

Specimen: illustrative example

ISO/IEC 42001 certification readiness report

The organisation named in this document is fictional. This document comes from the scenario described on riskwoven.com/examples, and is not an assessment of any real entity. It is advisory output to support your own decisions: not legal advice, not a certification, and not an audit.

Written and reviewed by RiskWoven.com. Written by RiskWoven.com's AI drafting agent and checked by RiskWoven.com's independent review stage before release. The review is automated. It is not a human, legal or audit review.

The pages that follow are the document exactly as the product produced it.

SPECIMEN

Northvale Health Analytics

ISO/IEC 42001 certification readiness report

Artificial Intelligence Management System · edition 2023

This is an advisory readiness report produced by RiskWoven from the answers supplied. It is not an audit report, a certification decision, or a guarantee of readiness. Only the independent certification body you select can decide certification.

Written and reviewed by RiskWoven.com. Written by RiskWoven.com's AI drafting agent and checked by RiskWoven.com's independent review stage before release. The review is automated. It is not a human, legal or audit review. The readiness assessment and the information requests are AI-written. The readiness position, priority actions, plan and clause coverage are built by fixed rules from RiskWoven.com's verified library.

Engagement

Organisation	Northvale Health Analytics
Industry and size	Healthcare analytics · 51-200
Operating model	Single office plus remote staff
Certification goal	Initial certification
Regulated information in scope	Personal health information
Cloud dependency	AWS
Supplier dependency	Several named SaaS suppliers
Project start	October 1, 2026
Target timeline	Standard, within 6 months
Report generated	September 21, 2026

Readiness position

Readiness band	Early-stage foundation
Preparation indicator	0 of 100
Maturity signals at the highest state	0 of 11

The indicator is a questionnaire-based planning signal. It is not an audit score, and it does not predict a certification outcome.

Priority actions

1. Confirm and approve the certifiable scope, boundaries, interfaces, dependencies and exclusions.
2. Establish a repeatable risk-assessment method with criteria, ownership, approvals and retained results.
3. Build and approve a risk-treatment plan linked to risks, controls, owners, target dates and residual-risk acceptance.
4. Create or complete the ISO/IEC 42001:2023 Statement of Applicability using risk-based inclusion and exclusion rationale.
5. Plan and complete an objective internal audit after enough operating evidence has accumulated.
6. Schedule a formal management review with defined inputs, decisions, actions and retained minutes.

Readiness assessment

Part of this assessment is flagged for specialist review. 3 of 4 parts were released and the gaps listed are complete for those parts. Not covered here: clause 8.1 to clause 10.2. RiskWoven's independent review stage did not clear those requirements for automatic release, so they have gone to a RiskWoven advisor, who will review them and contact you at the address on your account with the completed section. Everything else is complete and needs no further action. Regenerating will not release the flagged section sooner.

The areas covered are clause 4.1 to clause 7.5.3, A.2.2 to A.6.2.8 and A.7.2 to A.10.4. Each is summarised in turn below.

Clause 4.1 to clause 7.5.3: Northvale Health Analytics is at the earliest stage of its ISO/IEC 42001:2023 journey. Across all 20 clauses assessed here, no readiness signals at the highest state were returned from the questionnaire, and the answers confirm no formal management system, no established risk process, no document control, and no defined scope. The band reflects that position: no clause has evidence in place, and several foundational decisions — what AI systems are in scope, which SaaS suppliers are relied upon, and what role Northvale plays with respect to those systems — have not yet been recorded. The organisation handles personal health information and depends on AWS and several named SaaS suppliers, which raises the stakes for the impact-assessment and risk-treatment requirements; those gaps are therefore among the highest-effort items. To move from early to developing, Northvale must first define its scope and AI policy, establish its context and interested-party analysis, and stand up document control — because every other clause depends on those foundations. A six-month timeline to initial certification is achievable only if work begins at the start date of 1 October 2026 and proceeds in the sequence described below.

A.2.2 to A.6.2.8: Northvale Health Analytics is at the earliest stage of ISO/IEC 42001:2023 readiness across all 23 controls assessed here. The readiness indicator is 0 out of 11 readiness signals at the highest state, and the readiness answers confirm no formal management system, no risk process, no document control, and no evidence organised. Every control in this area requires work to be started from scratch. The band is driven not by a single missing item but by the complete absence of documented AI governance, impact assessment, resource documentation, and responsible-design processes — none of which exist in any form the answers describe. The organisation handles personal health information and depends on AWS and several named SaaS suppliers, which raises the consequence of gaps in impact assessment and operational controls. Moving from early to developing would require, at minimum: a documented AI policy reviewed by a named role, AI-related roles assigned and recorded, a functioning impact-assessment process with retained results, and resource documentation covering data, tooling, systems and people for each AI system in scope. None of those conditions is currently met.

A.7.2 to A.10.4: Northvale Health Analytics is at the earliest stage of readiness across all 15 controls assessed here. The readiness indicator is 0 out of 11 readiness signals at the highest state, and the readiness answers confirm no formal management system, no documented processes, no organised evidence, and no defined scope. Every control in this area requires work to be started from scratch. The band reflects that no documented data management, provenance, quality, or preparation processes exist; no user-facing information or incident communication plans have been produced; no responsible-use objectives or processes are in place; and no accountability structure across Northvale's own staff, its AWS environment, and its several named SaaS suppliers has been defined. The band would move to 'developing' once Northvale has documented its AI systems in scope, produced initial versions of its data management and provenance processes, assigned named role holders for AI life-cycle accountability, and established a mechanism for users and interested parties to report adverse impacts. It would move to 'operating' only when those documents are in active use, reviewed by named role holders with dates recorded, and supported by operating evidence accumulated over a meaningful period.

This assessment covers 3 of 4 assessed areas. The remaining part is flagged for specialist review and not represented above; the notice at the top of this assessment says what happens next.

Identified gaps (53)

Every document and record named below needs an owner, a version, and a named reviewer with the review date recorded. The steps assume this and do not repeat it.

1. Clause 4.1: Context and the organisation's role with AI

Effort (estimate): Medium — Estimated medium because the context analysis is a new document with no prior draft, and the role classification cannot be completed until the AI system inventory exists; however, Northvale is a focused healthcare analytics organisation of 51 to 200 people, which limits the breadth of issues to document.

Current state

Northvale has not documented the external or internal issues that affect its ability to achieve AI management system outcomes. The organisation's role with respect to the AI systems it uses or provides — whether as provider, customer, or another role — has not been defined. Because the systems in scope have not yet been named, it is not possible to confirm which roles apply, but the answers indicate Northvale uses SaaS-delivered AI capabilities and processes personal health information, which typically involves at least a customer and subject role.

Evidence a reviewer would expect

A documented context analysis covering external factors (health-sector regulation, technology landscape, competitive environment, the obligations that apply in the jurisdictions where Northvale operates) and internal factors (organisational structure, data assets, technical capabilities, existing policies). A separate role-classification statement identifying Northvale's role for each AI system once the inventory is established. Both documents reviewed by a named member of top management, with the date recorded.

Practical sequence

1. Convene a workshop with senior leadership to identify and record external and internal issues relevant to AI.
2. Draft the context analysis document, covering health-sector and data-protection considerations relevant to the jurisdictions Northvale operates in (see customerMustSupply).
3. Once the AI system inventory is drafted (see clause 4.4 sequence), annotate each system with Northvale's role.
4. Consolidate into a single context and roles document, reviewed by a named member of top management with the date recorded.

2. Clause 4.2: Interested parties and their requirements

Effort (estimate): Medium — Estimated medium because Northvale processes personal health information and has dependencies on AWS and several SaaS suppliers, meaning the interested-party set is broader than a typical single-product organisation; mapping each party's requirements will take structured effort across legal, technical, and operational perspectives.

Current state

Northvale has not identified the interested parties relevant to its AI management system, their requirements, or which requirements the management system will address. Given that Northvale processes personal health information and relies on AWS and several SaaS suppliers, the interested-party set will include patients or data subjects, clinical customers, regulators, and those suppliers — but none of this has been recorded.

Evidence a reviewer would expect

A documented interested-party register listing each party (including data subjects whose health information is processed, clinical or organisational customers, AWS, the named SaaS suppliers, and relevant regulators), their relevant requirements, and a clear statement of which requirements the AI management system commits to addressing. Reviewed by a named role, with the date recorded.

Practical sequence

1. Using the context analysis from clause 4.1 as input, identify all parties with a stake in Northvale's AI systems.
2. For each party, record their relevant requirements — regulatory, contractual, ethical, or operational.
3. Determine and document which requirements fall within the AI management system's remit.

