

What AICMS checks. And what happens next.

A detailed guide to submission checks, workflow safeguards, calculations and conditional guidance. Each control explains its scope and practical effect.



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

For practitioners, assessors and implementation teams

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 / Read a control by its effect	3
02 / Understand the submission gates	4
03 / Keep records, access and relationships consistent	5
04 / Control versions and review decisions	6
05 / Preserve FRIA reasoning and reassessment	7
06 / Know what a calculation really measures	8
07 / Interpret generated outputs correctly	10
08 / Follow-up services and attention views	12
09 / Guided assessments and input constraints	12
10 / Legal relevance is a separate decision aid	17
11 / Identity and classification	18
12 / Transparency and disclosure	21
13 / Risk management and safeguards	25
14 / Human oversight and literacy	32
15 / Performance, robustness and cybersecurity	35
16 / Data governance	38
17 / Fundamental rights assessments	42
18 / Technical documentation and instructions	47
19 / Quality management	54
20 / Logging, retention and review dates	56
21 / Conformity, declarations and certificates	58
22 / Registration and Article 6 exceptions	62
23 / Operators, agreements and modifications	67
24 / Incidents, corrective action and emergency use	69
25 / General-purpose AI	72
26 / Transitional provisions	75

01 / Read a control by its effect

This reference explains the detailed logic in the reviewed AICMS edition. Use it when preparing a dossier, evaluating the product or discussing a particular finding with an implementation or compliance specialist.

The first chapters explain controls around editing, assessment, review, dates, outputs and follow-up. The catalogue then covers **all 226 distinct identifiers emitted by the submission validator**. Some identifiers have more than one trigger; a finding can also appear for several affected records. The count describes this particular inventory, not statutory obligations, independent tests, visible warnings or a percentage of legal coverage.

BLOCK

Prevents a workflow action

GUIDE

Helps a person decide

RECORD

Preserves a declared fact

Three different questions

Question	What the answer means
Can the record be saved?	Field constraints, access, ownership, relationships and lifecycle restrictions may refuse a change.
Can the dossier enter review?	Submission checks examine specified recorded facts and consistency conditions. Every returned section finding blocks submission.
Has the underlying duty been fulfilled?	This still needs factual evidence, substantive assessment and any required external action. A successful software check cannot settle it.

Read each catalogue entry together

The **identifier** is a stable reference for discussing a finding. **Scope** gives the surrounding conditions. **Finding** describes the specific recorded condition. **Effect** says whether it blocks submission or is only calculated as advice. **Legal context** identifies the provision or product policy that motivated the rule; it does not mean the whole provision is enforced.

"Blank" generally means missing, empty or whitespace. A check for text does not assess its quality. "Confirmed" generally means the recorded answer is yes, not that AICMS independently verified the fact. Scope and finding must both hold.

Edition: 29 September 2026. This reference describes inspected implementation and screens. It is not a fresh application test run or deployment attestation. Read the Responsibility Map for the current legal edition, application dates and retained duties.

02 / Understand the submission gates

The assessment follows recorded scope

1. **Basic identity comes first.** Name, description, purpose, lifecycle, classification, clarity confirmation and responsible-party information are checked for every tier.
2. **Prohibition stops the route.** A Prohibited tier, or a conflicting positive prohibited-practice answer, blocks submission. The cessation-record check also runs, then later submission checks are skipped on that branch.
3. **Transparency can cross tiers.** The general mechanism check runs for Limited Risk and High Risk. Conditional Article 50 checks run for all remaining tiers.
4. **The principal high-risk group has an exception.** A recognised High Risk category normally opens the detailed requirements. The product-only Annex I Section B branch skips that group and several other checks when its recorded conditions hold.
5. **FRIA history and later conditions still matter.** Open assessments, reassessment flags, incidents, certificates, GPAL and other individually gated checks follow their own rules.

An **Annex III signal** can come from an actual area record, a wizard selection, the uses-Annex-III answer or profiling. It is broader than a fully resolved statutory use case. A custom classification without a recognised built-in category identity can pass the presence check without entering the named-tier branches.

Yellow is not the same as optional

The current editor shows submission section findings as errors or yellow warnings. **Both block submission.** The server also calculates a separate set of non-blocking advisories. That separate collection is not displayed by the current editor. This reference labels those entries openly; do not expect every advisory listed here to appear on screen.

Three disclosure checks block when the organisation has a Deployer role, a referenced role cannot be resolved, or no recognised role is recorded anywhere. Otherwise they produce an unshown advisory. External parties are excluded from the organisation's own role membership but still affect the unresolved/absent-role fallbacks. Most high-risk checks do not use this same distinction. Registration and the legal applicability map use other role rules, which can include external parties.

Dates and legal scope are not universal switches

Submission checks are not all disabled until a legal application date. Nor do all of them share the legal Navigator's exceptions. The Section B message in the validator retains older legal wording, while the Navigator has newer amended wording. Treat that message as an explanation of a product branch, then verify the current law in the Responsibility Map.

03 / Keep records, access and relationships consistent

Controls around ordinary editing

Control	Behaviour and boundary
Company and access scope	Server queries and saves apply company scope and system/version access rules. Related references must belong to an accessible context. This review is source evidence, not a security certification.
Separate permissions	Viewing, creating, editing, submitting, approving and configuring are distinct operations. A business-role label does not grant an application permission.
Draft-only ordinary changes	The server checks the persisted parent status. Ordinary version content, child records and comments cannot be changed after Draft. Dedicated later actions are narrower exceptions.
One open working edition	The lifecycle service refuses another Draft or InReview sibling when cloning. The ordinary save path also checks for an existing open sibling.
Edit lock	An active lock belongs to an editor and expires after 30 minutes. Ordinary saves refuse a different active owner. This is not a universal lock over every dedicated command.
Stable parentage	A version cannot silently move to another AI system. Ownership of existing and new child records is checked rather than trusting only the submitted parent identifier.
Related evidence and people	Attachments, people, configuration, parties, risks and linked records are checked for accessible ownership. Cross-version incident/risk or party references are refused.
Links to organisational standards	A linked norm item must be accessible in the company context. A valid link does not prove that the norm's control has been implemented.
Audit ownership	The server manages audit timestamps and protected workflow/assessment fields. Client edits cannot simply clear a FRIA reassessment flag.
Completed corrective action	An ordinary save of Completed or Verified status requires an outcome. The Published post-market append command has a narrower input and does not run that same outcome gate.
Retention configuration	Configured log-retention choices below six months are refused. Choosing an accepted duration does not retain actual logs.

Field lengths, number ranges and model validation provide additional basic input constraints. They are distinct from conditional submission requirements and from the legal adequacy of the content. The guided-assessment chapter explains the most relevant user-facing differences.

Evidence is linked, not automatically authenticated

Typed attachments can support risks, mitigations, assessments, certificates, technical documentation and other records. Normal uploads belong to an editable Draft. After approval, readers can use the retained evidence, while ordinary further editing or upload uses a new Draft.

The software cannot establish from an upload alone that a report concerns the right AI build, that a signature is valid, that a result is reproducible or that an external URL will remain available. Those are evidence-review and retention responsibilities.

04 / Control versions and review decisions

Starting and revising a dossier

Creating a system requires a name, description and intended purpose. The service creates its first Draft, resolves company-specific lifecycle/role/person choices and records the event.

A new Draft can be cloned from a Published or Archived version, with a chosen major, minor or patch increment. Related records and their stable comparison identities are copied; workflow stamps are reset. The latest completed FRIA can be carried forward with provenance and reassessment due. This is not automatic confirmation that the new use still meets the previous assessment.

Version increments are chosen by a person. They do not decide whether a legal substantial modification has occurred. The implementation has its own version-number limits and comparison rules; the useful customer commitment is a versioned, reviewable record, not a promise of every convention in the Semantic Versioning standard.

Submission and review are separate controls

Action	Enforced condition or result
Submit	Draft status; relevant derived declaration/QMS rows are prepared; the full submission validator runs; blocking section findings refuse the transition.
Enter review	Status becomes InReview, the submitter is recorded, and workflow history/notifications are created.
Approve	InReview status, a nonblank comment and an independent eligible reviewer; the Article 5 prohibition/classification pair is rechecked.
Reviewer independence	The reviewer must differ from both the original draft creator and current submitter. If neither author can be determined, review fails closed. More than two people may be involved.
Publish internally	The candidate becomes Published; the previous published version becomes Archived; the comparison and event are retained. This is not approval by an authority or deployment of the AI.
Reject	The same independence and comment requirements apply; the record returns to Draft with a recorded decision.

Approval does not rerun the complete submission validator. Do not describe the two stages as identical checks. Check Readiness is also a point-in-time view; editing can make its displayed result stale.

Comparisons preserve the meaning of a change

Comparisons require accessible versions of the same AI system. They cover the main record and many related collections: risks, measures, groups, data, parties, metrics, documentation, certificates, declarations, QMS, incidents, authority records, agreements, literacy and GPAI records. The latest completed FRIA is compared separately. Discussion comments, open FRIA drafts and the entire historical assessment collection are not part of the content comparison.

Stable record identities help avoid showing every cloned row as new. Counts group changes by item rather than treating each changed field as a separate feature or unit of effort. Draft comparisons are recomputed; cached comparisons between non-Draft versions should not be assumed to remain a live view of later dedicated post-market additions.

Narrow changes remain possible after publication

Record risk review records an outcome, review date and next-review information on a Published version. **Add post-market record** can append a corrective action, authority notification or authority request, immediately frozen. It does not add a serious incident or monitoring activity, or expose every Draft field. A supplied duplicate-prevention key protects replay of that particular append request; it is not a general duplicate-detection service.

05 / Preserve FRIA reasoning and reassessment

A three-way scope decision

The derivation combines a High Risk classification, relevant non-excluded Annex III areas other than point 2, and deployer context. Public bodies, private providers of public services, and the specified creditworthiness or insurance subpoints have particular significance. Missing category or subpoint information can leave the result **unknown**; it is not silently treated as no duty.

The organisation can override the derived answer with a rationale. The product preserves the derived facts and the chosen answer; it does not grant a legal exemption.

Control	What it does
Editable parent	Starting, completing and controlled notification updates require an editable Draft dossier. These are not general post-publication actions.
One draft assessment	Only one Draft FRIA is allowed for a version. The service also protects concurrent assessment updates.
First assessment versus reassessment	Reassessment needs a previous completed run. A new draft can reuse prior content, while resetting completion and override/notification details.
Changed facts	Completion re-derives applicability and compares the acknowledged input fingerprint. Changed decision inputs refuse completion until reassessed. This detects changed inputs, not false inputs.

