GSDC
Global Skill Development Council

ISO/IEC 27701

Quick Reference Guide

www.gsdcouncil.org

1. Introduction to ISO/IEC 27701:2025

What is ISO/IEC 27701?

ISO/IEC 27701:2025 is an international standard for establishing, implementing, maintaining, and continually improving a Privacy Information Management System (PIMS). It helps organizations manage privacy risks and demonstrate accountability for the processing of Personally Identifiable Information (PII).

The 2025 revision brings this standard to full standalone status, strengthening its applicability across a wide range of regulatory environments, including GDPR, CCPA, and other regional privacy frameworks. It provides a comprehensive, auditable structure for privacy governance that goes beyond documentation to verify real-world effectiveness.

Objectives of ISO/IEC 27701

Protect Personal Data

Safeguard PII from unauthorized access, disclosure, and misuse.

Strengthen Privacy Governance

Establish clear accountability and oversight structures.

Demonstrate Regulatory Compliance

Support alignment with global privacy regulations.

Reduce Privacy Risks

Systematically identify, assess, and treat privacy threats.

Support Continual Improvement

Drive ongoing enhancement of the PIMS lifecycle.

2. Privacy Information Management System (PIMS)

A PIMS is a structured management system used to govern the collection, processing, storage, sharing, retention, and disposal of personal information. It provides the organizational framework that ensures PII is handled responsibly, transparently, and in accordance with applicable legal and regulatory requirements.

A mature PIMS integrates policies, procedures, risk assessments, monitoring activities, and continual improvement mechanisms into a cohesive system. It enables organizations to not only meet compliance obligations but to demonstrate that privacy is embedded into their culture and operations.

Privacy Policies

Governance and strategic direction for PII handling across the organization.

Risk Management

Identification, assessment, and treatment of privacy-related risks.

Controls

Technical and organizational safeguards to protect personal information.

Audits

Internal and external verification of conformity and effectiveness.

Monitoring

Ongoing performance evaluation through metrics and reviews.

Improvement

Structured approach to corrective actions and continual enhancement.

3. Key Terms and Definitions

Personally Identifiable Information (PII)

Information that can directly or indirectly identify an individual. PII is the core subject matter of the standard and includes any data point – or combination of data points – that could reasonably link back to a specific natural person.

- Name & Email
- Phone Number
- Passport Number
- Employee ID
- IP Address

Core Role Definitions

PII Controller

Entity that determines the purposes and means of processing PII. Bears primary accountability for lawful and fair processing.

PII Processor

Entity that processes PII on behalf of a controller, acting under documented instructions and contractual safeguards.

Data Subject

The individual whose personal information is being processed and who holds associated privacy rights.

Privacy Risk

Potential impact arising from inappropriate collection, processing, storage, disclosure, or destruction of PII.

4. ISO Management System Structure

ISO/IEC 27701 follows the High-Level Structure (HLS) used by modern ISO management system standards. This harmonized framework enables seamless integration with ISO/IEC 27001 and other management systems, reducing duplication of effort and supporting a unified approach to governance. Auditors must understand how Clauses 4 through 10 map to PIMS requirements.

Each clause builds on the previous, creating a plan-do-check-act cycle that drives continual improvement. Lead Auditors must assess conformity across all seven clauses during a certification or surveillance audit, examining both documented evidence and practical implementation.

5. Clause 4 – Context of the Organization

Clause 4 requires organizations to understand the internal and external factors that can affect their ability to achieve the intended outcomes of the PIMS. This contextual analysis forms the foundation for all subsequent planning and risk management activities. Auditors verify that the scope of the PIMS is clearly defined and that relevant factors have been systematically identified and documented.

Internal Issues

- Organizational structure and culture
- Technology environment and infrastructure
- Business processes involving PII
- Existing management systems and controls
- Governance frameworks and accountability structures

External Issues & Interested Parties

External Issues include:

- Privacy regulations and legal requirements
- Industry expectations and standards
- Customer and stakeholder requirements
- Emerging privacy threats and technologies

Interested Parties include: Customers, Employees, Regulators, Business Partners, Data Subjects, and Supervisory Authorities.

