

From an AI inventory to everyday governance.

Follow the work from registering a system to documenting safeguards, approving a version and keeping its record current.



- Purpose and ownership
- Safeguards and evidence
- Decisions and follow-up

For compliance teams and system owners

English customer edition | 29 September 2026

Product capabilities described from the reviewed edition. Availability is agreed during onboarding.

Find your starting point

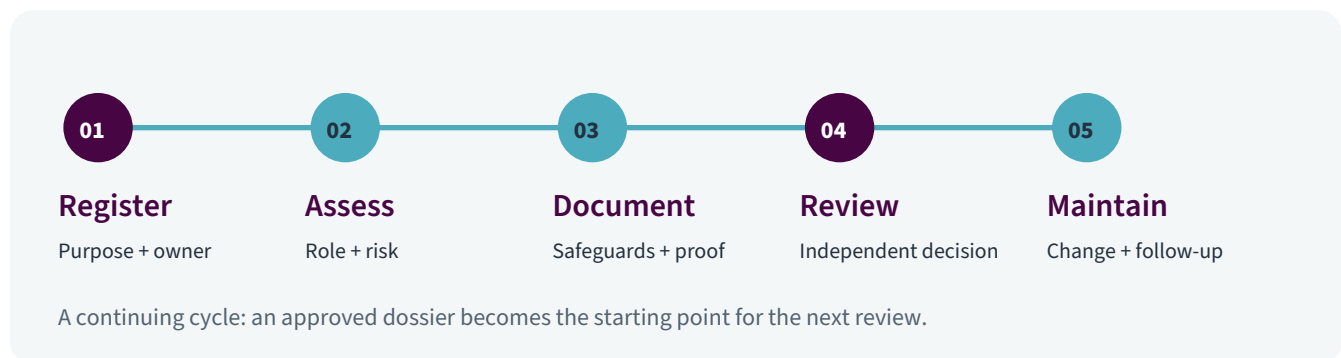
This guide is part of the English AICMS customer bundle. The introduction explains the value; the feature guide follows the work; the controls reference and responsibility map provide the detail.

01 / One system, one connected working record	3
02 / Build an AI register that people can use	4
03 / Work through classification with reasons	5
04 / Make responsibilities and handovers explicit	6
05 / Connect each risk to the people and safeguards involved	7
06 / Assess fundamental rights and preserve the assessment history	8
07 / Document data governance at a useful level of detail	9
08 / Put human oversight and competence into the record	10
09 / Record performance, resilience and transparency measures	11
10 / Build technical documentation and connect quality management	12
11 / Track conformity, standards and certificate decisions	13
12 / Document general-purpose AI within the system dossier	14
13 / Control changes and make review meaningful	15
14 / Follow events after the dossier is approved	16
15 / See where attention is needed	17
16 / Share the dossier and navigate the legal context	18
17 / Keep access, evidence and retention under control	19

01 / One system, one connected working record

AICMS is the AI Compliance Management System within Coach2Lead. It helps a team identify an AI system, assess its context, document safeguards, assemble evidence, review the dossier and maintain its history.

The **AI system** is the registered subject. A **version** is a particular edition of its dossier. A **draft** is work in progress. **Published** means internally approved in Coach2Lead; it is not a regulatory authorisation or the market release of the AI itself.



How to read this guide

Each chapter describes a customer task, the available product support and its practical boundary. The Controls Reference explains individual checks. The Responsibility Map explains the legal context, exceptions and continuing duties.

There are three different forms of support:

- **Controls:** checks that prevent a specified save, submission or workflow action.
- **Guidance:** questions, contextual explanations, prompts and links that help a person assess the case.
- **Records:** structured information and evidence that preserve what the organisation says it has done.

A record can be valuable without automatically enforcing the underlying obligation. A check can confirm that a rationale is present without judging whether that rationale is legally sound.

Edition: reviewed implementation, 29 September 2026. These guides do not attest deployment to a particular customer environment. Confirm rollout, enabled features, permissions and scheduled services during onboarding. The legal baseline is Regulation (EU) 2024/1689 as amended through Regulation (EU) 2026/1744; official sources and current-date qualifications appear in the Responsibility Map.