Control	What it does
Required content	For an effectively required assessment, process, duration/frequency, affected persons, harms, oversight and mitigation content must be present.
Completed history	Completion preserves the derivation, evidence snapshot, person and time. Ordinary saves cannot rewrite or delete completed/imported runs or their protected metadata.
Notification completion	A date and method are required. A date more than one day beyond today's UTC date is refused; the one-day allowance accommodates time zones.
Forward-only notification	On the latest completed required assessment, Not Started may move to In Progress or Completed; In Progress may move to Completed. The expected current state protects against conflicting updates.
Separate readiness	The assessment can be completed while notification remains pending. The relevant submission check then blocks the dossier from entering review.

Changes that trigger reassessment

With a prior non-Draft assessment, meaningful purpose or classification changes can mark reassessment due. Annex III additions, removals or relevant area/subpoint/carve-out edits, and deployer-role/legal-category changes also trigger the recorded flag. Whitespace-only purpose changes do not. The first outstanding reason is retained rather than overwritten by every later edit.

Any set reassessment-due date can block relevant submission; the validator does not wait for that date to arrive. Conformity resets have a related but different scope: purpose/classification changes and Annex III additions or removals reset specified conformity/wizard/CE completion fields. Do not assume every material edit automatically resets every approval.

06 / Know what a calculation really measures

Risk and accuracy

Risk severity and likelihood use a 1-5 input scale. Residual-risk consistency checks compare recorded severity and mitigation values; levels 4 and 5 trigger certain stronger requirements. These are product choices, not numerical formulas prescribed by Article 9.

Accuracy checks compare numbers only when both measurement and threshold are supplied and parse in an invariant decimal format. They assume **higher is better**. A missing value can skip the comparison, and lower-is-better measures such as error rate need separate interpretation. Measurement dates are recorded claims, not evidence that AICMS ran a test. A same-day measurement does not satisfy the check requiring a measurement strictly before market placement.

Incident-reporting clock

Recorded category	Product default
Critical Infrastructure or Serious	2 calendar days
High	10 calendar days
Other values	15 calendar days

The clock starts from awareness date when present, otherwise incident date. It uses calendar dates and today's UTC date, with no working-day or holiday extension. Unreported incidents due today or tomorrow are Approaching; only dates before today are Overdue. A report on or before its deadline is Met; a later report remains historically Overdue.

An authorised override accepts 1 through the category default, inclusive. It cannot extend that default, but it can increase a previously shortened window back towards the default. The visible dialog requires a nonblank reason; the server command permits it to be omitted and records that omission. Direct ordinary-save attempts to set the override are reset; a severity change selects its new default.

Legal boundary: Article 73's outer limits depend on the event, not merely these labels. Death, widespread infringement and specified serious critical-infrastructure disruption have particular conditions. Immediate reporting requirements still apply. The product's High category is broader than a verified death case; selecting it does not establish the ten-day legal rule. GPAI incidents use their own legal framework.

Retention and review schedules

Calculation	Exact practical meaning
Documentation retention	Recorded market-placement date plus 10 calendar years. Missing placement means no calculated date. Internal approval fills a missing placement date with today's UTC date, so confirm the actual market event rather than treating this default as evidence.
Log-retention interpretation	A configured duration takes precedence, then numeric months, then parsable legacy text. Years/months/weeks/days can be interpreted, with weeks/days approximately converted and rounded down. This describes a duration; it does not retain logs.
Risk review	The Published review action requires an outcome, a review date no later than today, and any next date after that review.
Review-frequency inference	Recognised six-month, annual and quarterly descriptions add those periods. Other text containing month adds one month. An unrecognised frequency supplies no next date. Confirm the displayed date.
Retention protection	Individual non-Draft versions resist ordinary deletion, but authorised whole-system deletion can remove all versions. A retention date is not a deletion lock.

Certificates

When both dates exist, expiry must follow issue. The implemented maximum is four years for an Annex III route, five for Annex I alone, and a conservative four when unresolved. Four wins when both routes apply. A reassessment date on or after issue can become the date used to calculate the maximum. Missing issue or expiry skips that maximum-period check.

The product treats only Active and Extended certificates as in force. Restricted is excluded from that state. A certificate expires after its recorded expiry day. Supplements must stay in the same version and cannot form self-references or cycles; their effective expiry can inherit the parent's, and loaded parent validity matters.

The Article 36(8)(b) helper concerns a recorded authority finding that the body lacks capability, with a Suspended or Restricted certificate. It uses the latest corresponding lifecycle event plus three months. Missing dates prevent a calculated deadline; recorded confirmation suppresses the overdue condition. The statutory case and required authority steps still need professional verification.

GPAI computation and date proxies

A systemic-risk suggestion arises from recorded compute at or above **10²⁵ FLOPs**, a high-impact-capability answer or Commission designation. It does not change the stored classification automatically. The Act's compute presumption says **greater than** 10²⁵; the product's inclusive boundary is a conservative discrepancy, not an official determination.

For an applicable stored-systemic notification record, the suggested deadline is its creation date plus 14 days. The scheduled escalation uses that suggestion, not the separately entered deadline. Creation is not proof of the date on which the provider became aware of the legal trigger.

The initial reassessment floor uses the Commission decision plus six months. After a refused previous request, it uses that **request** plus six months because a separate reassessment-decision date is not captured. A newly supplied or changed request is checked against the persisted floor; an unchanged historical invalid date is not automatically corrected. Verify the legal clock before acting.

07 / Interpret generated outputs correctly

Readable dossier and register

The register exports a filtered Excel list. The implemented version Print / Save as PDF route produces a readable dossier through browser printing, with status, dates, tables, evidence references and missing-data notes. This is distinct from the structured files described below.

Annex IV preparation file

Generation creates a JSON attachment from an eligible Draft in the High Risk / Prohibited view and needs editing permission plus the configured attachment type. It replaces the previous generated dossier attachment. Recorded technical points, evidence references and gaps are assembled; the builder does not run a fresh full submission validation or judge document adequacy.

The evidence matrix has 16 traceability rows. Instructions for Use and Risk-management Documentation have blocking coverage labels within that matrix; other rows are advisory, including cross-cutting entries. A typed document can count as covered when it has an attachment reference. A declaration row can be covered by any addressed declaration element or a signed attachment. These package labels are not a complete legal-compliance assessment or the same as a successful submission.

Annex VIII registration preparation file

The Draft-only generation action appears when recorded facts select a package section. It prepares JSON and evidence references; generation can be requested on an incomplete Draft. It does not submit to an EU or national database, verify an official upload schema or confirm acceptance.

Package route	What the builder does
Section A	High Risk with a provider and not national-only. Unlike the corresponding submission scope, the builder does not require an Annex III signal; a product-only route receives a caution.
Section B	Non-high-risk with actual Annex III area records and a selected Article 6(3) condition. A provider record may be absent at generation time.
Section C	High Risk with a public-authority deployer and not national-only. The latest completed FRIA supplies its outcome summary.
Restricted areas 1, 6 or 7	Selects restricted routing and removes specified public package fields, including certain descriptions, documents or assessment summaries. This is data selection, not a secure authority transmission.
Critical infrastructure, point 2 only	For High Risk, omits EU sections and indicates national routing. Mixed point 2/other areas retain EU sections with national-route advice.
Product integration	Adds product-route advice. It does not suppress every EU section because an independent Annex III basis may exist.

The builder selects first matching provider/deployer/mandate records and a deterministically selected submitter. A separate submission check addresses multiple submitters; generation itself is not that check. Certificates are ordered by recorded status and other fields, not certified as valid. Registration-specific descriptions can override the general dossier description in the package.

An externally Registered status or reference entered by a person remains a recorded assertion. Retain the actual registration confirmation. The AI Act EU database is distinct from the medical-device EUDAMED database.

08 / Follow-up services and attention views

The code registers the following scheduled services. Their execution and delivery depend on the running host, configuration, eligible recipients and messaging infrastructure. They create application follow-up and queued mail; they do not make regulatory filings.

Service	Cadence and recorded trigger
Certificate expiry	Daily. Published versions, Active/Extended certificates within the company threshold, including previously missed expired records; default threshold 90 days. Notification state prevents repeat selection.
Documentation subscriptions	Hourly. Changed-version timestamps after the previous notification/subscription date. The rendered customer subscription control is the bell on the AI-system page. This is not a semantic comparison of every child edit.
Incident deadline	Hourly. Refreshes deadline state, then escalates unreported overdue incidents. An already reported late incident retains history without repeated unreported escalation.
Risk review	Daily. Published versions with a known next-review date approaching or overdue. Missing next-review dates are excluded from this routine, though other readiness/attention checks may find them.
Retention	Daily. Published and Archived versions with known approaching or elapsed dates. Reminders do not delete records or enforce retention.
Authority response	Daily. Unanswered requests with a known approaching or past response deadline; uses dates rather than relying only on the recorded status.
Monitoring review	Daily. Published versions with a known last-review date more than six months old. No date does not trigger this routine. Six months is product policy.
Notified-body capability loss	Daily. The specified Article 36 confirmation case with no confirmation and a passed calculated deadline.
GPAI systemic notification	Daily. Stored systemic classification, existing unnotified notification record and passed creation-based suggested deadline. A missing notification record is not discovered by this routine.

Dashboard attention and job selection are not interchangeable. For example, a dashboard can highlight missing information that a scheduled routine excludes because it has no date from which to calculate an alert. Follow a signal to its underlying record and check who owns the response.

09 / Guided assessments and input constraints

The eight guided assessment families provide sequences, conditional explanations and linked record editing. Finishing a wizard records a workflow event. It does not mean that every related submission requirement is satisfied or that an external authority action took place.

Know which stage enforces the answer

Some Next buttons require a specific answer. Other pages allow progression while content is incomplete. Conditional field validation can show a missing follow-up answer without independently disabling the main Save or a wizard's Finish. Ordinary entity validation and server safeguards can still refuse the save. **Submission for review is a separate, broader check.**

Seven wizard families mark their run complete, attempt to save and record the event. FRIA has a separate substantive completion service. The completion history records the workflow act, not proof that every underlying obligation was met. A guard against repeated clicks prevents accidental duplicate actions; it does not itself validate the answers.

Classification

Four pages cover prohibited practice, high risk, transparency and the proposed tier. Next requires an explicit answer to each of the first three decisions. A positive prohibited-practice answer prevents ordinary progression and provides **Record Finding**, which records Prohibited classification. Ordinary Finish also refuses a prohibited result.