Audit Tip: Verify that the organization's PIMS scope statement explicitly reflects the context analysis and identifies all relevant interested parties and their privacy-related requirements.

6. Clause 5 – Leadership

Leadership Responsibilities

Top management must visibly demonstrate commitment to the PIMS. This goes beyond signing a policy – it includes allocating adequate resources, integrating privacy into strategic objectives, and ensuring that accountability is clearly defined throughout the organization. Auditors look for evidence of active sponsorship, not passive endorsement.

01

Demonstrate Commitment

Active participation in PIMS governance at the executive level.

02

Establish Privacy Policies

Approved, communicated, and regularly reviewed privacy policy.

03

Define Responsibilities

Clear assignment of privacy roles and authorities across functions.

04

Provide Resources

Budget, personnel, and technology to support PIMS operations.

05

Promote Continual Improvement

Drive a culture of ongoing privacy enhancement.

Privacy Policy Requirements

The privacy policy is a cornerstone artifact of the PIMS. It must be aligned with the organization's strategic direction, address all applicable privacy obligations, and be communicated effectively to all relevant personnel and interested parties.

Supports Business Objectives

Policy aligns privacy commitments with organizational strategy.

Addresses Privacy Obligations

References applicable legal, regulatory, and contractual requirements.

Communicated Organization-Wide

Accessible to all employees and relevant external parties.

7. Clause 6 – Planning

Planning under ISO/IEC 27701 requires organizations to apply risk-based thinking to identify, assess, and treat privacy risks. Effective planning ensures that controls are proportionate to identified risks and that privacy objectives are measurable, monitored, and aligned with business needs. Auditors examine the rigor and completeness of risk assessments and the relevance of defined privacy objectives.

1

Risk Identification

Identify privacy threats, vulnerabilities, and potential impacts.

2

Risk Assessment

Evaluate the likelihood and potential impact of identified risks.

3

Risk Treatment

Select and implement appropriate controls and mitigation strategies.

4

Privacy Objectives

Set measurable, monitored goals aligned with business needs.

Privacy Objectives must be: **Measurable** – so progress can be tracked; **Monitored** – with defined metrics and review cycles; **Aligned** – with organizational strategy and applicable regulatory requirements.

8. Clause 7 – Support

Clause 7 addresses the enabling resources and infrastructure that underpin an effective PIMS. Without adequate support – in terms of people, tools, awareness, and documented information – even a well-designed management system will fail in practice. Lead Auditors pay close attention to the competence of personnel and the completeness of documented information during support audits.

Personnel

Sufficient, competent staff assigned to PIMS roles.

Technology

Systems and tools to support privacy controls.

Budget

Adequate financial resources allocated to PIMS activities.

Training

Role-based privacy awareness and competence programs.

Documented Information

The standard requires organizations to maintain and retain specific documented information as evidence of PIMS conformity and effectiveness. Auditors verify the existence, adequacy, and control of these records.

- Privacy Policy and supporting procedures
- Risk assessment and treatment records
- Audit programs and audit reports
- Corrective action and nonconformity records
- Training and awareness records
- Privacy incident logs
- Management review minutes and outputs

9. Clause 8 – Operation

Clause 8 is where the PIMS moves from theory into practice. Organizations must implement and control the processes needed to meet privacy requirements and to manage identified risks. This clause also introduces the principle of Privacy by Design, requiring that privacy considerations be embedded into systems, processes, and products from the outset – not retrofitted after the fact.

Collection

Ensure lawful basis for all PII collection. Minimize data gathered to what is strictly necessary.

Processing

Process information only for authorized, documented purposes consistent with original collection intent.

Storage

Protect confidentiality, integrity, and availability of stored PII through appropriate technical controls.

Sharing

Control all disclosures through agreements, access controls, and transfer mechanisms.

