GSDC
Global Skill Development Council

ISO/IEC 27701

Nonconformity & Corrective Action Guide

www.gsdcouncil.org

1. Understanding Nonconformities

What is a Nonconformity?

A nonconformity is the failure to meet a requirement specified by any of the following authoritative sources. Each represents a binding obligation the PIMS must satisfy in order to maintain certification and operational integrity.

- ISO/IEC 27701:2025 standard requirements
- Organizational privacy policies
- Applicable regulatory requirements
- Customer and contractual obligations
- Internal procedures and controls

Sources of Nonconformities

Nonconformities can emerge from a wide range of organizational activities. Recognizing where findings originate is the first step toward building a proactive detection capability across the PIMS lifecycle.

Internal Audits

Issues identified during scheduled audit activities.

External Audits

Certification body findings and third-party assessments.

Privacy Incidents

Breaches or unauthorized personal data disclosures.

Regulatory Reviews

Compliance failures identified by data protection authorities.

Management Reviews

Governance weaknesses surfaced during leadership oversight.

Employee Reports

Issues raised through internal reporting channels.

2. Why Nonconformity Management Matters

Effective nonconformity management is not simply a compliance exercise – it is a strategic discipline that strengthens privacy governance, builds organizational resilience, and sustains stakeholder confidence over time. Organizations that treat nonconformities as learning opportunities consistently outperform those that view them purely as audit deficiencies. The business case for rigorous CAPA programs is clear and measurable.

Improved Privacy Governance

Systematic tracking drives accountability and oversight.

Better Compliance Posture

Proactive corrections reduce regulatory exposure.

Reduced Privacy Risks

Root cause elimination prevents future incidents.

Stronger Customer Trust

Demonstrated corrective rigor builds stakeholder confidence.

Improved Audit Performance

Fewer repeat findings and faster closure rates.

Enhanced Accountability

Clear ownership and deadlines drive resolution.

3. ISO/IEC 27701 Corrective Action Requirements

ISO/IEC 27701:2025 imposes explicit requirements on organizations to manage nonconformities systematically and with documented evidence. These requirements are not discretionary – certification bodies will assess the completeness and effectiveness of the corrective action process as a core element of surveillance and recertification audits. Understanding these obligations in precise terms is essential for any PIMS owner or lead auditor responsible for system integrity.

1

React to Nonconformities

Organizations must respond promptly when any nonconformity is identified, regardless of source or severity.

2

Control and Correct Issues

Immediate containment and correction measures must be applied to limit the impact of the finding.

3

Address Consequences

The downstream effects of the nonconformity – regulatory, operational, and reputational – must be evaluated and managed.

4

Determine Root Causes

A formal root cause analysis must be performed to understand why the failure occurred, not merely what failed.

5

Implement Corrective Actions

Actions must be planned, assigned, resourced, and executed to eliminate the identified root cause.

6

Verify Effectiveness

Each corrective action must be independently reviewed to confirm the root cause has been eliminated.

7

Prevent Recurrence

Preventive measures must be embedded into the PIMS to reduce the probability of the same issue recurring.

8

Maintain Records

Full documentation of all nonconformities, analyses, actions, and verifications must be retained as objective evidence.

4. Types of Nonconformities

Not all nonconformities carry the same weight. ISO/IEC 27701:2025 audits distinguish between findings on a spectrum of severity, which directly influences the urgency and scope of corrective action required. Understanding the distinction between a major nonconformity, a minor nonconformity, and an opportunity for improvement (OFI) is critical for appropriately prioritizing organizational response and resource allocation.

Major Nonconformity

A significant failure affecting the effectiveness of the entire PIMS. Certification may be withheld or suspended until resolved.

- No privacy risk assessment process in place
- Missing privacy governance structure
- Failure to manage data subject rights
- Repeated incidents without corrective action
- No internal audit program

Minor Nonconformity

An isolated issue that does not significantly impact overall PIMS effectiveness. Must still be corrected within a defined timeframe.

- Incomplete training records
- Missing review signatures on documents
- Delayed document updates
- Isolated process deviations

Opportunity for Improvement (OFI)

A recommendation to enhance PIMS effectiveness without indicating a formal failure. Not a requirement but valuable for maturity.