3. Clause 4.3: Scope of the management system

Effort (estimate): Medium — Estimated medium because the scope cannot be drafted until the AI system inventory and context analysis exist, and because the combination of AWS hosting, several SaaS suppliers, and personal health information processing means the boundary and interface descriptions require careful thought; the organisation's single-site-plus-remote model is straightforward by comparison.

Current state

The scope of Northvale's AI management system is explicitly recorded as 'not yet defined'. No boundaries,

interfaces, locations, or exclusions have been documented. This is the single most urgent gap because every other clause depends on a defined scope.

Evidence a reviewer would expect

A written scope statement that names the AI systems covered, the organisational functions and locations included (Northvale's single office and remote staff), the interfaces with AWS and the SaaS suppliers, and any justified exclusions. The statement must be consistent with the context and interested-party analyses. Reviewed by a named member of top management, with the date recorded.

Practical sequence

1. Complete the context (clause 4.1) and interested-party (clause 4.2) analyses first, as the scope must be consistent with them.
2. Draft a scope statement that names each AI system Northvale intends to bring into certification, specifies the office and remote-working locations, identifies the AWS hosting dependency and the SaaS supplier interfaces, and states any exclusions with justification.
3. Circulate for comment among the leadership team.

4. Clause 4.4: The management system itself

Effort (estimate): High — Estimated high because Northvale is starting from no formal management system, meaning every process must be created from scratch; with no existing documentation baseline and personal health information in scope across AWS and several SaaS suppliers, the process map will need to cover a materially complex operating environment.

Current state

Northvale has no formal management system. No processes have been established, documented, or linked. The answers confirm that controls are not mapped and evidence is not organised. This gap underpins every other clause in this assessment.

Evidence a reviewer would expect

A documented AI management system framework describing the processes required, how they interact, and how the system will be maintained and improved. In practice this means a master process map or system description document, supported by the individual process documents called for by each clause. Reviewed by a named member of top management, with the date recorded.

Practical sequence

1. Once the scope is defined, produce a high-level process map identifying every process the AI management system requires.
2. Assign a process owner to each process.
3. Draft individual process documents progressively as each clause is addressed.
4. Produce a master system description document that cross-references all processes and shows their interactions.

5. Clause 5.1: Leadership and commitment

Effort (estimate): Medium — Estimated medium because the leadership commitment artefacts are relatively straightforward to produce, but embedding AI management system requirements into Northvale's existing business processes will require structured engagement across functions in a 51-to-200-person organisation with no prior management system.

Current state

There is no evidence that top management at Northvale has taken a demonstrable leadership role in the AI management system. No AI policy exists, no resources have been formally allocated to the programme, and no communication of the system's importance has been recorded. The answers indicate no formal management system of any kind.

Evidence a reviewer would expect

Documented evidence of top management leadership: meeting minutes or a leadership commitment statement showing alignment of AI objectives with Northvale's strategy; records of resource allocation decisions; internal communications from senior leadership about the AI management system; and evidence that AI management system requirements have been embedded into relevant business processes. Auditors typically look for a named executive sponsor whose commitment is traceable in records.

Practical sequence

1. Identify and formally designate an executive sponsor for the AI management system.
2. Record a leadership commitment statement, reviewed by the executive sponsor, with the date recorded.
3. At the first leadership team meeting after the start date, table the AI management system programme and record the discussion and resource decisions in the minutes.
4. Issue an internal communication from the executive sponsor to all staff explaining the programme and its importance.
5. Retain all records as evidence of ongoing leadership engagement.

6. Clause 5.2: AI policy (also A.2.2)

Effort (estimate): Medium — Estimated medium because drafting a policy for a healthcare analytics organisation that processes personal health information and relies on external cloud and SaaS infrastructure requires careful alignment with regulatory obligations and supplier relationships, beyond a generic template exercise.

Current state

Northvale has no AI policy. No document exists that frames how AI objectives are set, commits to meeting applicable requirements, or commits to continual improvement. There is no record of any policy being communicated internally or shared externally.

Evidence a reviewer would expect

A documented AI policy that fits Northvale's purpose as a healthcare analytics organisation, sets the frame for AI objectives, commits to meeting applicable requirements (including those arising from processing personal health information), and commits to continual improvement. The policy must be reviewed by a named member of top management with the date recorded, cross-referenced to any related policies Northvale holds, communicated to all staff, and made available externally where appropriate. A communication record and review history must be retained.

Practical sequence

1. Draft the AI policy, drawing on the context analysis and interested-party register. Ensure it references Northvale's handling of personal health information and its use of AWS and SaaS-delivered AI capabilities.
2. Cross-reference any existing information security, data protection, or clinical governance policies.
3. Communicate the policy to all staff (office and remote) and retain the communication record.
4. Determine whether and how the policy will be shared externally, and record that decision.

7. Clause 5.3: Roles, responsibilities and authority (also A.3.2)

Effort (estimate): Medium — Estimated medium because no role structure exists yet, the organisation spans office and remote staff across a 51-200 headcount, and AI-related responsibilities will need to be mapped across development, supplier oversight, data handling and incident management before assignments can be made.

Current state

No roles with responsibility or authority for the AI management system have been assigned or communicated. It is not recorded who is responsible for ensuring the system conforms to requirements or who reports its performance to top management.

Evidence a reviewer would expect

A documented role and responsibility assignment — for example, a RACI or responsibility matrix — naming the individual or role responsible for AI management system conformance and the individual or role responsible for reporting performance to top management. The assignment must be communicated to the relevant people, with a communication record retained.

Practical sequence

1. As part of the leadership commitment work (clause 5.1), identify the roles needed: at minimum, an AI management system lead responsible for conformance and a reporting role.
2. Formally assign these responsibilities in writing, reviewed by a named member of top management with the date recorded.
3. Communicate the assignments to the relevant individuals and retain the communication record.
4. Confirm the reporting mechanism — for example, a standing agenda item at leadership meetings.

8. Clause 6.1.1: Risks and opportunities

Effort (estimate): High — Estimated high because Northvale is starting with no risk process, processes personal health information, and operates AI systems via AWS and several SaaS suppliers whose risk profiles must be considered; establishing criteria and running the first identification exercise from scratch in a healthcare analytics context is a substantial undertaking.

Current state

Northvale has not identified the risks and opportunities relevant to its AI management system, has not set AI risk criteria, and has not planned or documented any actions to address them. The questionnaire confirms no risk process is established.

Evidence a reviewer would expect

A documented risk and opportunity identification record covering the AI management system's intended outcomes, potential undesired effects, and continual improvement drivers. Documented AI risk criteria (likelihood and consequence scales, risk appetite, and acceptance thresholds). A record of planned actions, their owners, and how their effectiveness will be evaluated. Reviewed by a named role, with the date recorded.

Practical sequence

1. Once the scope and context are defined, convene a risk identification workshop with the AI management system lead and relevant technical and clinical staff.
2. Document identified risks and opportunities, linking each to the relevant AI system or process once the inventory exists.
3. Define and document risk criteria, including likelihood and consequence scales appropriate to a healthcare analytics context where personal health information is involved.
4. Record planned actions for each risk and opportunity, with owners and evaluation methods.

9. Clause 6.1.2: Risk assessment method

Effort (estimate): High — Estimated high because the process must be designed from nothing, must account for individual and societal consequences given the personal health information Northvale processes, and must then be applied to every in-scope AI system — the number of which is not yet known because the inventory has not been created.

Current state

No AI risk-assessment process exists. The questionnaire confirms the risk process is not established. There are no documented criteria, no analysis of likelihood or consequence, and no risk register.

Evidence a reviewer would expect

A documented AI risk-assessment process aligned with the AI policy, describing how risks to AI objectives are identified, how likelihood and consequence are analysed (including consequences for individuals and society, relevant given Northvale's use of personal health information), how risk levels are determined, and how risks are prioritised against documented criteria. Completed risk-assessment records for each in-scope AI system. Reviewed by a named role, with the date recorded.

Practical sequence

1. Draft the risk-assessment process document, building on the risk criteria established under clause 6.1.1.
2. Define the consequence dimensions explicitly — operational, reputational, and impacts on individuals whose health information is processed.
3. Pilot the process against one AI system to validate the method.
4. Run the full assessment across all in-scope systems once the inventory is complete.

10. Clause 6.1.3: Risk treatment and control applicability

Effort (estimate): High — Estimated high because the Statement of Applicability must cover every Annex A control with individual rationale, the treatment plan must be linked to a risk register that does not yet exist, and the personal health information and SaaS supplier dependencies mean the control mapping will require input from technical, clinical, and legal perspectives.

