GSDC
Global Skill Development Council

ISO/IEC 27701

Audit Checklist & Audit Program Guide

www.gsdcouncil.org

1. Introduction to ISO/IEC 27701 Auditing

What is an ISO/IEC 27701 Audit?

An ISO/IEC 27701 audit is a systematic, independent, and documented process used to evaluate whether an organization's Privacy Information Management System (PIMS) conforms to standard requirements, is effectively implemented, is maintained and monitored, supports privacy objectives, and demonstrates accountability for PII processing. These audits serve as a cornerstone of any robust privacy governance program, providing objective assurance to stakeholders that privacy commitments are being met in practice – not merely on paper.

Audits under ISO/IEC 27701 extend beyond simple documentation review. They require auditors to evaluate the effectiveness of implemented controls, the adequacy of privacy risk management, and the degree to which the organization's privacy culture supports continual improvement. A well-executed audit produces actionable insights that strengthen the PIMS and build organizational resilience against privacy risks.

Audit Objectives

Verify Compliance

Confirm conformance with ISO/IEC 27701 requirements across all clauses

Assess Governance

Evaluate the effectiveness of privacy governance structures and accountability

Evaluate Risk Mgmt

Assess whether privacy risks are identified, treated, and monitored appropriately

Identify Nonconformities

Detect deviations from requirements and drive corrective action

Support Improvement

Identify opportunities to strengthen the PIMS and privacy outcomes

2. Audit Types

ISO/IEC 27701 audits are conducted at three distinct levels, each serving a different stakeholder purpose and carrying different implications for the organization being assessed. Understanding the differences between audit types is essential for proper scoping, resource allocation, and setting appropriate audit objectives.

First-Party Audit

Internal audit conducted by the organization.

- Assess internal PIMS compliance
- Prepare for certification audits
- Improve privacy management processes
- Identify gaps before external review

Second-Party Audit

Audit conducted on suppliers or service providers.

- Evaluate PII processors and vendors
- Assess privacy obligations in contracts
- Verify processor compliance posture
- Manage supply chain privacy risk

Third-Party Audit

Independent certification audit by accredited body.

- Certification or surveillance audits
- Independent compliance verification
- Provides formal certification evidence
- Conducted by accredited certification bodies

3. Audit Principles

The following core principles underpin every ISO/IEC 27701 audit engagement. These principles are not optional guidelines – they represent the professional and ethical foundation upon which audit credibility rests. Auditors who internalize and consistently apply these principles produce audit results that are trusted, defensible, and genuinely useful for organizational improvement.

Integrity

Auditors must act ethically and professionally at all times. Personal integrity is the foundation of professionalism. Auditors should be honest, diligent, and responsible in their work, and never allow personal interests or external pressure to influence findings.

Fair Presentation

Audit findings, conclusions, and reports must be accurate, truthful, and objective. Findings must reflect the actual state of the PIMS, neither overstated nor minimized. Significant obstacles and unresolved divergences should be disclosed.

Due Professional Care

Auditors must exercise sound judgment commensurate with the importance of the task and the confidence placed in them. This includes recognizing the potential to make errors and applying appropriate diligence throughout the process.

Confidentiality

Sensitive information acquired during the audit must be safeguarded. Auditors shall not use audit information for personal advantage or in a manner that would be detrimental to the legitimate interests of the auditee.

