

GOVERNANCE DOCS

ISO/IEC 27701:2025

Gap Assessment Report

ISO/IEC 27701:2025 Privacy Information Management System

Meridian HR Cloud (sample)

The privacy information management system for the HR SaaS platform, as both controller and processor.

ASSESSED	25 September 2026
EDITION	2025 (second edition, published 14 October 2025)
IN SCOPE	48 requirements, 47 applicable
PROFILE	Technology, software and SaaS · 50 to 249 people
PREPARED BY	Governance Docs

CONTENTS

- 1 Executive summary
- 2 Readiness by area and where the next points come from
- 3 Remediation plan
- A About this report

Confidential. Prepared for Meridian HR Cloud (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

Where Meridian HR Cloud (sample) stands against ISO 27701

OVERALL READINESS

67.6%

Level 2 · Developing

The programme is under way, with material gaps an auditor would find.

Held at Developing while a management-system clause scores under 50%; the score alone would place it higher.

Initial

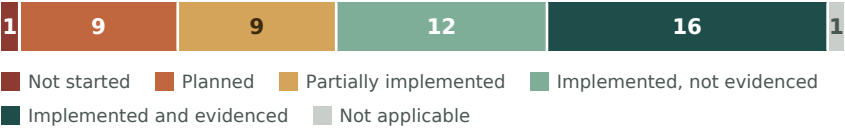
Developing

Established

Audit-ready

APPLICABLE	EVIDENCED	OPEN GAPS	HIGH PRIORITY
47	16	31	10

STATUS OF EVERY REQUIREMENT



GAPS WITH AN OWNER	WITH A TARGET DATE	NOT ANSWERED
12 of 31	6 of 31	0

WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 67.6% against ISO 27701 across 47 applicable controls. 16 of them are implemented and evidenced.
- Most open gaps: Annex A.1 - PII controller controls, with 7 at 65%. Strongest area: Clause 5 - Leadership at 100%.
- 1 management-system clause scores under half: Clause 10 - Improvement (38%). Clauses cannot be excluded, and this is a likely major nonconformity at a certification audit.
- 12 controls are operating but not evidenced. Collecting their records alone lifts the score to 73.9% (+6.3 points), the cheapest gain available.
- 10 gaps are high priority (not started or only planned); 4 of them are in Annex A.2 - PII processor controls.

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	Bring every management-system clause above 50%, starting with 10.2 Nonconformity and corrective action	HR Manager	Nonconformity and Corrective Action Procedure
2	HIGH	Put an owner and date against the 4 high-priority gaps in Annex A.2 - PII processor controls	Operations Manager	PII Processor Policy
3	MEDIUM	Adopt and tailor the PIMS Context and Scope, which closes 5 open gaps	To assign	PIMS Context and Scope

Analysis and priorities

IN ONE SENTENCE

With a 67.6% score at Developing readiness, focus immediately on establishing core processor controls and corrective action processes.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

Our privacy programme scores 67.6%, placing us at Level 2 of 4, or Developing. While leadership commitment is proven at 100%, we carry 31 open gaps, including 10 high priority gaps. Our primary exposures sit in PII processor controls at 33.3% and improvement mechanisms at 37.5%, leaving customer commitments and corrective action tracking unverified. To remediate these material findings, leadership must approve target timelines, assign owners to all remaining unassigned gaps, and empower teams to finalize critical operating procedures.

WHERE YOU STAND

Your self-assessment places the organization at Developing readiness, Level 2 of 4, with an overall score of 67.6%. Out of 47 applicable requirements, you have 31 open gaps, including 10 high priority gaps. While Leadership and Information security controls stand at 100%, Clause 10 - Improvement sits at 37.5% and Annex A.2 - PII processor controls is at 33.3%. The readiness rating is held back by a weak management clause. Currently, only 12 gaps have an assigned owner and only 6 have a target date.

WHAT IT MEANS FOR THE ORGANIZATION

The pattern reveals strong executive direction and baseline security, but significant vulnerabilities remain in operational privacy and formal governance. Developing status indicates the programme is under way, with material gaps an auditor would find. A low score in Annex A.2 - PII processor controls exposes client-facing SaaS delivery, specifically regarding customer instructions and subprocessors. Furthermore, having 12 requirements implemented without evidence means current practices cannot be verified during an audit. Without documented operational controls and corrective procedures, the organization faces substantial operational and contractual scrutiny.

