EU AI Act Annex IV Template — Technical Documentation for High-Risk AI

**Fictional sample template. Not legal advice.**

This template is aligned to Annex IV items (1)–(9) and designed to be “living documentation”: fill v1 once, then keep it current via change control, monitoring, and review records.

# Document control (front matter)

## Document metadata

|  |  |
| --- | --- |
| Field | Value |
| Document title | EU AI Act Annex IV — Technical Documentation |
| AI system name | <system\_name> |
| AI system version | <system\_version> |
| Provider / responsible entity | <legal\_entity\_name> |
| Document owner (role + name) | <owner\_role\_and\_name> |
| Approvers (roles + names) | <approvers> |
| Confidentiality level | Public / Internal / Confidential / Restricted |
| Effective date | <yyyy-mm-dd> |

## Revision history

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Version | Author | Summary of change | Approved by |
| <yyyy-mm-dd> | v0.1 | <name> | Initial draft | <name> |

## Scope statement

* Intended purpose (1–2 sentences): <purpose>
* Boundaries / exclusions: <what\_is\_out\_of\_scope>
* Target users / deployers: <who\_operates\_and\_uses\_the\_system>

## Disclaimer

This template is provided for informational purposes only and does not constitute legal advice. You are responsible for determining applicable obligations and for producing complete and accurate technical documentation.

# Annex IV conformance map (quick index)

This table helps reviewers jump to the right section in this document.

|  |  |  |
| --- | --- | --- |
| Annex IV item | Title | Where in this document |
| (1) | General description of the AI system | Section 1 |
| (2) | System elements and development process | Section 2 |
| (3) | Monitoring, functioning and control | Section 3 |
| (4) | Appropriateness of performance metrics | Section 4 |
| (5) | Risk management system | Section 5 |
| (6) | Relevant changes through lifecycle | Section 6 |
| (7) | Standards and technical specifications used | Section 7 |
| (8) | EU declaration of conformity | Section 8 |
| (9) | Post-market monitoring system and plan | Section 9 |

# Section 1 — General description of the AI system (Annex IV item 1)

## 1.1 Intended purpose

* Intended purpose (what the system does): <text>
* Intended users / deployers: <text>
* Intended populations / environments (if applicable): <text>
* Foreseeable misuse (high-level): <text>

## 1.2 Provider and versioning

* Provider name: <text>
* System versioning scheme: <text>
* Relationship to prior versions (what changed, why): <text>

## 1.3 System context and integrations

* Interaction with hardware/software and other AI systems (if applicable): <text>
* External services, dependencies, and critical integrations: <text>

## 1.4 Software/firmware versions and updates

* Relevant software/firmware versions: <text>
* Update requirements (how updates are delivered and validated): <text>

## 1.5 Forms of placing on the market / putting into service

* Delivery models: API / SaaS / embedded / downloadable / on-prem / hybrid
* Packaging details (endpoints, regions, deployment topology): <text>

## 1.6 Intended hardware environment

* Compute/runtime environment (if relevant): <text>
* Hardware constraints / dependencies: <text>

## 1.7 User interface and instructions for use

* Basic user interface description for deployers: <text>
* Instructions for use (deployer-facing): <text>

## Evidence pointers (optional, for provability)

|  |  |  |
| --- | --- | --- |
| Evidence artifact name | Where it is generated | Integrity proof reference |
| System overview | Product documentation | Manifest entry: <sha256> |
| Release manifest / build info | CI/CD pipeline | Manifest entry: <sha256> |
| Deployment topology | IaC repository | Manifest entry: <sha256> |
| Deployer instructions | Docs / runbooks | Manifest entry: <sha256> |

# Section 2 — System elements & development process (Annex IV item 2)

## 2.1 Development methods, steps, and tools

* Development lifecycle (phases): <text>
* Third-party tools and services used (and how integrated/modified): <text>
* Roles and responsibilities (RACI summary): <text>

## 2.2 Design specifications and key choices

* System logic (high-level): <text>
* Key design choices and assumptions: <text>
* What is optimized (objectives): <text>
* Output quality expectations and trade-offs (including compliance trade-offs): <text>