Retention

Define and enforce documented retention schedules aligned with legal requirements.

Disposal

Securely destroy or anonymize PII when retention periods expire or purpose is fulfilled.

Privacy by Design: Integrate privacy controls into the design of systems, products, and processes from inception. Auditors look for evidence that privacy impact assessments and design reviews occur before deployment, not after.

10. Clause 9 – Performance Evaluation

Organizations must establish a systematic approach to monitoring, measuring, analyzing, and evaluating the performance of the PIMS. Clause 9 ensures that the system remains effective over time and that issues are identified proactively. Lead Auditors assess whether monitoring mechanisms are robust, internal audits are conducted at planned intervals, and management reviews are substantive rather than ceremonial.

Monitoring Activities

- Privacy metrics and KPI tracking
- Compliance reviews against regulatory requirements
- Internal audit program execution
- Management review cycles
- Third-party and supplier performance monitoring

Internal Audit Requirements

Internal audits must verify conformity to ISO/IEC 27701, assess the effective implementation of controls, and confirm ongoing regulatory compliance. Audits should be planned based on risk and conducted by competent, impartial personnel.

Management Review Inputs

1

Audit Findings

Summary of internal and external audit results.

2

Privacy Incidents

Status of reported incidents and resolution trends.

3

Risk Assessments

Updated risk register and treatment plan status.

4

Regulatory Changes

New or amended privacy laws affecting the PIMS.

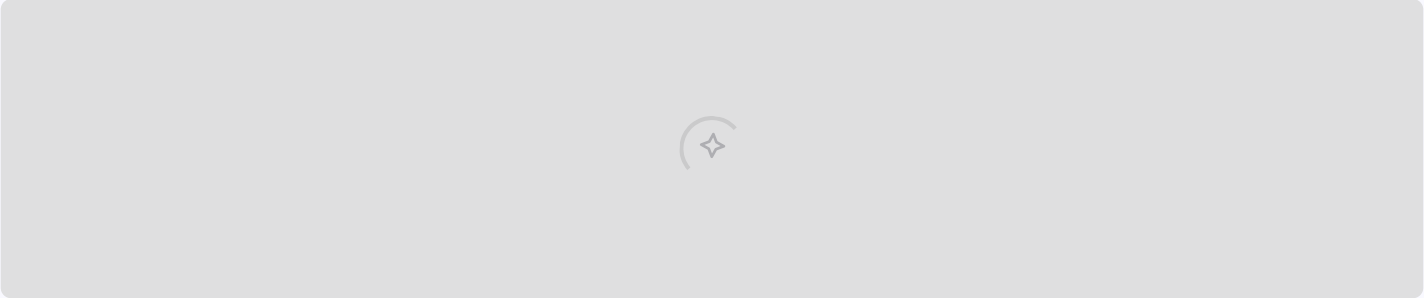
5

KPI Performance

Progress against defined privacy objectives and metrics.

11. Clause 10 – Improvement

Clause 10 closes the PDCA cycle by requiring organizations to act on identified nonconformities and to continually improve the PIMS. A strong corrective action process is a hallmark of a mature PIMS, and auditors pay close attention to whether root cause analysis is genuinely performed and whether corrective actions are effective in preventing recurrence.



Beyond corrective actions, Clause 10 requires proactive identification of improvement opportunities – even in the absence of nonconformities. Organizations should demonstrate that they continuously seek to enhance the effectiveness of their privacy controls, not merely react to failures. Auditors look for evidence of improvement initiatives driven by management reviews, audit findings, and performance data.

Identify Issues

Systematic detection of nonconformities through audits, monitoring, and reporting channels.

Investigate Causes

Rigorous root cause analysis to understand underlying drivers, not just symptoms.

