MANUAL

AI Management System Manual

The controlling document of [Company Name]'s AI management system. It demonstrates, clause by clause, how the organisation meets ISO/IEC 42001:2023 and provides traceability between the requirements of the standard and the supporting procedures, forms, tools and records.

DOCUMENT NO	REVISION	EFFECTIVE DATE	OWNER
MAN-01	**[Revision]**	**[Date]**	**[Designation Here]**

2.4 Integration with existing governance

Although ISO/IEC 42001 is the organisation's first formal management system, the organisation does not manage AI in isolation from its established clinical and information governance. The AIMS is designed to connect to the organisation's clinical-safety arrangements, so that an AI-related clinical risk is handled through both the AIMS and the clinical-safety process; to its information-governance and data-protection arrangements, so that the privacy dimension of AI is managed consistently; and to its procurement arrangements, so that responsible-AI expectations are applied when AI systems are acquired. Where the AIMS and an existing process both apply, the roles matrix (QF-03-01) records which process leads and how they interact, avoiding duplication while ensuring nothing falls between them.

2.5 The deployer life cycle applied by [Company Name]

Because [Company Name] deploys rather than develops AI, the AIMS is organised around the stages at which a deployer exercises control over an AI system. The stages below define where the operating controls of the AIMS apply, and each stage generates records that provide evidence of conformity. The stages are elaborated in the operating procedures QP-09 to QP-14 and are the frame for the operational controls described in Section 8.

Life-cycle stage (deployer)	What [Company Name] controls	Primary procedure
Need and requirements	Defining the clinical need and the requirements the AI system must meet	QP-09
Selection and evaluation	Evaluating and selecting a supplier and system against requirements and responsible-AI expectations	QP-09, QP-14
Impact and risk assessment	Assessing impact on people and society and assessing and treating risk before use	QP-05, QP-04
Verification and validation	Validating performance for the local context against defined acceptance criteria	QP-09
Deployment	Authorising deployment once requirements and controls are met	QP-09
Operation and monitoring	Operating with human oversight; monitoring performance and event logs	QP-09, QP-13, QP-15
Change and decommissioning	Controlling supplier updates and the retirement of a system	QP-06, QP-09

2.3 Manual usage and maintenance

This manual is a controlled document maintained by the AIMS Manager under procedure QP-01, Control of Documented Information. It is reviewed at least annually and whenever significant change to the AIMS occurs. The current, approved version is held in the AIMS shared workspace; printed copies

PROCEDURE

AI Risk Management

Defines how [Company Name] establishes its AI risk criteria and assesses, treats and monitors the risks of the AI systems it deploys, and how it produces and maintains the Statement of Applicability and the AI risk treatment plan.

DOCUMENT NO	REVISION	EFFECTIVE DATE	OWNER
QP-04	[Revision]	[Date]	[Designation Here]

Document Control

Field	Detail
Document number	QP-04
Title	AI Risk Management
Standard reference	ISO/IEC 42001:2023, Clauses 6.1.1, 6.1.2, 6.1.3, 8.2, 8.3
Version	[Revision]
Date of issue	[Date]
Prepared by	ISO Consultant Panel
Reviewed by	[Name] / [Designation Here]
Approved by	[Name] / [Designation Here]
Next review date	[Date]

Revision History

Version	Date	Description of change	Author	Approved
1	[Date]	First issue of the document.	ISO Consultant Panel	[Name]

Contents

PROCEDURE

AI Risk Management

1 Purpose

This procedure ensures that [Company Name] identifies, analyses, evaluates, treats and monitors the risks arising from the AI systems it deploys, using consistent criteria, so that the level of control applied to each system is proportionate to the risk it presents to the organisation, to individuals and groups of individuals, and to society. It gives effect to Clauses 6.1.1, 6.1.2 and 6.1.3 and to the operational risk requirements of Clauses 8.2 and 8.3 of ISO/IEC 42001:2023.

Risk management is the engine of the AIMS. It is the process by which the organisation's understanding of its context and of the impact of its AI systems is turned into concrete controls, and by which the Statement of Applicability, the risk treatment plan and the operational controls are derived and justified. For a healthcare deployer, the risks that matter most are those that can reach a patient, and the procedure is written so that such risks are neither understated nor lost among administrative concerns.

2 Scope

This procedure applies to every AI system within the AIMS scope, at each stage of its life with the organisation, and to any grouping of AI systems where a common risk is more usefully assessed together. It covers the establishment and maintenance of risk criteria, the risk assessment process, the risk treatment process including the Statement of Applicability, and the operational performance and updating of assessments and treatments. It applies to the AIMS Manager, who coordinates the process, to clinical system owners, who bring knowledge of each system's use and consequences, and to the AI Governance Committee, which approves the risk treatment plan and accepts residual risk.

3 References

ISO/IEC 42001:2023, Clauses 6.1.1 to 6.1.3, 8.2, 8.3; Annex A; Annex B implementation guidance; Annex C potential objectives and risk sources. QP-05 AI System Impact Assessment (a key input). MAN-01 AI Management System Manual, Section 6. Supporting forms and tools: AI risk criteria (QF-04-01), AI risk assessment register (QF-04-02), AI risk treatment plan (QF-04-03), Statement of Applicability record (QF-04-04), risk register tool (T-01) and Statement of Applicability tool (T-02). References are supplementary; the criteria needed to apply this procedure, including the full scales, are contained within it.