WHERE TO FOCUS FIRST

Start by assigning accountability and dates to all 31 open gaps, addressing the 10 high priority items first. Gathering evidence for the 12 items already implemented would lift the score to 73.9%. Next, focus on drafting the foundational PIMS Context and Scope document, which helps close 5 open gaps across context and operational controls. In parallel, address the lagging management system requirements in Clause 10 - Improvement by formalizing corrective actions. Finally, complete planned processor commitments to align customer obligations and subprocessor oversight with operational realities.

1 · EXECUTIVE SUMMARY

PRIORITIES

PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN	
1	Formalize Customer Obligations and Subprocessor Controls A.2.a Customer obligations and instructions · A.2.c Subprocessors	Annex A.2 - PII processor controls is at 33.3% with 6 open gaps. Incomplete processor terms and subprocessor oversight directly expose customer contracts and processing operations.	Draft the Data Processing Agreement and evaluate vendor agreements against the Sub-Processor Agreement.	Data Processing Agreement ISO 27701 Toolkit - Comprehensive 75+ Templates	30 DAYS
2	Establish Nonconformity and Corrective Action Procedures 10.2 Nonconformity and corrective action · 10.1 Continual improvement	Clause 10 - Improvement is at 37.5% and holds back the overall readiness level. Without formal corrective action tracking, recurring privacy defects cannot be systematically remediated.	Set up the Nonconformity and Corrective Action Log to record active operational issues.	Nonconformity and Corrective Action Log ISO 27701 Toolkit - Comprehensive 75+ Templates	30 DAYS
3	Define and Document PIMS Context and Scope 4.1 Organisation and its context · 4.3 Scope of the PIMS · 4.4 Privacy information management system	Clarifying context and scope resolves core management clause gaps and directly helps close 5 open gaps across the framework.	Collate organizational parameters and processing boundaries into the PIMS Context and Scope document.	PIMS Context and Scope ISO 27701 Toolkit - Comprehensive 75+ Templates	60 DAYS
4	Execute Transition and Role Alignment TR.2 References re-pointed · TR.1 Edition you are working to	Transition and role scored 43.8% with 4 open gaps, leaving references not started. Re-pointing references ensures alignment with the current standard.	Review the ISO 27701:2019 to 2025 Transition Guide (PDF) to map required reference updates.	ISO 27701:2019 to 2025 Transition Guide (PDF) ISO 27701 Toolkit - Comprehensive 75+ Templates	60 DAYS
5	Implement Controller Collection and Sharing Governance A.1.a Conditions for collection and processing · A.1.i Sharing, transfer and disclosure	Annex A.1 - PII controller controls has 7 open gaps. Establishing clear transfer records and processing conditions mitigates unapproved data sharing.	Complete the PII Analysis Procedure to map lawful bases and third-party data flows.	PII Analysis Procedure ISO 27701 Toolkit - Comprehensive 75+ Templates	90 DAYS

30 / 60 / 90-DAY ROADMAP**FIRST 30 DAYS**

- Assign named owners and target completion dates to all 31 open gaps.
- Establish the Nonconformity and Corrective Action Log to track open operational defects.
- Issue standard templates for the Data Processing Agreement and Sub-Processor Agreement.
- Gather existing records to evidence the 12 implemented but unevidenced requirements.

DAYS 31 TO 60

- Finalize and approve the foundational PIMS Context and Scope document.
- Review the transition guide and update cross-references using Documented Information Control Procedure.
- Complete processor records of processing activities and execute employee confidentiality agreements.

DAYS 61 TO 90

- Execute the PII Analysis Procedure and Legitimate Interest Assessment Procedure.
- Document international transfer mechanisms and maintain the Records of PII Transfers.
- Complete the internal audit programme and finalize the privacy risk treatment plan.

Maturity across the standard

Each bar shows how the requirements in one area break down by status, weakest on the left. The score is the average across applicable requirements; the chips count open gaps by priority.

