

Teteza360

From fragmented privacy activity to accountable
readiness

ITES • sales@itesmw.com

The operating problem

Privacy obligations become fragmented work

- Requirements sit apart from operating facts
- Actions travel through email and spreadsheets
- Evidence loses ownership, validity and review state
- Leadership receives manually assembled, quickly stale reports

The market gap

Knowing the rule is not the same as operating it

Generic task tools manage tasks. Shared drives store files. Point solutions run assessments. Ungoverned AI answers questions.

The missing layer is a traceable chain from **source and facts** to **decision, action, evidence and assurance**.

The Teteza360 proposition

One governed privacy-compliance operating system

1. Understand the organisation and what applies
2. Assess current position with reproducible scoring
3. Convert gaps into owned, reviewed work
4. Connect current, controlled evidence
5. Operate incidents, requests and governance registers
6. Produce point-in-time management and reviewer assurance

What connects in one record

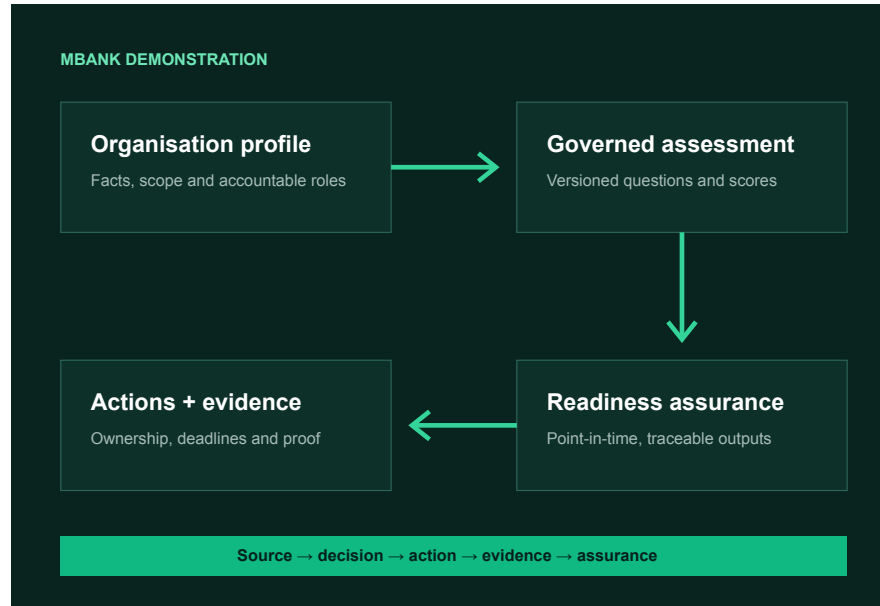
- Organisation, people, roles and access reviews
- Assessments, findings, actions and evidence
- ROPA, DPIAs, incidents, rights and consent
- Vendors, transfers, DPO, security and training
- Registration, regulatory updates and policies
- Reports, audit rooms and lifecycle governance

Why Teteza360 is different

Governance is part of the product—not a presentation layer

- Independent approval for high-impact transitions
- Versioned legal/content foundations
- Frozen inputs, decisions and report manifests
- Private evidence quarantine, checksum and review
- Layered tenant isolation and scoped support access
- Default-off AI/document/voice with human gates

MBank: demonstration journey



MBank readiness journey

Outcomes by stakeholder

Leadership	DPO / compliance	Operating teams
Current risk and readiness view	One programme workspace	Bounded, assigned contribution
Traceable management reports	Review gates and evidence lifecycle	Clear owners and dates
Controlled external assurance	Ongoing registers and attention	Less spreadsheet coordination

Implementation approach

Discover → Configure and pilot → Roll out → Improve

- Start with accountable owners and priority processing
- Establish a governed baseline and evidence standard
- Pilot end-to-end workflows with separate reviewers
- Roll out by department and measure operational adoption

Indicative commercial framework

Non-binding; subject to discovery and ITES approval

- Foundation: **\$350–\$750/month** illustrative
- Professional: **\$800–\$1,800/month** illustrative
- Enterprise: **from \$2,000/month** illustrative
- Implementation: **\$2,500–\$12,000** illustrative one-time

Migration, governed-tool enablement, integrations, enhanced service and taxes are separately scoped.

Honest current boundary

Not currently implemented: general public API/webhooks, enterprise SSO/SCIM, arbitrary tenant branding, automated regulator submission, OCR for scans, deployed cloud AI connectors, vector search or physical tenant purge.

Requirements in these areas move through discovery, security design, delivery and acceptance—not a demo promise.

Recommended next step

A 60-minute tailored discovery and MBank demonstration

Bring your accountable owner, DPO/compliance lead and technology/security representative.

sales@itesmw.com