02 / Build an AI register that people can use

Bring the portfolio into view

Register an AI system with its purpose, context, ownership and first draft dossier. The list supports text search and filters across classification, lifecycle, responsible people and roles, deployment environment, market status, review status and other recorded characteristics.

More detailed filters help locate systems with particular oversight, privacy, certificate, registration, GPAL, product-safety, Annex III, documentation or monitoring facts. Export the filtered register to an Excel file for a meeting or working review.

Keep versions together

The system page groups published, draft/in-review and archived versions. Open a version, inspect its history, compare editions or subscribe to updates. The history of a system stays attached to the same registered subject as the dossier develops.

Your team supplies	AICMS provides
A genuine inventory of systems in use or under consideration	A searchable, filterable register and version lineage
Business purpose, responsible people and supplier information	Structured records and links to existing Coach2Lead people
Consistent reference categories	Company configuration lists and controlled reuse of reference data

Configuration that fits the organisation

Settings include classifications, lifecycle stages, roles, document and attachment types, Annex I legislation, Annex III areas, mitigation categories, affected groups, retention periods, competent authorities and notified bodies. Authorised users can import configuration from another company context they are entitled to access, adding, updating or archiving reference items.

Boundary: this is a register maintained by people. It does not automatically discover shadow AI or import arbitrary AI-system spreadsheets. Custom labels do not automatically gain the legal meaning of the built-in statutory categories.

03 / Work through classification with reasons

The classification wizard follows a sequence: prohibited practices, high-risk routes, transparency questions and a final review. It records the answers and assessment rationale against the version.

Specific branches, not one risk question

- **Prohibited practices:** record the relevant category and consider the displayed exceptions or qualifications. A positive prohibited finding stops ordinary wizard progression and can be recorded as a prohibited classification.
- **Product route:** capture the Annex I connection and product/safety-component context.
- **Use-case route:** capture an Annex III area and relevant use case.
- **Profiling:** identify profiling of natural persons. If the system profiles people, the wizard does not allow the Article 6(3) exception.
- **Article 6(3) exception:** record the selected condition and a justification for treating an Annex III use as not high-risk.
- **Transparency:** consider relevant Article 50 characteristics alongside the risk classification.

Submission checks catch prohibited classifications, mismatches between a prohibited finding and the selected tier, and certain missing or inconsistent classification evidence.

Explain the decision to the next reviewer

The value is the recorded reasoning. A later reviewer can see which facts supported the classification and revisit them when purpose, users, data or functionality changes.

The wizard is an assessment aid. It relies on the facts supplied by the organisation and does not inspect the actual behaviour of an AI model.

Legal context: Articles 2, 3, 5 and 6; Annexes I and III. A valid Article 6(3) conclusion involves the significant-risk and decision-influence conditions as well as a listed task category. Specialist interpretation remains necessary. Product risk tiers are working categories, not a complete substitute for the Act's overlapping duties.

04 / Make responsibilities and handovers explicit

A single AI system may involve a provider, deployer, importer, distributor, authorised representative and product manufacturer. AICMS records responsible parties with their roles, people or organisations, contact information and relevant role-specific facts.

Capture the relationships behind the dossier

Record	What your team can document
Responsible party	Role, contact, linked person and organisation; deployer category where relevant
Authorised representative mandate	Representative, scope, dates, termination reasons and supporting evidence
Value-chain agreement	Counterparty, agreed scope, dates, expiry and evidence
Importer or distributor checks	Which check was performed, who it relates to, verification date and notes
Substantial modification	The change, role/classification implications, reassessment and handover information
Deployer duties	Measures for following instructions; active monitoring; suspension and its reason; data-protection impact assessment reference; deployer registration status. Oversight and logging arrangements have their own sections.

Distinguish your organisation from a supplier

Party attribution helps distinguish the company's own operator role from external organisations. This matters when the system applies role-dependent submission checks, including transparency checks. Different parts of the product do not yet apply that distinction identically; verify the responsibility map for your case.