OTHER REQUIREMENTS	STATUS MIX	SCORE	GAPS H · M · L
Transition and role	1 1 2	44%	2 0 2
MANAGEMENT SYSTEM CLAUSES	STATUS MIX	SCORE	GAPS H · M · L
Clause 4 - Context	1 2 1	69%	1 0 2
Clause 5 - Leadership	3	100%	0 0 0
Clause 6 - Planning	1 3 1	75%	0 1 3
Clause 7 - Support	2 2	88%	0 0 2
Clause 8 - Operation	1 1 1	75%	0 1 1
Clause 9 - Performance evaluation	1 2	83%	0 1 0
Clause 10 - Improvement	1 1	38%	1 1 0
OTHER REQUIREMENTS	STATUS MIX	SCORE	GAPS H · M · L
Annex A.1 - PII controller controls	2 3 2 3	65%	2 3 2
Annex A.2 - PII processor controls	4 2 1	33%	4 2 0
Annex A.3 - Information security controls	3	100%	0 0 0

Not started
Planned
Partially implemented
Implemented, not evidenced
Implemented and evidenced
Not applicable

WHERE THE NEXT POINTS COME FROM

The score after each kind of work, cheapest first. Gold is what that step adds.

Today		67.6%
Evidence what already runs 12 requirements		73.9% +6.3
Finish what is partly in place 9 requirements		83.5% +9.6
Implement what is planned 9 requirements		97.9% +14.4
Start what has not begun 1 requirement		100.0% +2.1

DOCUMENTS THAT CLOSE THE MOST GAPS

Each bar counts the open gaps that name the document as the way to close them.

PIMS Context and Scope		5
ISO 27701:2019 to 2025 Transition Guide (PDF)		2
Documented Information Control Procedure		2
PII Analysis Procedure		2
Privacy Risk Assessment and Treatment Methodology		2
Competence, Training and Awareness Procedure		2

All of these are in the ISO 27701 Toolkit (66 documents).

Every open gap, grouped by what has to happen next

Work from the top. Requirements not yet started or only planned are the ones a certification auditor reaches first; the last group already operates and needs only its records.

HIGH Not started · 1

Start from a documented baseline: adopt and tailor the document named below, then put it into operation.

Ref	Requirement	Area	Owner · target	Closes it
TR.2	References re-pointed	Transition and role	To assign	ISO 27701:2019 to 2025 Transition Guide (PDF) · Documented Information Control Procedure

HIGH Planned · 9

Move from plan to implementation. Assign an owner and a date, then put the control into operation.

Ref	Requirement	Area	Owner · target	Closes it
TR.1	Edition you are working to	Transition and role	Operations Manager	ISO 27701:2019 to 2025 Transition Guide (PDF)
4.1	Organisation and its context	Clause 4	Risk Manager	PIMS Context and Scope
10.2	Nonconformity and corrective action	Clause 10	To assign	Nonconformity and Corrective Action Procedure · Nonconformity and Corrective Action Log
A.1.a	Conditions for collection and processing	Annex A.1	To assign	PII Analysis Procedure · Legitimate Interest Assessment Procedure +1 more
A.1.i	Sharing, transfer and disclosure	Annex A.1	To assign	Procedure for International Transfers of PII · Records of PII Disclosures +1 more
A.2.a	Customer obligations and instructions	Annex A.2	Operations Manager 7 Jan 2027	PII Processor Policy · Data Processing Agreement
A.2.b	Processor records of processing	Annex A.2	To assign	Records of Processing Activities
A.2.c	Subprocessors	Annex A.2	To assign	Sub-Processor Agreement · PII Processor Assessment Procedure +1 more
A.2.g	Confidentiality of personnel	Annex A.2	To assign	Processor Employee Confidentiality Agreement

MEDIUM Partially implemented · 9

Extend the existing approach to the whole scope and apply it consistently, then evidence it.

