SEVEN STEP
CONSULTING
ENABLING TRUST!

CASE STUDY

INDUSTRY: FINTECH DATA AND PAYMENTS PLATFORM

COMPLIANCE FRAMEWORK: ISO 27701 (PIMS)

COPYRIGHT AND DISCLAIMER

.

CASE STUDY FINTECH DATA AND PAYMENTS PLATFORM ISO 27701 (PIMS) IMPLEMENTATION TO EXTEND PRIVACY GOVERNANCE ON TOP OF AN ISO 27001-ALIGNED SECURITY PROGRAM

Note: This case study is prepared for marketing/portfolio use. Operational details are presented in ranges and generalized language to avoid disclosure of confidential information.

Engagement Snapshot	
Primary service	ISO 27701 (PIMS)
Industry focus	FinTech & Financial Services
Delivery model	Seven Step Framework (Define to Drive) + evidence-led audit readiness
Website	https://www.sevenstepconsulting.com/

CLIENT OVERVIEW

Field	Details
Client	FinTech platform handling customer and transaction data (client anonymized) APIs and data processing for partner ecosystems
Industry	FinTech & Financial Services
Company size (range)	Approx. 120-300 employees
Geography	India with customers/partners across multiple regions

BUSINESS CONTEXT

As privacy expectations increased, the organization needed a structured Privacy Information Management System (PIMS) to manage personal data responsibilities consistently across products, vendors, and operations. ISO 27701 was selected to formalize privacy governance and demonstrate accountability.

Trigger points included:

- Customer and partner contracts required clearer privacy commitments and proof of privacy controls.
- The platform processed personal data across multiple systems and vendors, increasing privacy risk exposure.
- Regulatory expectations (India privacy requirements and global customer expectations) required stronger governance.
- Leadership wanted a unified approach to privacy risk, DPIAs, and incident handling.

CHALLENGES

- Privacy responsibilities and roles were not consistently defined across teams (controller/processor obligations).
- Data inventory and processing purposes required better documentation and review discipline.
- Vendor and sub-processor privacy oversight needed standard criteria and repeatable assessments.
- Incident response needed privacy-specific escalation and notification decision workflows.
- Sustaining privacy controls across new features required SDLC integration.

.

ENGAGEMENT OBJECTIVES

- Implement ISO 27701-aligned PIMS integrated with existing security governance.
- Create data inventory, privacy risk assessment approach, and supporting processes (DPIA, DSR handling).
- Establish vendor privacy assurance workflow and evidence repository.
- Prepare audit-ready privacy artefacts and training for relevant stakeholders.

SEVEN STEP CONSULTING APPROACH

Phase	What we did
Define	Confirm PIMS scope, roles (controller/processor), and privacy objectives aligned to product and customer needs.
Discover	Identify data flows, processing activities, and existing privacy controls; perform gap assessment.
Design	Define process architecture, KPIs, and control points aligned to customer outcomes.
Document	Develop privacy policies, notices, procedures, and registers with ownership and cadence.
Deploy	Operationalize privacy controls and embed checks into SDLC, vendor onboarding, and incident workflows.
Do & Check	Run internal readiness checks, validate evidence quality, and remediate gaps
Drive	Establish periodic privacy reviews and management reporting to sustain ongoing compliance.

- Privacy policy framework, roles and responsibilities, and accountability model.
- Data inventory / records of processing activities (RoPA) and data flow documentation.
- Vendor privacy assessment checklist and sub-processor oversight workflow.
- Privacy incident response addendum (notification decision logic, escalation templates).
- Evidence repository structure and control-wise evidence checklists.
- Internal readiness review report and corrective action tracker.

OUTCOMES AND BUSINESS IMPACT

- Improved privacy governance through defined roles, data inventory, and repeatable processes.
- Better partner confidence via structured vendor privacy oversight and documented accountability.
- Reduced privacy risk through DPIA discipline and treatment tracking.
- Improved incident readiness by adding privacy-specific escalation and notification workflows.
- Sustained privacy posture through SDLC integration and periodic reviews.

STANDARDS AND FRAMEWORKS COVERED

- ISO/IEC 27701 - Privacy Information Management System (PIMS).
- ISO/IEC 27001:2022 - ISMS alignment (where integrated).
- GDPR and DPDP alignment considerations (where applicable).

SEVEN STEP
CONSULTING
ENABLiNG TRUST!

Seven Step Consulting Pvt. Ltd.

+91 8115609560

info@sevenstepconsulting.com

www.sevenstepconsulting.com

1006, 10th Floor, EMAAR Capital Tower 1, MG Road Sikanderpur, Sector 26, Gurugram, Haryana – 122002 (INDIA)