Implement Corrections

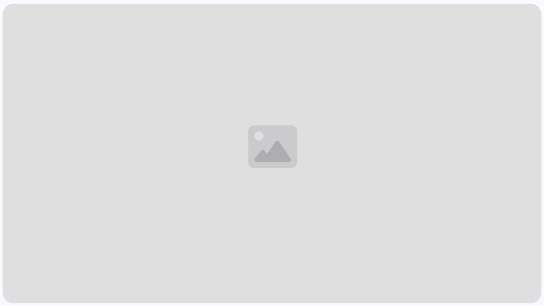
Time-bound corrective actions with assigned ownership and progress tracking.

Prevent Recurrence

Systemic changes to processes, controls, or training to eliminate root causes.

12. Privacy Risk Management Framework

Effective privacy risk management is central to the ISO/IEC 27701 framework. Organizations must establish a structured process for identifying, assessing, evaluating, treating, and monitoring privacy risks throughout the PII lifecycle. The risk management process must be repeatable, documented, and proportionate to the nature and scale of PII processing activities.



Privacy risk sources are diverse and evolve continuously. Organizations must consider both internal threats – such as employee error or system misconfiguration – and external threats, including third-party processors, cyber attacks, and regulatory enforcement actions. Risk treatment options include implementing technical controls, revising processes, accepting residual risk with documented justification, or avoiding high-risk processing activities altogether.

13. PII Controller Responsibilities

PII Controllers bear the primary accountability for all personal data processing within their sphere of control, including activities carried out by processors on their behalf. Under ISO/IEC 27701:2025, controllers must be able to demonstrate not only that they comply with privacy obligations but that they have systematically operationalized those obligations through documented policies, procedures, and controls.

Determine Processing Purposes

Define the lawful basis and specific purpose for all PII processing activities before collection begins.

Manage Consent

Obtain, record, and honor data subject consent where required. Maintain audit trails demonstrating valid consent mechanisms.

Respond to Data Subject Requests

Handle access, correction, deletion, and portability requests within mandated timeframes.

Monitor Processors

Maintain contracts with processors, conduct due diligence, and verify processor compliance through audits and assessments.

Demonstrate Accountability

Maintain comprehensive records of processing activities, impact assessments, and compliance evidence.

14. PII Processor Responsibilities

PII Processors act under the authority and instructions of the controller, but they carry independent obligations under ISO/IEC 27701:2025. A processor cannot simply claim compliance by pointing to contractual agreements – they must operationalize those agreements with real technical and organizational controls, and be prepared to provide evidence of this during an audit.

Process Per Instructions

Process PII solely in accordance with documented controller instructions. Any deviation requires explicit authorization.

Protect PII

Implement appropriate technical and organizational measures to ensure the security and confidentiality of personal data.

Notify Incidents

Promptly inform the controller of any privacy incidents or suspected breaches involving PII under processor custody.

Maintain Processing Records

Keep accurate records of all processing activities carried out on behalf of the controller, including sub-processor arrangements.

