TRANSITION AUDIT APPROACH

ISO/IEC 27701:2019 → ISO/IEC 27701:2025

Privacy Information Management Systems (PIMS)

Document Reference	SIS-TAP-27701-001
Applicable Standard	**ISO/IEC 27701:2025** (replaces ISO/IEC 27701:2019)
Issue No. & Date of Issue	01 & June 2026
Prepared by	Compliance Head, SIS Certifications Pvt. Ltd.
Approved by	Managing Director, SIS Certifications Pvt. Ltd.
Transition Deadline (CB)	**October 31, 2026**
Transition Deadline (Clients)	**October 31, 2027**

1. Introduction

ISO/IEC 27701:2025 – the revised edition of the Privacy Information Management Systems (PIMS) standard – was published on **31 October 2025**. SIS Certifications Pvt. Ltd. (IAS Accreditation No. MSCB-131), as an IAS-accredited Certification Body, is required to complete its transition to this revised standard by **31 October 2026**, in accordance with IAS Technical Bulletin IAS/MSCB/127.

This document sets out the complete Transition Audit Approach adopted by SIS Certifications and is published for the benefit of all stakeholders – certified clients, prospective clients, associate auditors, CB staff, and other interested parties.

IMPORTANT NOTICE FOR ALL ISO/IEC 27701 CERTIFIED CLIENTS

All existing ISO/IEC 27701:2019 certificates must be transitioned to ISO/IEC 27701:2025 by 31 October 2027. Certificates not transitioned by this date will be withdrawn. Please contact SIS Certifications at the earliest to plan your transition audit.

2. Key Changes: ISO/IEC 27701:2019 vs ISO/IEC 27701:2025

The following table summarises the principal changes between the two versions of the standard.

Area of Change	ISO/IEC 27701:2019	ISO/IEC 27701:2025
Dependency	Extension to ISO/IEC 27001 and ISO/IEC 27002 – mandatory prerequisites	Standalone standard – no mandatory dependency on ISO 27001 or ISO 27002
Structure	Structured as extension clauses supplementing ISO 27001	Clauses 4–10 follow ISO Harmonized Structure (HLS) for independent use
PII Controllers	Annex A: Privacy controls for PII controllers	Annex A: Restructured with expanded, updated controls for PII controllers
PII Processors	Annex B: Privacy controls for PII processors	Annex B: Restructured with more comprehensive controls for PII processors
AI & Emerging Risks	No specific guidance on AI-driven data processing	Explicit guidance on AI-driven data processing and cross-border data transfers
Integration	Primarily integrated with ISMS (ISO 27001)	Easier integration with any management system via HLS alignment
Certification Scope	PIMS as an extension of existing ISMS certification	PIMS as independent certification or integrated with other MS certifications
ISO/IEC 27706	Not referenced	ISO/IEC 27706:2025 now referenced as companion document

Note: You can refer GAP ANALYSIS- 27701_2019 & 27701_2025 file for more details.

3. Transition Timeline

The following timeline governs the transition process for both SIS Certifications (as the CB) and its certified clients:

Date / Milestone	Activity / Obligation	Responsibility
31 October 2025	Publication of ISO/IEC 27701:2025	ISO/IEC
25 February 2026	IAS Technical Bulletin IAS/MSCB/127 issued	IAS
31 March 2026	SIS Certifications completes internal gap analysis & procedure updates	SIS Certifications
30 April 2026	New initial accreditation applications must be against ISO/IEC 27701:2025	SIS Certifications

By 30 June 2026	SIS Certifications submits Gap Analysis, updated procedures, personnel competence evidence to IAS	SIS Certifications
From CB transition date	All initial and recertification audits must be conducted against ISO/IEC 27701:2025	SIS Certifications
31 October 2026	IAS deadline: all accredited CBs must complete transition. CBs not transitioned lose PIMS accreditation.	IAS / SIS Certifications
By 31 October 2027	All certified clients must complete transition to ISO/IEC 27701:2025. Old certificates are withdrawn.	Certified Clients / SIS

4. SIS Certifications – CB Transition Actions

4.1 Gap Analysis & Procedure Updates

SIS Certifications has completed the following actions to demonstrate readiness for ISO/IEC 27701:2025 certification activities:

- Documented gap analysis mapping changes between ISO/IEC 27701:2019 and 2025
- Revision of SIS-P-09 (PIMS Certification Procedure) to incorporate standalone certification pathway
- Update of application review forms and audit checklists to reflect HLS structure and new Annex A/B controls
- Update of certification decision criteria and technical review procedures

