

MANG MORGAN CAPITAL LIMITED

# PIMS INTERNAL AUDIT EXTRACT

ISO/IEC 27701:2025 | Fictional pre-certification internal audit

Representative fictional sample - not a historical client engagement.

| Document control       | Value                                            |
|------------------------|--------------------------------------------------|
| Fictional organisation | Cedar Vale Health Technologies Limited           |
| Business               | Fictional remote-care coordination SaaS provider |
| Provider               | Mang Morgan Capital Limited                      |
| Audit delivery         | Remote                                           |
| Version / issue date   | 1.0 / 13 August 2026                             |
| Status                 | Controlled representative sample                 |

## Use limitation

This wholly fictional extract demonstrates one possible structure for a risk-based PIMS internal audit. It is not a historical client engagement, certification report or legal opinion. It does not reproduce ISO/IEC 27701 requirements. A live engagement would use the client’s licensed criteria, approved scope, role analysis and evidence.

## What this extract demonstrates

| Audit information       | Traceable output                                                                  |
|-------------------------|-----------------------------------------------------------------------------------|
| Scope and privacy roles | Boundaries, PII-controller/processor roles, locations and processing context      |
| Criteria and objectives | Standard reference, organisational arrangements and applicable obligations        |
| Risk-based sampling     | Population, rationale, evidence identifier, activity and limitation               |
| Results                 | Evidence basis, evaluation, result and finding reference                          |
| Client ownership        | Root cause, correction and corrective action remain with the audited organisation |

# 1. Audit overview

| Field                   | Fictional audit position                                                                                                                                                                                |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Audit type              | Full-scope PIMS internal audit supporting an initial certification-readiness decision                                                                                                                   |
| Standard                | ISO/IEC 27701:2025                                                                                                                                                                                      |
| Audit objectives        | Evaluate conformity with agreed PIMS criteria, implementation of planned arrangements, effectiveness of privacy-risk treatment, achievement of privacy objectives and opportunities for improvement     |
| PIMS scope              | Privacy governance and PII processing supporting the Cedar Vale remote-care coordination platform, including customer onboarding, service delivery, support, product development and supplier oversight |
| Roles in scope          | PII processor for customer-configured care workflows; PII controller for workforce, prospect, billing and service-security records                                                                      |
| Locations               | Fictional Dublin headquarters and remote workforce; remote audit delivery                                                                                                                               |
| Audit period            | 1 July to 31 July 2026                                                                                                                                                                                  |
| Audit team              | Lead auditor and independent quality reviewer                                                                                                                                                           |
| Representative sampling | Conclusions are based on risk-based samples and available evidence; they do not imply identical testing of every process or record                                                                      |

## Criteria

The agreed criteria comprise ISO/IEC 27701:2025, Cedar Vale’s PIMS policies and procedures, privacy-risk and treatment arrangements, privacy objectives, contracts and recorded statutory/regulatory obligations applicable to the defined scope. ISO/IEC 27001 arrangements are considered only where they are shared with or relied upon by the PIMS.

## Independence and responsibility

The audit team did not design or implement the fictional PIMS. Cedar Vale management remains responsible for the PIMS, privacy risks, legal interpretations, correction, root-cause analysis, corrective action and implementation. Mang Morgan does not issue ISO certificates.

## 2. Method and planned coverage

| Method                | How it was applied                                                                                                                           |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Document review       | Reviewed approved governance, scope, role analysis, processing inventory, privacy-risk records, objectives, procedures and retained evidence |
| Interviews            | Interviewed leadership, privacy, security, product, engineering, people operations, support and supplier owners                              |
| Walkthroughs          | Traced selected PII processing from collection through use, disclosure, retention and deletion                                               |
| Sampling              | Selected higher-risk processing, recent events and role-specific obligations; combined tests supported related conclusions where justified   |
| Evaluation            | Recorded criterion reference, evidence, sample rationale, activity, result, limitation and conclusion                                        |
| Validation and review | Discussed potential findings for factual accuracy; an independent reviewer checked traceability, classification and report consistency       |