Profiling disables the Article 6(3) exception choice; Finish clears a conflicting existing claim. Missing exception condition or justification produces visible red guidance, but that particular guidance is not itself wired into Next or Finish. The separate submission rules check the recorded exception information.

Fundamental rights assessment

The first page needs a resolved derived answer or an explicit override with meaningful rationale. A Not Required answer takes an outcome-only route to the final page; Finish is still needed. Later content pages do not block Next merely because a narrative is missing.

Finish saves the assessment draft and calls the dedicated server completion checks described in chapter 05. An acknowledged-facts mismatch returns the workflow to its first decision. Notification can still be pending after assessment completion; submission readiness remains separate.

Data governance

Six pages cover sources, quality/provenance, bias/fairness, privacy, special-category safeguards and summary. No page has a content-based Next blocker. The special-category checklist is reachable; its six assertions concern necessity, pseudonymisation, security measures, non-transfer, deletion and processing records.

Finish records the run after an ordinary save. The summary's special-category badge is shown when **any** safeguard is selected; it is not an all-six verification. There is no dedicated Article 4a safeguard-completeness submission gate in this edition. Assess the legal conditions and actual safeguards independently.

Human oversight

Six pages cover type, people/roles, intervention, understanding, monitoring and summary. The first Next requires a nonempty oversight type; later pages do not add content-based progression gates. **None is an available selection**, so this guard alone does not establish effective oversight. Finish saves the record and completion event. It neither operates an intervention mechanism nor checks all detailed oversight evidence.

Conformity

Six pages cover route, assessment evidence, certificates, declaration, marking and penalty context. The first Next requires a route; later Next buttons do not test completeness. Progression can prepare an external-assessment row for the Notified Body route and a declaration row for later completion.

Finish sets both the wizard-completed and conformity-assessment-completed confirmations, then saves. It does not independently verify that an external assessment took place, a certificate is valid or a declaration was signed. Review those confirmations against the actual evidence.

Registration

Five pages organise role, contact, system, conformity and registration-reference information. The role starts as **Provider**; the first Next tests that a role exists. Subsequent pages have no content-based Next guard, and the registration URL is optional.

Finish marks the wizard and Annex VIII information complete and sets a route-derived Registered status. Restricted categories take priority; otherwise the recorded High Risk critical-infrastructure route uses national registration, with the general Registered status for other cases. **Finish does not verify external registration or check that the Annex VIII information is complete.** Retain authority confirmation and verify that the recorded status describes what actually happened.

Quality management

Five pages cover the QMS reference, elements, technical documents, logging and summary. Next has no content-based guard. An integrated-documentation choice reveals a reference field; numeric log retention presents a six-month minimum. Finish does not inspect the wizard form's invalid state or run the full readiness validator. Input, configuration-save and submission retention checks are separate layers.

General-purpose AI

Four pages cover use, model details, systemic-risk criteria and obligations. A No-use answer can go directly to completion. The use question blocks only an unanswered value; its underlying record is a nonnullable yes/no field, so this is not proof of a fresh decision. Model details have no content-based Next gate. The systemic-risk step needs a nonempty category, but **Not Classified and Unknown are selectable categories.**

Finish saves and records the run without requiring every GPAI obligation to be complete. The wizard edits the first model-document record in the version or creates one. An open-source claim hides certain Article 53/54 blocks unless the stored category is Systemic Risk; Unknown or Not Classified can also satisfy that visibility test. Hidden content is retained. Hiding a block is not a legal exemption decision.

Which wizards are available?

Classification is available on editable dossiers. Data Governance, Oversight, Conformity, Registration and QMS launchers specifically require **High Risk**. GPAI's surrounding panel allows **High Risk or Prohibited**, not ordinary Minimal/Limited Risk dossiers. FRIA has separate summary/history conditions, including existing assessment state. Ordinary editing needs Draft status, edit permission and no other active editor lock; the server separately protects completion actions.

Conditional follow-up questions

Recorded situation	What the interface does
Non-high-risk Annex III use	Shows the Article 6(3) condition and, after selection, its justification as conditional required text in the main dossier. Historical exception information can also remain visible on a High Risk dossier without being newly required.
Synthetic content	Shows marking method and standard from the declared obligation or generated-content types. These describe safeguards; they do not mark output.
Emotion recognition or biometric categorisation	Shows the relevant disclosure to affected people from the selected obligation.
Deepfakes	Shows disclosure from the Deep Fake/Synthetic Content flags or image/audio/video types. Claiming an exception reveals a rationale. The screen's prompting is broader than a complete legal scope determination.
Public-interest text	Shows disclosure and any editorial-responsibility rationale from the relevant flags or generated text.
Human-interaction exception	Shows a rationale when the exception is claimed. The yes/no field is not forced to Yes simply because it is visible.
Continued learning	Shows feedback-loop mitigation questions, recognising the recorded learning indicators.
Integrated sectoral documentation	Shows a reference when integration is indicated. A visible required marker is distinct from a wizard Finish guard.
Authorised representative	Shows relevant instructions-for-use confirmation. A checkbox's conditional visibility does not force it to Yes; the submission rule handles that requirement.
Annex III subpoint exclusion	Shows the exclusion and reasoning in the collection dialog. The scalar editor's conditional-required logic is not automatically applied to the dialog's text areas.

The generic collection dialog's **Done** accepts edits into the working dossier; it is normally not an independent server save. A specific record type can supply its own Done guard. Cancelling rejects that record's pending edits.

Input and relationship safeguards

Input or action	Behaviour to understand
Names and risk/mitigation titles	Model constraints use bounded text; risk and mitigation titles require 3-150 characters. A meaningful title still needs a person's judgement.
References and narratives	Common limits are 256 characters for references, 512 for short text, 2,000 for medium text and 4,000 for long narratives. These are product limits, not statutory evidence requirements.
Text counters and format	Shared inputs show applicable length counters and constraints where supplied. Email/URL input types provide format guidance, not network verification; registration URL remains optional.
Risk values	Severity, likelihood and residual ratings are offered on a 1-5 scale. Missing values and submission requiredness are distinct from an allowed numeric range.
GPAI numbers	Parameter count, compute, training time and energy have numeric input types, but no universal positive-number or plausibility limit is defined by those inputs.
Accuracy values	Threshold and measurement are entered as text; the separate submission check compares them numerically when both are supplied and parse.
Risk-to-mitigation relationship	Add is disabled without both record types. A new link initially selects the first risk and first mitigation; verify that the pair is intentional.
Risk-to-affected-group relationship	Both record types must exist. Initial first-record selections are convenience defaults, not an inferred relationship.
Annex III area	Available lookup entries are needed, and the first is initially selected. This is not automatic legal classification.
Measure-to-standard control	A norm must be available and the dialog cannot finish without the selected norm item. The server checks its accessible company ownership separately.

Small aids that support continuing work

Checklist progress counts visible **Yes** confirmations, not answered questions or legally sufficient evidence. A No does not add to that count. A group can remain expanded when dependent answers already exist, although outer visibility conditions still matter.

Certain confirmations fill an empty associated date. Existing dates are preserved, unchecking does not clear the date, and the date can remain editable. This is convenience, not an immutable signature time. Application-date quick choices also fill a selected deadline from the legal phase information; a person chooses the relevant date.

Repeated wizard runs and named workflow events help a reviewer follow the dossier's history. They do not prove that every page was examined or every duty completed.

10 / Legal relevance is a separate decision aid

The EU AI Act Navigator relates accessible AI systems to supported provisions using recorded facts and application phases. Its result means a provision is relevant to examine, not that the duty has passed a compliance test.

The map distinguishes positive, negative and unresolved facts. Missing information can remain unknown. Its high-risk relevance can arise from the stored tier, an Annex I product signal or Annex III use, even when a lower tier or exception claim is also recorded. This is conservative navigation, not a binding reclassification.

Decisions the map can support

Family	Facts it uses and the important boundary
Literacy and special-category data	Recorded provider/deployer roles and relevant answered governance/safeguard facts. Special-category safeguard presence is a relevance clue, not an enforced completeness test.
Prohibited practices	Answered classification and recorded categories, including inserted 2026 categories. Exception prose is retained as context, not automatically accepted.
High-risk routes	Annex I product and Annex III signals, plus the recorded Article 6(3) claim. That claim does not automatically suppress every high-risk provision.
Requirements and operator duties	High-risk relevance plus recorded role where the particular rule needs it. The loader can include external-party roles; it is not exact attribution of every duty to the customer's own organisation.
FRIA	Latest completed, effectively required assessment and deployer role. An open Draft is not a completed answer.
Standards, conformity and registration	Recorded standards, route, certificates, declarations, marking, roles and use-case signals. A missing record may be unknown when its assessment was never answered.
Article 50	Separate interaction, synthetic-output, emotion, biometric, deepfake and public-interest-text facts with provider/deployer roles. Some newer flags on older records remain unknown rather than treating a legacy default as a deliberate no.
GPAI	Model-document scope and provider role. Merely selecting uses-GPAI does not emit Chapter V provider duties in this map, unlike some submission checks.
Monitoring and incidents	High-risk/provider relevance can be shown even when there are no monitoring or incident records.
Explanation	Relevant Annex III/deployer context, with conservative missing-input handling. There is no individual explanation-generation or request-response service.

Explicitly unsupported determinations

The map declares limits for the Article 2(13) requirements limitation; Article 5(1a)/(1b) foreseeable prohibited outcomes and specified intimate-material protections; Article 6(1a)/(1c) non-safety/assessment carve-outs; and the Article 42(3) Cyber Resilience Act presumption. Relevant facts are not structured sufficiently to determine those cases automatically.

Application-phase calculations use Brussels calendar dates and retain distinct phases where a system has both Annex I and Annex III populations. They can show upcoming, in force, transitional, unknown or mixed. Legacy placement, changes, public-authority use and GPAI have particular rules. Missing Annex X component information can leave a legacy case unresolved. These states concern legal timing, not dossier readiness.

The accompanying Responsibility Map provides the article-by-article view, including provisions outside the automated map. Neither an article reference nor a successful software check establishes legal completeness.

11 / Identity and classification

Start with a named system, a purpose, responsible parties and a recorded classification. A prohibited classification ends the submission assessment early; later checks are not all evaluated on that attempt.

Prohibited Classification

Identifier: ProhibitedClassification

Effect: Blocks submission.

Scope: The stated top-level branch. Open-FRIA, reassessment and limited-regime checks follow prohibited-practice early stops.

Finding: The recorded classification is Prohibited. Baseline checks and the prohibited-system cessation check run, then this branch stops the remaining submission assessment.

Legal context: Art. 5.