Independence

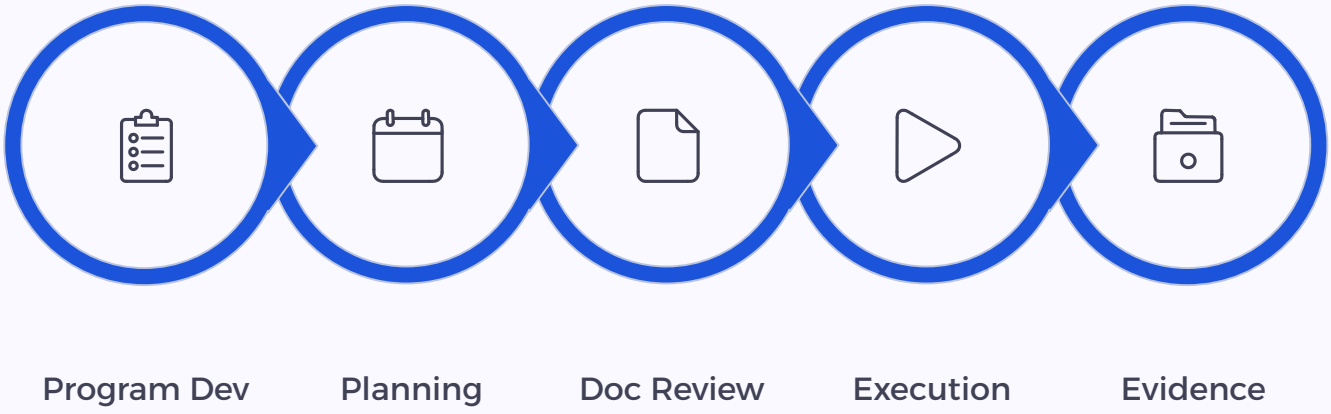
Auditors must remain impartial and free from bias or conflict of interest. Independence is the basis for the impartiality of the audit and objectivity of audit conclusions.

Evidence-Based Approach

Audit conclusions must rely on verifiable, reproducible evidence. The audit evidence must be sufficient and appropriate to support audit findings. Sampling is necessary since a complete audit is rarely feasible.

4. ISO/IEC 27701 Audit Lifecycle

A successful PIMS audit follows a defined and structured lifecycle. Each phase builds upon the previous one, ensuring that audit activities are purposeful, well-documented, and lead to meaningful outcomes. Adhering to this lifecycle helps audit teams maintain consistency, thoroughness, and professional rigor across all engagements. Understanding the full lifecycle also helps auditees prepare more effectively and allocate resources appropriately at each stage.



Each phase of the audit lifecycle serves a distinct purpose. The early phases – program development, planning, and document review – lay the groundwork for an efficient on-site execution. The middle phases focus on gathering and evaluating objective evidence. The final phases translate that evidence into actionable findings, formal reports, and verified corrective actions that close the loop and drive genuine improvement in the PIMS.

5. Audit Program Development

An audit program defines the overarching framework within which individual audits are planned, scheduled, managed, and monitored over a defined period – typically one year. A well-constructed audit program ensures that all significant areas of the PIMS receive appropriate audit attention, that resources are allocated efficiently, and that audit activities are coordinated to minimize disruption to the organization while maximizing coverage and value.

Audit Program Components

01

Scope

Areas and processes to be audited within the PIMS boundary

02

Objectives

Desired outcomes aligned with privacy and compliance goals

03

Frequency

Audit schedule reflecting risk levels and operational cycles

04

Resources

Audit team composition, tools, and budget requirements

05

Risk Considerations

Privacy and compliance risks informing audit prioritization

06

Reporting Requirements

Communication process, distribution, and escalation paths

Sample Annual Audit Program

Quarter	Audit Area	Focus
Q1	Privacy Governance	Leadership, policy, objectives
Q2	PII Processing Activities	Lawfulness, purpose, retention
Q3	Third-Party Processors	DPAs, vendor controls, oversight
Q4	Incident Management & Compliance	Detection, response, improvement

Audit frequency should be risk-based. High-risk areas may require more frequent review than the standard annual cycle.

6. Audit Planning Template

Effective audit planning is critical to ensuring the audit is conducted efficiently and achieves its objectives. The planning phase establishes the scope, criteria, methods, and logistics that guide all subsequent audit activities. A well-structured audit plan communicates expectations clearly to both the audit team and the auditee, reducing surprises and enabling productive cooperation during execution.