Connect to Coach2Lead people

Where appropriate, responsible-party and oversight records link existing people. Application permissions remain separate: being named as a provider or oversight contact does not automatically grant permission to approve a dossier.

Boundary: verification boxes are recorded human attestations. AICMS does not inspect a supplier's business, execute contracts or transfer legal responsibility. Several missing-agreement and checklist checks are non-blocking advisories that the current editor does not display. Articles 16 and 22-26 provide the main legal context.

05 / Connect each risk to the people and safeguards involved

The risk register supports a detailed account of possible harm, rather than a single overall risk label.

Follow a risk through its treatment

1. Describe the risk, intended-use or misuse context, category, severity and likelihood.
2. Identify the people or groups who may be affected and the responsible owner.
3. Choose and explain the treatment: design measures, mitigation or another recorded approach.
4. Link safeguards, their owners, implementation status, target and completion dates, supporting evidence and the assessed risk remaining after mitigation.
5. Record that residual risk and the overall acceptance decision.
6. Plan the next review and retain the result of the previous one.

A risk can have several linked mitigations; affected groups can connect to relevant risks. The editor prevents empty linking records before the underlying risk or mitigation exists. Visible notices draw attention to societal risks and mitigations when vulnerable groups have been recorded.

More than severity multiplied by likelihood

The dossier also captures foreseeable misuse, the interaction between requirements, the competence expected of deployers, testing metrics and thresholds, and the context in which the system will be used. Checks examine specified missing treatment, residual-risk, mitigation and quality-management information before review.

Continue after approval

The dedicated **Record risk review** action can update the review schedule for a Published version, with a required outcome and a recorded event. Future-dated reviews and an invalid next-review sequence are refused.

Boundary: severity and likelihood are assessments supplied by people. AICMS does not calculate the real probability of harm or test whether a mitigation works. Its scoring and readiness indicators are internal decision aids. The legal purpose is the continuing risk-management process in Article 9.

06 / Assess fundamental rights and preserve the assessment history

A fundamental rights impact assessment, or **FRIA**, examines how a particular deployment may affect people. It is not required for every high-risk system or every deployer.

Decide whether an assessment is needed

AICMS indicates whether a FRIA is required from the recorded classification, deployer category and Annex III details. It distinguishes relevant public bodies, private providers of public services and the particular creditworthiness or insurance uses. Missing inputs can remain unresolved instead of being silently treated as an exemption.

The wizard shows the decision evidence and supports a reasoned override. An override is an accountable decision by the organisation, not a legal exemption granted by the software.

Build a separate, dated assessment

The record covers the processes using the AI, duration and frequency, affected people, particular harms, oversight, mitigation, relevant data-protection assessment material, the outcome and authority-notification details. Completed runs remain available as history; reassessment creates a new draft rather than overwriting the previous completed assessment.

Catch stale or unfinished work

Completion rechecks the underlying facts. It refuses a change to the facts used for the applicability decision, unresolved requiredness without an accepted rationale, missing required content or invalid notification information. Only one FRIA draft can be open for a version. Relevant changes can mark reassessment due in the dossier and attention views.

Authority notification is tracked through forward-only states, with a date and method required for completion. Dates more than one day beyond today's UTC date are refused; the one-day allowance accommodates time zones. Notification progress is updated while the parent dossier is still Draft. Completing the assessment can leave notification pending, but the relevant submission check then prevents the dossier entering review.

Boundary: AICMS records the assessment and external notification; it does not send the authority notification. FRIA can complement an existing data protection impact assessment but does not replace it. Articles 26(9) and 27 explain that relationship and the applicable scope.

07 / Document data governance at a useful level of detail

The data-governance wizard organises sources, provenance, quality, bias and privacy information. It gives specialists a structured place to explain the work performed on training, validation and test data.