Current state

No risk-treatment process exists. No treatment options have been selected, no controls have been mapped to Annex A, no Statement of Applicability has been created, and no risk-treatment plan has been produced or reviewed by management. The questionnaire confirms all three of these points explicitly.

Evidence a reviewer would expect

A documented risk-treatment process. A completed Statement of Applicability listing every Annex A control with a justified inclusion or exclusion rationale and its implementation state. A risk-treatment plan linking each risk to its selected treatment, the controls applied, the owner, and the target date. Evidence that management has reviewed and accepted the plan and the residual risk position, with the date recorded.

Practical sequence

1. Complete the risk-assessment process (clause 6.1.2) first, as treatment options must be linked to assessed risks.
2. Draft the risk-treatment process document.
3. Map each assessed risk to candidate controls, checking against Annex A and identifying any additional controls needed for the healthcare analytics context.
4. Draft the Statement of Applicability, recording inclusion and exclusion rationale for every Annex A control.
5. Produce the risk-treatment plan with owners and target dates.
6. Present the plan and residual risk position to a named member of top management for review, and retain the record with the date.

11. Clause 6.1.4: AI system impact assessment (also A.5.2)

Effort (estimate): High — Estimated high because Northvale's AI systems operate in a healthcare analytics context where consequences for individuals — patients whose health information is processed — can be significant, and because the impact assessment must address foreseeable misuse and jurisdictional obligations that have not yet been identified; this requires clinical, legal, and technical input.

Current state

Northvale has not defined or carried out any process for assessing the potential consequences of its AI systems for individuals or society. Given that Northvale processes personal health information and its AI systems produce analytics that may influence clinical or operational decisions, this gap carries material risk.

Evidence a reviewer would expect

A documented impact-assessment process that accounts for deployment context, intended use, foreseeable misuse, and the obligations that apply in the jurisdictions where Northvale operates. Completed impact-assessment records for each in-scope AI system, feeding their findings into the risk assessment. Reviewed by a named role, with the date recorded.

Practical sequence

1. Draft the impact-assessment process, defining the factors to consider: deployment context, intended and foreseeable uses, affected individuals (including patients whose health information is processed), and societal effects.
2. Align the process with the risk-assessment method (clause 6.1.2) so that impact findings feed directly into risk records.
3. Once the AI system inventory exists, conduct an impact assessment for each system.
4. Document results and link them to the corresponding risk-assessment records.

12. Clause 6.2: AI objectives and plans (also A.9.3)

Effort (estimate): Medium — Estimated medium because objective-setting is a structured but bounded task once the policy and context are in place; the main complexity is ensuring objectives are meaningful for a healthcare analytics organisation rather than generic, and that they are distributed across relevant functions including data science, clinical operations, and supplier management.

Current state

No AI objectives have been set. There are no measurable targets, no ownership assignments, no timelines, and no plan for achieving objectives. The questionnaire confirms no formal management system exists from which objectives could have been derived.

Evidence a reviewer would expect

A documented set of AI objectives covering relevant functions and levels within Northvale, each consistent with the AI policy, measurable where practicable, and linked to applicable requirements. For each objective: the action plan, the resources required, the named owner, the timeline, and the evaluation method. Reviewed by a named member of top management, with the date recorded.

Practical sequence

1. Once the AI policy is in place (clause 5.2), derive a set of objectives that reflect Northvale's strategic intent and the requirements of interested parties.
2. For each objective, define a measure, a target, an owner, and a timeline.
3. Document the action plan for achieving each objective.
4. Establish a mechanism for monitoring and updating objectives as the management system matures.

13. Clause 6.3: Planned changes

Effort (estimate): Low — Estimated low because change control is a process design task that can be kept proportionate to Northvale's size; the main dependency is having the management system framework in place, and the process itself does not require extensive new infrastructure.

Current state

Northvale has no change-control process for the AI management system. Changes to the system — whether to scope, processes, or controls — are not being managed in a planned or controlled manner.

Evidence a reviewer would expect

A documented change-management process for the AI management system, describing how proposed changes are identified, assessed, reviewed, and recorded. Change records for any changes made after the management system is established. Reviewed by a named role, with the date recorded.

Practical sequence

1. Draft a change-control process as part of the broader management system documentation (clause 4.4).
2. Define the trigger events that require a formal change record (for example, adding a new AI system, changing a SaaS supplier, or revising the scope).
3. Establish a change log template and assign ownership.
4. Apply the process from the point the management system is established, retaining all change records.

14. Clause 7.1: Resources (also A.4.2)

Effort (estimate): High — Estimated high because the systems in scope have not yet been identified, no resource documentation exists, and the requirement spans every life-cycle stage — meaning the work cannot begin in earnest until the AI system inventory is complete, after which each system will need its own resource analysis.

Current state

No formal determination of the resources needed for the AI management system has been made. No budget, staffing, tooling, or infrastructure allocation has been recorded in the context of the management system programme.

Evidence a reviewer would expect

A documented resource plan identifying the people, skills, tools, and budget required to establish, implement, maintain, and improve the AI management system. Evidence that top management has reviewed and committed to providing those resources, with the date recorded.

Practical sequence

1. Once the scope and process map are drafted, produce a resource plan covering personnel (internal and any external support), tooling (for example, risk register and document management), and budget.
2. Present the plan to top management for review and commitment.
3. Retain the record of that review with the date.
4. Update the resource plan as the programme progresses and new needs are identified.

15. Clause 7.2: Competence

Effort (estimate): Medium — Estimated medium because Northvale employs 51 to 200 people across a healthcare analytics function, meaning the number of roles to assess is non-trivial; the healthcare and AI-specific competence requirements add complexity beyond a generic skills framework.

Current state

No competence requirements for AI management system roles have been defined, and no assessment of current competence has been carried out. There are no training records or gap-closure plans in place.

Evidence a reviewer would expect

A documented competence framework identifying the knowledge and skills required for each role that affects AI performance at Northvale. Evidence of how current competence was assessed for each person in those roles. Records of any training, education, or experience used to close gaps. Evidence that the effectiveness of gap-closure actions was evaluated. Retained as documented evidence.

Practical sequence

1. Identify the roles whose work affects AI performance — including data scientists, engineers, clinical analysts, and supplier managers.
2. Define the competence requirements for each role.
3. Assess current competence against those requirements and document the gaps.
4. Plan and deliver training or other gap-closure actions, retaining records of completion.
5. Evaluate whether the actions were effective and record the outcome.

16. Clause 7.3: Awareness

Effort (estimate): Medium — Estimated medium because Northvale's distributed workforce (single office plus remote staff) means the awareness programme must be designed to reach all staff reliably, and the healthcare analytics context means the content must be specific enough to be meaningful to clinical and technical roles alike.

Current state

No awareness programme exists. Staff have not been informed of the AI policy (which does not yet exist), how their work contributes to the AI management system, or the consequences of non-conformance.

Evidence a reviewer would expect

Records showing that all people working under Northvale's control — including remote staff — have received awareness communication covering the AI policy, their contribution to the management system's effectiveness, and the consequences of not conforming. Auditors typically look for attendance records, completion logs, or acknowledgement records tied to named individuals.

Practical sequence

1. Once the AI policy is in place (clause 5.2), design an awareness programme appropriate for Northvale's single-office-plus-remote model.
2. Deliver the programme to all staff, covering the three required topics.
3. Retain completion or acknowledgement records for each individual.
4. Refresh the programme when the policy or management system changes materially.

17. Clause 7.4: Communication

Effort (estimate): Low — Estimated low because a communication plan is a structured document task that builds directly on the interested-party register; the main effort is ensuring external communications to AWS and the SaaS suppliers are appropriately scoped, which is bounded work.

Current state

No internal or external communication plan for the AI management system exists. There is no record of what is communicated, to whom, when, or through which channel.

Evidence a reviewer would expect

A documented communication plan covering internal communications (to staff, including remote workers) and external communications (to customers, AWS, SaaS suppliers, regulators, and other interested parties) about the AI management system. The plan must specify the subject, audience, timing, and channel for each communication type. Retained as documented information.

Practical sequence

1. Using the interested-party register (clause 4.2) as the audience list, draft a communication plan.
2. Define the content, frequency, channel, and owner for each communication type.
3. Implement the plan and retain records of communications sent.

18. Clause 7.5.1: Documented information

Effort (estimate): High — Estimated high because every required document must be created from scratch, the list spans the full management system, and the healthcare analytics context with personal health information and multiple supplier dependencies means many documents will require input from several functions.

Current state

Northvale has no documented information in place for the AI management system. The questionnaire confirms document control is not established and evidence is not organised. No register of required documents exists.

