Teteza360 Client Demonstration

Guided MBank privacy-programme journey

ITES · sales@itesmw.com

23 August 2026

Today’s outcome

See how one governed record connects:

organisation facts → assessment → gaps → actions → evidence → ongoing duties → assurance

Demonstration safety

- MBank is fictional and contains demonstration data
- No production passwords, tokens or customer records
- Teteza360 supports human accountability; it does not certify compliance
- Default-off tools will be identified explicitly

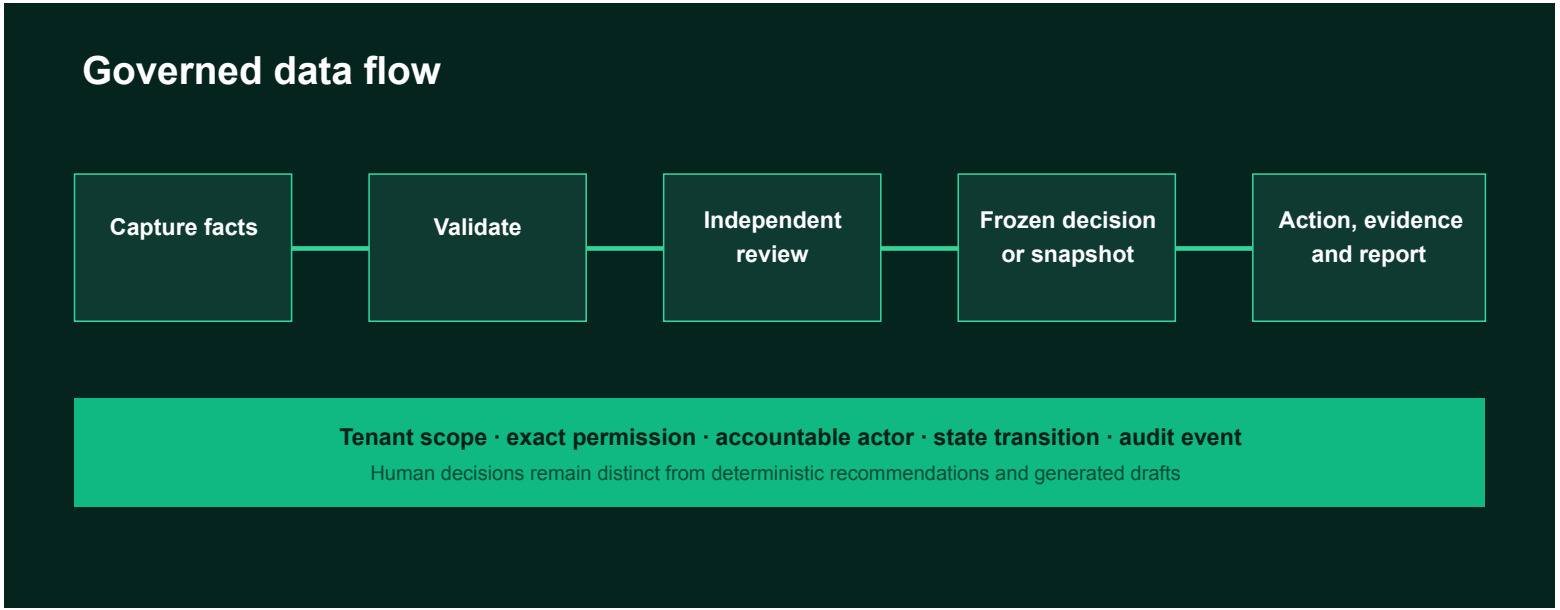
Why the workflow matters

Disconnected documents answer “what did we write?”

Teteza360 helps answer:

- What source and version informed the work?
- Who supplied facts and who independently reviewed?
- What action followed, by when, and with what evidence?
- What remained unresolved at the reporting date?