- Improve privacy awareness materials
- Enhance KPI reporting dashboards
- Automate risk monitoring workflows

5. Nonconformity Management Lifecycle

The nonconformity management lifecycle provides a consistent, repeatable framework for moving from initial detection through to verified closure and documented improvement. Each phase builds on the previous, creating an unbroken chain of accountability and evidence. Skipping any phase – particularly root cause analysis or effectiveness verification – is itself a nonconformity under ISO/IEC 27701:2025 clause requirements.

This lifecycle applies equally to major and minor nonconformities, with the depth and rigor of each phase scaled proportionally to the severity and risk level of the finding. High-risk or major findings require executive-level oversight at each stage, while minor findings may be managed at the operational level with periodic management review check-ins.

6. Step 1: Identification of Nonconformities

Identification Sources

Nonconformities enter the management system through multiple detection pathways. Each source must feed into a centralized finding register to ensure no issue is tracked in isolation or lost between organizational functions. Establishing clear intake procedures for each source type is essential for completeness and auditability.

Source	Example
Audit	Missing processing records
Incident	Unauthorized personal data disclosure
Review	Policy not reviewed within schedule
Complaint	Unresolved data subject access request
Monitoring	KPI threshold exceeded

Nonconformity Recording Template

Every identified nonconformity must be captured with sufficient detail to support investigation and corrective action planning.

- **Finding Number** – Unique identifier
- **Date Identified** – Detection timestamp
- **Identified By** – Auditor or reporter
- **Process Area** – Affected function
- **Clause Reference** – ISO/IEC 27701 clause
- **Description** – Factual finding statement
- **Severity** – Major / Minor / OFI

7. Step 2: Immediate Containment Actions

Containment is the bridge between detecting a nonconformity and implementing a permanent fix. Its purpose is to prevent the issue from spreading, escalating, or causing additional harm while the root cause investigation and corrective action planning are underway. Containment does not resolve the underlying problem – it buys time for a thorough, well-designed corrective response. Failure to contain promptly is a common audit finding in its own right.

Privacy Incident Containment

- Disable unauthorized system access immediately
- Isolate affected systems from network
- Suspend active data processing activities
- Notify the privacy officer and legal counsel

Documentation Failure Containment

- Suspend use of outdated or unapproved procedures
- Notify all affected personnel immediately
- Revert to last approved version where applicable
- Flag records created during the gap period

Containment Checklist: Issue isolated ✓ | Impact minimized ✓ | Stakeholders informed ✓ | Temporary controls implemented ✓ | Containment documented with timestamps ✓

8. Step 3: Impact Assessment

Before launching a full root cause investigation, auditors and privacy officers must assess the breadth and depth of the nonconformity's impact. A structured impact assessment ensures that the corrective action is proportionate to the actual risk – neither under-resourced for a critical issue nor disproportionately burdensome for a minor deviation. The assessment should be documented as part of the nonconformity record and reviewed by management for high-risk findings.

Impact Dimensions to Evaluate

Privacy Impact

Has personal data been affected? What categories of PII are involved?

Regulatory Impact

Could applicable data protection regulations be violated or triggered?

Customer Impact

Could data subject trust or contractual obligations be compromised?

Business Impact

Could operations, services, or revenue be disrupted?

Reputation Impact

Could media exposure or public confidence be damaged?

Risk Rating Matrix

Use likelihood and impact scores to assign an overall risk level that governs response priority and escalation thresholds.

Likelihood	Impact	Risk Level
Low	Low	Low
Medium	Medium	Moderate
High	High	Critical
Low	High	High
High	Low	Moderate

⚠ Critical and High risk findings must be escalated to senior management and tracked at management review level until closed.

9. Step 4: Root Cause Analysis

Root cause analysis (RCA) is the intellectual core of the corrective action process. Organizations that address symptoms without diagnosing underlying causes will experience recurring nonconformities – a pattern that itself becomes a major finding during surveillance audits. ISO/IEC 27701:2025 explicitly requires that the root cause be identified and documented before any corrective action is planned. The investment in thorough RCA consistently delivers the greatest return in terms of sustained PIMS effectiveness and reduced repeat findings.

Key Principle: Fixing symptoms without identifying the root cause almost always leads to recurring nonconformities, wasted resources, and declining audit performance over time.