Evidence a reviewer would expect

A complete set of documented information required by ISO/IEC 42001:2023, plus any additional documents Northvale determines are necessary for the management system's effectiveness. A document register listing each item, its owner, version, and status. The volume and detail of documentation should be proportionate to Northvale's size and the complexity of its AI operations.

Practical sequence

1. Compile a list of all documents required by the standard across the management system.
2. Assign an owner and a target completion date to each document.
3. Produce each document progressively as the corresponding clause is addressed.
4. Maintain a document register that tracks status.
5. Review the register periodically to confirm completeness.

19. Clause 7.5.2: Creating and updating documents

Effort (estimate): Low — Estimated low because a document control procedure is a well-understood artefact and Northvale's single-site-plus-remote model does not introduce unusual complexity; the main discipline required is applying it consistently from the outset.

Current state

No document creation or update controls are in place. Documents are not being produced with consistent identification, format, or review steps. This means that even as documents are drafted to address other gaps, they may not meet the standard's requirements for documented information.

Evidence a reviewer would expect

A documented procedure for creating and updating documented information, specifying the required identification elements (title, date, author, reference number), the format and media standards, and the review step confirming suitability and adequacy before a document is issued. Evidence that the procedure is applied to all AI management system documents.

Practical sequence

1. Draft a document control procedure as one of the first management system documents, so it governs all subsequent documents.
2. Define the identification convention (title, version number, date, author, reference) and the format standard.
3. Define the review step: who reviews, what they confirm, and how the review is recorded.
4. Apply the procedure to every document produced thereafter.

20. Clause 7.5.3: Controlling documents

Effort (estimate): Medium — Estimated medium because Northvale's remote workforce and reliance on AWS and several SaaS suppliers means document accessibility and the management of externally originated documents require deliberate design; the controls themselves are not technically complex but must be implemented and evidenced as operating, not merely documented.

Current state

No controls are in place for the distribution, access, retrieval, storage, version control, retention, or disposition of AI management system documents. Externally originated documents — such as AWS terms, SaaS supplier contracts, and any applicable regulatory guidance — are not being managed as part of the system.

Evidence a reviewer would expect

A documented procedure or set of controls covering: where documents are stored and how they are accessed (including by remote staff); version control and the prevention of use of obsolete versions; retention periods and disposition rules; protection of confidentiality and integrity; and the management of externally originated documents that Northvale relies on, including AWS and SaaS supplier documentation. Evidence that the controls are implemented and operating.

Practical sequence

1. As part of the document control procedure (clause 7.5.2), add a section covering storage, access, version

control, retention, and disposition.

2. Identify the platform or system that will hold AI management system documents and confirm it is accessible to remote staff.
3. List the externally originated documents Northvale relies on (AWS terms, SaaS supplier contracts, regulatory guidance) and record how each is obtained, stored, and kept current.
4. Define retention periods for each document category.
5. Have the controls reviewed by a named role, with the date recorded, and confirm they are operating before the certification audit.

21. A.2.3: Other policies that touch AI

Effort (estimate): Medium — Estimated medium because the organisation has no existing mapping and the healthcare analytics context means several policy areas — data protection, clinical data handling, supplier oversight — are likely to intersect with AI objectives, each requiring individual assessment.

Current state

No mapping exists between AI-related objectives and other organisational policies. The answers confirm controls are not mapped and evidence is not organised, so there is no record of which existing policies — for example those covering data protection for personal health information, information security, or supplier management — intersect with AI activities.

Evidence a reviewer would expect

A documented mapping or register that identifies each organisational policy relevant to AI objectives at Northvale Health Analytics — including at minimum any data protection, information security, and supplier management policies — and records how each intersects with or is affected by AI-related activities. The mapping should be reviewed by a named role with the date recorded.

Practical sequence

1. List all current organisational policies held by Northvale Health Analytics.
2. For each policy, assess whether it intersects with the organisation's AI-related objectives or activities, particularly those touching personal health information, AWS hosting, and SaaS supplier use.
3. Document the intersections and any gaps where a policy does not yet exist but should.

22. A.2.4: Reviewing the AI policy

Effort (estimate): Low — Estimated low because this control is addressed largely within the policy document itself and its associated review log; the main effort is in establishing the schedule and trigger conditions, which can be done as part of the A.2.2 drafting work.

Current state

No review schedule or review history exists for an AI policy, because no AI policy has yet been created. Once the policy required by A.2.2 is in place, a defined review cycle and a trigger-based review process will also need to be established.

Evidence a reviewer would expect

A defined review schedule for the AI policy, documented either within the policy itself or in a document control register. Evidence of each review cycle: the date of review, the name and role of the reviewer, any changes made, and the rationale for those changes or for leaving the policy unchanged.

Practical sequence

1. When drafting the AI policy, include a stated review frequency and the conditions that would trigger an out-of-cycle review (for example, a material change to an AI system, a regulatory development affecting personal health information, or a significant incident).
2. Record the initial review in a review log against the policy.
3. Diarise the next scheduled review and assign ownership to a named role.

23. A.3.3: Raising concerns

Effort (estimate): Medium — Estimated medium because the process must be designed from scratch, communicated across a distributed workforce, and integrated with whatever corrective-action tracking Northvale establishes — none of which currently exists.

Current state

No process exists for staff or other parties to raise concerns about Northvale Health Analytics' role in an AI system at any stage of its life cycle. The answers confirm no formal management system and no corrective-action tracker, which means there is no structured channel for concern-raising.

Evidence a reviewer would expect

A documented concern-raising process that covers: how a concern can be raised (channel and format), who receives and triages it, how it is investigated, how the outcome is communicated to the person who raised it, and how records are retained. Evidence that the process has been communicated to all relevant staff, including remote workers.

Practical sequence

1. Design a concern-raising process appropriate to Northvale's size, covering internal staff and, where relevant, external parties such as SaaS supplier contacts.
2. Document the process, including escalation paths and confidentiality protections.
3. Communicate the process to all staff across the single office and remote locations.
4. Retain evidence of communication.
5. Assign a named role as process owner.

24. A.4.3: Data resources

Effort (estimate): High — Estimated high because personal health information is in scope, AWS and several SaaS suppliers are involved in data flows, and no data resource documentation exists — mapping data across multiple systems and suppliers in a healthcare analytics context requires significant structured effort.

Current state

No documentation of data resources used by any AI system exists at Northvale Health Analytics. Given that the organisation handles personal health information and relies on AWS for cloud hosting, the data resource picture is likely to be complex, but it has not been captured anywhere.

Evidence a reviewer would expect

For each AI system in scope: a documented record of the data resources used, covering data sources, data types (including personal health information), data owners, storage locations (including AWS), data flows to and from named SaaS suppliers, and any data quality or provenance considerations. This record should sit within or link to the broader resource register.

Practical sequence

1. For each AI system confirmed in scope, identify all data inputs, training data sets, reference data, and output data.
2. Record data types, noting where personal health information is involved.
3. Document storage locations, including AWS services used, and data flows to named SaaS suppliers.
4. Assign a data owner for each data resource.
5. Incorporate into the resource register.

25. A.4.4: Tooling

Effort (estimate): Medium — Estimated medium because tooling documentation, while absent, is typically more bounded in scope than data or people documentation — the main effort is in conducting the catalogue exercise across each in-scope system and recording it consistently.

Current state

No documentation of tooling used to build or run any AI system exists at Northvale Health Analytics. The answers confirm evidence is not organised and controls are not mapped.

Evidence a reviewer would expect

For each AI system in scope: a documented record of the tools used across development and operation, including software frameworks, model-training platforms, testing tools, and any tools provided by or hosted on AWS or named SaaS suppliers. The record should include tool versions where relevant and link to the broader resource register.

Practical sequence

1. For each AI system confirmed in scope, catalogue the tools used at each life-cycle stage.
2. Record tool names, versions, providers, and whether they are hosted on AWS or delivered by a named SaaS

supplier.

3. Note any tooling dependencies or constraints.
4. Incorporate into the resource register.

26. A.4.5: System and computing resources

Effort (estimate): Medium — Estimated medium because AWS is already identified as the cloud provider, giving a starting point, but the specific services supporting each AI system are undocumented and will need to be mapped system by system.

Current state

No documentation of system and computing resources relied on by any AI system exists at Northvale Health Analytics. AWS is named as the cloud dependency, but no record describes which AWS services or infrastructure components support which AI systems.

Evidence a reviewer would expect

For each AI system in scope: a documented record of the system and computing resources it relies on, including AWS services (for example compute, storage, networking), any on-premises infrastructure at the single office, and computing resources provided by named SaaS suppliers. The record should link to the broader resource register.