4.2 Personnel Competence & Training

All personnel involved in ISO/IEC 27701:2025 certification activities – including auditors, application reviewers, and decision makers – shall demonstrate competence against the revised standard prior to being authorised:

- Awareness training on ISO/IEC 27701:2025 changes conducted for all PIMS auditors
- Competence evaluation records updated (training records, evaluation scores, certificates)
- Authorisation of audit team members evidenced and maintained in auditor competency files
- Internal MCQ-based training evaluation forms circulated to all PIMS-scheme personnel

4.3 Audit Programme Transition Plan

SIS Certifications has established a transition audit programme covering all currently certified PIMS clients. The programme includes:

- Identification of all clients holding ISO/IEC 27701 certificates with expiry dates
- Scheduling of transition audits within their existing certification cycle wherever possible
- Communication to each client via formal email outlining transition requirements and timeline
- Recording of transition status for each client in the certification management system

5. Transition Audit Approach – For Certified Clients

5.1 Transition Audit Duration (Mandays)

In accordance with IAS Technical Bulletin IAS/MSCB/127, the following minimum audit durations apply for transition audits:

Transition Audit Scenario	Minimum Auditor Days
Transition audit conducted together with a Recertification Audit	Minimum 0.5 auditor day
Transition audit conducted together with a Surveillance Audit	Minimum 1.0 auditor day
Transition audit conducted as a standalone / separate audit	Minimum 1.0 auditor day

Note: Transition audits shall not rely solely on document review. Verification of technological information security controls through on-site or remote assessment is required.

5.2 Transition Audit Scope & Focus Areas

The transition audit shall specifically review the following areas arising from changes introduced in ISO/IEC 27701:2025:

- Standalone implementation: evidence that the PIMS operates independently without mandatory linkage to ISO 27001/27002
- HLS alignment: how the organisation's management system documentation and processes have been updated to reflect Clauses 4–10 of the revised HLS structure
- Revised Annex A controls (PII Controller): updated privacy controls, documented implementation and effectiveness evidence
- Revised Annex B controls (PII Processor): updated controls covering data processor obligations, contracts, and accountability
- AI-driven data processing: identification, risk assessment, and controls for personal data processed through AI/automated systems
- Cross-border data transfers: policies, safeguards, and documented compliance with applicable data protection regulations (GDPR, PDPB, etc.)
- Updated Statement of Applicability (SoA) or equivalent reference document
- Internal audit and management review records against the revised standard
- Training and awareness records for personnel handling PII

5.3 Transition Audit Method

- **Interview of key roles:** Privacy/DPO, IT Security, Legal/Compliance, Process Owners
- **Document review:** updated policies, procedures, SOA, risk assessment, legal register
- Process observation and/or technical verification of information security and privacy controls (on-site or remote per IAF MD 4:2025 criteria)
- Review of corrective actions for any previously identified nonconformities
- **Sampling of records:** training, incident logs, data subject requests, vendor agreements

5.4 Possible Audit Outcomes

Finding Type	Description	Client Action Required
No Finding	Full conformance with ISO/IEC 27701:2025 demonstrated	Certificate upgraded to :2025
Observation	Minor improvement opportunity noted; no nonconformity	Address at next scheduled audit
Minor Nonconformity	Single/isolated gap not indicating system failure	Root cause and correction within 90 days
Major Nonconformity	Systematic or critical gap; PIMS effectiveness compromised	Immediate corrective action; certificate on hold until resolved
Transition Not Completed by Deadline	Client fails to complete transition by Oct 31, 2027	ISO/IEC 27701 certificate withdrawn by SIS Certifications

6. Consequences of Non-Transition

IMPORTANT: Consequences of Failing to Transition

If a certified client does not complete the transition audit to ISO/IEC 27701:2025 before **31 October 2027:**

- SIS Certifications will be required to WITHDRAW the client's ISO/IEC 27701 certificate.
- The client will no longer be able to claim ISO/IEC 27701 certification.
- Re-certification under ISO/IEC 27701:2025 will require a fresh initial audit cycle.
- SIS Certifications itself will lose IAS accreditation for PIMS activities if it does not complete its own transition by **31 October 2026**.