The 5 Whys Method — Worked Example

1 **Problem: Privacy training records missing from PIMS**

The finding is confirmed and documented with objective evidence.

2 **Why? Records were not uploaded to the system**

The training occurred but the administrator did not complete the documentation step.

3 **Why? Administrator was unaware of the upload requirement**

The obligation was not communicated during role onboarding.

4 **Why? The training procedure was incomplete**

The procedural documentation omitted the record submission step entirely.

5 **Why? The procedure had never been updated**

Document review cycles had lapsed without management intervention.

> **Root Cause Identified:** The document management review process is ineffective – procedures are not being reviewed, updated, or enforced on schedule, creating systemic gaps across multiple PIMS functions.

9. Step 4: Root Cause Analysis (Continued)

Fishbone (Ishikawa) Analysis

The Fishbone diagram is particularly effective for complex nonconformities involving multiple contributing factors across organizational functions. By categorizing potential causes into structured dimensions, it prevents premature convergence on a single explanation and surfaces systemic issues that the 5 Whys may miss. Use this method when the initial investigation reveals multiple contributing factors or when repeat findings suggest a deeper systemic problem.

People

Insufficient training, unclear responsibilities, high staff turnover.

Process

Undefined or undocumented procedures, no exception handling.

Technology

System failures, tool limitations, integration gaps.

Governance

Poor oversight, absent accountability, inadequate escalation paths.

Documentation

Incomplete records, version control failures, missing approvals.

Root Cause Worksheet

Document findings across all cause categories before converging on the primary root cause. This ensures completeness and defensibility in audit evidence packages.

Category	Findings
People	
Process	
Technology	
Governance	
Documentation	

Complete one worksheet per nonconformity. Retain as objective evidence for certification auditors.

10. Step 5: Corrective Action Planning

A corrective action plan (CAP) translates the root cause finding into a concrete, time-bound, and accountable program of work. Vague or incomplete action plans are a frequent source of additional nonconformities during verification audits. Every element of the plan must be specific, measurable, and defensible – answering not just what will be done, but who will do it, when it will be complete, what resources are required, and how effectiveness will be confirmed. The quality of the CAP is often a stronger indicator of PIMS maturity than the absence of findings.

Action Description

Describe specifically what will be changed, created, or eliminated to address the root cause – not just the symptom.

Owner Assignment

A named individual – not a team or department – must be accountable for completion and escalation.

Due Date

Set realistic but firm deadlines based on risk level. Major findings require accelerated timelines.

Resources Required

Identify budget, personnel, technology, and time needed. Resource gaps must be escalated immediately.

Success Criteria

Define measurable, pre-agreed criteria that will confirm the corrective action has achieved its intended effect.

Field	Details
Nonconformity ID	Link to finding register entry
Root Cause	Summarize confirmed root cause
Corrective Action	Specific action description
Action Owner	Named responsible individual
Due Date	Target completion date
Status	Open / In Progress / Completed / Verified

11. Step 6: Implementation

Implementation is where planning becomes action. This phase requires disciplined project management, clear communication, and diligent documentation. Many corrective actions fail not because the solution was wrong, but because implementation was incomplete, inconsistently applied, or poorly communicated to affected staff. Auditors conducting verification reviews will look for objective evidence that each implementation activity was completed – not merely planned or initiated. Every change made during this phase must be traceable to the nonconformity record.

Policy Updates

Revise and approve privacy policies to close identified gaps.

Process Improvements

Redesign workflows, procedures, and controls.

Training Delivery

Deliver targeted education to affected personnel.

Technology Enhancements

Deploy or configure technical controls.

Governance Improvements

Strengthen oversight, escalation, and accountability mechanisms.

Implementation Checklist: Action approved by management ✓ | Resources formally assigned ✓ | Changes fully implemented ✓ | Affected staff informed and trained ✓ | Documentation updated and version-controlled ✓

12. Step 7: Effectiveness Verification

Verification is the evidence-based confirmation that the corrective action achieved its intended effect – specifically, that the root cause has been eliminated and the nonconformity has not recurred. This step must be performed independently from those who implemented the action to maintain objectivity. Certification auditors routinely scrutinize verification records; incomplete or self-certified verification is itself a basis for a new finding. Effective verification programs combine multiple methods to build a robust evidence base.