Practical sequence

1. For each AI system confirmed in scope, identify the AWS services and any other computing infrastructure it depends on.
2. Document the dependencies, including service names, configurations relevant to AI operation, and any SaaS-provided compute.
3. Incorporate into the resource register.

27. A.4.6: People and skills

Effort (estimate): High — Estimated high because no competence or people documentation exists, the requirement spans every life-cycle phase for each in-scope system, and the organisation has a distributed workforce of 51-200 people — the mapping exercise is substantial even before gap analysis begins.

Current state

No documentation of the people and competencies involved in AI system activities exists at Northvale Health Analytics. The answers confirm no formal management system and no competence records. This applies across all life-cycle phases including development, deployment, operation, change management, maintenance, transfer, decommissioning, verification, and integration.

Evidence a reviewer would expect

For each AI system in scope: a documented record of the roles involved at each life-cycle phase, the competencies required for each role, and the individuals or job titles assigned. This should cover internal staff across the office and remote locations, and any relevant competencies held by named SaaS supplier contacts. The record should link to the broader resource register.

Practical sequence

1. For each AI system confirmed in scope, list the life-cycle phases that apply.
2. For each phase, identify the roles required and the competencies those roles need.
3. Map current staff to those roles and record any competency gaps.
4. Incorporate into the resource register and link to competence records held elsewhere in the management system.

28. A.5.3: Impact assessment records

Effort (estimate): Medium — Estimated medium because the effort here is primarily in executing the process established under A.5.2 and setting a retention period — the design work sits in that control, and this one requires disciplined record-keeping once the process is running.

Current state

No impact-assessment results have been documented or retained at Northvale Health Analytics, because no assessment process exists. There is no retention policy for such records.

Evidence a reviewer would expect

Completed impact-assessment records for each in-scope AI system, retained for a defined period. Each record should identify the system assessed, the date of assessment, the parties affected, the impacts identified, the controls applied, and the name and role of the person who conducted and reviewed the assessment. A documented retention period for these records.

Practical sequence

1. Once the process required by A.5.2 is in place, conduct assessments for each in-scope AI system and retain the results.
2. Define and document the retention period for assessment records, consistent with any obligations relating to personal health information.
3. Store records in a controlled location with access restricted to appropriate roles.

29. A.5.4: Impacts on individuals and groups

Effort (estimate): High — Estimated high because personal health information is in scope, meaning individual impacts are potentially serious and require careful analysis; no assessment has been done for any system; and the life-cycle scope means impacts must be considered from development through to decommissioning.

Current state

No assessment of potential impacts on individuals or groups has been carried out for any AI system at Northvale Health Analytics. The answers confirm no risk process and no evidence organised. Given the organisation's use of personal health information, impacts on individuals are a primary concern that has not been addressed.

Evidence a reviewer would expect

For each in-scope AI system: documented assessment of potential impacts on individuals and groups throughout the system's life cycle, including impacts arising from model outputs, data use, and system failures. The assessment should identify affected parties, describe the nature and severity of potential impacts, and record the controls or mitigations in place. Records should be reviewed by a named role with the date recorded.

Practical sequence

1. As part of the impact-assessment process established under A.5.2, ensure the methodology explicitly addresses impacts on individuals and groups at each life-cycle stage.
2. For each in-scope AI system, conduct and document the individual and group impact assessment.
3. Record mitigations and link them to the risk register.

30. A.5.5: Impacts on society

Effort (estimate): Medium — Estimated medium because the societal impact assessment builds on the methodology and records being developed for A.5.2 through A.5.4 — the incremental effort is in extending the criteria and analysis rather than building a separate process.

Current state

No assessment of potential impacts on individuals, groups, or society has been documented at Northvale Health Analytics. This control extends the individual and group focus of A.5.4 to societal impacts, which in a healthcare analytics context could include effects on health equity, access to care, or clinical decision-making at population level.

Evidence a reviewer would expect

For each in-scope AI system: documented assessment of potential societal impacts, in addition to individual and group impacts. The assessment should consider population-level effects relevant to healthcare analytics, such as algorithmic bias affecting patient groups or systemic effects on clinical pathways. Records should be retained alongside those produced under A.5.3.

Practical sequence

1. Extend the impact-assessment methodology developed under A.5.2 to include explicit societal impact criteria relevant to healthcare analytics.
2. For each in-scope AI system, assess and document societal impacts alongside individual and group impacts.
3. Retain the combined assessment records under the retention policy established for A.5.3.

31. A.6.1.2: Responsible design

Effort (estimate): High — Estimated high because no design processes exist, the healthcare analytics context requires careful consideration of responsible design principles for systems that may affect patient outcomes, and the

documentation must be specific enough to be auditable — this is substantive policy and process work.

Current state

No documented processes for responsible AI system design exist at Northvale Health Analytics. The answers confirm no formal management system and controls are not mapped. There is no evidence that design-stage responsibilities, principles, or procedures have been defined.

Evidence a reviewer would expect

A documented set of design processes that Northvale Health Analytics follows when designing AI systems, covering how responsible AI principles (such as fairness, transparency, and human oversight) are applied at the design stage. The document should be specific to the organisation's healthcare analytics context and reference the personal health information it handles. Reviewed by a named role with the date recorded.

Practical sequence

1. Define the design principles and processes Northvale Health Analytics will follow for responsible AI system design, drawing on the organisation's healthcare analytics context.
2. Document the processes, including decision points, responsible roles, and how design choices are recorded.
3. Communicate the processes to all staff involved in AI system design.

32. A.6.1.3: Responsible development

Effort (estimate): High — Estimated high because no development processes exist, the organisation uses AWS and several SaaS suppliers whose roles in the development pipeline must be documented, and responsible development in a healthcare analytics context requires detailed process design.

Current state

No documented processes for responsible AI system development exist at Northvale Health Analytics. The answers confirm no formal management system. Development-stage processes — covering how AI systems are built, tested, and prepared for deployment — have not been defined.

Evidence a reviewer would expect

A documented set of development processes that Northvale Health Analytics follows when building or materially enhancing AI systems, covering responsible development practices such as data governance during development, bias testing, and version control. The document should reference the organisation's use of AWS and named SaaS suppliers in the development pipeline. Reviewed by a named role with the date recorded.

Practical sequence

1. Define the development processes Northvale Health Analytics will follow, including how AWS and named SaaS supplier tools are used responsibly during development.
2. Document the processes, including roles, checkpoints, and how development decisions are recorded.
3. Communicate the processes to all staff involved in AI system development.

33. A.6.2.2: System requirements

Effort (estimate): High — Estimated high because no specification process or templates exist, the requirement applies to each in-scope AI system individually, and healthcare analytics requirements involving personal health information are complex enough to require careful drafting and review.

Current state

No requirements specification process exists at Northvale Health Analytics. The answers confirm no formal management system and evidence is not organised. There is no record of requirements being specified or documented before building or enhancing any AI system.

Evidence a reviewer would expect

For each AI system in scope: a documented requirements specification produced before development or material enhancement begins, covering functional requirements, data requirements, performance criteria, safety and fairness requirements relevant to healthcare analytics, and any constraints arising from the use of personal health information. Each specification should carry a version number, a date, and a record of review by a named role.

Practical sequence

1. Define a requirements specification template appropriate to Northvale's healthcare analytics AI systems.
2. For each in-scope AI system, produce a requirements specification before any new development or material enhancement begins.

- Record the specification in a controlled document with version number and effective date.

34. A.6.2.3: Design and development traceability

Effort (estimate): Medium — Estimated medium because traceability documentation builds on the requirements specifications being developed under A.6.2.2 — the incremental effort is in maintaining the linkage throughout development rather than in a separate design exercise.

Current state

No traceability documentation exists at Northvale Health Analytics linking AI system design and development decisions back to organisational objectives, documented requirements, or specification criteria. The answers confirm controls are not mapped and evidence is not organised.

Evidence a reviewer would expect

For each in-scope AI system: a traceability record or matrix that maps design and development decisions to the requirements specification produced under A.6.2.2, to Northvale's AI-related objectives, and to the specification criteria. The record should be maintained throughout the development life cycle and reviewed by a named role with the date recorded.

Practical sequence

- Once requirements specifications are in place under A.6.2.2, establish a traceability approach — for example a requirements traceability matrix — for each in-scope AI system.
- Populate the matrix as design and development decisions are made, linking each decision to its originating requirement or objective.
- Maintain the matrix through the development life cycle.
- Have the matrix reviewed by a named role at key development milestones.

35. A.6.2.4: Verification and validation

Effort (estimate): High — Estimated high because no verification or validation framework exists, healthcare analytics AI systems require rigorous validation criteria given their potential effect on patient-related decisions, and the work must be completed for each in-scope system before deployment.