Architecture of trust



Teteza360 governed data flow

Step 1 — Establish MBank

Show: Dashboard · Organisation profiler · Structure · People

- Bounded operating facts and explainable flags
- Branches, departments and memberships
- Action-based system roles
- MFA gate for high-risk roles

MBank role personas

Persona	Demonstration focus
Organisation Owner	Configuration, access and accountability
DPO / Compliance Lead	Review, privacy programme and assurance
Executive Viewer	Read-focused management oversight
Department Champion	Assigned assessments, evidence and actions
Data Steward	Processing records and privacy operations
Procurement / Vendor Manager	Vendor, contract and transfer assurance

Step 2 — Assess current position

Show: Assessments

- Independently published definition
- Conditional, weighted questions
- Exact evidence and control mappings
- Reproducible score contributions
- Findings created from governed risk options

Step 3 — Put remediation in motion

Show: Action plans

- Plan approval before activation
- Owners, priorities, dates and state transitions
- Assigned contributors and attributable comments
- Closure criteria and independent decision

Step 4 — Connect credible proof

Show: Evidence

- Private file or HTTPS reference
- Classification, checksum and validity
- Quarantine and clean-scan requirement
- Control/finding mappings
- Independent review and expiry

Step 5 — Know the processing

Show: Data inventory (ROPA)

Relational record of purposes, recorded lawful bases, data/data-subject categories, systems, recipients and retention schedules.

Approved records are protected. CSV export is audited and spreadsheet-formula protected.

Step 6 — Assess privacy risk

Show: DPIAs

- Screening combines answers with ROPA facts
- Every trigger is preserved
- Likelihood × impact and treatment are deterministic
- High residual risk requires measures and DPO consultation
- Independent approval protects accountability

Choose a live operational scenario

A. Incident response

Provisional/confirmed awareness, protected clock, impact triage, human notification decision, draft and external reference.

B. Privacy rights request

Public intake, contact confirmation, separate identity gate, assigned searches, approved response and disclosure snapshot.

C. Vendor and cross-border transfer

Frozen due diligence, contract review, safeguards, risk and

Sustaining the programme

- DPO appointments, programmes, advice and board reports
- Security catalogue, tests, evidence-adjusted scores and exceptions
- Versioned training, quizzes, campaigns and certificates
- Registration readiness and checksum-protected exports
- Regulatory updates, policy versions and compliance inbox

Step 7 — Demonstrate readiness

Show: Reports · Audit room

- Point-in-time source manifest and checksum
- Executive readiness and incident report types
- Selected compatible snapshots only
- Email-bound, scoped, expiring guest access
- Watermark, history and immediate revocation

Access assurance

Show: Assurance ledger

- Frozen membership, role and MFA access reviews
- Purpose-bound ITES support capability
- Confirmed MFA and maximum eight-hour default
- Immediate revocation and minimised ledger export

Governed innovation — optional

Tool	Implemented guardrail	Current boundary
Malamulo	Approved route/prompt/source; cited fixed answer contract	Default off; local extractive reference
Document intelligence	Private extraction; reviewed non-destructive proposals	Default off; scans need manual transcription
Voice intake	Private file; reviewed transcript; explicit incident hand-off	Default off; private worker separately deployed

What Teteza360 does not automate

- Legal accountability and professional judgement
- Independent reviewer responsibility
- Regulator or data-subject submission
- Physical deletion across database, objects and backups
- Accuracy of customer facts or imported evidence

Implementation path

1. Discover operating model, priority data and success criteria
2. Configure access, profile, assessment and evidence standard
3. Pilot end-to-end with accountable reviewers
4. Roll out by department and priority workflow
5. Operate monthly attention and quarterly assurance cadence

Questions to settle in discovery

- Which entities, departments and users are in scope?
- Which registers and evidence are authoritative today?
- Which workflows and reports create the most risk or effort?
- What hosting, support, residency and recovery requirements apply?
- Which integrations or bespoke items are mandatory?

Next step

Tailored discovery and proposal

We will confirm fit, boundaries, implementation, service targets and commercial terms.

sales@itesmw.com