7. Action Required from Certified Clients

Clients currently holding ISO/IEC 27701 (PIMS) certification issued by SIS Certifications are requested to take the following steps without delay:

1. Review the changes introduced by ISO/IEC 27701:2025 (detailed in Section 2 of this document & Gap Analysis document) and assess your organisation's current PIMS against the revised requirements.
2. Conduct an internal gap analysis and update your PIMS documentation, Statement of Applicability, and controls accordingly.
3. Contact SIS Certifications Compliance Head at compliance@siscertifications.com to schedule your transition audit at the earliest opportunity.
4. Ensure that internal audits and management reviews against ISO/IEC 27701:2025 are completed prior to the transition audit.
5. Plan your transition well in advance to avoid last-minute scheduling constraints and risk of certificate withdrawal.

8. Information for Associate Auditors

All associate auditors empanelled with SIS Certifications for PIMS (ISO/IEC 27701) scheme audits must comply with the following prior to conducting ISO/IEC 27701:2025 transition or certification audits:

- Complete the SIS Certifications ISO/IEC 27701:2025 awareness training and pass the internal competence evaluation (minimum score 70%)
- Obtain authorisation from the Compliance Head / Diector-Operations for conducting audits under the revised standard
- Demonstrate familiarity with AI-driven data processing risks, cross-border transfer safeguards, and updated Annex A/B controls
- Maintain updated CPD records reflecting 27701:2025-specific training
- **Note:** Auditors authorised only for ISO/IEC 27701:2019 cannot independently conduct 2025 transition audits until re-authorised

9. Contact Information

For queries relating to ISO/IEC 27701:2025 transition, please contact:

Contact Point	Details
Organisation	SIS Certifications Pvt. Ltd.
Accreditation No.	MSCB-131 (IAS Accredited)
Reference Bulletin	IAS/MSCB/127 – February 25, 2026

Document Control

This document is issued for public information purposes on the SIS Certifications website. It shall be reviewed and updated whenever material changes occur to the transition requirements or IAS/ other AB instructions.

For the latest version, visit: www.siscertifications.com

GAP ANALYSIS: ISO/IEC 27701:2019 vs ISO/IEC 27701:2025 with Impact Level

#	Clause / Section	ISO/IEC 27701:2019 Requirement	ISO/IEC 27701:2025 Requirement	Change Type	Impact Level
S-01	Overall Standard Structure	Extension to ISO/IEC 27001:2013 and ISO/IEC 27002:2013. Must be used in conjunction with these two standards. Clause numbering follows ISO 27001/27002.	Standalone Privacy Information Management System (PIMS) standard. No longer dependent on ISO 27001 or ISO 27002. Clauses 4–10 follow ISO Harmonized Structure (HS).	**RESTRUCTURED**	**HIGH**
S-02	Normative References	Normative references: ISO/IEC 27000, ISO/IEC 27001:2013, ISO/IEC 27002:2013, ISO/IEC 29100	Normative reference: ISO/IEC 29100 only. ISO 27001/27002 referenced as optional information security programme guidance.	**MODIFIED**	**HIGH**
S-03	Scope	Specifies requirements for PIMS as extension to ISO 27001. Applicable within context of ISMS.	Specifies requirements for establishing, implementing, maintaining and continually improving a standalone PIMS. No ISMS prerequisite.	**MODIFIED**	**HIGH**
S-04	Terms & Definitions	References ISO/IEC 27000 and ISO/IEC 29100. Limited PIMS-specific definitions (joint PII controller, PIMS).	Comprehensive standalone definitions: organization, interested party, top management, management system, policy, objective, risk, process, competence, documented information, performance, continual improvement, effectiveness, requirement, conformity, nonconformity, corrective action, audit, measurement, monitoring, joint PII controller, customer, PIMS, information security programme, SoA.	**EXPANDED**	**MEDIUM**

#	Clause / Section	ISO/IEC 27701:2019 Requirement	ISO/IEC 27701:2025 Requirement	Change Type	Impact Level
C-01	Clause 4 – Context (4.1 Org & Context)	ISO 27001 cl.4 applied with PIMS extension. Organization determines role (PII controller/processor), applicable legislation, etc.	New standalone requirement: Org determines external/internal issues, its role as PII controller/processor, and relevant context. Climate change as new explicit consideration.	**MODIFIED**	**MEDIUM**
C-02	Clause 4.2 – Interested Parties	Extension of ISO 27001 cl.4.2 – must include PII principals as interested parties.	Standalone requirement to determine interested parties, their relevant requirements, which will be addressed by PIMS. PII principals explicitly included. Customer definition expanded with detailed notes.	**MODIFIED**	**LOW**
C-03	Clause 4.3 – Scope	Extension of ISO 27001 cl.4.3 – PIMS scope must include PII processing.	Standalone scope determination considering internal/external issues and interested party requirements. PII processing explicitly in scope.	**RETAINED**	**LOW**
C-04	Clause 4.4 – PIMS	Extension of ISO 27001 cl.4.4 – establish/implement/maintain/improve PIMS per 27001 cls 4-10 + this document.	Standalone: establish/implement/maintain/improve PIMS including processes and their interactions per THIS document only.	**MODIFIED**	**HIGH**
C-05	Clause 5 – Leadership (5.1 Leadership & Commitment)	ISO 27001 cl.5.1 applies with PIMS extension. Top management demonstrates leadership for information security AND privacy.	New standalone leadership requirements specific to PIMS: ensuring privacy policy and objectives are set; integrating PIMS into business processes; providing resources; communicating importance; directing continual improvement.	**MODIFIED**	**MEDIUM**

