AIACTO · REGULATION (EU) 2024/1689

Annex IV Workbook

Build and manage the technical documentation for a high-risk AI system

48 operational control points, evidence examples and fillable fields to turn Annex IV into an assignable work plan.

48 controls	9 regulatory parts	Fillable PDF	Evidence register

Who is it for?

Providers of high-risk AI systems, compliance leads, and product, data, security and legal teams.

What you get

A ready-to-use matrix to qualify each requirement, appoint an owner, link existing evidence and prioritise gaps.

Important

This checklist helps prepare the technical file required by Article 11. It is not a substitute for an applicability assessment, the full documentation or legal advice.

Official source: Regulation (EU) 2024/1689 consolidated on 27 July 2026 — Article 11 and Annex IV

August 2026 edition

How to use this workbook

48 operational control points, evidence examples and fillable fields to turn Annex IV into an assignable work plan.

How to use this workbook

1. Identify the system and freeze the version being assessed.
2. Select a status and appoint an owner for every control.
3. Add a direct link to the evidence, not just a folder name.
4. Turn every gap into a dated action in the final plan.
5. Obtain technical, compliance and management sign-off.

Status scale

- ■ Compliant
- ■ In progress
- ■ Not started
- ■ Not applicable

Use “Not applicable” only with a documented and approved rationale.

Useful evidence is…

- □ named and directly accessible
- □ dated and versioned
- □ assigned to an owner
- □ linked to a requirement
- □ reviewed or signed where needed

Example of a properly managed control

2.d · Data provenance and quality	Status: In progress	Owner: Lead Data Engineer	Evidence: data_lineage_v1.2.pdf	Action: complete the bias analysis by 15 Oct

Important

This checklist helps prepare the technical file required by Article 11. It is not a substitute for an applicability assessment, the full documentation or legal advice.

System identity and scope

Complete this page before the assessment. Every link, test and decision in the workbook must relate to the same system version.

System trade name	Internal identifier	Assessed version	Reference date
Provider / accountable entity	Business owner	Technical owner	Compliance owner
Intended purpose	Target users / deployers	Affected persons or groups	Countries of availability
High-risk classification and basis	Third-party components / models	Environments in scope	Main evidence repository

Scope decision to document

Why does this system fall (or not fall) within the obligations for high-risk AI systems? Reference the Article 6 / Annex I or III assessment.

Scope exclusions, assumptions and reservations

Record any environment, function, version, data or use intentionally excluded, together with the rationale and the person who approved the decision.

Readiness dashboard

Record the prevailing status of each part after review. The objective is not to show nine green lights too early, but to make every gap visible, owned and dated.

Part	Owner	Compliant	In progress	To do	N/A	Next review
1. General description of the AI system 8 controls		☐	☐	☐	☐	
2. System elements and development process 8 controls		☐	☐	☐	☐	
3. Monitoring, functioning and control 6 controls		☐	☐	☐	☐	
4. Appropriateness of performance metrics 3 controls		☐	☐	☐	☐	
5. Risk management system — Article 9 6 controls		☐	☐	☐	☐	
6. Changes throughout the lifecycle 4 controls		☐	☐	☐	☐	
7. Harmonised standards and technical solutions 4 controls		☐	☐	☐	☐	
8. EU declaration of conformity 4 controls		☐	☐	☐	☐	
9. Post-market monitoring — Article 72 5 controls		☐	☐	☐	☐	

Use “Not applicable” only with a documented and approved rationale.

1 General description of the AI system

Identify the system, its intended purpose, version, interfaces and forms of supply without ambiguity.

1 / 2

Ref.	Requirement / self-assessment question	Expected evidence and examples	Tracking
1.a	Are the intended purpose, provider and version defined, including the relationship with previous versions?	**Evidence:** System identity sheet; intended-purpose statement; version and change matrix. **Watch out:** Avoid an overly broad purpose: specify decisions, context, users and affected persons.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
1.b	Are interactions with external hardware, software and other AI systems mapped?	**Evidence:** Context diagram; inventory of APIs, sensors, databases, third-party models and dependencies.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
1.c	Are relevant software or firmware versions and update requirements recorded?	**Evidence:** SBOM; version manifests; update policy; compatibility matrix.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
1.d	Are all forms in which the system is placed on the market or put into service described?	**Evidence:** Distribution catalogue: SaaS, API, download, embedded component, package or appliance.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date

1 General description of the AI system

Identify the system, its intended purpose, version, interfaces and forms of supply without ambiguity.

