AI Assurance Institute

PRODUCT BROCHURE

EN 18286

Quality Management System Solution

EN 18286
Quality Management System Solution

A protective operating system for high-risk AI — from organisational establishment through system realisation, lifecycle control, post-market monitoring and continual improvement.

Health	Safety	Fundamental Rights	Regulatory Readiness

Aligned to EN 18286 (Quality management system for AI systems) under the EU AI Act framework, with integrated support for risk management and cybersecurity technical specifications.

Version 2026 ·Product overview for providers, deployers' partners, auditors and notified-body readiness

1. Why a dedicated AI quality system matters

High-risk AI systems must demonstrate a living quality management system — not a static binder of policies. EN 18286 specifies how providers establish, implement, maintain and continually improve that system so that health, safety and fundamental rights are protected throughout the AI system life cycle.

Providers face four structural challenges:

- Regulatory pressure — demonstrate conformity with applicable Union law and the EN 18286 technical specification at every life-cycle stage.
- Protection is the outcome — the QMS exists to reduce harm, not to perform paperwork theatre.
- People change; evidence must not — durable processes, clear roles and objective records keep the organisation compliant over years.
- Fragmented tools fail audits — scattered files and informal habits break under notified-body and authority scrutiny

Our response
An integrated EN 18286 operating model: one AI system register as the compliance spine; structured workflows for every major clause; pervasive controls for traceability, review, evidence, nonconformity and change; and tamper-evident evidence packages ready for inspection.

2. Solution overview

2.1 What the product is

The EN 18286 Quality Management System Solution from the AI Assurance Institute is a collaborative, role-based platform that turns the standard's requirements into day-to-day controlled work. Organisations define scope, assign accountability, plan quality objectives, realise and gate AI systems, govern data, manage suppliers and change, monitor post-market performance, and drive continual improvement — with written evidence retained for the periods required by law.

2.2 Design principles

- Clause-faithful structure — screens and records follow EN 18286 clause order and granularity (including sub-points a–f and numbered factors where the standard requires them).
- Single system of record per concern — lifecycle gates, product content, risk, data, monitoring and support each have a clear home, linked by shared AI system identity.
- AI system spine — every controlled artefact carries AI system identity, reference, version and intended purpose for end-to-end traceability.
- Continuous QMS processes — traceability, review and approval, evidence generation, nonconformity/CAPA and change management run on every controlled record, not only at annual review.
- Inspection-ready evidence — structured fields, gate snapshots, cryptographic integrity options, consolidated exports and long-term retention archives.
- Switchable AI types and quality objectives — control packs and stage plans adapt to the selected AI type and in-scope quality objectives (Clause 6.2).

2.3 Capability breadth at a glance

Capability area	Product depth (illustrative)
Context & scope (Clause 4)	AI system register; regulatory obligation matrix; scope and classification; compliance strategy; documented information control with mandatory records matrix
Leadership (Clause 5)	Quality policy; roles, responsibilities and authorities; RACI across life-cycle processes; top-management review and sign-off workflows
Planning (Clause 6)	QMS-level risk actions; quality objectives catalogue; plans for achievement (what, measures, who) at functions, processes and each life-cycle stage
Support (Clause 7)	Resources; competence and training linked to AI systems; awareness; internal and external communication including authority requests
System realisation (Clause 8)	Life-cycle stage model (ISO/IEC 5338-aligned); process model 8.1.1–8.1.4; risk management system; design & development; V&V; data management; identification; continuous learning; retirement; technical documentation & IFU
Operation & control (Clause 9)	Deployment and operational control; supply chain; change management (including substantial modification and pre-determined changes); post-market monitoring; serious incidents; nonconformity and CAPA
Performance & improvement (Clause 10)	Internal audit; management review inputs; effectiveness of quality objectives; continual improvement loops from monitoring and CAPA
Essentials & related standards	Integrated risk management and cybersecurity frameworks; human oversight; transparency/logging design; accuracy and robustness evidence paths

3. Fulfilment of the EN 18286 technical specification

The tables below summarise how the solution implements the standard's structure. Depth is delivered through structured tab workflows with clause-aligned prompts, mandatory sub-fields, ownership, versioning and evidence binding — not free-text-only documents.