### Audit plan extract

| Session         | Topic                                                                 | Key participants               | Expected evidence                             |
|-----------------|-----------------------------------------------------------------------|--------------------------------|-----------------------------------------------|
| Opening         | Scope, objectives, roles, logistics                                   | Leadership; PIMS manager       | Approved scope; role analysis; audit contacts |
| Governance      | Context, interested parties, leadership, responsibilities             | Leadership; privacy lead       | Governance records; policies; objectives      |
| Processing      | Inventory, purpose, lawful basis records, notices and rights handling | Privacy; product; support      | Processing records; notices; rights log       |
| Risk and design | Privacy risk, change, development and default settings                | Privacy; security; engineering | Risk assessments; design reviews; decisions   |
| Suppliers       | Processors, sub-processors and transfers                              | Procurement; legal/privacy     | Due diligence; contracts; monitoring          |
| Operations      | Retention, deletion, incidents, requests and monitoring               | IT; support; privacy           | Tickets; logs; metrics; review records        |
| Closing         | Conclusions, findings, limitations and next steps                     | Leadership; process owners     | Validated factual record                      |

### 3. Evidence and sampling register

| ID   | Population / sample                    | Rationale                                                                                     | Evidence and activity                                                           | Result              |
|------|----------------------------------------|-----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|---------------------|
| P-01 | 12 processing activities / 4 selected  | Represented controller and processor roles, higher sensitivity and different lifecycle stages | Processing inventory; purpose and role records; owner walkthrough               | Conforming          |
| P-02 | 18 suppliers / 5 selected              | Covered hosting, communications, analytics, support and recruitment processing                | Due diligence, contractual privacy terms, transfer records and monitoring       | Minor NC PIMS-NC-01 |
| P-03 | 21 rights requests / 5 selected        | Included access, erasure and correction across different request channels                     | Request log, identity-verification steps, response records and closure evidence | Conforming          |
| P-04 | 9 product changes / 3 selected         | Selected changes with new data fields, analytics or disclosure pathways                       | Change tickets, privacy-risk decisions, design review and release evidence      | OFI PIMS-OFI-01     |
| P-05 | 42 deletion jobs / 6 selected          | Covered customer offboarding, support attachments and workforce records                       | Retention schedule, job logs, exception tickets and owner demonstration         | Minor NC PIMS-NC-02 |
| P-06 | 7 privacy/security events / 4 selected | Covered suspected disclosure, misdirection and supplier notification                          | Event records, assessment, escalation and lessons learned                       | Conforming          |

#### Sampling limitations

Samples were selected to obtain sufficient, relevant evidence for the audit objectives; they were not statistical samples. Records outside the audit period, legal conclusions on applicable privacy law, technical penetration testing and certification decisions were outside this fictional audit.

## 4. Assessment extract

| Area                          | Audit activity and evidence basis                                                                                               | Evaluation                                                                                  | Result / reference    |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|-----------------------|
| PIMS context and scope        | Reviewed scope statement, privacy roles, interested-party register and processing map; interviewed leadership and privacy owner | Boundaries and roles were consistently described and supported by records                   | Conforming            |
| Leadership and accountability | Reviewed policy approval, assigned responsibilities, meeting decisions and resources                                            | Leadership involvement and delegated responsibilities were evidenced                        | Conforming            |
| Privacy risk and objectives   | Traced four processing activities to risk assessment, treatment and two privacy objectives                                      | Risks were evaluated and treatment ownership was recorded; objective measures were reviewed | Conforming            |
| Supplier privacy management   | Tested five suppliers against onboarding, contract, transfer and monitoring records                                             | Two active sub-processors lacked evidence of the scheduled annual privacy review            | Minor NC / PIMS-NC-01 |
| Retention and deletion        | Walked through six scheduled deletion jobs and associated exceptions                                                            | Two failed deletion jobs remained unresolved beyond the approved escalation period          | Minor NC / PIMS-NC-02 |
| Privacy by design             | Reviewed three product changes and privacy-risk decisions                                                                       | Decisions were recorded; a common trigger checklist could improve consistency               | OFI / PIMS-OFI-01     |
| Rights handling               | Tested five completed requests from intake through identity checks, response and closure                                        | Samples supported timely, controlled handling in accordance with internal procedure         | Conforming            |
| Performance and improvement   | Reviewed metrics, internal review, management review and improvement actions                                                    | Monitoring and review inputs supported evaluation of PIMS performance                       | Conforming            |