2 / 2

Ref.	Requirement / self-assessment question	Expected evidence and examples	Tracking
1.e	Is the intended execution hardware and its minimum constraints documented?	**Evidence:** CPU/GPU/memory specifications; reference configuration; minimum and maximum capacity.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
1.f	For a product component, are external features, markings and internal layout illustrated?	**Evidence:** Annotated photographs or diagrams; integration plan; location of markings. **Watch out:** Explicitly justify non-applicability for a software-only system.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
1.g	Is the deployer interface described in the actual released version?	**Evidence:** Dated screenshots; key journeys; roles and permissions; warning and error messages.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
1.h	Are the instructions for deployers complete and consistent with the intended purpose?	**Evidence:** Article 13 instructions; prerequisites; limitations; expected oversight; maintenance and support.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date

2 System elements and development process

Show how the system was designed, built, trained, validated and secured, including third-party components.

1 / 2

Ref.	Requirement / self-assessment question	Expected evidence and examples	Tracking
2.a	Are development methods and steps, including the use of pre-trained systems or third-party tools, traceable?	**Evidence:** Development lifecycle; make-or-buy decisions; model cards; contracts and versions for third-party components.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
2.b	Are the general logic, algorithms, design choices, assumptions, target populations and trade-offs justified?	**Evidence:** Design specification; decision records; optimisation objectives; key parameters; trade-off analysis. **Watch out:** Document why choices were made, not only what they are.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
2.c	Does the architecture explain component flows and the compute used to develop, train, test and validate?	**Evidence:** Logical and deployment diagrams; data flows; component inventory; compute logs.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
2.d	Are training, validation and test data covered by datasheets addressing provenance, selection, labelling and cleaning?	**Evidence:** Datasheets; provenance and licence register; cleaning scripts; labelling guide; quality controls. **Watch out:** Keep training, validation and test sets distinct and prevent data leakage.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date

2 System elements and development process

Show how the system was designed, built, trained, validated and secured, including third-party components.

2 / 2

Ref.	Requirement / self-assessment question	Expected evidence and examples	Tracking
2.e	Have human oversight needs and technical means for output interpretation been assessed?	**Evidence:** Human oversight assessment; human-decision matrix; usability tests; stop/override mechanisms.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
2.f	Are predetermined changes to the system and its performance defined with continuous-compliance safeguards?	**Evidence:** Change protocol; permitted ranges; retraining criteria; non-regression tests; rollback.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
2.g	Do validation and testing cover accuracy, robustness, discriminatory impacts and applicable requirements with dated, signed reports?	**Evidence:** Test plan; datasets and characteristics; metrics and thresholds; logs; signed reports; subgroup results. **Watch out:** A single aggregate score often hides gaps between populations and conditions of use.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
2.h	Do cybersecurity measures cover the model, data, interfaces, supply chain and operations?	**Evidence:** Threat model; penetration tests; access control; poisoning, evasion and extraction protection; patch plan.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date

3 Monitoring, functioning and control

Make system capabilities, limitations, foreseeable risks and operational controls visible.

1 / 2

Ref.	Requirement / self-assessment question	Expected evidence and examples	Tracking
3.1	Are performance capabilities and limitations quantified for relevant persons or groups?	**Evidence:** Performance card; disaggregated results; confidence intervals; limitations by environment or use case.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
3.2	Is the expected overall accuracy linked to the intended purpose and acceptance thresholds?	**Evidence:** Metric/threshold/use matrix; business rationale; validation results; go/no-go criteria.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
3.3	Are foreseeable unintended outcomes and sources of risk to health, safety, fundamental rights and non-discrimination described?	**Evidence:** Scenario catalogue; misuse cases; impact assessment; link to the risk register.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
3.4	Do human oversight measures genuinely allow outputs to be understood, challenged, stopped or corrected?	**Evidence:** Operator procedures; scenario tests; override/stop controls; training; escalation. **Watch out:** A purely formal human validation step is not effective oversight.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date

3 Monitoring, functioning and control

Make system capabilities, limitations, foreseeable risks and operational controls visible.

2 / 2

Ref.	Requirement / self-assessment question	Expected evidence and examples	Tracking
3.5	Are input-data specifications and controls suitable for actual conditions of use?	**Evidence:** Input schema; validation rules; drift and out-of-distribution detection; missing-value handling.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
3.6	Can operational monitoring, logs and alerts detect degradation or out-of-scope use?	**Evidence:** Observability plan; log catalogue; dashboards; alert thresholds; investigation procedure.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date

4 Appropriateness of performance metrics

Justify that the selected metrics actually evaluate the system in context and for affected persons.