3.1 Clauses 4–7 — Establish the QMS

Clause	Focus	How the solution fulfils the technical specification
4.1–4.3	Context, requirements, scope	Register of in-scope AI systems; determination of applicable regulatory requirements; boundaries and intended purpose captured per system
4.4	Compliance strategy & essentials	Strategy records; essentials coverage for risk, data, technical documentation, record-keeping, transparency, human oversight, accuracy/robustness/cybersecurity
4.5	Documented information	Mandatory records matrix; version control; controlled changes; retention and archive of signed records
5.1–5.3	Leadership & roles	Policy and management review; role matrices; decision authority; outsourced role controls with provider accountability retained
6.1	QMS risk actions	Planning for risks to the functioning of the QMS, distinct from AI system operational risk management
6.2	Quality objectives	Verifiable objectives consistent with quality policy; stage-level plans (what will be done, measures, responsible roles) per AI system and life-cycle stage
7.1–7.4	Support	Resource planning; competence assessments and training evidence; awareness of policy and QMS contribution; communication procedures including competent-authority requests

3.2 Clause 8 — AI system realisation

Clause 8 is the operational heart of EN 18286. The solution separates stage control (determining and gating the life cycle) from product content (design, V&V, data, documentation) while keeping both linked to the same AI system.

Clause	Focus	How the solution fulfils the technical specification
8.1	Life-cycle stages & processes	Visible ISO/IEC 5338 stage model (inception through retirement, including continuous validation); full capture of 8.1.1–8.1.4 (stages; processes a–f; establishment factors 1–10; documented information and effectiveness); stage gates with immutable snapshots
8.2	Risk management system	Dedicated RMS aligned to the risk management technical specification: context, hazards, treatment, residual risk, verification and post-market risk loops
8.3	Design & development	Intended purpose; requirements quality criteria; specifications; design reviews; design controls with structured mandatory fields
8.4	Verification & validation	V&V plans with acceptance criteria; examination and test procedures; model documentation; readiness gates before deployment
8.5	Data management	Design-time and live data governance: acquisition through retention; lineage; quality metrics; drift signals feeding change and CAPA
8.6–8.8	Retirement, ID, continuous learning	Controlled retirement and data disposition; system identification and versioning; continuous learning within pre-determined boundaries
8.9	Technical documentation & IFU	Annex IV-style technical documentation structure; instructions for use; amendment control linked to change and nonconformity

3.3 Clauses 9–10 — Operate, monitor, improve

Clause	Focus	How the solution fulfils the technical specification
9.1	Deployment & operation	Deployment plans; version management; operational procedures; support to deployers; logging and oversight interfaces
9.2	Supply chain	Supplier and component accountability; contractual and due-diligence checklists for third-party AI elements
9.3	Change management	Full change lifecycle; substantial modification handling; pre-determined change configurations; risk re-evaluation and documentation updates
9.4–9.5	Post-market & incidents	Post-market monitoring plans and records; serious incident workflows with notification timelines; feedback into design and risk
9.6 / 10	NC, CAPA & improvement	Nonconformity and corrective action; internal audit programmes; management review with closed-loop quality objective actuals; continual improvement

4. AI system life cycle — made visible

The solution implements a stage model consistent with ISO/IEC 5338 (AI system life cycle processes) and EN 18286 Clause 8.1. Stages are visible as a controlled progression with entry/exit evidence — not an informal checklist.

4.1 Stage model

- **Inception** - business need, intended purpose, misuse, stakeholder consultation
- **Design and development** - requirements, architecture, data engineering, model build
- **Verification and validation** - test against specifications and intended purpose

- **Deployment (transition)** - release readiness, identification, documentation currency
- **Operation and monitoring** - performance, drift, support interfaces
- **Continuous validation** - post-deployment testing and continuous learning control
- **Re-evaluate / maintenance** - material change, focused re-V&V, re-baseline
- **Retirement** - decommission, data disposition, record retention close-out

4.2 Process model (8.1.1–8.1.4)

For each AI system, providers record how stages were determined; how processes cover design control, development/QA, data management, examination/test/validation (with frequency), post-market monitoring and support; how establishment criteria and factors 1–10 are addressed; and how documented information and effectiveness monitoring are maintained — with corrective action when intended results are not achieved.