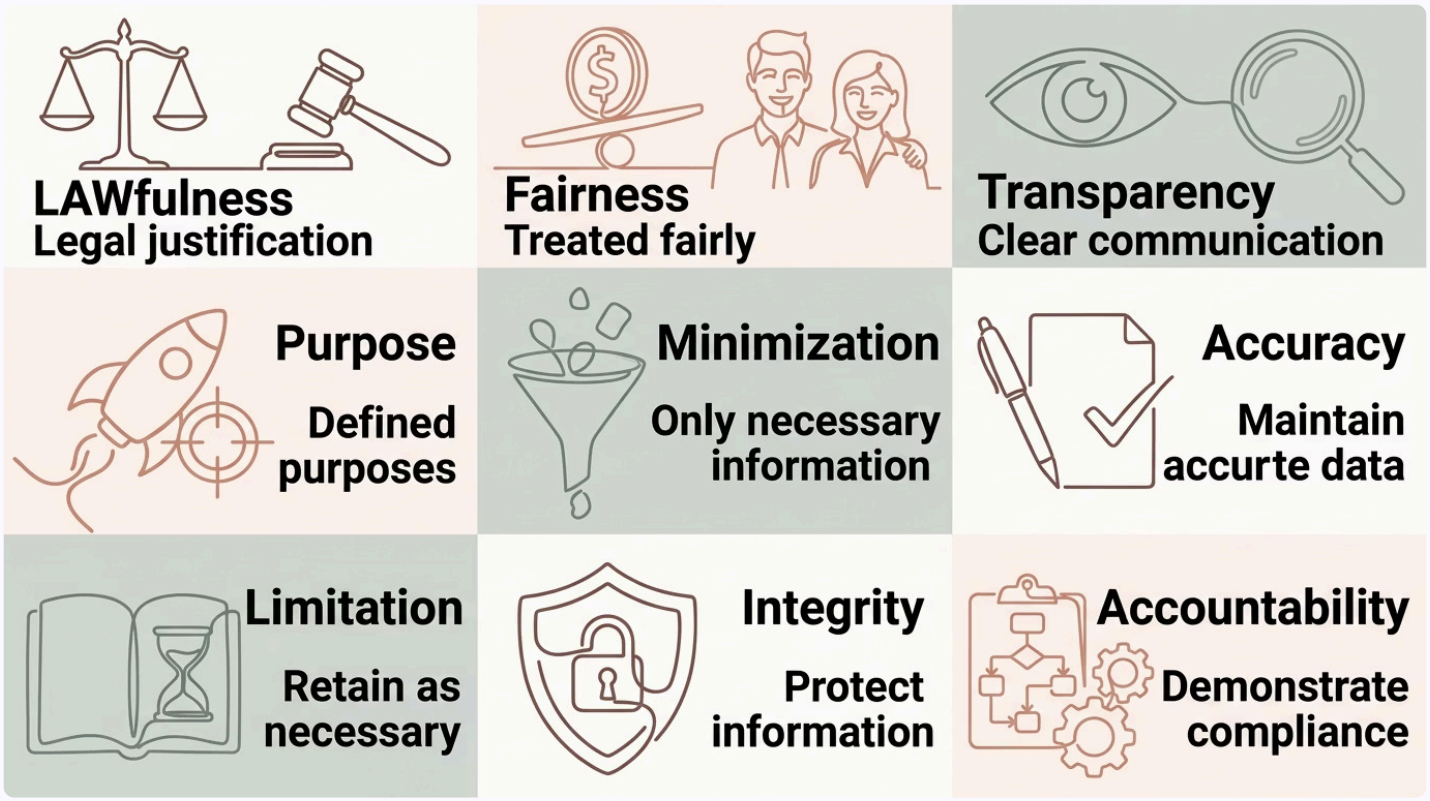
Support Controller Compliance

Cooperate with and assist the controller in meeting their obligations, including data subject rights fulfillment and regulatory enquiries.

⚠ Audit Focus: When auditing a PII Processor, verify that sub-processor agreements are in place, that incident notification timelines are defined, and that the processor can demonstrate independent control implementation – not just contractual acknowledgment.

15. Privacy Principles

The privacy principles embedded in ISO/IEC 27701:2025 reflect internationally recognized standards for responsible data handling. These principles underpin every clause of the standard and serve as the evaluative lens through which auditors assess the overall maturity and integrity of a PIMS. They are not isolated requirements – they are interconnected commitments that collectively define what it means to process PII responsibly.



16. Internal Audit Process

A well-executed internal audit is one of the most powerful tools available for verifying PIMS effectiveness. It goes beyond checking documentation – it examines whether privacy controls are genuinely implemented, consistently applied, and producing the intended outcomes. Lead Auditors must be proficient in planning and executing internal audits that are risk-based, evidence-driven, and impartial.

Audit Objectives

- Verify conformity to ISO/IEC 27701 requirements
- Assess the effectiveness of implemented controls
- Identify opportunities for improvement
- Confirm ongoing regulatory compliance
- Provide management with objective assurance

Audit Evidence Examples

Policies & Procedures

Documented controls and governance frameworks.

Records & Logs

Processing records, incident logs, consent registers.

Interviews

Conversations with personnel to verify awareness and practice.

