hours, RPO/RTO and termination assistance must be negotiated in the signed schedule.

Customer-specific annex template

Customer legal name: [insert]
Teteza360 tenant(s): [insert]
Effective date and term: [insert]
Executive sponsor / tenant owner / DPO: [insert]
In-scope entities, branches and departments: [insert]
Active-user bands and roles: [insert]
Enabled workspaces: [insert]
Default-off governed tools approved: [none / Malamulo / document intelligence / voice intake; record prerequisites]
Hosting and data residency: [insert]
Customer-provided data/migration: [insert]
Authentication/MFA policy: [insert]
Support hours, contacts and escalation: [insert]
Availability, RPO and RTO: [insert after validation]
Backup/retention/offboarding terms: [insert]
Implementation milestones and acceptance: [insert]
Fees, taxes, currency and payment: [insert approved quotation]
Dependencies/exclusions: [insert]
Special security/privacy controls: [insert]
Authorised signatories: [insert]

Proposal checklist

- Discovery responses validated with customer stakeholders.
- Scope separates implemented, configurable and bespoke/roadmap capabilities.
- Named tenant(s), users, workspaces, data migration and integrations are explicit.
- Hosting, residency, security roles, support, availability and recovery targets are feasible.
- Price/currency/tax assumptions and third-party costs are clear.

- Implementation responsibilities, acceptance criteria and change control are agreed.
- Data protection, confidentiality, incident, audit and offboarding terms are reviewed.
- Demonstration used fictional MBank data and no production secrets.

Important limitations

Current repository scope excludes general-purpose public API/webhooks, enterprise SSO/SCIM, arbitrary tenant branding, automatic regulator submission, OCR for scans, deployed cloud AI connectors, vector search and physical tenant purge. Any such requirement needs discovery, design, security review, testing and a separate commercial commitment.

Book a demonstration

Email **sales@itesmw.com** with your organisation, sector, priority challenge, approximate users and preferred dates. ITES will tailor the MBank journey without requesting confidential production information before an appropriate agreement is in place.