Current state

No verification and validation measures or criteria have been defined or documented for any AI system at Northvale Health Analytics. The answers confirm no formal management system and evidence is not organised.

Evidence a reviewer would expect

For each in-scope AI system: a documented verification and validation plan that defines the measures to be applied, the criteria used to determine whether the system meets its requirements, and the conditions under which validation is considered complete. Records of verification and validation activities carried out, including results and the name and role of the person who reviewed them.

Practical sequence

- Define verification and validation measures and criteria for each in-scope AI system, appropriate to the healthcare analytics context and the personal health information involved.
- Document the plan, including who is responsible for each measure and what constitutes a passing result.
- Carry out and record verification and validation activities before deployment.

36. A.6.2.5: Deployment

Effort (estimate): Medium — Estimated medium because the deployment plan builds on the validation and requirements work being done under other controls — the incremental effort is in defining pre-deployment conditions and completing the checklist for each system.

Current state

No deployment plan exists for any AI system at Northvale Health Analytics, and no pre-deployment conditions have been defined or checked. The answers confirm no formal management system and evidence is not organised.

Evidence a reviewer would expect

For each in-scope AI system: a documented deployment plan that sets out the steps for going live, the pre-deployment conditions that must be met (for example, completion of validation under A.6.2.4, data protection checks for personal health information, and confirmation of AWS infrastructure readiness), and a record

confirming those conditions were met before deployment. The record should name the role that confirmed readiness and carry the date.

Practical sequence

1. Define the pre-deployment conditions applicable to each in-scope AI system, drawing on the validation criteria from A.6.2.4 and any data protection requirements for personal health information.
2. Document a deployment plan for each system.
3. Before each deployment, complete a pre-deployment checklist and record the outcome, naming the role that confirmed readiness and the date.

37. A.6.2.6: Operation and monitoring after deployment

Effort (estimate): High — Estimated high because no operational framework exists, the requirement covers multiple operational dimensions for each in-scope system, and the healthcare analytics context means performance monitoring must be designed with patient-safety considerations in mind — this is substantive operational design work.

Current state

No post-deployment operational requirements have been defined or documented for any AI system at Northvale Health Analytics. The answers confirm no formal management system. There is no record of how system performance is monitored, how repairs or updates are managed, or what support arrangements are in place.

Evidence a reviewer would expect

For each in-scope AI system: a documented operational framework covering at minimum system and performance monitoring (including how AWS infrastructure performance is tracked), the process for repairs and updates (including how named SaaS supplier updates are managed), and support arrangements. The framework should define who is responsible for each element and how issues are escalated. Reviewed by a named role with the date recorded.

Practical sequence

1. For each in-scope AI system, define the monitoring, repair, update, and support requirements for responsible post-deployment operation.
2. Document the operational framework, including responsibilities, escalation paths, and how AWS and named SaaS supplier arrangements are managed.
3. Implement monitoring and record the results.

38. A.6.2.7: Technical documentation

Effort (estimate): High — Estimated high because no technical documentation exists for any audience, the healthcare analytics context is likely to involve multiple interested-party categories with different documentation needs, and producing audience-appropriate documentation for each in-scope system is a substantial writing and review exercise.

Current state

No technical documentation has been produced or structured for any interested-party audience at Northvale Health Analytics. The answers confirm evidence is not organised. There is no record of what documentation users, partners, or supervisory authorities would need, or in what form.

Evidence a reviewer would expect

For each in-scope AI system: a documented analysis of the technical documentation needs of each category of interested party — including at minimum system users, partner organisations, and any supervisory authorities relevant to the healthcare analytics context. Documentation produced for each audience in an appropriate form and level of detail. A record of how documentation is maintained and updated.

Practical sequence

1. Identify the categories of interested party for each in-scope AI system, including internal users, partner organisations, and any supervisory authorities.
2. For each category, determine what technical documentation they need and in what form.
3. Produce the documentation for each audience.
4. Establish a process for keeping documentation current as systems change.

39. A.6.2.8: Event logs

Effort (estimate): Medium — Estimated medium because AWS provides logging infrastructure that Northvale can leverage, reducing the technical effort — the main work is in making and documenting the life-cycle phase decisions,

configuring logging consistently across in-scope systems, and setting retention periods appropriate to personal health information obligations.

Current state

No event-log record-keeping has been defined or enabled for any AI system at Northvale Health Analytics. The answers confirm no formal management system and evidence is not organised. There is no record of which life-cycle phases require logging or what logging is currently active.

Evidence a reviewer would expect

For each in-scope AI system: a documented decision on which life-cycle phases require event-log record-keeping, with a clear rationale. Evidence that logging is active at minimum during the period when each system is in active use, including records of what is logged, where logs are stored (for example in AWS), how long they are retained, and who has access. Auditors typically look for a log configuration record and sample log outputs.

Practical sequence

1. For each in-scope AI system, determine which life-cycle phases require event-log record-keeping and document the rationale.
2. Confirm that logging is enabled and active for all systems currently in use, using AWS logging capabilities where applicable.
3. Define log retention periods consistent with any obligations relating to personal health information.
4. Document the log configuration and assign a named role as owner.
5. Retain sample log outputs as evidence.

40. A.7.2: Data management

Effort (estimate): High — Estimated high because Northvale processes personal health information across AWS and several named SaaS suppliers with no existing documented processes, meaning the data flow mapping and process drafting must be built entirely from scratch across multiple system and supplier boundaries.

Current state

Northvale has no documented data management processes to support AI system development. With personal health information in scope, AWS as the cloud environment, and several named SaaS suppliers involved, the absence of any formal process means there is no documented basis for how data flows into, through, or out of AI development activities. No evidence is organised and no management system exists from which such a process could be derived.

Evidence a reviewer would expect

A documented data management process covering how personal health information is handled across the AI development life cycle, including roles responsible for each stage, controls applied within the AWS environment and at each named SaaS supplier boundary, and records showing the process has been followed for each AI system Northvale develops or operates.

Practical sequence

1. Identify every AI system in scope and map the data flows that feed each one, including data received from or processed within AWS and each named SaaS supplier.
2. Draft a data management process document that covers ingestion, storage, transformation, use in model development, and disposal of personal health information.
3. Assign a named role holder as process owner.
4. Implement the process for each in-scope system and retain records of its application.

41. A.7.3: Data acquisition and selection

Effort (estimate): Medium — Estimated medium because the documentation work is bounded by the number of AI systems Northvale operates, but the involvement of AWS and several named SaaS suppliers means acquisition routes must be traced across multiple external boundaries before the documentation can be completed.

Current state

Northvale has not documented how data used in its AI systems is acquired or selected. Given that personal health information is the regulated data type and that AWS and several named SaaS suppliers are involved in data handling, the absence of any acquisition and selection documentation represents a material gap with direct implications for both certification and the health-sector context in which Northvale operates.

Evidence a reviewer would expect

A documented description, for each AI system in scope, of where data originates, the criteria used to select it, any filtering or exclusion decisions made at acquisition, and the rationale for those decisions. Records should show who made each selection decision and when.

Practical sequence

1. For each AI system identified in scope, document the data sources, including those hosted on AWS and those provided through named SaaS suppliers.
2. Record the criteria applied when selecting which data to use, including any exclusions of data categories or populations.
3. Capture the rationale for each selection decision and name the role holder who made it.

42. A.7.4: Data quality

Effort (estimate): Medium — Estimated medium because defining quality requirements is a bounded analytical task, but confirming that existing data meets them requires assessment work across each in-scope system and its data sources, which span AWS and named SaaS suppliers.

Current state

No documented data-quality requirements exist for any AI system at Northvale, and there is no evidence that data used in development or operation has been assessed against any quality criteria. For a healthcare analytics organisation handling personal health information, the absence of quality requirements creates risk both to AI system outputs and to the individuals whose data is processed.

Evidence a reviewer would expect

A documented set of data-quality requirements for each AI system in scope, covering dimensions relevant to the system's purpose (such as completeness, accuracy, timeliness, and representativeness). Records showing that data used in development and operation has been assessed against those requirements, with outcomes and any remediation actions noted.

Practical sequence

1. For each AI system in scope, define the data-quality dimensions that matter for that system's intended outputs, taking into account the nature of personal health information involved.
2. Set measurable thresholds or acceptance criteria for each dimension.
3. Assess the data currently used against those criteria and document the results.
4. Where data does not meet requirements, record the remediation action taken and by whom.

43. A.7.5: Data provenance

Effort (estimate): High — Estimated high because provenance tracking must span the full data and system life cycle across AWS and several named SaaS suppliers, none of which have been mapped, and because no existing process or records provide a starting point.