Verification Methods

01

Follow-Up Audit

Conduct a targeted audit of the affected process to confirm implementation and operating effectiveness.

02

Process Testing

Execute the revised process end-to-end and validate outputs against success criteria.

03

KPI Monitoring

Track relevant metrics over a defined observation period to confirm sustained improvement.

04

Personnel Interviews

Verify that staff understand and apply updated procedures in practice.

05

Record Review

Inspect objective evidence confirming the action was completed and controls are operating.

Verification Outcomes

Result	Required Action
Effective	Proceed to formal finding closure
Partially Effective	Define and implement additional actions
Ineffective	Reopen investigation; escalate to management

Verification Questions

- Was the confirmed root cause eliminated?
- Has the issue recurred since implementation?
- Are controls operating as designed?
- Are employees consistently following updated procedures?

⚠ A partially effective or ineffective result must be treated as a new nonconformity input – restarting the management lifecycle from root cause analysis.

13. Corrective Action Closure

Formal closure of a corrective action finding is a deliberate, documented act – not merely the passage of time or the completion of an activity. Closure requires that all prescribed conditions have been met, evidence has been assembled and reviewed, and an authorized individual has confirmed effectiveness. Premature closure is one of the most common PIMS weaknesses identified during external certification audits and can result in major nonconformities being raised against the corrective action process itself.

Closure Requirements

All of the following conditions must be satisfied before a finding may be formally closed:

- Root cause formally identified and documented
- All corrective action steps confirmed as complete
- Objective evidence collected and filed
- Independent effectiveness verification performed
- Management or authorized reviewer approval obtained

Closure Record Template

The following fields must be completed in the finding register upon closure. Incomplete closure records are treated as open findings by certification bodies.

Field	Details
Finding Number	Link to original record
Closure Date	Date formally closed
Verified By	Independent reviewer name
Effectiveness Confirmed	Yes / No
Supporting Evidence	Record reference(s)

Retain all closure documentation for a minimum period aligned to your certification body's record retention requirements and applicable regulations.

14. Privacy-Specific Nonconformities

While ISO/IEC 27701:2025 covers the full spectrum of privacy information management, certain categories of nonconformity appear with particular frequency and carry elevated regulatory and reputational risk. Each of the following represents a distinct failure mode requiring tailored corrective strategies. Privacy officers and lead auditors should treat these categories as priority focus areas during both internal audit planning and corrective action program design.

Data Subject Rights Failure

Access requests not completed within the required regulatory timeframe. Corrective actions: Redesign the rights request workflow with defined SLAs, implement a centralized tracking system, and deliver targeted personnel training on obligations and timelines.

Inadequate Consent Management

Consent records unavailable or incomplete at point of audit. Corrective actions: Deploy a consent repository with audit trail capability, standardize collection procedures, and establish periodic consent record reviews.

Excessive Data Retention

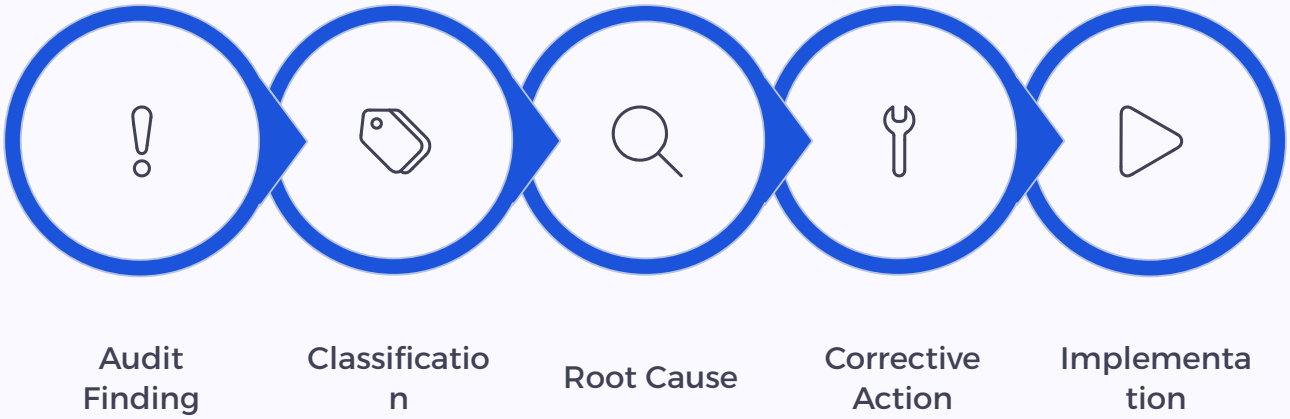
Personally identifiable information retained significantly beyond defined retention periods. Corrective actions: Implement automated retention and deletion controls, conduct a data inventory cleanup, and schedule recurring retention compliance reviews.