Ref	Requirement	Area	Owner · target	Closes it
-----	-------------	------	----------------	-----------

6.2	Privacy objectives	Clause 6	Operations Manager 24 Dec 2026	Privacy Objectives and Plan
8.1	Operational planning and control	Clause 8	Compliance Lead	PIMS Context and Scope
9.2	Internal audit	Clause 9	Risk Manager 7 Jan 2027	PIMS Internal Audit Procedure · PIMS Internal Audit Programme and Report
10.1	Continual improvement	Clause 10	HR Manager 12 Nov 2026	Continual Improvement Procedure
A.1.b	Consent	Annex A.1	Operations Manager	Consent Request Form
A.1.f	Obligations to PII principals - requests	Annex A.1	HR Manager	PII Principal Request Procedure · PII Principal Request Form +2 more
A.1.h	Retention and disposal	Annex A.1	Operations Manager	PII Retention and Disposal Procedure · Data Retention Schedule +1 more
A.2.d	Assisting the customer	Annex A.2	HR Manager 10 Dec 2026	Processor Assistance to PII Principals Procedure · Letter to Processors
A.2.e	Return and deletion at termination	Annex A.2	Risk Manager 29 Oct 2026	PII Retention and Disposal Procedure · PII Disposal Record

LOW Implemented, not evidenced · 12

Collect and file evidence an auditor can sample. The control is operating; what is missing is the record of it.

Ref	Requirement	Area	Owner · target	Closes it
TR.3	Standalone or alongside an ISMS	Transition and role	To assign	PIMS Context and Scope
TR.4	Role determined per processing activity	Transition and role	To assign	PII Analysis Procedure · Records of Processing Activities – Controller
4.3	Scope of the PIMS	Clause 4	To assign	PIMS Context and Scope
4.4	Privacy information management system	Clause 4	To assign	PIMS Context and Scope · PIMS Roles and Responsibilities
6.1.1	Actions to address risks and opportunities	Clause 6	To assign	Privacy Risk Assessment and Treatment Methodology
6.1.3	Privacy risk treatment and Statement of Applicability	Clause 6	To assign	Statement of Applicability · Privacy Risk Treatment Plan
6.3	Planning of changes	Clause 6	To assign	Documented Information Control Procedure
7.2	Competence	Clause 7	To assign	Competence, Training and Awareness Procedure
7.3	Awareness	Clause 7	To assign	Competence, Training and Awareness Procedure
8.2	Operational privacy risk assessment	Clause 8	To assign	Privacy Risk Assessment and Treatment Methodology · Privacy Impact Assessment Procedure

A.1.e	Obligations to PII principals - notices	Annex A.1	To assign	Privacy Notice Procedure · Website Privacy Policy +2 more
A.1.g	Privacy by design and by default	Annex A.1	To assign	Privacy by Design and by Default Policy

How it was scored

STATUS WEIGHTS

Status	Weight	Meaning
■ Not started	0.00	No policy, process or activity exists for this requirement.
■ Planned	0.25	Approach agreed and scheduled, but nothing is in place yet.
■ Partially implemented	0.50	In place for part of the scope, or inconsistently applied.
■ Implemented, not evidenced	0.75	Operating as intended, but you could not prove it to an auditor today.
■ Implemented and evidenced	1.00	Operating as intended, with records an auditor can sample.
■ Not applicable	—	A justified exclusion. Removed from the score - record why in your notes.

READINESS LEVELS

1 • Initial (0%+)

Most requirements are not yet in place. Build the foundations before thinking about an audit.

2 • Developing (40%+)

The programme is under way, with material gaps an auditor would find.

3 • Established (65%+)

Most controls operate. Remaining work is closing specific gaps and evidencing what runs.

4 • Audit-ready (85%+)

Controls operate and are evidenced. Ready for an internal audit and a certification body.

A management-system clause scoring under 50% holds the level at Developing, because clauses cannot be excluded from certification scope.

WHAT THIS REPORT IS

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The scores, readiness levels, gaps, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.

A control that is running but cannot be evidenced scores 0.75, not 1.00. Auditors sample records, not intentions. Closing that distance is usually the fastest route to a higher score.

All assessment questions and guidance are original wording by Governance Docs. Clause and control references are used as identifiers; no text from the standard is reproduced. You need your own licensed copy of the standard to implement it.

YOUR WORKBOOK

The Excel workbook that comes with this report follows the same sections and colours. Dashboard: sections 1 and 2, recalculated live. Assessment: every requirement; change a status and every score, chart and level updates. Remediation Plan: section 3, with owners, dates and progress since this report. How it was scored: this page.

Governance Docs · governancedocs.com