## 2.3 Architecture and components

* Architecture diagram reference: <link/identifier>
* Components and interactions (data flow): <text>
* Compute resources used to develop/train/test/validate (if applicable): <text>

## 2.4 Data requirements and dataset documentation

* Data requirements (types, sources, constraints): <text>
* Dataset documentation (“datasheets”) references: <links/identifiers>
* Provenance, selection, labeling, cleaning methods (where relevant): <text>

## 2.5 Human oversight assessment (Article 14)

* Oversight goals (what humans must be able to do): <text>
* Measures that help deployers interpret outputs: <text>
* Escalation and override mechanisms: <text>

## 2.6 Pre-determined changes and continuous compliance

* Pre-determined changes (if applicable): <text>
* How changes are evaluated and approved: <text>
* How continuous compliance is ensured: <text>

## 2.7 Validation and testing

* Validation/testing procedures: <text>
* Test datasets used (references): <links/identifiers>
* Metrics used (accuracy, robustness, compliance): <text>
* Discriminatory impact assessment (where relevant): <text>
* Signed reports/logs references: <links/identifiers>

## 2.8 Cybersecurity measures

* Security controls relevant to this system: <text>
* Threat model reference (if available): <link/identifier>
* Access control, secrets, and key management: <text>

## Evidence pointers (optional, for provability)

|  |  |  |
| --- | --- | --- |
| Evidence artifact name | Where it is generated | Integrity proof reference |
| Architecture diagram | Design repo / docs | Manifest entry: <sha256> |
| Training data sheet excerpts | Data governance | Manifest entry: <sha256> |
| Model card excerpts | Model registry | Manifest entry: <sha256> |
| Validation & testing excerpts | CI/CD / evaluation harness | Manifest entry: <sha256> |
| Policy pack excerpts (policy-as-code) | Policy engine | Manifest entry: <sha256> |

# Section 3 — Monitoring, functioning, and control (Annex IV item 3)

## 3.1 Capabilities and limitations

* Capabilities (what it can do reliably): <text>
* Limitations and known failure modes: <text>
* Assumptions required for safe operation: <text>

## 3.2 Expected accuracy and performance (overall and subgroups)

* Overall performance summary (high-level): <text>
* Subgroup / intended population performance (where relevant): <text>

## 3.3 Foreseeable unintended outcomes and risk sources

* Foreseeable unintended outcomes: <text>
* Risk sources (safety, fundamental rights, discrimination, privacy): <text>

## 3.4 Human oversight measures (operationalized)

* Oversight checkpoints (what triggers review): <text>
* Decision records and accountability: <text>

## 3.5 Input data specifications

* Input data types and constraints: <text>
* Data quality expectations: <text>
* Handling of missing/invalid inputs: <text>

## Evidence pointers (optional, for provability)

|  |  |  |
| --- | --- | --- |
| Evidence artifact name | Where it is generated | Integrity proof reference |
| Dynamic sampling & quality monitoring report | Runtime telemetry | Manifest entry: <sha256> |
| Human oversight decision records | Review queue | Manifest entry: <sha256> |
| Monitoring dashboards / alert rules | Observability stack | Manifest entry: <sha256> |

# Section 4 — Appropriateness of performance metrics (Annex IV item 4)

## 4.1 Metrics selection rationale

* Metrics used and why they fit intended purpose: <text>
* Known metric limitations and mitigations: <text>

## 4.2 Thresholds and acceptance criteria

* Thresholds that constitute acceptable performance: <text>
* Why the thresholds are appropriate: <text>
* Who approved the thresholds and when: <text>

## Evidence pointers (optional, for provability)

|  |  |  |
| --- | --- | --- |
| Evidence artifact name | Where it is generated | Integrity proof reference |
| Metric definitions | Engineering / governance docs | Manifest entry: <sha256> |
| Baseline evaluation report | CI/CD / evaluation harness | Manifest entry: <sha256> |
| Threshold approval record | Review queue / change control | Manifest entry: <sha256> |

# Section 5 — Risk management system (Annex IV item 5)

## 5.1 Risk management process

* Risk identification approach: <text>
* Risk evaluation and prioritization: <text>
* Mitigation measures: <text>
* Residual risk assessment and acceptance: <text>
* Verification loops (how mitigations are tested): <text>