Third-Party Oversight Failure

Processor audits and vendor assessments not conducted on schedule. Corrective actions: Establish a formal vendor review calendar, assign named vendor risk owners, and integrate processor oversight into the annual audit program.

15. Audit Finding Management

Audit findings represent the most systematically generated source of nonconformities in any PIMS. Managing them effectively requires a structured workflow that ensures no finding is lost, delayed without justification, or closed without verification. The audit finding register serves as the single source of truth for all open, in-progress, and closed findings – and is a primary artifact reviewed during certification and surveillance audits. Maintaining register hygiene is as important as the quality of individual corrective actions.



Audit Finding Register Template

Finding ID	Process Area	Severity	Owner	Due Date	Status
NC-2025-001	Data Subject Rights	Major	[Name]	[Date]	In Progress
NC-2025-002	Training Records	Minor	[Name]	[Date]	Open
OFI-2025-001	KPI Reporting	OFI	[Name]	[Date]	Open

Update register status at minimum monthly, or upon any change in finding status. Overdue findings must be escalated to the PIMS owner and reviewed at the next management review cycle.

16. CAPA Framework

The Corrective and Preventive Action (CAPA) framework extends the standard corrective action model by adding a forward-looking preventive dimension. While corrective actions address identified failures, preventive actions target conditions that could lead to future nonconformities – even where no actual failure has yet occurred. Together, they form a complete quality management loop that drives both reactive resolution and proactive risk reduction. ISO/IEC 27701:2025-compliant organizations are expected to demonstrate both capabilities in their PIMS documentation.

Corrective Action

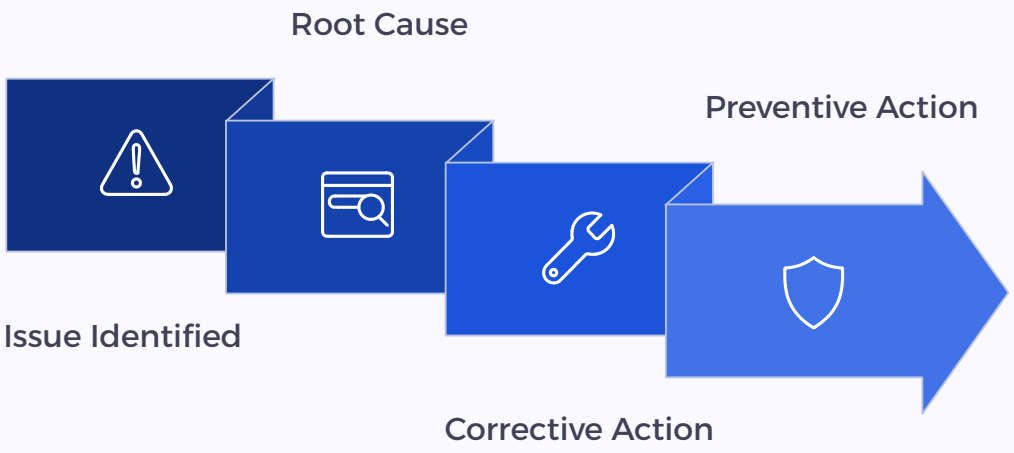
Addresses an existing, confirmed problem by eliminating its root cause. Always reactive – triggered by an identified nonconformity, incident, or audit finding.

- Triggered by a confirmed finding
- Focused on root cause elimination
- Requires effectiveness verification
- Example: Redesign risk assessment process following finding of missing assessments

Preventive Action

Addresses a potential future problem by eliminating conditions that could lead to a nonconformity. Proactive – triggered by risk analysis, trend data, or near-miss events.