Prohibited Flag Classification Mismatch

Identifier: ProhibitedFlagClassificationMismatch

Effect: Blocks submission.

Scope: The stated top-level branch. Open-FRIA, reassessment and limited-regime checks follow prohibited-practice early stops.

Finding: The classification wizard records a prohibited practice, but the selected tier is not Prohibited. Baseline and cessation checks run before the remaining assessment stops.

Legal context: Art. 5.

Prohibited Sub Category Stale

Identifier: ProhibitedSubCategoryStale

Effect: Advisory calculated; not displayed in the current editor.

Scope: The stated top-level branch. Open-FRIA, reassessment and limited-regime checks follow prohibited-practice early stops.

Finding: Prohibited subcategory remains on a non-prohibited record, wizard prohibition is not yes, and exemption rationale is blank.

Legal context: Art. 5.

Article 2(2) limited regime identified

Identifier: Article22LimitedRegimeApplied

Effect: Advisory calculated; not displayed in the current editor.

Scope: The stated top-level branch. Open-FRIA, reassessment and limited-regime checks follow prohibited-practice early stops.

Finding: The dossier is High Risk, Annex I Section B is resolved, a product route is claimed and there is no Annex III signal. This identifies the limited-regime branch; the code label refers to Article 2(2), not Article 22. Its older message does not fully reflect amended Article 2(2).

Legal context: Article 2(2); current amended scope needs separate review.

Name Required

Identifier: NameRequired

Effect: Blocks submission.

Scope: Every tier, before a prohibited-practice early stop.

Finding: Name blank.

Legal context: Product record prerequisite.

Description Required

Identifier: DescriptionRequired

Effect: Blocks submission.

Scope: Every tier, before a prohibited-practice early stop.

Finding: Description blank.

Legal context: Product record prerequisite.

Intended Purpose Required

Identifier: IntendedPurposeRequired

Effect: Blocks submission.

Scope: Every tier, before a prohibited-practice early stop.

Finding: Intended purpose blank.

Legal context: Product record prerequisite.

Lifecycle Stage Required

Identifier: LifecycleStageRequired

Effect: Blocks submission.

Scope: Every tier, before a prohibited-practice early stop.

Finding: Lifecycle stage absent.

Legal context: Product record prerequisite.

Risk Classification Required

Identifier: RiskClassificationRequired

Effect: Blocks submission.

Scope: Every tier, before a prohibited-practice early stop.

Finding: Risk classification absent.

Legal context: Product record prerequisite; Art. 6 context.

Clarity Confirmation Required

Identifier: ClarityConfirmationRequired

Effect: Blocks submission.

Scope: Every tier, before a prohibited-practice early stop.

Finding: Clarity confirmation no.

Legal context: Product record prerequisite.

Responsible Party Required

Identifier: ResponsiblePartyRequired

Effect: Blocks submission.

Scope: Every tier, before a prohibited-practice early stop.

Finding: No responsible-party records.

Legal context: Product accountability prerequisite.

Responsible Party Incomplete

Identifier: ResponsiblePartyIncomplete

Effect: Blocks submission.

Scope: Every tier, before a prohibited-practice early stop.

Finding: Responsible-party record lacks role or nonblank display name; one message per record.

Legal context: Product accountability prerequisite.

Annex Area Or Derogation Required

Identifier: AnnexAreaOrDerogationRequired

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: No Annex III signal and no product-safety pathway claim; advisory despite code name.

Legal context: Art. 6.

12 / Transparency and disclosure

Article 50 duties can overlap the high-risk regime. These checks inspect recorded methods and statements. They do not add notices, labels or machine-readable marks to the external AI service.

Transparency Mechanism Required

Identifier: TransparencyMechanismRequired

Effect: Blocks submission.

Scope: Limited Risk or High Risk, including the Section B branch, after prohibited-practice early stops.

Finding: Transparency mechanism blank.

Legal context: Art. 13 / Art. 50 context.

Transparency Human Interaction Mechanism Required

Identifier: TransparencyHumanInteractionMechanismRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: Human Interaction flag set and transparency mechanism blank.

Legal context: Art. 50(1).

Transparency Synthetic Content Obligation Declaration Required

Identifier: TransparencySyntheticContentObligationDeclarationRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: Recorded output types imply synthetic generation, but Synthetic Content is not selected, and either marking is undocumented or the relevant deepfake disclosure is undocumented. This declaration check takes precedence over the detailed marking/disclosure findings.

Legal context: Art. 50(2), 50(4).

Transparency Synthetic Content Marking Required

Identifier: TransparencySyntheticContentMarkingRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: Synthetic Content is selected or an output type indicates generation; the preceding undeclared-obligation finding did not occur; and the marking method is blank.

Legal context: Art. 50(2).

Transparency Deep Fake Disclosure Required

Identifier: TransparencyDeepFakeDisclosureRequired

Effect: Blocks when the organisation has a recorded Deployer role, a referenced role cannot be resolved, or no recognised role is recorded at all. Otherwise it is an unshown advisory. External operators are excluded from own-role membership, but their recorded roles can affect these fallback checks..

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: The synthetic branch is reached without the undeclared-obligation finding; image, audio or video is selected (or Synthetic Content has no specified type); and deepfake disclosure is blank. A creative-work exception changes the requested wording but still needs limited disclosure.

Legal context: Art. 50(4).

Transparency Deep Fake Exemption Rationale Required

Identifier: TransparencyDeepFakeExemptionRationaleRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: The deepfake-capable synthetic branch applies, the creative-work exception is selected, and its rationale is blank.

Legal context: Art. 50(4).

Transparency Deep Fake Exemption Not Assessed

Identifier: TransparencyDeepFakeExemptionNotAssessed

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: The deepfake-capable synthetic branch applies and the exception question is unanswered.

Legal context: Art. 50(4).

Transparency Human Interaction Exemption Rationale Required

Identifier: TransparencyHumanInteractionExemptionRationaleRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: Human Interaction is selected, the exception is selected, and its rationale is blank. The exception does not suppress the separate mechanism requirement in this implementation.

Legal context: Art. 50(1).

Transparency Human Interaction Exemption Not Assessed

Identifier: TransparencyHumanInteractionExemptionNotAssessed

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: Human Interaction flag; exemption answer unanswered.

Legal context: Art. 50(1).

Public Interest Text Exemption Rationale Required

Identifier: PublicInterestTextExemptionRationaleRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: Synthetic Content or Text is selected, a public-interest-text exception is selected, and its rationale is blank.

Legal context: Art. 50(4).

Public Interest Text Exemption Not Assessed

Identifier: PublicInterestTextExemptionNotAssessed

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: Synthetic Content or Text is selected and the public-interest-text exception question is unanswered.

Legal context: Art. 50(4).

Transparency Emotion Recognition Disclosure Required

Identifier: TransparencyEmotionRecognitionDisclosureRequired

Effect: Blocks when the organisation has a recorded Deployer role, a referenced role cannot be resolved, or no recognised role is recorded at all. Otherwise it is an unshown advisory. External operators are excluded from own-role membership, but their recorded roles can affect these fallback checks..

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: Emotion Recognition flag; corresponding disclosure blank.

Legal context: Art. 50(3).

Transparency Biometric Categorisation Disclosure Required

Identifier: TransparencyBiometricCategorisationDisclosureRequired

Effect: Blocks when the organisation has a recorded Deployer role, a referenced role cannot be resolved, or no recognised role is recorded at all. Otherwise it is an unshown advisory. External operators are excluded from own-role membership, but their recorded roles can affect these fallback checks..

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: Biometric Categorisation flag; corresponding disclosure blank.

Legal context: Art. 50(3).

Transparency Info Timing Required

Identifier: TransparencyInfoTimingRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: Any transparency flag or synthetic-generation trigger; timing description blank.

Legal context: Art. 50(5).

Transparency Accessibility Compliance Required

Identifier: TransparencyAccessibilityComplianceRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: Any transparency flag or synthetic-generation trigger; accessibility description blank.

Legal context: Art. 50(5).

13 / Risk management and safeguards

Connect harms, affected people, treatment choices, safeguards and remaining risk. The numeric scales and consistency tests below are product rules, not statutory formulas or tests of actual effectiveness.

Risk Required

Identifier: RiskRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: No risk records.

Legal context: Art. 9.

Risk Without Mitigation

Identifier: RiskWithoutMitigation

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Risk has no risk-mitigation link; one message per such risk.

Legal context: Art. 9.

Mitigation Without Risk

Identifier: MitigationWithoutRisk

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Mitigation has no risk-mitigation link; one message per such mitigation.

Legal context: Art. 9.

Affected Group Required

Identifier: AffectedGroupRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: No affected-group records.

Legal context: Art. 9 / Art. 10.

Article 9 Harm Domain Required

Identifier: Art9HarmDomainRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Risks exist, but none is recorded against health, safety or fundamental-rights harm. The check examines the three recorded harm-domain answers, not the separate risk category or the actual risk analysis.

Legal context: Art. 9(2)(a)-(b).

Risk Category Required

Identifier: RiskCategoryRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Risk record has no category.

Legal context: Art. 9 context; product taxonomy requirement.

Article 9 Foreseeable Misuse Risk Required

Identifier: Art9ForeseeableMisuseRiskRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: No risk has Foreseeable Misuse usage context.

Legal context: Art. 9(2)(b).

Reasonably Foreseeable Misuse Not Described

Identifier: ReasonablyForeseeableMisuseNotDescribed

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Version-level foreseeable-misuse description blank.

Legal context: Art. 9(2)(b).

Article 9 Post Market Risk Reevaluation Due

Identifier: Art9PostMarketRiskReevaluationDue

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: An incident links to a risk and its last-modified time is later than that risk's last-modified time. This is a timestamp-based signal to revisit the risk, not an interpretation of the incident's significance.

Legal context: Art. 9(2)(c), Art. 72.

Article 9 Treatment Outcome Required

Identifier: Art9TreatmentOutcomeRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Statutory-harm risk has treatment outcome Not Set.

Legal context: Art. 9(3).

Article 9 Treatment Outcome Contradicts Harm Domain

Identifier: Art9TreatmentOutcomeContradictsHarmDomain

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Statutory-harm risk marked Outside Article 9 Scope.

Legal context: Art. 9(3).

Article 9 Overall Residual Risk Required

Identifier: Art9OverallResidualRiskRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Overall residual-risk assessment blank.

Legal context: Art. 9(5).

Article 9 Residual Risk Level Required

Identifier: Art9ResidualRiskLevelRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Statutory-harm risk lacks residual level.

Legal context: Art. 9(5).