Subject	Detail the team can retain
Origin and purpose	Source, collection purpose, provenance and relevant privacy or consent context
Preparation	Annotation, labelling, cleaning, updates, enrichment and other processing
Suitability	Representativeness, completeness, availability, assumptions, gaps and the intended population or context
Bias and fairness	Examination performed, potential impacts, preventive or corrective measures and evidence
Traceability	Dataset descriptions, lineage or external references and supporting documents
Special-category data	Necessity and safeguards for a particular bias-detection or correction use

Conditional questions help avoid empty assurances

High-risk submission checks examine specific recorded data-governance content. Separate special-category-data fields record necessity, pseudonymisation, security measures, non-transfer, deletion and processing records. These assertions give a reviewer specific matters to challenge; their completeness is not enforced by a dedicated Article 4a submission gate in this edition.

The distinction between trained models and systems using testing data is relevant to the scope of the data requirements. The detailed Controls Reference records the conditions used by the current checks.

Keep the evidence behind the description

Attach or reference the team's actual assessments, dataset descriptions and supporting material. A concise narrative can then point to the evidence rather than attempting to reproduce it all in a text field.

Boundary: AICMS does not scan, cleanse or test a dataset, establish a lawful basis for processing, or independently verify fairness. The amended Article 4a exception is conditional permission, not blanket authorisation to use sensitive data. Articles 4a and 10 are the main legal anchors.

08 / Put human oversight and competence into the record

The oversight wizard asks how people will understand, question and intervene in the AI's operation. It distinguishes the measures provided by the supplier from those implemented by the deployer.

Describe how oversight actually works

- Who has the competence, authority and support to oversee the system?
- How will they understand its capabilities and limitations?
- How will they recognise anomalies and avoid over-reliance on its output?
- What enables them to interpret, disregard, override or reverse a result?
- How can they interrupt operation safely, and where does an issue escalate?
- Where applicable, how is the required separate verification by two people arranged?

The dossier records oversight type, responsible people and roles, procedures, explanation tools and evidence. Relevant submission checks examine missing oversight information; they do not operate the mechanism themselves.

Keep training evidence close to the responsibility

AI-literacy records capture training type, date, provider, personnel scope, competency result and supporting evidence. Records can reference Coach2Lead training certificates. This connects the compliance dossier to existing training information.

Certificate selection and expiry checks help avoid some obvious mismatches. Personnel scope in an AI-literacy record is free text, so a selected certificate is not proof that everyone named has received the training.

Boundary: AICMS does not install a stop button in the AI or guarantee a person's competence. The independent dossier-review rule is separate from Article 14(5)'s two-person verification of certain biometric identification results. Article 4 concerns measures supporting AI literacy; Articles 14 and 26 concern oversight and its operation.

09 / Record performance, resilience and transparency measures

Make technical claims inspectable

Accuracy records can describe the target, metric, measurement method and relevant evidence. Robustness and cybersecurity sections cover limitations, redundancy, feedback loops, continuous learning and protection against issues such as data poisoning, adversarial inputs and model vulnerabilities.

These fields allow a technical specialist to explain what was tested, how it was tested and what the findings mean for the intended use. Safeguards can be connected to controls already recorded against organisational standards in Coach2Lead.

Distinguish the transparency duties

The record separates direct interaction with people, synthetic-content marking, emotion recognition or biometric categorisation, deepfakes and public-interest text. It captures methods, disclosure statements, exemptions or justifications, timing and accessibility.

The same AI system may have high-risk requirements and transparency duties. AICMS does not treat Article 50 as relevant only to a lower product risk tier. Some checks use the organisation's recorded provider or deployer role to decide whether an omission blocks submission or produces an advisory.

Explain a decision to an affected person

The dossier records a reference to the explanation mechanism and the team's reasoned assessment of when it applies. It does not provide a dedicated explanation-request or response-management workflow.

Boundary: the product does not execute accuracy benchmarks, secure the AI model, watermark generated content or send disclosures to people. It does not automatically generate an Article 86 explanation. Those are technical and organisational measures to implement in the real service. Articles 13-15, 26, 50 and 86 provide the context.

10 / Build technical documentation and connect quality management

Technical documentation should tell a reviewer what the system is, how it was developed, what its limitations are and how its risks are controlled. AICMS offers typed document records, structured descriptions and evidence attachments for that purpose.