- Triggered by risk or trend analysis
- Focused on eliminating potential causes
- Requires monitoring to confirm sustained prevention
- Example: Automate risk review reminders before assessment deadlines are missed



17. Common ISO/IEC 27701 Nonconformities

Across organizations at all stages of PIMS maturity, certain nonconformity patterns emerge consistently in both internal and external certification audits. Awareness of these recurring failure modes allows privacy officers and audit teams to target pre-audit readiness activities more effectively, prioritize internal audit scope, and allocate preventive resources where they will deliver the greatest risk reduction. Each of the following represents a high-frequency finding category with well-established corrective action pathways.

Missing Privacy Risk Assessments

Formal PIAs or privacy risk assessments absent for key processing activities.

Incomplete Processing Records

Records of processing activities incomplete, outdated, or not maintained under Article 30 equivalents.

Weak Vendor Oversight

Data processor assessments, contracts, or periodic reviews not performed on schedule.

Missing Internal Audits

Internal audit program absent, incomplete, or not covering all PIMS clauses within the audit cycle.

Inadequate Incident Management

Privacy incident procedures undefined, untested, or not triggered consistently for qualifying events.

Poor Documentation Control

Documents not version-controlled, approved, or reviewed on schedule.

Incomplete Training Records

Privacy awareness training not delivered, tracked, or evidenced for all in-scope personnel.

Ineffective Corrective Action Management

Findings not tracked to closure, root causes not identified, or effectiveness not verified.

Missing Management Reviews

Scheduled management reviews not conducted or not covering all required agenda inputs.

Weak Data Subject Rights Processes

Rights request procedures undefined, untrained, or consistently failing to meet regulatory timelines.

18. Nonconformity Metrics & KPIs

Metrics transform the nonconformity management program from a reactive compliance activity into a strategic performance management capability. Well-designed KPIs enable management to detect trends before they become major findings, allocate resources to the highest-risk areas, and demonstrate to certification bodies that the PIMS is operating under meaningful continual improvement. KPI data should be reviewed monthly by PIMS owners and formally presented at every management review meeting as a standing agenda item.

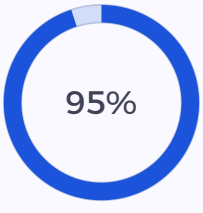
Recommended KPIs

KPI	Purpose
Open Findings Count	Monitor active workload and backlog
Overdue Findings Rate	Track deadline compliance and delays
Repeat Finding Rate	Measure corrective action effectiveness
Corrective Action Closure Rate	Evaluate overall program performance
Average Resolution Time (days)	Measure organizational responsiveness
Major vs. Minor Finding Ratio	Assess PIMS maturity trajectory

KPI Targets

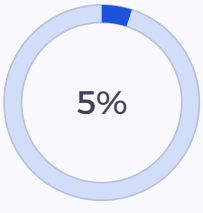
The following targets represent best-practice benchmarks for a mature PIMS program. Organizations should calibrate initial targets to their current baseline and progressively tighten them as the program matures.

KPI	Target
Closure Rate	>95%
Repeat Finding Rate	<5%
Overdue Findings	<10%
Avg. Closure Time	<30 days



Closure Rate Target

Minimum corrective action closure rate for a mature PIMS program.



Max Repeat Findings

Repeat nonconformity rate above this threshold indicates systemic RCA failure.

Max Overdue Rate

Overdue findings above this level trigger mandatory management escalation.

19. Management Review of Nonconformities

Management review is the governance mechanism through which organizational leadership exercises oversight of the PIMS – including its nonconformity management program. ISO/IEC 27701:2025 requires that management reviews consider the results of audits, the status of corrective actions, and the performance of the PIMS against its objectives. An effective management review agenda treats nonconformity data not as a reporting formality but as a decision-making input that drives resource allocation, policy decisions, and strategic improvement priorities.

Open Findings

Review all open nonconformities with status updates and accountability confirmation.

Improvement Opportunities

Capture OFIs and proactive improvement initiatives for inclusion in the PIMS improvement plan.

Resource Requirements

Identify and approve resource needs for outstanding corrective actions.

High-Risk Issues

Scrutinize major findings and critical-risk items requiring executive decision or resource support.