Observations

Direct observation of processes and system configurations.

17. Audit Findings

Accurate classification of audit findings is a critical competency for Lead Auditors. Misclassifying a major nonconformity as minor – or failing to recognize a genuine opportunity for improvement – can undermine the credibility of the audit and expose the organization to unmanaged risk. Auditors must apply consistent, evidence-based judgment when categorizing findings and communicate them with precision in the audit report.

Conformity

The requirement is fully met. Objective evidence confirms that the control or process is implemented and effective. No action required beyond maintaining current practice.

Opportunity for Improvement (OFI)

A recommendation to enhance effectiveness or efficiency. Does not indicate a failure of conformity but signals a potential area to strengthen the PIMS.

Minor Nonconformity

An isolated deviation from a requirement that does not systematically undermine PIMS effectiveness. Requires a documented corrective action and follow-up verification.

Major Nonconformity

A significant failure that threatens the integrity or effectiveness of the PIMS, or indicates a systemic breakdown. Requires immediate corrective action and may affect certification status.

18. Lead Auditor Responsibilities

The Lead Auditor plays a pivotal role in the success of a PIMS audit program. Beyond technical knowledge of the standard, an effective Lead Auditor must demonstrate strong interpersonal skills, sound judgment, and an unwavering commitment to impartiality. Audit practices for Lead Auditors are commonly aligned with ISO 19011 auditing principles and certification auditing approaches.

01

Plan the Audit

Define scope, objectives, criteria, and schedule. Develop the audit plan and checklist based on identified risks and prior findings.

02

Manage the Audit Team

Assign responsibilities, brief team members, and ensure competence and impartiality across all assigned auditors.

03

Conduct Opening Meeting

Introduce the audit team, confirm scope and objectives, and establish communication protocols with auditee management.

04

Review Evidence

Collect and evaluate objective evidence through document review, interviews, observation, and system testing.

05

Evaluate Findings

Classify observations accurately as conformities, OFIs, minor nonconformities, or major nonconformities.

06

Lead Closing Meeting

Present findings to auditee management, confirm understanding, and outline next steps for corrective actions.

07

Prepare Audit Report

Produce a clear, objective, and complete audit report within agreed timelines. Ensure impartiality throughout.

19. Audit Principles

The principles that govern auditor conduct are not bureaucratic formalities – they are the ethical and professional foundation upon which audit credibility rests. These principles, aligned with ISO 19011, define how Lead Auditors must conduct themselves throughout every phase of the audit lifecycle. Violations of these principles – even perceived ones – can invalidate audit findings and compromise the organization's certification standing.

Integrity

Act with honesty, diligence, and responsibility throughout all audit activities. The foundation of auditor professionalism.

Fair Presentation

Report audit findings, conclusions, and obstacles accurately and completely. Avoid selective or misleading communication.

Due Professional Care

Exercise sound judgment and apply appropriate competence at every stage. Recognize the limits of your expertise.

Confidentiality

Protect all information obtained during the audit. Never disclose findings or evidence outside authorized channels.

Independence

Remain free from bias and conflicts of interest. Auditors must not audit activities they are directly responsible for.

Evidence-Based Approach

Base all conclusions on verifiable, objective evidence. Avoid assumptions or subjective assessments unsupported by facts.

20. Privacy Incident Management

Privacy incidents represent some of the highest-stakes events in an organization's PIMS lifecycle. Whether caused by technical failures, human error, or malicious action, incidents must be managed through a structured, documented process that prioritizes containment, investigation, and prevention of recurrence. Auditors evaluate the maturity of incident detection, response capabilities, and post-incident learning mechanisms.

Privacy Incident Examples

Data Breach

Unauthorized access to PII through system compromise or insider threat.

Unauthorized Disclosure

PII shared with parties outside the authorized scope or consent framework.

Lost or Stolen Device

Unencrypted device containing PII lost or stolen, creating potential for unauthorized access.

Misdirected Email

Personal information sent to incorrect recipients due to human error.