Annex IV detail the dossier can organise

- Purpose, provider, system version and relationship to earlier versions.
- Software and firmware, hardware, interfaces, deployment form and instructions for use.
- Architecture, algorithms, design choices, assumptions and development methods.
- Training and operational computing resources, data requirements and third-party components.
- Human oversight, predetermined changes and cybersecurity measures.
- Validation procedures, performance metrics, test records and responsible sign-off references.
- Risks, lifecycle changes, standards, declaration evidence and post-market monitoring.

Show how quality management supports the system

The quality management system (QMS) wizard connects the quality-management reference, required elements, procedures, technical documents and logging arrangements. Individual elements can have their own status and documentation. This lets the team point to an existing organisational process where appropriate.

Instructions-for-use records address provider and representative identity, understandable and accessible format, accuracy and harm information, performance for affected groups, input requirements, oversight, expected lifetime and maintenance. They also describe how deployers collect, store and interpret logs.

Logging arrangements can specify event types, coverage of risk situations and monitoring, retention and access, and requirements for biometric use. These describe the external logging arrangements; AICMS does not collect those operational logs.

The generated Annex IV preparation file combines recorded content and evidence references and identifies specified missing information. It is a structured JSON attachment created from a Draft. The readable dossier uses the separate Print / Save as PDF route.

Boundary: having a QMS entry does not establish that the organisation operates an adequate QMS. Attached test reports remain the organisation's evidence. AICMS does not operate Article 12 AI event logging; it records logging arrangements and references. Articles 11, 12, 17-19 and Annex IV provide the legal context.

11 / Track conformity, standards and certificate decisions

The conformity wizard makes the selected assessment route explicit. It supports records for internal control, notified-body involvement and the relevant sectoral route, with assessment evidence, declaration elements and CE-marking information.

Retain the decision and its supporting material

Record	Customer use
Conformity route and assessment	Explain the route selected and retain assessment evidence
EU declaration elements	Record the system, issuer, applicable material and supporting declaration information
Harmonised standards	List references and evidence; connect relevant measures to available norm controls
Certificate	Record body, number, scope, issue/expiry, status, supplements and evidence
Certificate lifecycle and appeal	Retain status changes and appeal date/outcome against the relevant decision
Emergency authorisation	Record the basis, request, decision, dates, conditions and subsequent actions

Internal-control records separate QMS verification, technical-documentation examination and compliance verification, with assessor, date and evidence. External assessment records retain the auditor, date, outcome, findings, assessment stage, report and recorded consent to subcontracting.

Guard against some inconsistent records

Save-time logic includes certificate validity limits and supplement-cycle checks. Certificate changes generate lifecycle events. The appeal interface is available for specified adverse decisions. Scheduled routines can flag expiry and specified missing confirmations following a notified body's loss of capability.

Emergency-authorisation records can retain whether conformity work was completed, use stopped or results discarded after a refusal. Their presence does not authorise the deployment; some related checks remain non-blocking backend advisories.

Boundary: AICMS does not perform a conformity assessment, issue a notified-body certificate, sign an EU declaration, apply a CE mark, lodge an appeal or obtain emergency authorisation. A declared standard is not proof of conformity. Articles 36, 40-49 and Annexes V-VII are the relevant legal framework.

12 / Document general-purpose AI within the system dossier

General-purpose AI, or **GPAI**, needs more than a checkbox saying that a system uses an external model. AICMS provides detailed model-related documentation within an AI system's dossier. In the reviewed interface, the GPAI wizard is available for dossiers classified High Risk or Prohibited; it is not exposed in Minimal Risk or Limited Risk dossiers. Model information belongs to that system version, rather than a separate model register.

Model documentation and downstream information

Record model identity and version, tasks, acceptable-use policy, release and distribution, architecture, parameter count, input/output modalities, licence and integration information. Retain the copyright policy, rights-reservation statement and public training-content summary where relevant.

Training and evaluation descriptions include provenance, curation, design choices, computing resources, training duration, energy estimates and evidence. Separate downstream information helps explain what a system provider receives from the model provider.

Systemic-risk work and decisions

The wizard records capability and compute information, Commission designation, notification, rebuttal and reassessment. It offers a compute-threshold suggestion and visible open-source/systemic-risk guidance.