1 / 1

Ref.	Requirement / self-assessment question	Expected evidence and examples	Tracking
4.1	Is each metric tied to an explicit objective, risk and conformity decision?	**Evidence:** Metric definition sheet; rationale; owner; frequency; triggered decision.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
4.2	Are acceptance thresholds, uncertainty margins and calculation methods defined before evaluation?	**Evidence:** Pre-registered protocol; go/no-go thresholds; confidence intervals; statistical method.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
4.3	Does the metric set avoid misleading averages and cover robustness, relevant groups and degraded conditions?	**Evidence:** Segmented results; stress tests; calibration, false-positive/negative and robustness metrics. **Watch out:** A technically standard metric may still be unsuitable for the real consequences of errors.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date

5 Risk management system — Article 9

Demonstrate a continuous, documented process for identifying, assessing, controlling and reviewing risks.

1 / 2

Ref.	Requirement / self-assessment question	Expected evidence and examples	Tracking
5.1	Is the risk management process established, documented, iterative and maintained throughout the lifecycle?	**Evidence:** Policy and procedure; RACI; review frequency; trigger criteria; decision history.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
5.2	Are known and reasonably foreseeable risks under intended use and foreseeable misuse identified?	**Evidence:** Risk register; scenario workshops; misuse/abuse cases; sources and exposed persons.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
5.3	Are risks from post-market data and interaction with other systems incorporated?	**Evidence:** Field-feedback loop; incident watch; complaint analysis; dependencies and combined effects.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
5.4	Do measures follow the hierarchy of design-out/reduction, safeguards, then information and training?	**Evidence:** Risk-control matrix; design choices; technical safeguards; instructions; training plan.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date

5

Risk management system — Article 9

Demonstrate a continuous, documented process for identifying, assessing, controlling and reviewing risks.

2 / 2

Ref.	Requirement / self-assessment question	Expected evidence and examples	Tracking
5.5	Are residual risks deemed acceptable, communicated and linked to control-effectiveness testing?	**Evidence:** Signed acceptance; acceptability criteria; effectiveness tests; residual risks in instructions. **Watch out:** A risk does not become acceptable merely because it is mentioned.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
5.6	Are impacts on minors, vulnerable persons and other relevant groups assessed where applicable?	**Evidence:** Population analysis; consultation; accessibility measures; specific tests; non-applicability rationale.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date

6 Changes throughout the lifecycle

Trace changes and determine their effect on performance, risks and conformity.

1 / 1

Ref.	Requirement / self-assessment question	Expected evidence and examples	Tracking
6.1	Does a log link every relevant change to a version, date, author and rationale?	**Evidence:** Change log; tickets; commits/releases; approvals; component-version matrix.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
6.2	Is the effect of every change on data, performance, groups, risks and cybersecurity assessed before release?	**Evidence:** Change impact assessment; targeted tests; regression analysis; risk and security review.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
6.3	Are criteria distinguishing predetermined changes from substantial modifications formalised?	**Evidence:** Decision tree; thresholds; escalation protocol; compliance opinion; archived decision.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
6.4	Are the technical file and related documents updated in a synchronised way?	**Evidence:** Release checklist; matching versions of instructions, declaration, model card and monitoring plan.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date

7 Harmonised standards and technical solutions

Show which standards cover the requirements and how gaps or alternative solutions ensure conformity.

1 / 1

Ref.	Requirement / self-assessment question	Expected evidence and examples	Tracking
7.1	Are harmonised standards applied in full or in part listed with their OJEU references?	**Evidence:** Standards register; version/date; OJEU link; scope of application; owner.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
7.2	Does a matrix link each applied clause to the relevant requirements and evidence?	**Evidence:** Requirement-clause-evidence matrix; audit reports; certificates where relevant.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
7.3	Are exclusions, deviations and partial applications justified and compensated?	**Evidence:** Gap analysis; approved rationale; compensating controls; additional tests.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
7.4	Where no applicable harmonised standard exists, are adopted solutions described in detail?	**Evidence:** Common specifications; international standards; internal specifications; equivalence demonstration. **Watch out:** ISO certification alone does not prove that the AI system complies with the AI Act.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date

8 EU declaration of conformity

Keep a complete, signed declaration strictly aligned with the identity and version of the system.