Audit Information Fields

Field	Description / Guidance
Audit Title	Descriptive name identifying the audit engagement
Audit Type	Internal / External / Certification / Surveillance
Audit Scope	Boundaries and extent of the audit coverage
Audit Objectives	Specific outcomes the audit aims to achieve
Audit Criteria	ISO/IEC 27701 clauses, policies, and legal requirements
Lead Auditor	Name and qualifications of the responsible auditor
Audit Dates	Planned start and end dates for audit activities

Scope Statement Example

> The audit will assess the organization's Privacy Information Management System covering privacy governance, risk management, PII processing activities, data subject rights management, incident management, and third-party privacy controls.

The scope statement should be precise and unambiguous, identifying which organizational units, processes, locations, and system elements are included. A clearly defined scope prevents scope creep and helps audit teams allocate time and resources proportionally across areas of risk and regulatory exposure.

Always align audit scope with the organization's PIMS certification scope statement to ensure consistency with the registered PIMS boundary.

7. Audit Preparation Checklist

Before the audit commences, auditors should verify that essential documentation and records are available and accessible. Adequate preparation by both the audit team and the auditee is a prerequisite for an efficient, productive audit. The following checklist outlines the key documents and records that should be confirmed as in place prior to beginning formal audit activities. Missing items should be flagged as potential indicators of control weaknesses.

1

Privacy Policy

Current, approved, and communicated privacy policy available for review

2

Privacy Objectives

Documented, measurable privacy objectives aligned with business strategy

3

Risk Assessments

Completed privacy risk assessments with documented treatment decisions

4

Internal Audit Records

Previous internal audit reports and findings available for trend analysis

5

Management Review Records

Minutes and outputs from management review meetings

6

Incident Records

Privacy incident logs and investigation records maintained and current

7

Training Records

Evidence of privacy awareness training and competency assessments

8

PII Inventory & Processing Records

PII inventory, data flow documentation, and processing activity records

8. Clause 4 Audit Checklist – Context of the Organization

Clause 4 requires the organization to understand its privacy-related context – including internal factors such as culture and capabilities, and external factors such as legal, regulatory, and contractual requirements. Auditors must verify that this contextual understanding is documented, current, and actively informing the design and scope of the PIMS. Without a clear understanding of context, the PIMS cannot be properly tailored to the organization's actual privacy risk landscape.

Audit Questions

- Have internal privacy issues (culture, capabilities, organizational structure) been identified and documented?
- Have external privacy requirements (legal, regulatory, contractual) been identified and assessed?
- Have interested parties and their relevant privacy requirements been determined?
- Are privacy requirements of interested parties documented and reviewed for currency?
- Is the PIMS scope clearly defined, documented, and consistently applied?

Evidence to Request

- Context analysis documentation
- Regulatory and legal assessments
- Stakeholder / interested party registers
- PIMS scope documentation
- Privacy requirement registers

Context should be reviewed at planned intervals and whenever significant changes occur to the internal or external environment.

9. Clause 5 Audit Checklist – Leadership

Clause 5 addresses leadership commitment and accountability for the PIMS. Top management must demonstrate active, visible sponsorship of privacy – not merely nominal endorsement. Auditors should look for evidence that leadership has established a meaningful privacy policy, assigned clear responsibilities, integrated privacy objectives with strategic business goals, and created conditions in which privacy is treated as a genuine organizational priority rather than a compliance checkbox.

Audit Questions

- Has top management established, approved, and communicated a current privacy policy?
- Are privacy roles, responsibilities, and authorities clearly assigned and communicated?
- Is leadership actively involved in privacy governance, including attendance at review activities?
- Are privacy objectives aligned with and integrated into the organization's business strategy?
- Is accountability for privacy outcomes clearly demonstrated at senior management level?

Evidence to Request

- Approved privacy policy document
- Organizational charts with privacy roles
- Governance committee meeting records
- Leadership communications on privacy
- Privacy role definitions and assignments

Interview members of top management directly to assess the depth of their engagement with the PIMS and understanding of privacy obligations.

10. Clause 6 Audit Checklist – Planning

Clause 6 requires the organization to systematically address privacy risks and opportunities, and to establish measurable privacy objectives with defined plans for achieving them. Effective planning is what transforms good intentions into operational reality. Auditors must verify that risk assessments are genuinely risk-informed (not formulaic), that treatment plans are proportionate to risk levels, and that privacy objectives are tracked with sufficient rigor to drive meaningful progress.