Separate entries can record systemic-risk assessments, their mitigations and serious incidents. The model document also retains the adversarial-testing description, date, results and evidence, together with reporting dates, cybersecurity measures, representative details and the stated basis for compliance.

A role distinction that must remain visible

Using another company's model does not automatically make your organisation a GPAI model provider. In the reviewed edition, the legal applicability map recognises that distinction, while some submission checks still ask for provider documentation based on recorded GPAI use. Review those requests with the implementation team rather than treating them as a conclusive statement of your legal duties.

Boundary: AICMS records evaluations and model evidence; it does not perform model evaluation, red teaming or AI Office notification. Open-source conditions and systemic-risk classification need professional review. Articles 51-56 and Annexes XI-XIII are the principal legal anchors.

13 / Control changes and make review meaningful

Create a Draft from an existing version and choose a major, minor or patch increment. The version service copies the dossier and linked records, preserving a relationship with the source edition. Only one open Draft or InReview version is allowed for a system.

Work without losing the review boundary

The editor supports saving, discarding and periodic autosave when it is safe to do so. Collection dialogs and wizards pause autosave. Another editor's active lock makes the version read-only. The server also checks ordinary editing and relationship rules.

Check Readiness groups submission findings by dossier section and offers links back to the affected fields. Changing information can mark the displayed readiness result stale. The separate completeness percentage counts tracked filled fields; it is not an AI Act compliance percentage.

In the current editor, yellow findings can still block submission. The separate non-blocking advisory collection is calculated by the server but is not displayed there. Colour is not a reliable guide to whether a finding is optional.

Review with an independent person

The queue shows candidates with change context, classification changes and assessment-completion information. Compare two versions of the same system, including additions, removals, modifications and certain formatting-only changes.

Approval and rejection require a comment and an eligible reviewer. The draft creator and current submitter cannot perform either decision. Approval publishes the dossier internally and archives the previous published version; rejection returns it to Draft.

Version History shows named actions with the actor, date, time and recorded message. Guided-assessment completions and reruns are recorded events, helping reviewers reconstruct the dossier's progress.

Boundary: full submission checks run when entering review. Approval rechecks the Article 5 prohibition/classification pair, not the entire validator. Normal non-Draft content is frozen, with narrow post-publication actions described next. Version history is not a tamper-proof or guaranteed-retention archive.

14 / Follow events after the dossier is approved

Describe the monitoring plan and retain findings

Monitoring records capture what is observed, who owns it, review frequency, evidence location, thresholds, data collection and analysis, findings and corrective action. These records sit alongside the organisation's actual monitoring tools and procedures.

Manage the incident record

Record an incident, awareness date, severity, impact, actions taken, reporting deadline and authority-report date. The cross-system incident list supports date, severity and deadline filters and links back to the dossier.

The current calculator uses recorded severity to choose a 2-, 10- or 15-calendar-day default window. An authorised override stays within that default; the dialog requires a reason. The detailed reference explains the server boundary. The legal category and need for immediate reporting must be assessed separately; a countdown is never permission to wait.

Three narrow additions to a Published version

The **Add post-market record** action can append a corrective action, authority notification or authority request. These additions are immediately frozen. The current dialog does not create new serious incidents or monitoring activities and does not expose every field available in a Draft.

The separate **Record risk review** action records an outcome and updates the review schedule. Richer revisions, further evidence uploads and other changes use a new Draft.

Record cooperation with authorities

Capture the authority, request or notification, dates, response, outcome and supporting records. Where a response deadline has been recorded, attention views and scheduled routines can help track it.

Boundary: AICMS does not monitor the running model or submit an external report, response or notification. The organisation must operate the incident process and meet the applicable legal timing. Articles 20, 21, 26, 72 and 73 are the principal anchors.

15 / See where attention is needed

The Overview dashboard shows the registered portfolio and recently updated AI systems. The Compliance dashboard focuses on Published versions, with Pending Review covering InReview records. Retention attention can also include Archived versions whose retention period is still running.