Article 9 High Residual Risk Rationale Required

Identifier: Art9HighResidualRiskRationaleRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Risk residual at least 4 and acceptance rationale blank.

Legal context: Art. 9(5); product threshold 4 of 5.

Article 9 Residual Risk Exceeds Initial

Identifier: Art9ResidualRiskExceedsInitial

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Residual and initial severity exist, residual greater than initial severity.

Legal context: Art. 9(5); product consistency check.

Article 9 Residual Risk Above Best Mitigation

Identifier: Art9ResidualRiskAboveBestMitigation

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: The risk's recorded residual level exceeds the lowest residual level claimed by any linked mitigation that has a value. Review the consistency and meaning of both estimates; this arithmetic does not prove how measures interact.

Legal context: Art. 9(5); product consistency check.

Article 9 Design Elimination Not Recorded

Identifier: Art9DesignEliminationNotRecorded

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: A risk is recorded as mitigable through design; classified linked measures exist, but none is in the Design Elimination tier. Without resolved tier data, this advice is not emitted.

Legal context: Art. 9(5)(a).

Article 9 Information Measure Not Recorded

Identifier: Art9InformationMeasureNotRecorded

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: A risk is recorded as addressed by adequate information; classified linked measures exist, but none is in the Information and Training tier. Without resolved tier data, this advice is not emitted.

Legal context: Art. 9(5)(c).

Article 9 Information Measure Not Traceable

Identifier: Art9InformationMeasureNotTraceable

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Information and Training mitigation lacks literacy-record link.

Legal context: Art. 9(5)(c), Art. 4.

Article 9 Deployer Competence Profile Missing

Identifier: Art9DeployerCompetenceProfileMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Deployer competence profile blank.

Legal context: Art. 9(5).

Article 9 Combined Application Not Assessed

Identifier: Art9CombinedApplicationNotAssessed

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Cross-requirement interaction assessment blank.

Legal context: Art. 9(4).

Article 9 Overdue High Severity Mitigation

Identifier: Art9OverdueHighSeverityMitigation

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Target before today's UTC date, neither Implemented nor Verified, linked risk severity at least 4.

Legal context: Art. 9; product threshold 4 of 5.

Article 9 Residual Risk Rests On Unimplemented Measures

Identifier: Art9ResidualRiskRestsOnUnimplementedMeasures

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Risk residual recorded, links exist, all resolved linked mitigations neither Implemented nor Verified.

Legal context: Art. 9(5).

Risk Management Element Not Applicable

Identifier: RiskManagementElementNotApplicable

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Risk-management QMS element marked Not Applicable.

Legal context: Art. 17(1)(g).

Risk Management Procedure Reference Required

Identifier: RiskManagementProcedureReferenceRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Risk-management QMS record has neither notes nor evidence attachment.

Legal context: Art. 17(1)(g), Art. 9.

Vulnerable Group Societal Risk Advisory

Identifier: VulnerableGroupSocietalRiskAdvisory

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Minor/vulnerable groups but no Societal risk; method returns, skipping later FRIA advice.

Legal context: Art. 9(9).

Vulnerable Group Risk Mitigation Required

Identifier: VulnerableGroupRiskMitigationRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Societal risk links minor/vulnerable group but no mitigation.

Legal context: Art. 9(9).

Vulnerable Group FRIA Advisory

Identifier: VulnerableGroupFriaAdvisory

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Minor/vulnerable groups and Societal risk exist; latest completed FRIA effective requiredness not yes.

Legal context: Art. 27 context.

14 / Human oversight and literacy

Record the arrangements, people, competence and authority supporting human oversight. A training record, selected certificate or completed field is evidence for review, not proof of competence or an operational intervention mechanism.

Human Oversight Required

Identifier: HumanOversightRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: General human-oversight mechanism blank.

Legal context: Art. 14.

Fallback Plan Required

Identifier: FallbackPlanRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Fallback plan blank.

Legal context: Art. 14.

Oversight: anomaly-detection arrangements missing

Identifier: Oversight144aAnomalyDetectionMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Detailed anomaly-detection control blank.

Legal context: Art. 14(4)(a).

Oversight: automation-bias arrangements missing

Identifier: Oversight144bAutomationBiasMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Detailed automation-bias control blank.

Legal context: Art. 14(4)(b).

Oversight: interpretation tools missing

Identifier: Oversight144cInterpretationToolsMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Detailed output-interpretation control blank.

Legal context: Art. 14(4)(c).

Oversight: disregard or override arrangements missing

Identifier: Oversight144dDisregardOptionMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Detailed disregard/override control blank.

Legal context: Art. 14(4)(d).

Oversight: safe-halt arrangements missing

Identifier: Oversight144eSafeHaltMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Detailed safe-halt control blank.

Legal context: Art. 14(4)(e).

Oversight Split Missing

Identifier: OversightSplitMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Both provider and deployer human-oversight measures blank.

Legal context: Art. 14(3).

Accountability Role Required

Identifier: AccountabilityRoleRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: No accountability-role records.

Legal context: Art. 17.

Dual Person Verification Not Required

Identifier: DualPersonVerificationNotRequired

Effect: Blocks for the specific biometric subpoint; otherwise an unshown advisory for the broader unresolved biometric area..

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Two-person verification is not confirmed. The specific remote-identification subpoint blocks; a biometric area without a subpoint produces an unshown advisory. This is distinct from independent dossier approval.

Legal context: Art. 14(5).

Accountability Role Person Required

Identifier: AccountabilityRolePersonRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Accountability roles exist but none has linked person.

Legal context: Art. 26(2).

Accountability Role Training Incomplete

Identifier: AccountabilityRoleTrainingIncomplete

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Assigned role has training confirmation no.

Legal context: Art. 26(2) / Art. 4.

Accountability Role Competence Missing

Identifier: AccountabilityRoleCompetenceMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Assigned role has blank competence description.

Legal context: Art. 26(2).

Accountability Role Authority Missing

Identifier: AccountabilityRoleAuthorityMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Assigned role has blank authority scope.

Legal context: Art. 26(2).

AI literacy Record Recommended

Identifier: AiLiteracyRecordRecommended

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: No literacy records.

Legal context: Art. 4.

15 / Performance, robustness and cybersecurity

Make technical claims inspectable through recorded metrics and safeguards. The product does not run the tests. Its accuracy comparison assumes higher numbers are better and only runs when both values are supplied.

Accuracy Metric Required

Identifier: AccuracyMetricRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: No accuracy metric records.

Legal context: Art. 15.

Accuracy Metric Threshold Not Numeric

Identifier: AccuracyMetricThresholdNotNumeric

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Both threshold and measured value are supplied, including empty strings, but at least one cannot be read as an invariant-format decimal number. A missing value skips this comparison.

Legal context: Art. 9(8).

Accuracy Metric Below Threshold

Identifier: AccuracyMetricBelowThreshold

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Both recorded values parse as numbers and the measurement is below the threshold. This assumes that higher is better; it is not suitable without interpretation for lower-is-better metrics such as error rate.

Legal context: Art. 9(5).

Accuracy Metric Measured After Placement

Identifier: AccuracyMetricMeasuredAfterPlacement

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Market placement known; a metric measurement is after placement.

Legal context: Art. 9(8).

Accuracy Metric Not Measured Before Placement

Identifier: AccuracyMetricNotMeasuredBeforePlacement

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: The market-placement date is recorded and no metric has a measurement date strictly before it. A measurement on the same day does not satisfy this check.

Legal context: Art. 9(8).

Accuracy Target Required

Identifier: AccuracyTargetRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Accuracy target blank.

Legal context: Art. 15.

Robustness Measures Required

Identifier: RobustnessMeasuresRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Robustness measures blank.

Legal context: Art. 15.

Cybersecurity Measures Required

Identifier: CybersecurityMeasuresRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Cybersecurity measures blank.

Legal context: Art. 15.

Feedback Loop Mitigation Required

Identifier: FeedbackLoopMitigationRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Continues-learning-after-deployment or continuous-learning and feedback-loop mitigation description blank.

Legal context: Art. 15(4).

16 / Data governance

Document the assessment of data sources and the safeguards applied. For a system recorded as not using training techniques, per-source checks select Testing sources when at least one exists; otherwise all sources are examined. Version-level governance questions continue.

Data Source Required

Identifier: DataSourceRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: No data-source records.

Legal context: Art. 10.

Data Governance Assessment Required

Identifier: DataGovernanceAssessmentRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Data-governance assessment blank.

Legal context: Art. 10.

Data Governance Lineage Location Required

Identifier: DataGovernanceLineageLocationRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Data-governance lineage location blank.

Legal context: Art. 10.

Data Design Choices Required

Identifier: DataDesignChoicesRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Dataset design choices blank.

Legal context: Art. 10(2)(a).

Data Assumptions Required

Identifier: DataAssumptionsRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Dataset assumptions blank.

Legal context: Art. 10(2)(d).

Data Availability Assessment Required

Identifier: DataAvailabilityAssessmentRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Data-availability assessment blank.

Legal context: Art. 10(2)(e).

Bias Examination Required

Identifier: BiasExaminationRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Bias-examination description blank.

Legal context: Art. 10(2)(f).

Bias Mitigation Measures Required

Identifier: BiasMitigationMeasuresRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Both new bias-mitigation description and legacy bias assessment blank.

Legal context: Art. 10(2)(g).

Data Gaps Identified Required

Identifier: DataGapsIdentifiedRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Identified data-gaps description blank.

Legal context: Art. 10(2)(h).

Dataset Purpose Required

Identifier: DatasetPurposeRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate. If the system is recorded as not using training techniques and at least one Testing dataset exists, only Testing datasets are examined. Otherwise every recorded dataset is examined.

Finding: Assessable source has no dataset purpose.

Legal context: Art. 10(1), 10(6).

Data Preparation Operations Required

Identifier: DataPreparationOperationsRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate. If the system is recorded as not using training techniques and at least one Testing dataset exists, only Testing datasets are examined. Otherwise every recorded dataset is examined.

Finding: Assessable source has all six descriptions blank: annotation, labelling, cleaning, updating, enrichment, aggregation.

Legal context: Art. 10(2)(c).

Relevance Assessment Required

Identifier: RelevanceAssessmentRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate. If the system is recorded as not using training techniques and at least one Testing dataset exists, only Testing datasets are examined. Otherwise every recorded dataset is examined.

Finding: Assessable source relevance assessment blank.

Legal context: Art. 10(3).

Representativeness Required

Identifier: RepresentativenessRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate. If the system is recorded as not using training techniques and at least one Testing dataset exists, only Testing datasets are examined. Otherwise every recorded dataset is examined.