Audit Questions

- Has a thorough privacy risk assessment been conducted using a documented methodology?
- Are privacy risks formally documented with assigned owners and risk ratings?
- Are risk treatment plans implemented proportionately and within defined timelines?
- Are privacy objectives SMART – specific, measurable, and time-bound?
- Are privacy initiatives and objective progress monitored and reported regularly?

Evidence to Request

- Privacy risk registers with ratings
- Risk treatment plans and status
- Documented privacy objectives
- Action plans with owners and dates
- Risk assessment methodology documentation

Verify that risk assessments are reviewed whenever significant changes to processing activities, systems, or the regulatory environment occur.

11. Clause 7 Audit Checklist – Support

Clause 7 addresses the resources, competencies, awareness, communication, and documented information needed to operate and continually improve the PIMS. Support elements are frequently underestimated in their importance – a well-designed PIMS cannot function if personnel lack the knowledge to execute privacy controls, if resources are inadequate, or if documented information is not properly controlled. Auditors should probe for evidence of genuine capability-building, not just training attendance records.

Audit Questions

- Are adequate human, financial, and technical resources provided to support the PIMS?
- Have privacy responsibilities been communicated to all relevant personnel?
- Are personnel with privacy responsibilities trained to an appropriate level of competency?
- Are privacy awareness activities conducted regularly across the organization?
- Is documented information created, controlled, and maintained in accordance with requirements?

Evidence to Request

- Training records and completion data
- Privacy awareness campaign materials
- Competency matrices for key roles
- Document control procedures
- Resource allocation documentation

Test competency through interviews, not just training records. Ask staff to describe privacy obligations relevant to their role.

12. Clause 8 Audit Checklist – Operation

Clause 8 is the operational heart of ISO/IEC 27701, covering the full range of controls required for managing PII processing activities. This is typically the most extensive part of the audit, requiring auditors to evaluate how privacy controls function in practice across the entire data lifecycle – from collection and processing through retention and disposal. Auditors must go beyond documentation to verify that controls are implemented, monitored, and effective at the point of processing.

Audit Questions

- Are all PII processing activities comprehensively documented in a Record of Processing Activities (RoPA)?
- Is personal information collected only on a lawful basis with appropriate consent or legal justification?
- Are retention schedules defined, implemented, and applied consistently across all data categories?
- Are secure disposal procedures defined and verified as implemented?
- Are third-party processors managed through formal agreements and oversight mechanisms?

Evidence to Request

- Record of Processing Activities (RoPA)
- Consent records and mechanisms
- Retention schedules and disposal logs
- Data Processing Agreements (DPAs)
- Privacy Impact Assessments (PIAs/DPIAs)
- Privacy control implementation evidence

13. Clause 9 Audit Checklist – Performance Evaluation

Clause 9 requires the organization to monitor, measure, analyze, and evaluate the performance of the PIMS. This includes internal audits, management reviews, and ongoing monitoring of privacy KPIs and incident trends. Performance evaluation provides the evidence base for management decision-making and is the mechanism through which the organization maintains ongoing assurance that the PIMS remains effective. Auditors should verify that evaluation activities are substantive and produce actionable outputs – not merely box-checking exercises.

Audit Questions

- Are privacy KPIs established, measured, and reviewed at defined intervals?
- Are internal PIMS audits performed according to a planned audit program?
- Are management reviews conducted with appropriate inputs, outputs, and documented decisions?
- Are privacy incidents monitored and tracked as inputs to the management review?
- Are performance trends analyzed and used to inform improvement priorities?

Evidence to Request

- KPI dashboards and measurement records
- Internal audit reports and schedules
- Management review meeting minutes
- Privacy incident statistics and trends
- Performance analysis reports

Evaluate whether management review outputs translate into tangible decisions and resource allocations, not merely acknowledgment of reports.