Third-Party Compromise

Processor or supplier breach affecting PII under controller responsibility.

Incident Response Process

Detect

Identify the incident through monitoring, reporting, or third-party notification.

Assess

Evaluate severity, scope, and potential impact on data subjects and regulatory obligations.

Contain

Immediately limit the spread or impact of the incident through technical and procedural controls.

Investigate

Conduct root cause analysis to fully understand what happened and why.

Remediate

Implement corrective actions to address identified vulnerabilities and restore normal operations.

Review

Conduct post-incident review to capture lessons learned and improve future response.

21. Key Documentation

Documented information is the backbone of audit evidence. Without adequate documentation, organizations cannot demonstrate conformity – and auditors cannot draw objective conclusions about PIMS effectiveness. ISO/IEC 27701:2025 requires both maintained documented information (living documents like policies and procedures) and retained documented information (records of activities performed). Lead Auditors must verify that all mandatory documentation is current, controlled, and accessible.

Privacy Policy & Risk Records

The foundational governance document plus all associated risk assessment and treatment records. Must be reviewed and updated regularly to reflect changes in context, technology, and regulations.

Audit Program & Reports

Documented audit plans, schedules, checklists, and completed audit reports with findings and recommendations. Evidence that the internal audit program is functioning as planned.

Training & Corrective Action Records

Evidence that personnel have received appropriate privacy training, alongside records of nonconformities, corrective actions taken, and verification of closure.

Incident Logs & Management Reviews

Comprehensive records of all privacy incidents, their investigation and resolution, plus minutes and output records from management review meetings demonstrating active governance.

22. Privacy Metrics & KPIs

Meaningful measurement is essential to demonstrating PIMS effectiveness and driving continual improvement. Privacy metrics should be selected based on the organization's specific risk profile, regulatory context, and strategic objectives. They must be tracked consistently, reported to management, and used as inputs to the management review and improvement processes. Auditors evaluate whether metrics are genuinely informative or merely performative.

KPI	Purpose	Target Indicator
Privacy Incidents – Count & Severity	Risk monitoring and trend analysis	Declining trend over time
Data Subject Requests – Response Time	Compliance monitoring against legal deadlines	100% within mandated timeframes
Audit Findings – Open vs. Closed	PIMS effectiveness measurement	All findings closed within agreed timelines
Training Completion Rate	Awareness and competence measurement	⩾95% of relevant personnel trained annually
Corrective Action Closure Rate	Improvement monitoring	⩾90% closed on schedule
Risk Assessment Currency	Risk management effectiveness	All assessments reviewed within 12 months

KPIs should be reviewed at every management review cycle. If a metric consistently meets its target without variation, consider whether it is genuinely measuring performance or simply confirming that the activity occurred.

23. Common Audit Nonconformities

Understanding the most frequently cited nonconformities in ISO/IEC 27701 audits is essential preparation for both auditors and auditees. These recurring failures often reflect systemic weaknesses in PIMS implementation rather than isolated errors. Recognizing the patterns – and knowing what objective evidence to look for – enables Lead Auditors to conduct more targeted and impactful audits.

1

Missing Privacy Risk Assessments

No documented risk analysis covering PII processing activities. A fundamental requirement – its absence typically constitutes a major nonconformity.

2

Inadequate Consent Management

Organization cannot demonstrate valid consent was obtained or is maintained. Particularly critical where consent is the stated legal basis for processing.

3

Incomplete Data Retention Controls

No documented retention schedule, or schedule exists but is not operationalized. PII being retained beyond defined periods without justification.

4

Insufficient Training

Employees unable to articulate their privacy responsibilities or demonstrate awareness of applicable policies. Training records absent or outdated.

5

Weak Incident Response Procedures

Privacy breaches not properly detected, documented, or escalated. No evidence of post-incident learning or corrective action.

6

Missing Internal Audits

Audit program not implemented or internal audits not conducted at planned intervals. Critical gap in the performance evaluation clause.