Finding: Assessable source representativeness blank.

Legal context: Art. 10(3).

Error Rate Assessment Required

Identifier: ErrorRateAssessmentRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate. If the system is recorded as not using training techniques and at least one Testing dataset exists, only Testing datasets are examined. Otherwise every recorded dataset is examined.

Finding: Assessable source error-rate assessment blank.

Legal context: Art. 10(3).

Completeness Assessment Required

Identifier: CompletenessAssessmentRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate. If the system is recorded as not using training techniques and at least one Testing dataset exists, only Testing datasets are examined. Otherwise every recorded dataset is examined.

Finding: Assessable source completeness assessment blank.

Legal context: Art. 10(3).

Geographic Contextual Scope Required

Identifier: GeographicContextualScopeRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate. If the system is recorded as not using training techniques and at least one Testing dataset exists, only Testing datasets are examined. Otherwise every recorded dataset is examined.

Finding: Assessable source geographical/contextual scope blank.

Legal context: Art. 10(4).

Non Training System Has No Testing Data Set

Identifier: NonTrainingSystemHasNoTestingDataSet

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: The uses-training-techniques answer no, sources exist, none Testing; explains fallback to full checks.

Legal context: Art. 10(6).

17 / Fundamental rights assessments

A FRIA is a separate assessment run. The product derives whether it is required from recorded classification, Annex III and deployer facts; keeps unresolved answers distinct from no; and permits a reasoned override. Completion and external notification are separate steps.

FRIA Draft Open

Identifier: FriaDraftOpen

Effect: Blocks submission.

Scope: The stated top-level branch. Open-FRIA, reassessment and limited-regime checks follow prohibited-practice early stops.

Finding: An open Draft FRIA exists for the dossier. The check uses the separately loaded assessment history and applies to any non-prohibited tier.

Legal context: Art. 27(2).

FRIA Reassessment Outstanding

Identifier: FriaReassessmentOutstanding

Effect: Blocks submission.

Scope: The stated top-level branch. Open-FRIA, reassessment and limited-regime checks follow prohibited-practice early stops.

Finding: A reassessment-due date is set and either the current facts do not establish that FRIA is unnecessary, or the latest completed assessment is effectively required. Any set date can trigger this check, including a future date.

Legal context: Art. 27(2).

FRIA Process Description Required

Identifier: FriaProcessDescriptionRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Latest Completed FRIA effectively required; process description blank.

Legal context: Art. 27(1)(a).

FRIA Duration Required

Identifier: FriaDurationRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Latest Completed FRIA effectively required; duration/frequency blank.

Legal context: Art. 27(1)(b).

FRIA Categories Required

Identifier: FriaCategoriesRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Latest Completed FRIA effectively required; affected persons blank.

Legal context: Art. 27(1)(c).

FRIA Risks Required

Identifier: FriaRisksRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Latest Completed FRIA effectively required; specific harm risks blank.

Legal context: Art. 27(1)(d).

FRIA Oversight Required

Identifier: FriaOversightRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Latest Completed FRIA effectively required; oversight blank.

Legal context: Art. 27(1)(e).

FRIA Mitigation Required

Identifier: FriaMitigationRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Latest Completed FRIA effectively required; mitigation/governance measures blank.

Legal context: Art. 27(1)(f).

FRIA Notification Pending

Identifier: FriaNotificationPending

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Latest Completed FRIA effectively required; notification status Not Started or In Progress.

Legal context: Art. 27(3).

FRIA Notification Evidence Missing

Identifier: FriaNotificationEvidenceMissing

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Latest Completed FRIA effectively required, notification Completed, date/method missing or date later than today's UTC date plus one day.

Legal context: Art. 27(3).

FRIA Notification Status Invalid

Identifier: FriaNotificationStatusInvalid

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Latest Completed FRIA effectively required; notification status neither Not Started, In Progress nor Completed, including Not Required.

Legal context: Art. 27(3).

Creditworthiness or insurance FRIA requirement overridden

Identifier: Article27ConditionBFriaRequiredOverridden

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: The current facts derive a required FRIA solely from creditworthiness or insurance use (Annex III 5(b)/(c)); the latest completed assessment is not effectively required; and a documented override says it is unnecessary. The override produces an advisory, rather than silently resolving the difference.

Legal context: Art. 27(1).

Article 27 FRIA Required Overridden

Identifier: Article27FriaRequiredOverridden

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: The current facts derive a required FRIA on the other applicable route; the latest completed assessment is not effectively required; and a documented override says it is unnecessary. This difference produces an advisory.

Legal context: Art. 27(1).

FRIA required for creditworthiness or insurance

Identifier: Article27ConditionBFriaRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: Fresh derivation yes solely from 5(b)/5(c), latest completed effective requiredness not yes, no documented no override.

Legal context: Art. 27(1).

Article 27 FRIA Required

Identifier: Article27FriaRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: Fresh derivation yes on other branch, latest completed effective requiredness not yes, no documented no override.

Legal context: Art. 27(1).

Public Authority Deployer FRIA Recommended

Identifier: PublicAuthorityDeployerFriaRecommended

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: Fresh requiredness unresolved and latest completed effective requiredness unanswered.

Legal context: Art. 27(1).

FRIA Deployer Party Missing

Identifier: FriaDeployerPartyMissing

Effect: Blocks submission.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: Real FRIA context supplied; high-risk, derivation flags non-point-2 Annex III, no deployer party.

Legal context: Art. 27(1).

Section5 Deployer FRIA Recommended

Identifier: Section5DeployerFriaRecommended

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: High-risk, point 5 but no subpoint, FRIA not already derived required.

Legal context: Art. 27(1), Annex III 5(b)-(c).

18 / Technical documentation and instructions

The rules below examine selected structured content, typed records and evidence references. A complete presence check does not establish the adequacy of an Annex IV technical file or instructions for use.

Technical Document Required

Identifier: TechnicalDocumentRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: No technical-document records.

Legal context: Art. 11.

Technical Document Attachment Required

Identifier: TechnicalDocumentAttachmentRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: No single technical-document record has Title, document type and attachment reference all present.

Legal context: Art. 11.

Instructions Performance For Groups Missing

Identifier: InstructionsPerformanceForGroupsMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Affected groups exist and group-performance instruction confirmation no.

Legal context: Art. 13(3)(b)(v).

Annex IV point 2(b) Design Specification Incomplete

Identifier: Annexlv2bDesignSpecificationIncomplete

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Any of six fields blank: general logic, design choices, classification choices, optimisation target, expected outputs, trade-offs.

Legal context: Annex IV 2(b).

Annex IV point 1 General Description Incomplete

Identifier: Annexlv1GeneralDescriptionIncomplete

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Any of external interactions, software version, distribution method, user-interface description blank.

Legal context: Annex IV 1.

Annex IV point 2(c) Development Compute Missing

Identifier: Annexlv2cDevelopmentComputeMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Development compute description blank.

Legal context: Annex IV 2(c).

Annex IV point 2(f) Continuous Compliance Solutions Missing

Identifier: Annexlv2fContinuousComplianceSolutionsMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Continuous-compliance solutions blank.

Legal context: Annex IV 2(f).

Annex IV point 2(g) Validation Procedure Missing

Identifier: Annexlv2gValidationProcedureMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Validation/testing procedure blank.

Legal context: Annex IV 2(g).

Annex IV point 2(g) Test Log Reference Missing

Identifier: Annexlv2gTestLogReferenceMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Test-log reference blank.

Legal context: Annex IV 2(g).

Annex IV point 2(g) Test Report Signature Incomplete

Identifier: Annexlv2gTestReportSignatureIncomplete

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Exactly one of the recorded test-report signer and signature date is present. Either missing half can produce the same identifier.

Legal context: Annex IV 2(g).

Annex IV point 2(g) Test Report Unsigned

Identifier: Annexlv2gTestReportUnsigned

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Test-log reference present but neither signer nor signature date supplied.

Legal context: Annex IV 2(g).

Annex IV point 1(f) Product Illustration Missing

Identifier: Annexlv1fProductIllustrationMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Safety-component indicator yes and no attached Product Illustration typed document.

Legal context: Annex IV 1(f).

Annex IV Checklist Attestation Outruns Structured Capture

Identifier: AnnexlvChecklistAttestationOutrunsStructuredCapture

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: A technical document claims Annex IV sub-item coverage in free text, while fewer than 6 of 13 selected structured fields are completed. This is a heuristic prompt, not a legal completeness threshold.

Legal context: Annex IV.

Annex IV Declaration Copy Missing

Identifier: AnnexlvDeclarationCopyMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: No declaration element marked addressed and no signed declaration attachment.

Legal context: Annex IV 8.

Annex IV Risk Management Description Required

Identifier: AnnexlvRiskManagementDescriptionRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: No attached Risk-management Documentation typed record.

Legal context: Annex IV 5, Art. 9.

Annex IV Sections Incomplete

Identifier: AnnexIvSectionsIncomplete

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: At least one of 13 remaining document types has no attached record. Instructions for Use and Risk-management Documentation are checked separately. The finding lists the missing types.

Legal context: Annex IV.

Instructions Provider Identity Required

Identifier: InstructionsProviderIdentityRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Provider-identity instruction confirmation no.

Legal context: Art. 13(3)(a).

Instructions Accuracy Required

Identifier: InstructionsAccuracyRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Accuracy instruction confirmation no.

Legal context: Art. 13(3)(b)(ii).

Instructions Degradation Circumstances Required

Identifier: InstructionsDegradationCircumstancesRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Performance-degradation circumstances blank.

Legal context: Art. 13(3)(b)(ii).

Instructions Harm Scenarios Required

Identifier: InstructionsHarmScenariosRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Harm-scenario instruction confirmation no.

Legal context: Art. 13(3)(b)(iii).

Instructions Data Specs Advisory

Identifier: InstructionsDataSpecsAdvisory

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Input-data specification instruction confirmation no.

Legal context: Art. 13(3)(b)(vi).

Instructions Interpretability Advisory

Identifier: InstructionsInterpretabilityAdvisory

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Both explainability capabilities and interpretability features blank.

Legal context: Art. 13(3)(b)(iv), 13(3)(b)(vii).

Instructions Pre Determined Changes Advisory

Identifier: InstructionsPreDeterminedChangesAdvisory

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Pre-determined changes blank.

Legal context: Art. 13(3)(c).

Instructions Human Oversight Required

Identifier: InstructionsHumanOversightRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Human-oversight instruction confirmation no.

Legal context: Art. 13(3)(d).

Instructions Lifetime And Maintenance Required

Identifier: InstructionsLifetimeAndMaintenanceRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Any of resources, expected lifetime or maintenance description blank.