4.3 Quality objectives at every stage (6.2)

When planning how to achieve quality objectives, the provider determines what will be done (including process quality criteria), measures to implement the standard's requirements, and who is responsible — for each AI system and each life-cycle stage. The solution captures that plan and aligns control objectives to the selected AI type and objectives catalogue.

5. Cross-cutting product strengths

5.1 Five pervasive processes

EN 18286 expects certain processes to run continuously across the QMS. The platform embeds them on controlled records:

- **Traceability -** every artefact linked to AI system identity and source context

- **Review and approval** - role-based workflows including top-management sign-off where required
- **Evidence generation and record-keeping** - packages, matrices and retention schedules
- **Nonconformity and CAPA** - rapid capture with linkage to incidents and changes
- **Change management** - pre-filled change requests from the source of truth

5.2 Evidence integrity and retention

- Gate and programme snapshots for immutable stage completion evidence
- Optional cryptographic (Merkle) signing and verification of critical records
- Evidence packages (structured export) for risk, cyber, product realisation and operation
- Consolidated conformity export for multi-framework demonstration packages
- Long-term retention with archive second-copy options aligned to record-keeping obligations

5.3 Portfolio and programme scale

- Multi-project / multi-system portfolio with consistent process templates
- One-action suite establishment to instantiate the full QMS workflow set per AI system
- Dashboards for clause readiness, control effectiveness and management review inputs
- Configurable gate enforcement for high-risk systems (evidence completeness before advance)

6. QMS essentials and related technical specifications

EN 18286 requires the QMS to address the essentials for high-risk AI. The solution treats these as first-class operating capabilities:

Capability area	Product depth (illustrative)
Risk management	Full risk management system lifecycle: classification, analysis, treatment, residual risk acceptance, verification and post-market risk feedback
Data and data governance	Structured data management procedures plus live lineage, quality metrics and drift-driven governance actions
Technical documentation	Annex IV-aligned documentation structure, instructions for use, and controlled amendments
Record-keeping	Mandatory records catalogue, signing, retention end dates and archive controls
Transparency	Logging design readiness and transparency measures integrated with operational control
Human oversight	Oversight measures, effectiveness evidence and operational queues for human intervention
Accuracy, robustness, cybersecurity	V&V and design criteria; cybersecurity framework assessments linked to residual risk

Standards family
EN 18286 sits at the centre of the AI Act harmonised quality system. The product integrates risk management and cybersecurity technical specifications as structured frameworks — complementary to, not substitutes for, the QMS — so providers can demonstrate coherent selection of technical specifications under their compliance strategy.

7. Who the solution is for

- AI system providers placing high-risk AI on the Union market or putting it into service
- Quality, compliance and legal teams building Annex ZA-ready evidence programmes
- Risk, security and data governance functions requiring shared systems of record
- Engineering and product teams needing controlled design, V&V and release gates
- Internal auditors and external assessors seeking navigable, clause-referenced evidence
- Top management requiring portfolio visibility of QMS effectiveness and residual risk

8. Outcomes you can demonstrate

Completeness - structured coverage of EN 18286 Clauses 4–10 at the granularity the standard specifies.
Traceability - AI system identity carried through design, risk, data, operation and post-market records.
Control - stage gates, change control and high-risk enforcement that block progress without required evidence.
Accountability - roles and authorities assigned, including life-cycle consulted/informed roles and top-management duties.
Durability - retention, archive and closed-loop improvement so the QMS survives staff turnover and product evolution.
Inspectability - clause-referenced exports and integrity verification suitable for competent authorities and notified bodies.

9. Next steps

Organisations typically begin with scope and AI system registration, establish leadership and planning records, then stand up the full realisation and monitoring suite for each high-risk system. The solution is designed so that process structure exists before operational work begins - matching the EN 18286 expectation that the QMS is established and maintained, not improvised per release.

Protective quality, not ceremonial compliance

When implemented with organisational discipline, the EN 18286 Quality Management System Solution from the AI Assurance Institute provides a durable control environment for high-risk AI: clearer ownership, tighter life-cycle gates, stronger evidence, and a continuous line of sight from quality policy to post-market performance — in service of health, safety and fundamental rights.

Contact Us

Email: info@aiassurance.institute

Website: www.aiassurance.institute