#	Clause / Section	ISO/IEC 27701:2019 Requirement	ISO/IEC 27701:2025 Requirement	Change Type	Impact Level
C-06	Clause 5.2 – Privacy Policy	Extension of ISO 27001 cl.5.2. Policy extends to include privacy commitment alongside information security.	Standalone Privacy Policy requirements: appropriate to organization purpose; framework for privacy objectives; commitment to applicable requirements; commitment to continual improvement. Must be documented, communicated, available to interested parties.	**MODIFIED**	**MEDIUM**
C-07	Clause 5.3 – Roles & Responsibilities	Extension of ISO 27001 cl.5.3. Includes privacy-specific roles such as Data Protection Officer.	Standalone: Top management assigns responsibility for (a) PIMS conformity and (b) reporting PIMS performance to top management.	**MODIFIED**	**LOW**
C-08	Clause 6.1 – Risk Assessment (Privacy Risk)	ISO 27001 cl.6.1 extended: dual risk assessment – information security risk AND privacy risk assessment.	Standalone privacy risk assessment process: criteria, consistent/valid results, identify/analyse/evaluate privacy risks for org AND PII principals. Risk owners identified. References ISO/IEC 27557.	**RESTRUCTURED**	**HIGH**
C-09	Clause 6.1.3 – Risk Treatment	Extension of ISO 27001 cl.6.1.3. Controls compared against Annex A AND B (separate for controllers/processors) AND ISO 27001 Annex A.	Standalone risk treatment: select options; determine controls; identify/document information security programme (min. 15 areas including AI-related topics); compare with Annex A; produce SoA; formulate treatment plan; obtain risk owner approval.	**RESTRUCTURED**	**HIGH**
C-10	Clause 6.2 – Privacy Objectives	Extension of ISO 27001 cl.6.2 – information security and privacy objectives.	Standalone privacy objectives: consistent with privacy policy; measurable; account for requirements; monitored, communicated, updated; documented. Planning for how to achieve objectives.	**MODIFIED**	**MEDIUM**

#	Clause / Section	ISO/IEC 27701:2019 Requirement	ISO/IEC 27701:2025 Requirement	Change Type	Impact Level
C-11	Clause 6.3 – Planning of Changes	Not explicitly addressed as separate clause in 2019.	NEW CLAUSE: When changes to PIMS are determined, they shall be carried out in a planned manner.	**NEW**	**MEDIUM**
C-12	Clause 7 – Support (Resources, Competence, Awareness, Communication, Documented Info)	ISO 27001 cls 7.1–7.5 extended with PIMS-specific requirements (awareness of privacy risks, privacy-specific training, documented info for PIMS).	Standalone requirements for resources, competence (with documented evidence), awareness (of privacy policy, contribution to effectiveness, implications of non-conformity), communication (what/when/with whom/how), documented information control.	**MODIFIED**	**MEDIUM**
C-13	Clause 8 – Operation (Operational Planning & Control)	ISO 27001 cls 8.1–8.3 extended. Operational planning, risk assessment, risk treatment as PIMS extension.	Standalone operational requirements: plan, implement, control PIMS processes; control planned changes; review unintended changes; ensure outsourced processes controlled.	**MODIFIED**	**MEDIUM**
C-14	Clause 9 – Performance Evaluation (Monitoring, Internal Audit, Mgmt Review)	ISO 27001 cls 9.1–9.3 extended. Monitoring/measurement, internal audit, management review – all extended to include privacy.	Standalone performance evaluation: monitoring/measurement/analysis/evaluation with documented info; internal audit programme with criteria, scope, frequency, methods; management review inputs include previous review results, changes in context, KPIs, NCRs, opportunities for improvement.	**MODIFIED**	**MEDIUM**
C-15	Clause 10 – Improvement (Nonconformity, Continual Improvement)	ISO 27001 cls 10.1–10.2 extended. Nonconformity and corrective action; continual improvement.	Standalone: Nonconformity reaction; root cause analysis; corrective action effectiveness; documented information. Continual improvement of PIMS suitability, adequacy, effectiveness.	**MODIFIED**	**LOW**