Legal context: Art. 13(3)(e).

Instructions Log Mechanisms Advisory

Identifier: InstructionsLogMechanismsAdvisory

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Any of log collection, storage or interpretation mechanisms blank.

Legal context: Art. 13(3)(f).

Instructions For Use Document Required

Identifier: InstructionsForUseDocumentRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: No attached Instructions for Use typed technical-document record.

Legal context: Art. 13(2).

Instructions Format And Accessibility Not Declared

Identifier: InstructionsFormatAndAccessibilityNotDeclared

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Delivery format or accessibility description blank.

Legal context: Art. 13(2).

Instructions Authorised Representative Required

Identifier: InstructionsAuthorisedRepresentativeRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Authorised-representative party exists but corresponding instruction confirmation not yes.

Legal context: Art. 13(3)(a).

19 / Quality management

Quality-management records cover 13 named elements. A recorded Financial Institution sectoral regime narrows the Not Addressed check to Risk Management, Post-market Monitoring and Incident Reporting. All 13 types still need records, and the three retained types cannot simply be marked Not Applicable. The sectoral answer is not independent proof that Article 17(4) applies. The product does not operate or certify the organisation's quality management system.

The 13 recorded elements are compliance strategy; design and development techniques; quality control; testing; specifications; data management; risk management; post-market monitoring; incident reporting; authority communication; record keeping; resource management; and the accountability framework. Each has its own recorded status and supporting material.

QMS Reference Required

Identifier: QmsReferenceRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: QMS reference blank.

Legal context: Art. 17.

QMS Coverage Required

Identifier: QmsCoverageRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: QMS coverage confirmation no.

Legal context: Art. 17.

QMS Element Not Addressed

Identifier: QmsElementNotAddressed

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: A QMS element is Not Addressed. With Financial Institution selected as the sectoral regime, this status check still covers Risk Management, Post-market Monitoring and Incident Reporting; ten other element types are treated as fulfilled for this check. Other or unanswered regimes check all types. The separate missing-element check still requires records for all 13 types.

Legal context: Art. 17(1), 17(4).

QMS Elements Incomplete

Identifier: QmsElementsIncomplete

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: At least one of the 13 named quality-management element types has no record. Existing rows do not substitute for the missing type.

Legal context: Art. 17(1)(a)-(m).

QMS elements that cannot be treated as not applicable

Identifier: Art174NonDeemedElementNotApplicable

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Post-market Monitoring or Incident Reporting record marked Not Applicable; all high-risk versions, not just financial institutions.

Legal context: Art. 17(1)(h)-(i), 17(4).

20 / Logging, retention and review dates

These controls describe operational logging and documentation-retention arrangements and keep review dates visible. AICMS does not collect the AI's operational logs or guarantee that records are retained.

Log Storage Location Required

Identifier: LogStorageLocationRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Log storage location blank.

Legal context: Art. 12 / Art. 19.

Log Retention Required

Identifier: LogRetentionRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: No retention-period lookup and free-text period blank.

Legal context: Art. 19(1).

Log Retention Below Minimum

Identifier: LogRetentionBelowMinimum

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Effective retention months below 6; lookup duration takes precedence, then numeric months, then parsable text.

Legal context: Art. 19(1).

Log Retention Unverifiable

Identifier: LogRetentionUnverifiable

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: No lookup or numeric months and nonblank free-text period cannot parse.

Legal context: Art. 19(1).

Logging Coverage Unconfirmed

Identifier: LoggingCoverageUnconfirmed

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Any of risk-situation, post-market or operation-monitoring logging confirmations no.

Legal context: Art. 12(2).

Biometric Logging Fields Incomplete

Identifier: BiometricLoggingFieldsIncomplete

Effect: Blocks for the specific biometric subpoint; otherwise an unshown advisory for the broader unresolved biometric area..

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: One or more of four biometric logging details is blank: use period, reference database, input leading to a match and identities of verifying people. The specific remote-identification subpoint blocks; a biometric area without a subpoint produces an unshown advisory.

Legal context: Art. 12(3).

Retention Until Not Aligned

Identifier: RetentionUntilNotAligned

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Placement known; retention date absent or different from placement plus 10 calendar years.

Legal context: Art. 18.

Risk Review Schedule Required

Identifier: RiskReviewScheduleRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Neither next review date nor nonblank review frequency.

Legal context: Art. 9(2).

Risk Review Overdue

Identifier: RiskReviewOverdue

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Next risk review date before today's UTC date.

Legal context: Art. 9(2).

21 / Conformity, declarations and certificates

Record the selected conformity route, declarations, certificate decisions and supporting material. Internal dossier approval is separate from conformity assessment, regulatory approval, certification and CE marking.

CE marking Format Required

Identifier: CeMarkingFormatRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: CE-marking format absent.

Legal context: Art. 48.

CE marking Date Required

Identifier: CeMarkingDateRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: CE marked applied but date absent.

Legal context: Art. 48.

Conformity Assessment Route Required

Identifier: ConformityAssessmentRouteRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Conformity route absent.

Legal context: Art. 43.

Conformity Assessment Record Required

Identifier: ConformityAssessmentRecordRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: The selected Internal Control route has no internal-control record, or the Notified Body route has no external-assessment record with an assessment stage. These are alternative triggers for the same identifier.

Legal context: Art. 43.

Conformity Assessment Completion Required

Identifier: ConformityAssessmentCompletionRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Conformity completion confirmation no.

Legal context: Art. 43.

Sectoral Conformity Procedure Missing

Identifier: SectoralConformityProcedureMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Annex I selected, not Section B, and sectoral procedure reference blank.

Legal context: Art. 43(3).

Integrated Documentation Required For Section A

Identifier: IntegratedDocumentationRequiredForSectionA

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Resolved Section A, integrated-sectoral-file confirmation no.

Legal context: Art. 11(2).

Integrated Documentation Reference Required

Identifier: IntegratedDocumentationReferenceRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Resolved Section A, integrated-file confirmation yes but reference blank.

Legal context: Art. 11(2).

Declaration Required

Identifier: DeclarationRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: No declaration elements.

Legal context: Art. 47, Annex V.

Declaration Element Not Addressed

Identifier: DeclarationElementNotAddressed

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Unconditional declaration element unaddressed.

Legal context: Art. 47, Annex V.

Declaration Not Applicable Reason Required

Identifier: DeclarationNotApplicableReasonRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Conditional personal-data-law or notified-body element unaddressed without a reason.

Legal context: Art. 47, Annex V.

Declaration Content Required

Identifier: DeclarationContentRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Element addressed but content blank.

Legal context: Art. 47, Annex V.

Article 6(1) route and recorded tier differ

Identifier: Article61PathwayNotHighRisk

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: Product pathway claimed by flag/Annex I selection but tier not High Risk; advisory then method return.

Legal context: Art. 6(1).

Annex I legislation needed for the product route

Identifier: Article61AnnexILegislationRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: High-risk product pathway claimed without Annex I legislation.

Legal context: Art. 6(1)(a).

Evidence of the product assessment route needed

Identifier: Article61ThirdPartyConformityRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: A High Risk product route is claimed, but none of the following is recorded: Notified Body route, notified-body number, or general conformity-completed confirmation. Any one satisfies this particular product check; it is not proof that Article 6(1) is met.

Legal context: Art. 6(1)(b).

Certificate Lifecycle Event Lacks Justification

Identifier: CertificateLifecycleEventLacksJustification

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: Lifecycle event new status not Active, reason blank and evidence absent.

Legal context: Art. 44.

Certificate Language Not Recorded

Identifier: CertificateLanguageNotRecorded

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: Certificate language or issuing Member State blank.

Legal context: Article 44(2); source message still cites 44(1).

22 / Registration and Article 6 exceptions

Registration preparation depends on role and classification facts. Some checks use broader signals than the package builder or legal applicability map. Read each scope carefully and verify the actual Article 49 route before filing externally.

EU database Section A Member State Required

Identifier: EuDbSectionAMemberStateRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: High Risk, an Annex III signal and a provider party are recorded; Annex III membership is not resolved exclusively to critical infrastructure point 2; and the Member States of availability are blank.

Legal context: Art. 49(1), Annex VIII A.10.

EU database Submitter Required

Identifier: EuDbSubmitterRequired

Effect: Blocks submission.

Scope: Outside prohibited-practice early stops and the product-only Annex I Section B branch, any of these recorded situations: (1) High Risk, an Annex III signal, a provider party, and Annex III membership not resolved exclusively to critical infrastructure point 2; (2) a public-authority deployer; (3) a non-High-Risk tier, an Annex III signal and an Article 6(3) condition other than Not Applicable. An Annex III signal includes actual area records, relevant wizard/uses-Annex-III answers or profiling. Roles here can include external parties.

Finding: Within the scope above, no designated submitter party.

Legal context: Art. 49, Annex VIII.

EU database Single Submitter Required

Identifier: EuDbSingleSubmitterRequired

Effect: Blocks submission.

Scope: Outside prohibited-practice early stops and the product-only Annex I Section B branch, any of these recorded situations: (1) High Risk, an Annex III signal, a provider party, and Annex III membership not resolved exclusively to critical infrastructure point 2; (2) a public-authority deployer; (3) a non-High-Risk tier, an Annex III signal and an Article 6(3) condition other than Not Applicable. An Annex III signal includes actual area records, relevant wizard/uses-Annex-III answers or profiling. Roles here can include external parties.

Finding: Within the scope above, more than one designated submitter.

Legal context: Product responsibility rule for Art. 49.

EU database Electronic Instructions Advisory

Identifier: EuDbElectronicInstructionsAdvisory

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: High Risk, an Annex III signal, a provider party, and Annex III membership not resolved exclusively to critical infrastructure point 2, no areas 1/6/7, suppression flag no, electronic instructions URL blank.

Legal context: Annex VIII A.12.

EU database Electronic Instructions Restricted Area

Identifier: EuDbElectronicInstructionsRestrictedArea

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: High-risk, any area 1/6/7, electronic instructions URL present.

Legal context: Art. 49(4), Annex VIII A.12.

Article 49(1) Registration Advisory

Identifier: Article491RegistrationAdvisory

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: High Risk, an Annex III signal, a provider party, and Annex III membership not resolved exclusively to critical infrastructure point 2; status neither In Progress nor Registered.

Legal context: Art. 49(1).

Profiling with a non-high-risk tier

Identifier: Article63ProfilingBlocksDerogation

Effect: Blocks submission.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: The tier is not High Risk and profiling is recorded. The implementation blocks this combination even without an explicit Article 6(3) exception claim, so its trigger is broader than the identifier alone suggests.