14. Clause 10 Audit Checklist – Improvement

Clause 10 addresses the organization's commitment to continual improvement of the PIMS. This includes the systematic management of nonconformities and corrective actions, as well as proactive identification of improvement opportunities. Continual improvement is the hallmark of a mature PIMS – it distinguishes organizations that treat privacy as an evolving discipline from those that view compliance as a static state to be achieved and maintained unchanged. Auditors must verify that improvement is genuinely embedded in operating practices.

Audit Questions

- Are nonconformities identified, documented, and managed through a formal process?
- Is root cause analysis performed to prevent recurrence of identified nonconformities?
- Are corrective actions implemented within defined timeframes and with clear ownership?
- Is the effectiveness of corrective actions verified through follow-up activities?
- Are improvement opportunities tracked and prioritized systematically?

Evidence to Request

- Corrective action logs and tracking records
- Root cause analysis documentation
- Improvement plans and progress reports
- Nonconformity register
- Effectiveness verification records

15. PII Controller Audit Checklist

Organizations acting as PII Controllers bear primary responsibility for determining the purposes and means of personal data processing. The controller audit checklist addresses the governance, operational controls, and accountability mechanisms that controllers must demonstrate. Auditors should verify not only that policies exist, but that legal bases are properly documented for each processing activity, that data subject rights can be exercised effectively, and that the controller can demonstrate compliance to regulators on demand.

Governance

- Privacy responsibilities clearly assigned to named roles
- Legal basis documented for each processing activity
- Data subject rights process established and tested
- Privacy notices current and accessible

Processing Controls

- Purpose limitation implemented and enforced
- Data minimization applied at point of collection
- Retention controls established with deletion verification
- Data quality measures implemented

Accountability

- Processing records maintained and current
- Vendor oversight performed with documented evidence
- Compliance evidence organized and audit-ready
- Cross-border transfer mechanisms documented

16. PII Processor Audit Checklist

PII Processors handle personal data on behalf of controllers and must demonstrate compliance with processing instructions, contractual obligations, and applicable privacy requirements. Processor audits are increasingly important given the expanded liability that processors carry under modern privacy frameworks. Auditors should verify that processors understand their obligations, have implemented appropriate security and confidentiality measures, and can demonstrate compliance beyond the terms of their contractual commitments.

Processor Controls

Processing Instructions

Processing activities documented and limited to controller instructions

Security Measures

Appropriate technical and organizational security controls implemented

Incident Reporting

Breach notification process to controllers established and tested

Confidentiality

Confidentiality obligations enforced for all personnel with data access

Processing Records

Records of all processing activities maintained as required

Third-Party Compliance

Data Processing Agreements

Signed DPAs in place with all controllers and sub-processors

Processor Audits

Sub-processor audits conducted and findings documented

Compliance Reviews

Periodic compliance reviews documented with evidence retained

⚠ Sub-processor management is a high-risk area. Verify that controller authorization has been obtained before engaging sub-processors.

17. Privacy Risk Assessment Audit Checklist

Privacy risk assessments are foundational to an effective PIMS. They provide the evidence base for risk treatment decisions and demonstrate that the organization's controls are proportionate to actual privacy risks. A robust risk assessment process is dynamic – it responds to changes in processing activities, regulatory requirements, and the threat landscape. Auditors must probe whether risk assessments reflect genuine analysis or merely fulfill a documentation requirement, and whether risk owners are actively engaged in monitoring and treatment.

1

Risk Identification

- Privacy threats comprehensively identified
- Risk owners assigned to each identified risk
- PII asset inventory used as basis

2

Risk Evaluation

- Impact assessments completed for each risk
- Likelihood assessed using defined criteria
- Risk ratings assigned and documented

3

Risk Treatment

- Controls implemented to address rated risks
- Residual risks formally reviewed and accepted
- Treatment plan owners identified

4

Monitoring

- Risks reviewed at defined intervals
- Treatment effectiveness assessed continuously
- Risk register updated with changes

18. Data Subject Rights Audit Checklist

Data subject rights are among the most operationally visible aspects of privacy compliance. Organizations must be able to receive, authenticate, process, and respond to rights requests within legally mandated timeframes. Auditors should evaluate not only whether processes are documented, but whether they work in practice – including across complex, multi-system environments where fulfilling a single request may require coordination across multiple teams and technologies. Evidence of actual request handling is essential.