#	Clause / Section	ISO/IEC 27701:2019 Requirement	ISO/IEC 27701:2025 Requirement	Change Type	Impact Level
A-01	Annex Structure	Annex A (normative) – PII Controller controls (Table A.1, 31 controls across 4 domains) Annex B (normative) – PII Processor controls (Table B.1, 18 controls across 4 domains) SEPARATE annexes for controllers and processors	Single unified Annex A (normative) for both PII Controllers AND PII Processors combined. Controls restructured with expanded coverage including AI-driven data processing, cross-border transfers.	**RESTRUCTURED**	**HIGH**
A-02	PII Controller Controls – Conditions for Collection	A.7.2 – 8 controls: Identify purpose, Identify lawful basis, Determine consent process, Obtain/record consent, Privacy impact assessment, Contracts with processors, Joint PII controller, Records of processing.	Unified Annex A – Conditions for collection and processing controls retained and enhanced with: explicit AI processing guidance; enhanced cross-border transfer requirements; stronger lawful basis documentation.	**MODIFIED**	**HIGH**
A-03	PII Controller Controls – Obligations to PII Principals	A.7.3 – 10 controls: Obligations, Information for principals, Providing information, Consent mechanism, Objection mechanism, Access/correction/erasure, Informing third parties, Copy of PII, Handling requests, Automated decision making.	Retained in unified Annex A with enhanced automated decision making guidance to reflect AI-driven processing.	**MODIFIED**	**MEDIUM**
A-04	PII Controller Controls – Privacy by Design/Default	A.7.4 – 9 controls: Limit collection, Limit processing, Accuracy and quality, PII minimization objectives, De-identification and deletion, Temporary files, Retention, Disposal, PII transmission controls.	Retained in unified Annex A. Strengthened data minimization and de-identification requirements.	**RETAINED**	**LOW**
A-05	PII Controller Controls – Sharing/Transfer/Disclosure	A.7.5 – 4 controls: Basis for transfer between jurisdictions, Countries/orgs for transfer, Records of transfer, Records of disclosure.	Retained and expanded in unified Annex A with explicit guidance for cross-border transfers and AI-processed data.	**MODIFIED**	**HIGH**

#	Clause / Section	ISO/IEC 27701:2019 Requirement	ISO/IEC 27701:2025 Requirement	Change Type	Impact Level
A-06	PII Processor Controls	Annex B (separate) – 18 controls across: Conditions for collection (B.8.2 – 6 controls), Obligations to principals (B.8.3 – 1 control), Privacy by design (B.8.4 – 3 controls), Sharing/transfer (B.8.5 – 8 controls).	Merged into unified Annex A alongside controller controls. Processor-specific controls identified within unified structure.	**RESTRUCTURED**	**HIGH**
A-07	NEW – AI & Emerging Technology Controls	No explicit controls for AI-driven data processing in 2019 edition.	NEW explicit guidance and controls for: AI-driven data processing; automated profiling; AI-based decision making with PII implications; algorithm transparency.	**NEW**	**HIGH**
A-08	NEW – Cross-Border Transfer (Enhanced)	7.5.1–7.5.2 and 8.5.1–8.5.2 cover jurisdictional transfers but limited in scope.	Expanded cross-border transfer framework: adequacy decisions, appropriate safeguards, SCCs, BCRs, derogations – aligned with current global privacy law landscape.	**MODIFIED**	**HIGH**
A-09	Information Security Programme	Security controls derived from ISO 27002:2013 (mandatory normative reference). All 14 domains of ISO 27002 apply.	Organization identifies and documents its own information security programme (not mandated to use ISO 27002, but ISO 27002 is recommended). Programme must address 15 specified areas minimum.	**RESTRUCTURED**	**HIGH**
A-10	Statement of Applicability (SoA)	SoA references ISO 27001 Annex A controls + PIMS Annex A + PIMS Annex B controls. Three reference sets.	Standalone SoA references unified Annex A controls only. Includes: necessary controls, justification for inclusion, implementation status, justification for exclusion.	**RESTRUCTURED**	**HIGH**