## 5. Findings

### PIMS-NC-01 - Supplier privacy monitoring

| Finding element         | Statement                                                                                                                                                                      |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Requirement             | The agreed PIMS supplier-management criteria require approved monitoring activities to be performed and retained for relevant processors and sub-processors.                   |
| Objective evidence      | In a sample of five suppliers, the scheduled 2026 privacy review was not evidenced for fictional sub-processors CV-SP-04 and CV-SP-11. Both remained active at the audit date. |
| Conformity gap          | The approved monitoring arrangement was not implemented for two sampled active sub-processors.                                                                                 |
| Classification / status | Minor nonconformity / Open                                                                                                                                                     |

### PIMS-NC-02 - Deletion-job exception handling

| Finding element         | Statement                                                                                                                                           |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Requirement             | The organisation's approved retention procedure requires failed deletion jobs to be investigated, escalated and resolved within the defined period. |
| Objective evidence      | Two of six sampled deletion jobs, CV-DEL-118 and CV-DEL-124, had failed and remained open 19 and 23 days after the ten-day escalation period.       |
| Conformity gap          | Failed deletion jobs were not resolved within the organisation's approved escalation period.                                                        |
| Classification / status | Minor nonconformity / Open                                                                                                                          |

### PIMS-OFI-01 - Consistent change triggers

Three sampled product changes included recorded privacy consideration. Cedar Vale could consider one approved trigger checklist to make the decision path easier to reproduce across teams. This is an opportunity for improvement, not a nonconformity.

### Finding-writing boundary

Each nonconformity states the requirement, objective evidence and conformity gap without prescribing a solution. Cedar Vale owns root-cause analysis, correction, corrective action and implementation.

## 6. Overall conclusion and release controls

Based on the fictional scope, risk-based sampling and evidence available, Cedar Vale had established and implemented core PIMS arrangements. Two minor nonconformities require client-owned correction and corrective action. One opportunity for improvement was identified. No conclusion is expressed on activities not tested, legal compliance as a legal opinion, or certification outcome.

### Result summary

| Result                      | Count            | Meaning in this sample                                                        |
|-----------------------------|------------------|-------------------------------------------------------------------------------|
| Conforming                  | 6 assessed areas | Sampled evidence supported the agreed criteria                                |
| Minor nonconformity         | 2                | A traceable failure against agreed criteria requiring client response         |
| Opportunity for improvement | 1                | A non-mandatory observation that may improve consistency                      |
| Not tested                  | Other activities | Outside the selected sample or agreed scope; not equivalent to not applicable |
| Evidence pending            | 0                | No conclusion deferred at release                                             |

### Controlled release checklist

| Release check                                                     | Status                                                   |
|-------------------------------------------------------------------|----------------------------------------------------------|
| Scope, criteria, role analysis and dates agree across the extract | Pass                                                     |
| Evidence and samples trace to results and findings                | Pass                                                     |
| Finding references and classifications are consistent             | Pass                                                     |
| No real client identifiers or historical evidence are present     | Pass                                                     |
| No ISO requirements are reproduced verbatim                       | Pass                                                     |
| Representative fictional sample marking appears throughout        | Pass                                                     |
| Independent quality review                                        | Illustrative - required before a live controlled release |

### Final note

This extract demonstrates report architecture, not PIMS competence approval or availability for a live engagement. Mang Morgan would accept a PIMS assignment only after confirming competence, independence, licensed criteria, capacity and the agreed delivery boundary.