Right of Access

Access request process defined, timeliness tracked, and identity verification applied consistently

Rectification

Process established for correcting inaccurate data; downstream notification to processors documented

Erasure

Right to erasure requests handled with verified deletion and backup system coverage confirmed

Restriction

Processing restriction mechanism technically implemented and verifiable across all active systems

Portability

Data portability requests supported in machine-readable format; transfer mechanisms tested

Objection

Objection requests processed with appropriate balancing test documentation and outcomes recorded

Review a sample of actual request logs to verify that response timelines comply with applicable legal requirements and that escalation procedures are followed when deadlines are at risk.

19. Privacy Incident Management Audit Checklist

Privacy incident management capability is a critical indicator of PIMS maturity. Organizations must be able to detect, investigate, contain, and report privacy incidents in a timely and organized manner. Regulatory expectations around breach notification timelines are strict, and failure to meet them can result in significant penalties. Auditors should evaluate the end-to-end incident management process – from initial detection through root cause analysis and lessons learned – testing whether procedures function under realistic conditions.

Incident Detection

Detection Mechanisms

Technical and procedural detection mechanisms implemented and tested

Reporting Procedures

Internal reporting channels defined and communicated to all staff

Incident Response

Investigation Process

Incident investigations conducted with documented timelines and scope

Corrective Actions

Corrective actions documented with owners and completion dates

Lessons Learned

Post-incident reviews conducted and outputs fed into PIMS improvement

Audit Evidence

- Incident detection logs
- Investigation reports
- Response procedure documentation
- Notification records (regulatory)
- Lessons learned reports
- Corrective action tracking records

⚠ Verify that regulatory notification obligations (e.g., 72-hour reporting) are embedded in response procedures and tracked for all qualifying incidents.

20. Third-Party Privacy Audit Checklist

Third-party privacy management is a persistent area of risk for organizations. Processors and vendors with access to PII must be subject to appropriate governance mechanisms, including formal contractual requirements, risk-based due diligence, and ongoing monitoring. Regulators increasingly hold controllers accountable for processor compliance failures, making robust third-party oversight a compliance imperative rather than merely a best practice. Auditors should assess whether the organization's vendor governance program is proportionate to the actual risk posed by each third party.

Vendor Governance

- Vendor inventory maintained with PII access flagged
- Privacy risk assessments conducted prior to onboarding
- Data Processing Agreements (DPAs) executed for all PII processors
- Processor performance monitoring program established

Compliance Verification

- Vendor privacy audits completed on risk-based schedule
- Vendor compliance evidence reviewed and retained
- Remediation actions tracked to closure for all findings
- Sub-processor authorization and monitoring in place

⚠ High-risk processors (e.g., cloud providers, payroll processors, marketing platforms) should receive enhanced due diligence and more frequent compliance monitoring than lower-risk vendors.

21. Audit Evidence Collection Guide

The quality and sufficiency of audit evidence is the foundation upon which all audit findings rest. Auditors must collect evidence that is relevant, reliable, and sufficient to support their conclusions. Relying on a single type of evidence – such as documentation alone – creates blind spots and can result in findings that fail to withstand scrutiny. A balanced evidence collection strategy draws on multiple sources and methods, allowing auditors to triangulate findings and build a comprehensive, defensible picture of PIMS effectiveness.

Documentation Review

Examination of policies, procedures, and formal records to verify that required documentation exists and is current. Includes policies, procedures, contracts, standards, and formal records that constitute the PIMS documented information framework.

Records Examination

Review of operational records to verify that documented processes are actually being followed. Includes audit reports, training attendance records, risk assessment outputs, incident logs, and corrective action registers.