1 / 1

Ref.	Requirement / self-assessment question	Expected evidence and examples	Tracking
8.1	Does the declaration unambiguously identify the system, provider and, where applicable, authorised representative?	**Evidence:** Draft or signed copy; name/type; unique identifier; full contact details.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
8.2	Does it state provider responsibility and conformity with the Regulation and other applicable Union law?	**Evidence:** Annex V clauses; applicable-law matrix; legal approval.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
8.3	Are references to personal data, standards, specifications and the notified body included where applicable?	**Evidence:** GDPR references; standards; assessment procedure; body and certificate where applicable.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
8.4	Are the place, date, signatory and declared version checked before release?	**Evidence:** Signature workflow; delegation of authority; version control; declaration register. **Watch out:** Do not reuse a signed declaration after a change that alters its scope.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date

9

Post-market monitoring — Article 72

Organise continuous collection and analysis of field data to verify conformity throughout the lifetime.

1 / 2

Ref.	Requirement / self-assessment question	Expected evidence and examples	Tracking
9.1	Is the post-market monitoring system proportionate to the technology, intended purpose and risks?	**Evidence:** PMS procedure; scope; governance; resources; interfaces with quality and risk management.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
9.2	Does a documented plan define objectives, sources, indicators, methods, frequency and responsibilities?	**Evidence:** Versioned PMS plan; KPI/KRI catalogue; schedule; RACI; review arrangements.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
9.3	Is field data actively collected from deployers and other relevant sources?	**Evidence:** Feedback channels; telemetry; surveys; support; complaints; external sources and monitoring.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date
9.4	Do thresholds trigger investigation, correction, suspension, reassessment or incident reporting?	**Evidence:** Threshold/action matrix; playbooks; serious-incident procedure; exercise evidence.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date

9

Post-market monitoring — Article 72

Organise continuous collection and analysis of field data to verify conformity throughout the lifetime.

2 / 2

Ref.	Requirement / self-assessment question	Expected evidence and examples	Tracking
9.5	Do monitoring conclusions update risks, tests, documentation, instructions and change decisions?	**Evidence:** Review minutes; CAPA; revised versions; feedback loop to development and compliance. **Watch out:** A dashboard without an owner or triggered action is not a monitoring system.	Status ☐ Compliant ☐ In progress ☐ Not started ☐ Not applicable Owner Link / location Action / due date

Evidence register

List the artefacts that actually exist. Evidence should be versioned, dated, attributed and linked to the assessed system.

ID	Document / artefact	Part	Version / date	Owner	Link / location	Approved by
E-01						
E-02						
E-03						
E-04						
E-05						
E-06						
E-07						
E-08						

Evidence register

List the artefacts that actually exist. Evidence should be versioned, dated, attributed and linked to the assessed system.

ID	Document / artefact	Part	Version / date	Owner	Link / location	Approved by
E-09						
E-10						
E-11						
E-12						
E-13						
E-14						
E-15						
E-16						

Prioritised action plan

Convert “In progress” and “Not started” controls into concrete actions. A useful action produces verifiable evidence.

P1 = blocks the conformity case · P2 = material risk or incomplete evidence · P3 = improvement / consolidation

Priority	Observed gap	Expected deliverable	Owner	Due date	Status

Prioritised action plan

Convert “In progress” and “Not started” controls into concrete actions. A useful action produces verifiable evidence.

P1 = blocks the conformity case · P2 = material risk or incomplete evidence · P3 = improvement / consolidation

Priority	Observed gap	Expected deliverable	Owner	Due date	Status

Final review and approval

This checklist helps prepare the technical file required by Article 11. It is not a substitute for an applicability assessment, the full documentation or legal advice.

☐	The intended purpose, version and scope are consistent across all artefacts.
☐	Every material claim points to accessible, dated and versioned evidence.
☐	Test reports state the protocol, data, thresholds, results and signatory.
☐	Limitations, foreseeable misuse, affected groups and residual risks are explicit.
☐	Human oversight measures have been tested with future deployers.
☐	Predetermined changes and substantial-modification thresholds are documented.
☐	The EU declaration of conformity matches the exact system version assessed.
☐	The post-market monitoring plan has indicators, owners and action triggers.

Final decision

☐ Ready for conformity review

☐ Ready with reservations

☐ Not ready

Reservations, conditions and next review date

Technical owner

Owner

Next review

Compliance / legal owner

Owner

Next review

Management / authorised representative

Owner

Next review

Official source: Regulation (EU) 2024/1689 consolidated on 27 July 2026 — Article 11 and Annex IV