## 5.2 Linkages to operational processes

* Risk register reference: <link/identifier>
* Incident management process reference: <link/identifier>
* Escalation contacts and SLAs: <text>

## Evidence pointers (optional, for provability)

|  |  |  |
| --- | --- | --- |
| Evidence artifact name | Where it is generated | Integrity proof reference |
| Risk register export | GRC tooling | Manifest entry: <sha256> |
| Control tests / policy checks | Policy engine / CI | Manifest entry: <sha256> |
| Incident runbook excerpts | Operations docs | Manifest entry: <sha256> |

# Section 6 — Relevant changes through lifecycle (Annex IV item 6)

## 6.1 Change categories

* Model updates (weights, prompts, tools): <text>
* Data pipeline changes: <text>
* Policy/guardrail changes: <text>
* UI/UX changes (deployer-facing): <text>
* Retraining events and triggers: <text>

## 6.2 Approval and validation requirements

* Change approval matrix (what requires review/approval): <text>
* Validation requirements per change type: <text>
* Rollback procedures: <text>

## Evidence pointers (optional, for provability)

|  |  |  |
| --- | --- | --- |
| Evidence artifact name | Where it is generated | Integrity proof reference |
| Change log / release notes | CI/CD / product ops | Manifest entry: <sha256> |
| Policy bundle diffs | Policy engine | Manifest entry: <sha256> |
| Validation reports (per release) | CI/CD | Manifest entry: <sha256> |

# Section 7 — Standards and technical specifications (Annex IV item 7)

## 7.1 Harmonised standards applied

* List harmonised standards applied (full/partial): <text>
* Scope and applicability notes: <text>

## 7.2 If no harmonised standards applied

* Solutions adopted to meet requirements: <text>
* Other standards/specs used: <text>

## Evidence pointers (optional, for provability)

|  |  |  |
| --- | --- | --- |
| Evidence artifact name | Where it is generated | Integrity proof reference |
| Standards mapping | Governance docs | Manifest entry: <sha256> |
| Control framework mapping | Policy pack | Manifest entry: <sha256> |

# Section 8 — EU declaration of conformity (Annex IV item 8)

## 8.1 Declaration reference (stub)

* Declaration document reference: <link/identifier>
* Date of issue: <yyyy-mm-dd>
* Signatory: <name + title>

Public versions of this template may include a stub only.

## Evidence pointers (optional, for provability)

|  |  |  |
| --- | --- | --- |
| Evidence artifact name | Where it is generated | Integrity proof reference |
| EU declaration of conformity | Quality management system | Manifest entry: <sha256> |

# Section 9 — Post-market monitoring system + plan (Annex IV item 9)

## 9.1 Monitoring objectives and signals

* Monitoring objectives: <text>
* Signals tracked (safety, performance, drift, bias, misuse): <text>
* Thresholds and alerting rules: <text>

## 9.2 Post-market monitoring plan

* Plan owner and cadence: <text>
* Data sources and sampling approach: <text>
* Escalation and remediation workflow: <text>

## 9.3 Continuous improvement loop

* Incident reporting linkage: <text>
* Retrospective process: <text>
* Feedback into risk management and change control: <text>

## Evidence pointers (optional, for provability)

|  |  |  |
| --- | --- | --- |
| Evidence artifact name | Where it is generated | Integrity proof reference |
| Post-market monitoring plan | Ops / governance | Manifest entry: <sha256> |
| Drift/bias monitoring report | Runtime telemetry | Manifest entry: <sha256> |
| Incident records (sanitized) | Ticketing / IR | Manifest entry: <sha256> |

# Appendix A — Evidence integrity model (example)

Use this appendix to document how your evidence bundle can be verified.

* Per-artifact SHA-256 digests in a manifest
* A bundle root hash computed from the manifest
* Recording the root hash in an append-only audit ledger
* A verification procedure that re-computes and checks the hashes

## Verification steps (template)

1. Obtain the exported bundle and the manifest.

2. Re-compute SHA-256 digests for each file; compare with manifest entries.

3. Re-compute the bundle root hash from the manifest; compare with the recorded root hash.

4. Verify the root hash exists in the audit ledger and matches the expected entry.