Follow a signal to the underlying record

Views include risk distribution and severity, incident trends, conformity information, certificate status, documentation, data governance, prohibited-practice assessment, oversight, accuracy, monitoring and lifecycle. Chart drill-downs open a filtered list or the relevant dossier.

Attention items can identify expiring certificates, risks without recorded mitigation, incomplete declaration elements, stale monitoring, overdue unreported incidents, missing or overdue risk reviews, prohibited systems still recorded as in service, retention dates, authority-response deadlines and FRIA reassessment.

Subscribe to useful follow-up

Use the bell on the system page to subscribe to that AI system's updates. Lifecycle actions and scheduled routines create follow-up notifications for eligible recipients. The scheduled services include certificate expiry, changed-version subscriptions, incident-reporting deadlines, risk review, retention, authority responses, monitoring and specified Article 36/52 deadlines.

Recipients depend on linked people, subscriptions and active accounts. Jobs and mail infrastructure must be running. Their existence in the product is not evidence that a particular reminder was received.

Boundary: these are indicators of recorded information. A document count does not assess its quality; an oversight selection does not prove effective oversight; a completed monitoring field does not prove continuous monitoring. There is no single dashboard percentage that establishes legal compliance.

16 / Share the dossier and navigate the legal context

Use the output that fits the conversation

Output	Purpose and scope
Registry Excel file	Share the filtered system list for portfolio work.
Print / Save as PDF	Produce a readable dossier for a version, including status, dates, data tables, evidence references and missing-data notes. Uses browser printing.
Annex IV preparation file	Generate structured JSON from technical documentation and evidence references for an eligible Draft in the High Risk / Prohibited view. Generation saves a typed attachment.
Annex VIII preparation file	Prepare structured registration information from recorded roles and classification, including applicable public/restricted or national-route distinctions. Draft-only; the action appears when the recorded facts select an applicable package section.

Generated files can remain part of the evidence after a version is approved. A fresh structured package cannot be generated from a frozen version through the ordinary generation action.

The registration wizard records identity, contact, system, conformity and external-reference information. The prepared package does not submit that information to an authority. The AI Act's EU database is distinct from the medical-device EUDAMED database.

Explore the law alongside the portfolio

The EU AI Act Navigator offers searchable provisions, definitions, cross-references, topic/risk bands and application-phase information. Its system overlay associates accessible registered systems with supported provisions and links to dossier sections. It distinguishes missing, unassessed or restricted version information.

Boundary: a legal map is an aid to review, not an automatic legal opinion. One system can appear under several provisions, so counts overlap. The bundled corpus and mapping have a defined edition and supported scope. Neither a JSON file nor a printed dossier is an authority-approved form, signed declaration or certificate.

17 / Keep access, evidence and retention under control

Assign the right application permissions

AICMS separates viewing, creating, editing, submitting, approving and configuring. Company scoping and system/version access restrictions are applied at server boundaries. Related records such as people, risks, evidence and norms are checked for permitted ownership and linkage.

These are access controls in the reviewed implementation; this brochure is not a penetration-test report. Onboarding must establish appropriate users, responsibilities and deployment configuration.

Preserve useful evidence

Upload typed files while the version is Draft and link them to the relevant records. File names and open/download actions make the supporting material accessible to authorised reviewers. Attachments are evidence supplied by the organisation; their existence does not establish authenticity, currency or adequacy.

Treat retention as an operational commitment

The product records log-retention arrangements and can calculate documentation-retention dates from market-placement information. Scheduled reminders draw attention to upcoming or elapsed dates.

Individual non-Draft versions are protected from normal editing and individual deletion. However, an authorised whole-system deletion can remove its versions, including Published and Archived records. Retention dates do not prevent that operation.

**Establish retention, backup, access and deletion procedures outside the dossier workflow.
AICMS's controlled version history and reminders are not a guaranteed immutable legal archive.**

Evaluate with a real example

Use a representative system to check the complete journey: classification, applicable role, evidence, readiness, independent review, readable output and scheduled follow-up. The Controls Reference gives the detailed rules to inspect; the Responsibility Map keeps product behaviour separate from legal responsibility.