Interviews

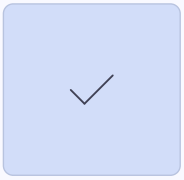
Structured conversations with Privacy Officers, Process Owners, IT Personnel, and operational staff to assess understanding, awareness, and practical implementation of privacy controls. Interviews reveal informal practices that documentation may not capture.

Observation

Direct observation of privacy controls and operational processes in action, providing first-hand evidence of how controls function in the real operating environment – often revealing gaps between documented procedures and actual practice.

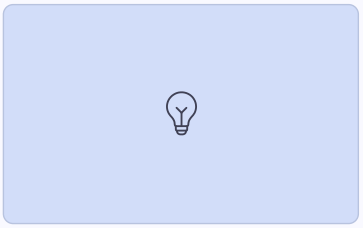
22. Audit Findings Classification

Consistent and precise classification of audit findings is essential for effective communication, appropriate management response, and accurate tracking of PIMS performance over time. Each finding classification carries specific implications for the urgency and scope of required corrective action. Auditors must apply classification criteria consistently and objectively – misclassification, whether overstating or understating the severity of findings, undermines the credibility of the audit and can lead to inappropriate organizational responses.



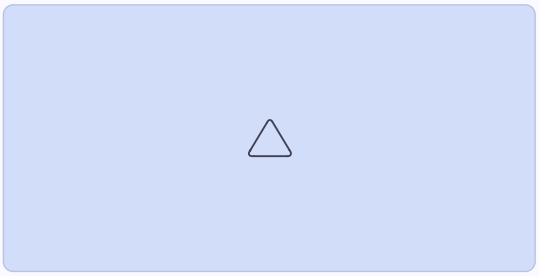
Conformity

Requirement fully satisfied with objective evidence. No action required.



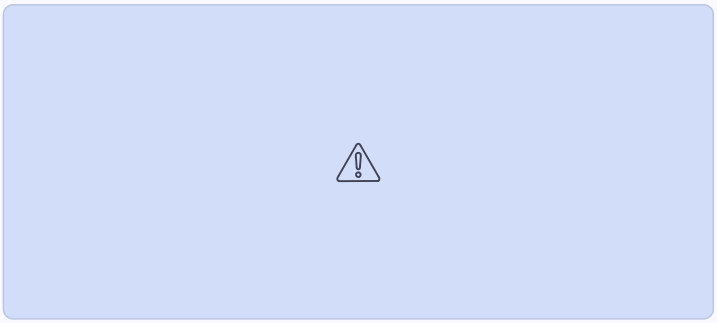
Opportunity for Improvement (OFI)

Potential enhancement identified. No nonconformity exists, but improvement would strengthen the PIMS.



Minor Nonconformity

Isolated deviation from a requirement. System effectiveness not materially compromised. Corrective action required within defined timeframe.



Major Nonconformity

Significant breakdown affecting system compliance or effectiveness. Requires immediate corrective action. May jeopardize certification status.

A major nonconformity must be resolved and verified before a certification or surveillance audit can be concluded favorably. Escalate major nonconformities to top management immediately upon identification.

23. Nonconformity Report Template

A Nonconformity Report (NCR) is the formal record of a deviation from ISO/IEC 27701 requirements identified during an audit. Each NCR must be precise, evidence-based, and clearly linked to a specific clause or requirement. The NCR forms the basis for the auditee's corrective action response and serves as a tracking record through to formal closure. Auditors should ensure NCRs are written with sufficient specificity that the auditee can understand exactly what was found and where, without ambiguity.

Finding Information

Field	Details
Finding Number	NCR-[Year]-[Sequence]
Audit Clause	ISO/IEC 27701 Clause Reference
Finding Type	Major / Minor Nonconformity / OFI
Description	Clear, factual statement of the deviation observed
Objective Evidence	Specific evidence observed or reviewed

Corrective Action Fields

Field	Details
Root Cause	Underlying reason the nonconformity occurred
Corrective Action	Specific actions planned to address root cause
Action Owner	Named individual responsible for implementation
Due Date	Target completion date for corrective action
Verification Date	Planned date for effectiveness verification
Status	Open / In Progress / Closed

Objective evidence must be specific – cite document names, record dates, and interview subjects. Generic statements such as "no evidence found" are insufficient without context.