24. Best Practices for ISO/IEC 27701 Auditors

Excellence in PIMS auditing requires more than clause knowledge. The best Lead Auditors combine deep technical understanding with sharp investigative instincts, strong communication skills, and an unrelenting focus on real-world effectiveness. These best practices represent the habits and disciplines that distinguish good auditors from great ones – and are especially relevant to exam candidates and practitioners seeking to elevate their audit quality.

Core Audit Disciplines

Understand Applicable Privacy Regulations

Know the regulatory landscape – GDPR, CCPA, sector-specific laws – and how they interact with PIMS requirements.

Focus on Privacy Risks

Use risk as your audit compass. Follow the risk trail to test whether controls are proportionate and effective.

Verify Effectiveness, Not Just Documentation

Documents describe intent. Observations, interviews, and records reveal reality. Always test both.

Maintain Auditor Independence

Declare and manage conflicts of interest. Never audit your own work or areas where you have advisory relationships.

Advanced Auditor Mindset

Review Objective Evidence

Seek corroborating evidence from multiple sources – document, interview, and observe independently.

Evaluate Continual Improvement

Ask not just "is it working?" but "is it getting better?" Evidence of genuine improvement distinguishes mature systems.

Assess Privacy Governance Maturity

Look beyond technical controls to examine whether privacy is embedded in culture, decision-making, and strategic planning.

Follow Evidence-Based Auditing

Every finding must be traceable to specific, documented evidence. Never raise findings based on intuition alone.

Quick Revision Checklist

Use this checklist as a final preparation tool before your exam or audit engagement. Each item represents a domain where Lead Auditor candidates must demonstrate competence. Work through each category systematically and revisit any area where your confidence is below full confidence.

Core Concepts

- [ ] PIMS – definition, purpose, and scope
- [ ] PII – examples and classification
- [ ] Controller vs. Processor – roles and responsibilities
- [ ] Privacy Principles – all nine, with definitions
- [ ] Privacy Risk – sources, assessment, and treatment

Clauses 4–10

- [ ] Clause 4 - Context of the Organization
- [ ] Clause 5 - Leadership and policy requirements
- [ ] Clause 6 - Planning and risk-based thinking
- [ ] Clause 7 - Support and documented information
- [ ] Clause 8 - Operation and Privacy by Design
- [ ] Clause 9 - Performance Evaluation and internal audits
- [ ] Clause 10 - Improvement and corrective actions

Auditing Competencies

- [ ] Audit Principles – all six, with application examples
- [ ] Audit Planning – scope, criteria, objectives
- [ ] Audit Evidence – types and collection methods
- [ ] Audit Findings – classification and reporting
- [ ] Corrective Actions – process and verification
- [ ] Lead Auditor Responsibilities – full lifecycle

Governance & Compliance

- [ ] Privacy Policy – requirements and communication
- [ ] Risk Management – full framework
- [ ] Incident Management – response process
- [ ] Internal Audit – program and execution
- [ ] Management Review – inputs and outputs
- [ ] Data Subject Rights – controller obligations
- [ ] Privacy Metrics & KPIs – selection and use

You are ready to audit when you can explain each item on this checklist with confidence, identify the objective evidence that would demonstrate conformity, and recognize when a finding should be classified as major, minor, or an opportunity for improvement.

GSDC
Global Skill Development Council

CERTIFIED ISO 27701 LEAD AUDITOR

ABOUT GSDC CERTIFICATION

EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.

LEARNING MATERIALS

Get access to learning materials such as videos, ebooks, templates, and practice exams, which will help you clear the certification exam.

CREATED BY EXPERTS

GSDC certifications are created and authored by world's leading experts in the field.

LEARNING OBJECTIVE

- Gain insights into autonomous decision-making processes
- Apply knowledge using ready-to-implement templates
- Demonstrate ability to work with Agentic AI models
- Validate your skills wit

Enroll now with the code **LEARN20** To avail **20%** discount

Enroll Now

www.gsdcouncil.org