Current state

Northvale has no documented provenance-tracking process for data used in its AI systems. No management system or risk process exists from which such a process could have emerged. Provenance tracking across both the data life cycle and the AI system life cycle is entirely absent, which is a significant gap given that personal health information is in scope and multiple external parties — AWS and several named SaaS suppliers — handle that data.

Evidence a reviewer would expect

A documented process for tracking data provenance from original source through all transformations, transfers, and uses, covering both the data's own life cycle and the life cycle of each AI system that uses it. Records produced by applying that process to each in-scope system, showing the chain of custody for personal health information at each stage.

Practical sequence

1. Define the provenance attributes to be tracked (origin, collection method, transformation steps, transfer events, version, and disposal).
2. Document the process for capturing and maintaining those attributes across the AWS environment and at each named SaaS supplier boundary.
3. Apply the process to each AI system in scope and produce provenance records.

4. Establish how provenance records are updated when a system or its data changes.
5. Assign a named role holder as process owner and have the process document reviewed by that person, with the review date recorded.

44. A.7.6: Data preparation

Effort (estimate): Medium — Estimated medium because the documentation is largely a structured capture of decisions already being made in practice, but the absence of any existing records means the work must reconstruct past decisions as well as formalise future ones for each in-scope system.

Current state

Northvale has not documented the criteria used to select data-preparation approaches, nor the methods applied. There is no evidence that data-preparation decisions have been recorded for any AI system. Without this documentation, a reviewer cannot assess whether preparation choices were appropriate for the personal health information being processed or consistent across systems.

Evidence a reviewer would expect

For each AI system in scope, a document recording the data-preparation approaches considered, the criteria used to select among them, and the specific methods applied (such as normalisation, de-identification, imputation, or resampling). The rationale for each choice should be traceable to the system's intended purpose and the nature of the data.

Practical sequence

1. For each AI system in scope, identify the data-preparation steps currently applied and document them.
2. Articulate the criteria that drove each preparation choice, including any considerations specific to personal health information (such as de-identification requirements).
3. Record who made each decision and when.
4. Establish that future preparation decisions follow the same documented criteria.

45. A.8.2: Information for users

Effort (estimate): Medium — Estimated medium because the scope of work is bounded by the number of AI systems and user groups, but producing clear, accessible information about healthcare analytics AI outputs requires careful drafting and review to avoid misleading users.

Current state

Northvale has not determined or provided users of its AI systems with the information they need to use those systems appropriately. No user-facing documentation, guidance, or information packages have been identified. For a healthcare analytics organisation whose AI outputs may inform clinical or operational decisions, this gap carries direct risk to users and to the individuals whose health information is processed.

Evidence a reviewer would expect

For each AI system in scope, a documented determination of what information users need (covering system purpose, capabilities, limitations, appropriate use, and known risks), and evidence that this information has been provided to users in a form they can access and understand. Records of how and when information was communicated.

Practical sequence

1. For each AI system in scope, identify who the users are and what decisions or actions they take based on the system's outputs.
2. Determine what information those users need, including limitations, confidence levels, and conditions under which outputs should not be relied upon.
3. Produce user-facing documentation or guidance in accessible language.
4. Distribute the information to users and retain a record of distribution.

46. A.8.3: Reporting adverse impacts

Effort (estimate): Low — Estimated low because establishing a reporting mechanism is primarily a process and communication task that does not depend on resolving the broader system or data documentation gaps, and can be implemented quickly once a named role holder is assigned.

Current state

Northvale has no mechanism through which users or other interested parties can report adverse impacts from its

AI systems. No reporting channel, process, or contact point has been established. Given that Northvale's AI systems process personal health information and their outputs may affect individuals, the absence of any reporting route is a material gap.

Evidence a reviewer would expect

A documented and accessible mechanism — such as a dedicated contact address, a form, or a defined process — through which users and other interested parties can report adverse impacts. Records showing the mechanism has been communicated to relevant parties and that any reports received have been logged and acted upon.

Practical sequence

1. Define what constitutes an adverse impact in the context of Northvale's AI systems and the personal health information they process.
2. Establish a reporting channel (for example, a named contact role and a dedicated address) and document the process for receiving, logging, and responding to reports.
3. Communicate the mechanism to users and other interested parties and retain a record of that communication.

47. A.8.4: Incident communication

Effort (estimate): Medium — Estimated medium because the plan must address incident scenarios across AWS and several named SaaS suppliers, and aligning notification timeframes with the obligations that apply to personal health information requires input from Northvale's legal and compliance function before the document can be finalised.

Current state

Northvale has no documented incident communication plan for notifying AI system users when incidents occur. No incident management process exists from which such a plan could be derived. For a healthcare analytics organisation, the absence of a plan for communicating AI-related incidents to users — who may be making health-related decisions based on system outputs — is a significant gap.

Evidence a reviewer would expect

A documented plan stating how Northvale will communicate AI system incidents to users, covering what triggers communication, who is responsible for initiating it, the timeframes for notification, the channels to be used, and the content of notifications. The plan should address incidents affecting personal health information processed through AWS and the named SaaS suppliers.

Practical sequence

1. Define the incident types that require user communication, including those arising from failures in the AWS environment or at named SaaS suppliers.
2. Document the communication plan, naming the role responsible for each step, the notification timeframes, and the channels to be used.
3. Align the plan with any incident response obligations that apply to personal health information in Northvale's operating context.
4. Test the plan at least once before the certification audit and retain a record of the test.

48. A.8.5: Reporting obligations

Effort (estimate): Medium — Estimated medium because identifying and documenting obligations requires legal and compliance input specific to the jurisdiction and health-sector context in which Northvale operates, which has not yet been confirmed, adding a dependency that extends the timeline for this task.

Current state

Northvale has not determined or documented its obligations to report AI system information to interested parties. No process exists for identifying those obligations, and no records have been produced. Given that personal health information is in scope and that Northvale operates in the healthcare analytics sector, reporting obligations to interested parties — including those arising from the health-sector and data protection framework applicable to Northvale — are likely to be material but have not been assessed.

Evidence a reviewer would expect

A documented record of Northvale's obligations to report AI system information to interested parties, including the basis for each obligation, the parties to whom reporting is owed, the information to be reported, and the frequency or trigger for reporting. The record should be reviewed and kept current as obligations change.

Practical sequence

1. Identify all categories of interested party relevant to Northvale's AI systems (users, data subjects, commissioners, oversight bodies, and others as applicable).
2. Determine, with input from Northvale's legal and compliance function, what reporting obligations apply in each case, referencing the jurisdiction and sector obligations confirmed by Northvale.
3. Document each obligation, its basis, the responsible role, and the reporting schedule or trigger.
4. Establish a process for reviewing the obligations record when the regulatory environment or Northvale's AI systems change.

49. A.9.2: Responsible use

Effort (estimate): High — Estimated high because responsible-use processes must be defined for each AI system in scope, none of which have been inventoried, and must address the operating model across Northvale's single office, remote staff, AWS environment, and named SaaS suppliers — all without any existing process foundation.

Current state

Northvale has no documented processes for the responsible use of its AI systems. No management system, risk process, or operational controls exist from which such processes could be derived. The absence of responsible-use processes means there is no documented basis for how Northvale's staff, its AWS-hosted systems, or its named SaaS suppliers are expected to behave when using or operating AI systems that process personal health information.

Evidence a reviewer would expect

Documented processes covering how AI systems are to be used responsibly, including the conditions of use, the human oversight arrangements, the actions required when outputs are uncertain or potentially harmful, and the escalation routes available to users. Processes should address use within Northvale's own operations and, where relevant, use by parties accessing outputs through named SaaS suppliers.

Practical sequence

1. For each AI system in scope, define the conditions under which it may be used and the human oversight arrangements that apply.
2. Document the actions users must take when outputs are uncertain, unexpected, or potentially harmful, including escalation routes.
3. Establish how compliance with responsible-use processes is monitored and by whom.
4. Communicate the processes to all relevant users and retain a record of that communication.

50. A.9.4: Intended use

Effort (estimate): Medium — Estimated medium because the work is bounded by the number of AI systems in scope, but producing credible intended-use documentation for healthcare analytics systems requires input from the teams that built or configured each system, which may involve coordination across Northvale's staff and named SaaS suppliers.

Current state

Northvale has not confirmed that any AI system is used consistently with its intended use or accompanying documentation. No intended-use documentation exists for any system, and no process for checking consistency of use has been established. This gap means there is no assurance that Northvale's AI systems — which process personal health information — are being applied within the boundaries for which they were designed.