4 Responsibilities

Activity	Committee	AIMS Mgr	Sys owner	DPO
Establish and maintain AI risk criteria	A	R	C	C
Identify and analyse AI risks	I	A	R	C
Evaluate and prioritise risks	C	A/R	C	C
Select risk treatment and controls	A	R	C	C
Produce and maintain the Statement of Applicability	A	R	C	C
Approve the risk treatment plan and accept residual risk	A/R	C	C	I
Perform operational reassessment (8.2) and verify treatment (8.3)	I	A	R	C

Key: **R** responsible, **A** accountable, **C** consulted, **I** informed.

5 Definitions and risk criteria

The organisation establishes and maintains the following AI risk criteria, which support distinguishing acceptable from non-acceptable risk, performing risk assessments, conducting risk treatment and assessing risk impacts (6.1.1). The criteria are fixed here so that repeated assessments produce consistent, valid and comparable results (6.1.2).

Consistent with Clause 6.1.1, this procedure addresses opportunities as well as risks. The organisation records the opportunities its AI systems present, for example faster and more consistent triage, earlier detection of deterioration, and improved patient access, and plans actions to pursue them alongside the actions that treat risk, so that the AIMS gives assurance it can achieve its intended results, prevents or reduces undesired effects, and achieves continual improvement. For both risks and opportunities the organisation plans the actions to address them, how to integrate and implement those actions into the AIMS processes, and how to evaluate their effectiveness, and it retains documented information on the actions taken.

5.1 Likelihood scale

Level	Descriptor	Meaning

1	Rare	Not expected to occur in normal operation.
2	Unlikely	Could occur but not expected.
3	Possible	Might occur at some time.
4	Likely	Expected to occur at some point.
5	Almost certain	Expected to occur frequently.

5.2 Consequence scale

The consequence scale is expressed so that harm to a patient or to society is made explicit and cannot be understated by a purely operational reading.

Level	Descriptor	Consequence to individuals / society	Consequence to the organisation
1	Insignificant	No effect on any person.	Negligible.
2	Minor	Minor inconvenience, no clinical effect.	Minor, contained locally.
3	Moderate	Temporary or reversible harm, or limited unfairness.	Audit finding; some disruption.
4	Major	Serious harm to a person, or systematic unfairness to a group.	Significant regulatory or reputational impact.
5	Severe	Death, permanent harm, or wide societal harm.	Loss of certification; major legal or reputational impact.

5.3 Risk score, bands and acceptance rule

The risk score is the product of likelihood and consequence, giving a value from 1 to 25. The bands and the acceptance rule below determine how each risk is handled. Borderline cases default to the higher band.

Band	Score	Acceptance rule and authority
Low	1 to 4	Acceptable with routine monitoring; recorded on the register; no further treatment required.
Medium	5 to 12	Treat to reduce so far as reasonably practicable; the responsible manager approves before the system proceeds.
High	15 to 25	Treat before deployment or continued use; the AI Governance Committee approves and explicitly accepts any residual risk.

8.3	Implement and verify risk treatment; treat new risks; revalidate ineffective treatments; retain results.	Step 7

FORM

AI System Information Sheet (System Card)

Associated procedure: QP-12 | [Company Name]

QF-12-01

Rev [Revision]
Issue [Date]

The concise information sheet provided to users of an AI system, giving its purpose, use, limitations and oversight. Provided under control A.8.2.

1 SYSTEM

SYSTEM / VERSION
[System]

PURPOSE AND INTENDED USE
[Detail]

HOW THE OUTPUT IS TREATED
[Detail]

2 USE AND OVERSIGHT

KNOWN LIMITATIONS
[Detail]

HUMAN-OVERSIGHT RULE
[Detail]

REPORT A CONCERN
[Detail]

VERSION / LAST REVIEWED
[Detail]

APPROVAL

PREPARED BY	REVIEWED BY	APPROVED BY
ISO Consultant Panel Signature: _____ Date: [Date]	[Name] / [Designation Here] Signature: _____ Date: [Date]	[Name] / [Designation Here] Signature: _____ Date: [Date]

FORM

AI Risk Assessment Register

Associated procedure: QP-04 | [Company Name]

QF-04-02

Rev [Revision]
Issue [Date]

Records the risks identified for an AI system, their consequence, likelihood, score, band and priority. Completed using WI-04-01 and the criteria in QF-04-01.

ID	System	Risk (event and cause)	Cons.	Like.	Score	Band

APPROVAL

PREPARED BY	COMPLETED BY	APPROVED BY
ISO Consultant Panel Signature: _____ Date: [Date]	[Name] / [Designation Here] Signature: _____ Date: [Date]	[Name] / [Designation Here] Signature: _____ Date: [Date]

FORM

AI Risk Assessment Register

Associated procedure: QP-04 | [Company Name]

QF-04-02

Rev [Revision]
Issue [Date]

Records the risks identified for an AI system, their consequence, likelihood, score, band and priority. Completed using WI-04-01 and the criteria in QF-04-01.

ID	System	Risk (event and cause)	Cons.	Like.	Score	Band
R1	Triage AI	Abnormal image not flagged (false negative)	5	2	10	Medium
R2	Triage AI	Unflagged images de-prioritised (over-reliance)	5	3	15	High
R3	Triage AI	Unequal performance across patient subgroups	4	3	12	Medium
R4	Sepsis model	Alert fatigue leads to ignored true alerts	4	3	12	Medium
R5	Chatbot	Emergency symptoms not escalated to urgent care	5	2	10	Medium
R6	All	Supplier model update changes behaviour silently	4	3	12	Medium

APPROVAL

PREPARED BY	COMPLETED BY	APPROVED BY
ISO Consultant Panel Signature: _____ Date: [Date]	[Name] / [Designation Here] Signature: _____ Date: [Date]	[Name] / [Designation Here] Signature: _____ Date: [Date]