

Teteza360 Product Walkthrough

See accountable privacy-compliance work in
action with MBank

ITES · sales@itesmw.com

What you will see today

See how one governed record connects:

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

A safe, realistic demonstration

- 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

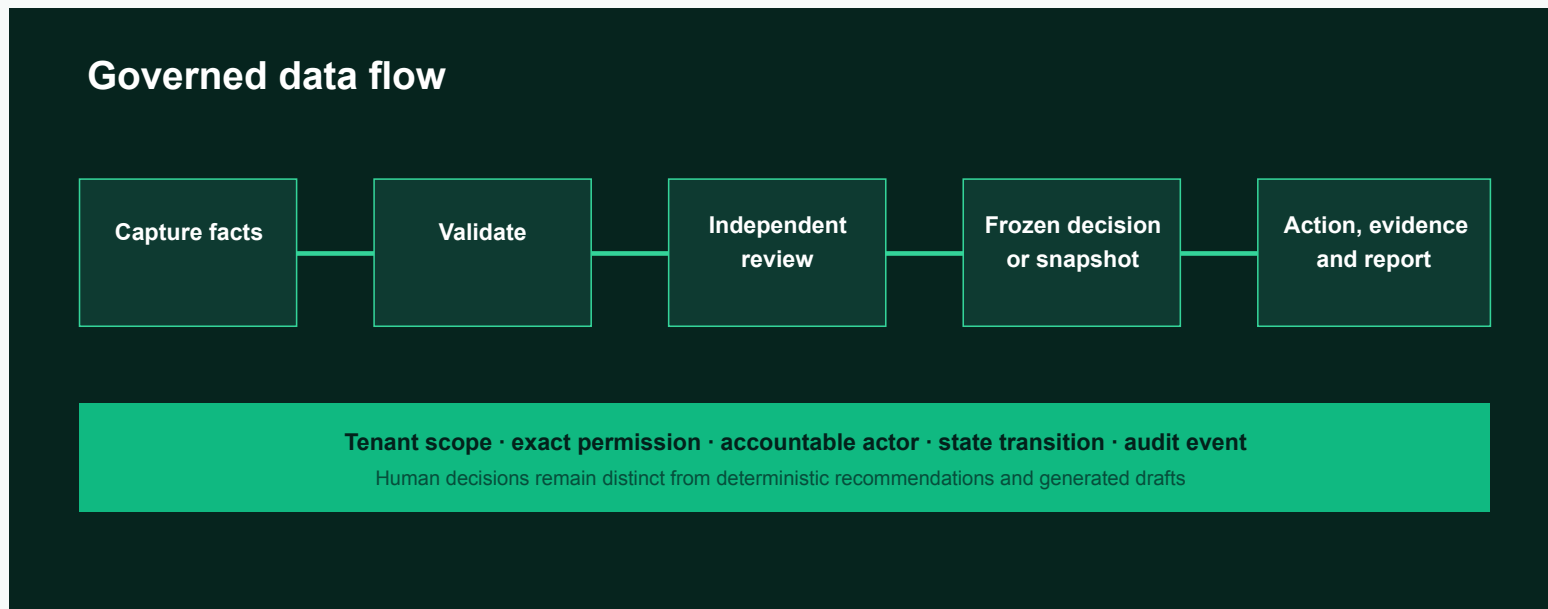
Why the workflow matters

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?

How Teteza360 protects accountable work



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

How different teams take part

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 the scenario most relevant to you

A. Incident response

Awareness, response clock, impact triage and notification decision.

B. Privacy rights request

Secure intake, identity checks, searches, response and disclosure.

C. Vendor and cross-border transfer

TE1127A369 · 1125
Due diligence, contracts, safeguards and transfer approval.

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

Optional tools, governed by design

Tool	How it helps	How it is governed
Malamulo	Provides source-grounded guidance with clear citations	Uses approved content and explicit human review
Document intelligence	Identifies data categories and potential clause gaps	Keeps extraction private and requires review before changes
Voice intake	Captures an incident account and supports structured follow-up	Protects recordings and requires transcript review before hand-off

Human judgement, supported by better evidence

- Authorised people retain responsibility for important decisions
- Independent review remains explicit in high-impact workflows
- Controlled drafts and records support approved external action
- Organisation facts and imported evidence remain reviewable
- Teteza360 preserves the context behind each decision

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

Help us tailor Teteza360 to your organisation

- 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?

Your next step

Tailored discovery and proposal

In a tailored discovery session, ITES will confirm fit, scope, implementation, service targets and commercial terms with your team.

sales@itesmw.com