Evidence a reviewer would expect

For each AI system in scope, documentation of its intended use. Records showing that actual use has been assessed against that intended use, that any deviations have been identified and addressed, and that the assessment has been reviewed by a named role holder with the date recorded.

Practical sequence

1. For each AI system in scope, document its intended use, including the user population, the decisions it is designed to support, and the conditions under which it should not be used.
2. Establish a process for periodically checking that actual use matches intended use, including a mechanism for users to flag deviations.
3. Conduct an initial assessment of current use against intended use for each system and document the results.
4. Address any identified deviations and record the actions taken.

51. A.10.2: Responsibilities across suppliers and partners

Effort (estimate): High — Estimated high because responsibility must be assigned across Northvale's own staff, AWS, and several named SaaS suppliers for every AI system in scope, none of which have been inventoried, and because confirming supplier responsibilities requires reviewing contracts that have not yet been assessed.

Current state

Northvale has not assigned AI life-cycle responsibilities across the parties involved in its AI systems. No accountability structure exists covering Northvale's own staff, its AWS environment, or its several named SaaS suppliers. With no formal management system and no controls mapped, responsibility for AI life-cycle activities — from development through operation to decommissioning — is undocumented and unassigned.

Evidence a reviewer would expect

A documented responsibility assignment covering every stage of the AI life cycle for each system in scope, naming the responsible party (Northvale role, AWS, or named SaaS supplier as appropriate) for each activity. The document should make clear where accountability sits when activities span more than one party, and should be supported by contractual or service-level provisions with each named supplier confirming their responsibilities.

Practical sequence

1. For each AI system in scope, map the life-cycle stages (design, data management, development, testing, deployment, operation, monitoring, and decommissioning).
2. For each stage, assign a named responsible party — a Northvale role, AWS, or a named SaaS supplier.
3. Identify any stages where responsibility is shared and document how accountability is maintained across the boundary.
4. Check that supplier contracts with AWS and each named SaaS supplier reflect the responsibilities assigned to them; note any gaps for resolution.

52. A.10.3: Supplier checks

Effort (estimate): High — Estimated high because the assessment must cover AWS and several named SaaS suppliers, Northvale's responsible-AI approach does not yet exist as a document, and the criteria for supplier assessment must be developed before any supplier can be evaluated.

Current state

Northvale has no process for confirming that AI-related services, products, or materials sourced from its named SaaS suppliers or from AWS are consistent with its own responsible-AI approach. No responsible-AI approach has itself been documented, and no supplier assessment process exists. This means Northvale currently has no basis for assuring that what it sources externally aligns with the principles it intends to operate under.

Evidence a reviewer would expect

A documented process for assessing AI-related products, services, and materials from suppliers — including AWS and each named SaaS supplier — against Northvale's responsible-AI approach before adoption. Records showing that the process has been applied to each current supplier and that the outcomes have been reviewed by a named role holder with the date recorded. Where a supplier's approach does not align, the record should show how the gap was addressed.

Practical sequence

1. Document Northvale's responsible-AI approach, or confirm it is captured in the AI policy being developed under the management-system workstream.
2. Define the criteria against which supplier AI products, services, and materials will be assessed.
3. Apply the assessment to AWS and each named SaaS supplier, documenting the outcome for each.
4. Where gaps are found, record the action taken (for example, contractual requirement, compensating control, or decision not to use the product).
5. Establish a trigger for re-assessment when a supplier changes its AI-related products or practices.

53. A.10.4: Customer expectations

Effort (estimate): Medium — Estimated medium because the process design is a bounded task, but gathering meaningful customer input in a healthcare analytics context requires structured engagement with customers who may themselves operate under regulated environments, adding coordination and documentation effort.

Current state

Northvale has not established a process for factoring customer expectations and needs into how it develops and uses AI systems responsibly. No mechanism exists for capturing customer input, and no records of customer expectations have been produced. For a healthcare analytics organisation whose AI outputs are used by customers to support health-related decisions, the absence of this process means customer needs may not be reflected in system design or responsible-use decisions.

Evidence a reviewer would expect

A documented process for identifying and incorporating customer expectations and needs into AI development and responsible-use decisions. Records showing that customer input has been sought and considered for each AI system in scope, and that the outcomes have influenced documented decisions about system design, use conditions, or responsible-use processes.

Practical sequence

1. Define who Northvale's customers are in the context of each AI system in scope and what expectations and needs are relevant to responsible AI use.
2. Establish a process for gathering customer input — for example, through structured engagement, feedback mechanisms, or contractual requirements.
3. Document how customer input is reviewed and how it feeds into AI development and responsible-use decisions.
4. Apply the process to each current AI system and record the outcomes.

Information you need to supply

1. Confirm the jurisdiction or jurisdictions in which Northvale Health Analytics operates, and the health-sector and data protection obligations that apply there — this is needed to complete the context analysis, the impact-assessment process, and the interested-party register.
2. Provide the names of all AI systems Northvale intends to bring into the certification scope, including their purpose, the data they process, and whether each is developed internally, procured from a SaaS supplier, or hosted on AWS.
3. Provide the names of the SaaS suppliers whose AI capabilities are in scope, so that supplier-specific risk, impact, and communication requirements can be assessed.
4. Confirm the name and role of the individual who will act as executive sponsor and the individual who will be designated AI management system lead, so that responsibility assignments can be finalised.
5. Confirm whether any existing policies — such as information security, data protection, or clinical governance policies — are in place that the AI policy should cross-reference.
6. Confirm the platform or system that will be used to store and control AI management system documents, and whether it is accessible to all remote staff.
7. Confirm whether any competence assessments, training records, or role descriptions for data science, engineering, or clinical analytics roles already exist, so that the gap between current and required competence can be scoped accurately.
8. Confirm whether any contracts with AWS or the SaaS suppliers contain AI-specific terms, data processing agreements, or audit rights that are relevant to the management system scope.

Implementation plan

142 activities in 12 phases, 408 effort days in total, from October 1, 2026 to March 31, 2027. Every activity, with its owner, dependencies, deliverable and evidence, is in the accompanying workbook.

The plan finishes by March 31, 2027, inside the 6-month target of April 1, 2027, with about three people working on it full time.

1. Mobilize and govern	October 1, 2026 to October 7, 2026 · 11 activities · 18 effort days · led by Executive sponsor, Management-system lead
2. Context, scope and obligations	October 9, 2026 to October 22, 2026 · 13 activities · 33 effort days · led by Management-system lead, Executive sponsor
3. Baseline and gap assessment	October 26, 2026 to November 4, 2026 · 12 activities · 28 effort days · led by Management-system lead, Executive sponsor
4. Risk assessment and treatment	November 6, 2026 to November 23, 2026 · 14 activities · 41 effort days · led by Management-system lead, Executive sponsor
5. Applicability and control design	November 25, 2026 to December 11, 2026 · 13 activities · 41 effort days · led by Management-system lead, Executive sponsor
6. Document and implement the system	December 15, 2026 to December 29, 2026 · 15 activities · 41 effort days · led by Management-system lead, Executive sponsor
7. Operate controls and collect evidence	December 31, 2026 to February 3, 2027 · 13 activities · 76 effort days · led by Management-system lead
8. Measure and evaluate	February 5, 2027 to February 15, 2027 · 8 activities · 26 effort days · led by Management-system lead
9. Internal audit	February 17, 2027 to February 26, 2027 · 12 activities · 29 effort days · led by Management-system lead, Executive sponsor
10. Management review and readiness	March 2, 2027 to March 9, 2027 · 10 activities · 23 effort days · led by Management-system lead, Executive sponsor
11. Certification-body preparation	March 11, 2027 to March 17, 2027 · 9 activities · 19 effort days · led by Management-system lead, Executive sponsor
12. External audit and closeout	March 19, 2027 to March 31, 2027 · 12 activities · 33 effort days · led by Management-system lead, Executive sponsor

Clause coverage

The workbook tracks 32 management-system clause requirements and 38 Annex A controls for ISO/IEC 42001, each with status, owner, evidence link and reviewer notes. The gaps above are the ones this assessment found material; a requirement not listed is not thereby met.

Basis and constraints

- The indicator is a planning aid based only on the selected answers; it is not an audit score or certification decision.
- All customer-provided statements and evidence links require validation by the assigned owner.
- Control applicability depends on scope, risks, legal and contractual duties, technology, suppliers and interested parties.
- Only an independent certification body can make the certification decision.

Standard	ISO/IEC 42001
Edition	2023
Official source	https://www.iso.org/standard/42001

Clause and control names in this report are RiskWoven's own paraphrases. The standard's text is not reproduced; refer to your licensed copy of the standard for the exact wording.