Repeat Nonconformities

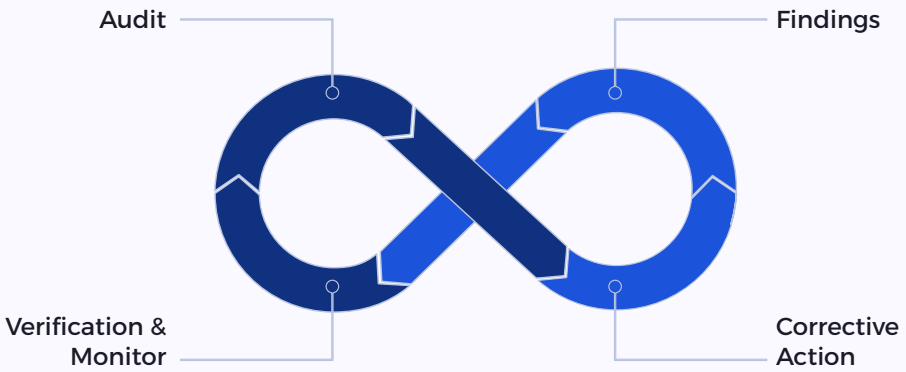
Analyze patterns in recurring findings to identify systemic PIMS weaknesses.

Corrective Action Effectiveness

Review verification results and confirm that closed findings are not recurring.

20. Continual Improvement Framework

Continual improvement is not an optional aspiration for ISO/IEC 27701:2025 certified organizations – it is a fundamental system requirement. The standard explicitly requires that organizations continually improve the suitability, adequacy, and effectiveness of the PIMS. Nonconformity management is the primary engine of this improvement cycle: each finding, when properly analyzed and resolved, generates organizational learning that elevates the maturity of the entire privacy information management system. Organizations that close the loop between audit findings, corrective action, and management review consistently achieve better certification outcomes and stronger privacy governance performance.



Best Practices for Managing Nonconformities

Address Root Causes, Not Symptoms

Every corrective action plan must be anchored to a confirmed root cause – surface-level fixes generate repeat findings.

Prioritize High-Risk Findings

Allocate the most experienced resources and shortest timelines to major findings and critical-risk issues.

Assign Clear, Named Ownership

Every finding must have a single named owner – shared or departmental ownership diffuses accountability.

Establish Realistic Deadlines

Set deadlines that are achievable given available resources, but tight enough to prevent indefinite deferral.

Verify Effectiveness Independently

Effectiveness reviews must be conducted by someone independent of the implementation team.

Use Metrics to Identify Trends

Monthly KPI reviews reveal emerging patterns before they crystallize into major nonconformities.

Promote Continual Improvement Culture

Leaders who reward early reporting and treat findings as learning opportunities build more resilient PIMS programs.

Quick Reference Checklist

Use this consolidated checklist as a field reference during audits, corrective action reviews, and management review preparation. Each checkpoint represents a documented obligation under ISO/IEC 27701:2025. No finding should be advanced to the next phase until all preceding checkpoints are confirmed and evidenced. This checklist may also be used as a self-assessment tool by PIMS owners preparing for external certification or surveillance audits.

Phase 1 — Identification

- ☐ Nonconformity formally recorded in the finding register
- ☐ Severity classification assigned (Major / Minor / OFI)
- ☐ Relevant ISO/IEC 27701:2025 clause(s) referenced

Phase 2 — Investigation

- ☐ Formal root cause analysis conducted and documented
- ☐ Impact assessment completed across all dimensions
- ☐ Containment actions implemented and recorded

Phase 3 — Action

- ☐ Corrective action plan defined with specific actions
- ☐ Named owner assigned with accountability confirmed
- ☐ Realistic timeline and success criteria established

Phase 4 — Verification

- ☐ Independent effectiveness review performed
- ☐ Objective evidence collected and filed
- ☐ Verification outcome documented (Effective / Partial / Ineffective)

Phase 5 — Closure

- ☐ All closure requirements met and confirmed
- ☐ Records retained per retention schedule
- ☐ Improvement documented for management review input

Certification Ready: When all checkpoints across all five phases are satisfied with objective evidence, the finding is ready for formal closure and the organization is positioned for a clean certification audit review.

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