24. Audit Report Template

The audit report is the primary output of the audit engagement and the document through which audit findings are communicated to management and other stakeholders. A high-quality audit report is objective, evidence-based, clearly structured, and free of ambiguity. It must provide a truthful picture of the PIMS's conformance status and effectiveness, supporting informed management decisions. The report should be issued promptly after the audit – delays reduce its relevance and impact.

Audit Summary Section

Item	Details
Audit Scope	Defined scope of the audit engagement
Audit Dates	Period over which audit activities were conducted
Lead Auditor	Name and qualifications
Audit Criteria	ISO/IEC 27701 and applicable requirements
Audit Methods	Interviews, document review, observation, sampling

Findings Summary

Finding Type	Count
Major Nonconformities	
Minor Nonconformities	
Opportunities for Improvement	
Conformities Noted	

Overall Conclusion

The audit report must conclude with one of the following determinations regarding the overall effectiveness of the PIMS:

✓ Effective

PIMS conforms to requirements and is operating effectively across all audited areas

⚠️ Effective with Improvements Required

PIMS is broadly effective but requires corrective action for identified nonconformities

□ Not Effective

Significant breakdown in PIMS effectiveness requiring immediate management attention

25. Corrective Action Follow-Up, Pitfalls & Best Practices

Follow-Up Checklist

01

Root Cause Identified

Documented root cause analysis completed by action owner

02

Corrective Action Implemented

Planned corrective actions completed within agreed timeframe

03

Evidence Provided

Objective evidence of implementation submitted to auditor

04

Effectiveness Verified

Auditor confirms the nonconformity condition no longer exists

05

Finding Closed

NCR formally closed in the tracking register with date

Common Audit Pitfalls

Documentation Only: Auditing records without verifying operational implementation

Insufficient Sampling: Interviewing too few staff to assess awareness and practice

Weak Evidence: Accepting vague assertions in place of objective, verifiable evidence

Risk Validation Gap: Failing to challenge the adequacy of privacy risk identification

Inadequate Follow-Up: Closing corrective actions without verifying effectiveness

Auditor Best Practices

Focus on Privacy Risks: Let risk drive sampling and interview selection

Follow Audit Trails: Pursue evidence chains rather than accepting first responses

Verify Implementation: Confirm controls function at the point of operation

Assess Privacy Culture: Evaluate whether privacy values are genuinely embedded

Professional Skepticism: Question evidence critically and maintain independence

Quick Audit Readiness Checklist

Use this consolidated checklist as a final readiness assessment before any ISO/IEC 27701 audit engagement. Organizations that can demonstrate consistent, documented evidence against each item below are well positioned to undergo internal, second-party, or third-party certification audits with confidence. Gaps identified through this checklist should be addressed as corrective actions in advance of the formal audit, with evidence of remediation retained.

Governance

- Privacy Policy – current, approved, communicated
- Roles & Responsibilities – documented and assigned
- Privacy Objectives – measurable and tracked

Risk Management

- Risk Assessments – completed and current
- Treatment Plans – implemented and monitored
- Risk Reviews – scheduled and evidenced

Operations

- Processing Records (RoPA) – complete and current
- Consent Management – mechanism and records in place
- Retention Controls – schedules implemented and enforced
- Vendor Management – DPAs executed and oversight performed

Compliance

- Internal Audits – conducted per program schedule
- Management Reviews – documented with decisions
- Incident Management – detection and response tested
- Data Subject Rights – processes verified in practice

Improvement

- Corrective Actions – tracked to verified closure
- Root Cause Analysis – documented for all nonconformities
- Continual Improvement – program active and evidenced

Organizations that satisfy all items in this readiness checklist with objective, documented evidence have built the foundation for a successful ISO/IEC 27701 certification audit and a genuinely effective Privacy Information Management System.

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