Legal context: Art. 6(3).

Derogation Reasoning Required

Identifier: DerogationReasoningRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: Article 6(3) exception claimed yes and reasoning blank.

Legal context: Art. 6(3)-(4).

Derogation Claimed Contradicts High Risk Tier

Identifier: DerogationClaimedContradictsHighRiskTier

Effect: Blocks submission.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: Derogation claimed with High Risk tier.

Legal context: Art. 6(3)-(4).

EU database Section B Article 6(3) Condition Required

Identifier: EuDbSectionBArticle63ConditionRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: Non-high-risk, Annex III signal, Article 6(3) condition Not Applicable.

Legal context: Art. 6(3), Annex VIII B.

EU database Section B Article 6(3) Justification Required

Identifier: EuDbSectionBArticle63JustificationRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: Non-high-risk, Annex III signal, condition selected, justification blank.

Legal context: Art. 6(4), Annex VIII B.

Article 49(2) Registration Advisory

Identifier: Article492RegistrationAdvisory

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: Non-high-risk, Annex III signal, registration status text blank.

Legal context: Art. 49(2).

EU database Section C Provider Entry Url Required

Identifier: EuDbSectionCProviderEntryUrlRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: High-risk, public-authority deployer, provider entry URL blank.

Legal context: Annex VIII C.3.

EU database Section C FRIA Outcome Summary Required

Identifier: EuDbSectionCFriaOutcomeSummaryRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: High-risk, public-authority deployer, latest completed FRIA outcome summary blank.

Legal context: Annex VIII C.4.

EU database Section C Dpia Advisory

Identifier: EuDbSectionCDpiaAdvisory

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: High-risk, public-authority deployer, DPIA summary and URL both blank.

Legal context: Annex VIII C.5.

EU database Section C Deployer Registration Advisory

Identifier: EuDbSectionCDeployerRegistrationAdvisory

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: High-risk public-authority deployer; deployer status neither In Progress nor Registered.

Legal context: Art. 49(3).

EU database Registration Reference Without Submission Record

Identifier: EuDbRegistrationReferenceWithoutSubmissionRecord

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: Registration reference present but submission date absent.

Legal context: Art. 49.

EU database Re Registration Advisory On Substantial Modification

Identifier: EuDbReRegistrationAdvisoryOnSubstantialModification

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: Provider or deployer marked Registered and a modification requires reassessment.

Legal context: Art. 43(4), Art. 49.

23 / Operators, agreements and modifications

The supply-chain record supports accountable handovers and role-specific evidence. A selected role or checklist answer does not establish that all legal duties of that party have been performed.

Provider Organization Required

Identifier: ProviderOrganizationRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Provider party organisation blank; one message per provider.

Legal context: Art. 16 / Art. 13(3)(a).

Provider Address Required

Identifier: ProviderAddressRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Provider party address blank; one message per provider.

Legal context: Art. 16 / Art. 13(3)(a).

Authorised Representative Mandate Missing

Identifier: AuthorisedRepresentativeMandateMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: High-risk, no mandate with representative-party reference; no third-country gate.

Legal context: Art. 22.

Importer Checklist Incomplete

Identifier: ImporterChecklistIncomplete

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: Importer present and no checklist or any recorded item unverified; expected item-type completeness not compared.

Legal context: Art. 23.

Distributor Checklist Incomplete

Identifier: DistributorChecklistIncomplete

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: Distributor present and no checklist or any recorded item unverified; expected item-type completeness not compared.

Legal context: Art. 24.

Value Chain Agreement Recommended

Identifier: ValueChainAgreementRecommended

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: Modification has any modification trigger, no value-chain agreement.

Legal context: Art. 25.

Handover Information Pending

Identifier: HandoverInformationPending

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, except the product-only Annex I Section B limited branch; apply the specific condition below.

Finding: Modification has any modification trigger, no handover-information confirmation.

Legal context: Art. 25.

Substantial Modification Reassessment Required

Identifier: SubstantialModificationReassessmentRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: A modification requires reassessment and both the reassessment date and outcome are missing. Either field alone passes this check, although a complete assessment record should explain the result and its date.

Legal context: Art. 43(4).

24 / Incidents, corrective action and emergency use

Record events and actions, review timing, and preserve the basis for follow-up. The encoded incident categories are not an automatic legal classification. Reports, authorisations and real-world corrective measures remain external actions.

Monitoring Metric Required

Identifier: MonitoringMetricRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Monitoring performance-metric description blank.

Legal context: Art. 72.

Monitoring Frequency Required

Identifier: MonitoringFrequencyRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Monitoring frequency blank.

Legal context: Art. 72.

Withdrawal Recall Procedure Required

Identifier: WithdrawalRecallProcedureRequired

Effect: Blocks submission.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Corrective-action/withdrawal/recall procedure blank.

Legal context: Art. 20(1).

Corrective Action Overdue

Identifier: CorrectiveActionOverdue

Effect: Advisory calculated; not displayed in the current editor.

Scope: High Risk in a recognised built-in category, except the product-only Annex I Section B limited branch. Usually no separate provider/deployer role gate.

Finding: Planned/In Progress corrective action has recorded action date before today's UTC date; aggregated count.

Legal context: Art. 20.

Prohibited Practice Still On Market

Identifier: ProhibitedPracticeStillOnMarket

Effect: Blocks submission.

Scope: The prohibited-classification or conflicting prohibited-answer branch.

Finding: Prohibition branch, On the Market or In Service, no action typed Cessation/Withdrawal/Recall/Disable. Action status/outcome not examined.

Legal context: Art. 5.

Incident Approaching Reporting Deadline

Identifier: IncidentApproachingReportingDeadline

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: Unreported incident dynamically Approaching or Overdue.

Legal context: Art. 73.

Incident Awareness Date Before Incident Date

Identifier: IncidentAwarenessDateBeforeIncidentDate

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: Both dates recorded, awareness date before incident date.

Legal context: Art. 73; input consistency.

Emergency Authorisation Conformity Incomplete

Identifier: EmergencyAuthorisationConformityIncomplete

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: Prior Authorisation granted, not withdrawn, conformity incomplete.

Legal context: Art. 46(1).

Emergency Authorisation Refused Use Not Stopped

Identifier: EmergencyAuthorisationRefusedUseNotStopped

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: Urgency Use refused; use-stop date absent or results not discarded.

Legal context: Art. 46(2).

Emergency Authorisation Annex I Sectoral

Identifier: EmergencyAuthorisationAnnexISectoral

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: Any emergency authorisation plus product-pathway flag or Annex I selection.

Legal context: Art. 46(7).

25 / General-purpose AI

GPAI documentation belongs to the system version. The ordinary wizard is available only in High Risk or Prohibited dossiers. Several provider-style submission checks follow the uses-GPAI answer rather than a model-provider role; three other checks have independent triggers.

GPAI Annex XI technical documentation required

Identifier: GpaiAnnexXITechDocRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, including the Section B branch, with uses-GPAI selected. The first model-document record is used; there is no model-provider role gate.

Finding: The uses-GPAI-model answer, no open-source/non-systemic exemption, first GPAI document missing tasks or architecture.

Legal context: Art. 53(1)(a), Annex XI.

GPAI Training Content Summary Required

Identifier: GpaiTrainingContentSummaryRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, including the Section B branch, with uses-GPAI selected. The first model-document record is used; there is no model-provider role gate.

Finding: The uses-GPAI-model answer; first GPAI record does not confirm publication or has neither summary nor URL; open source does not waive.

Legal context: Art. 53(1)(d).

GPAI Downstream Info Missing

Identifier: GpaiDownstreamInfoMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch, with uses-GPAI selected. The first model-document record is used; there is no model-provider role gate.

Finding: The uses-GPAI-model answer, no open-source/non-systemic exemption; first GPAI record has no downstream URL, technical means or integration types.

Legal context: Art. 53(1)(b), Annex XII.

GPAI Copyright Policy Missing

Identifier: GpaiCopyrightPolicyMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch, with uses-GPAI selected. The first model-document record is used; there is no model-provider role gate.

Finding: The uses-GPAI-model answer; first GPAI record has neither policy description nor URL; open source does not waive.

Legal context: Art. 53(1)(c).

GPAI Designation Notification Missing

Identifier: GpaiDesignationNotificationMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch, with uses-GPAI selected. The first model-document record is used; there is no model-provider role gate.

Finding: The uses-GPAI-model answer, stored systemic classification, no designation notification.

Legal context: Art. 52(1).

GPAI Designation Notification Late

Identifier: GpaiDesignationNotificationLate

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch, with uses-GPAI selected. The first model-document record is used; there is no model-provider role gate.

Finding: The uses-GPAI-model answer, stored systemic, notification date later than recorded deadline.

Legal context: Art. 52(1).

GPAI Designation Notification Deadline Missing

Identifier: GpaiDesignationNotificationDeadlineMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch, with uses-GPAI selected. The first model-document record is used; there is no model-provider role gate.

Finding: The uses-GPAI-model answer, stored systemic, Not Started designation notification lacks deadline.

Legal context: Art. 52(1).

GPAI Reassessment Requested Too Early

Identifier: GpaiReassessmentRequestedTooEarly

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch, with uses-GPAI selected. The first model-document record is used; there is no model-provider role gate.

Finding: The uses-GPAI-model answer, stored systemic, reassessment request before recorded Commission decision plus six months.

Legal context: Art. 52(5).

GPAI Model Evaluation Missing

Identifier: GpaiModelEvaluationMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch, with uses-GPAI selected. The first model-document record is used; there is no model-provider role gate.

Finding: The uses-GPAI-model answer, stored systemic; first GPAI record has none of evaluation protocol, adversarial testing, results or evidence.

Legal context: Art. 55(1)(a).

GPAI Systemic Risk Assessment Missing

Identifier: GpaiSystemicRiskAssessmentMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch, with uses-GPAI selected. The first model-document record is used; there is no model-provider role gate.

Finding: The uses-GPAI-model answer, stored systemic, no systemic-risk assessment records.

Legal context: Art. 55(1)(b).

GPAI Serious Incident Unreported

Identifier: GpaiSeriousIncidentUnreported

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch, with uses-GPAI selected. The first model-document record is used; there is no model-provider role gate.

Finding: The uses-GPAI-model answer, stored systemic, any GPAI serious incident lacks AI Office reported date.

Legal context: Art. 55(1)(c).

GPAI Systemic Risk Classification Mismatch

Identifier: GpaiSystemicRiskClassificationMismatch

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: The first model-document record suggests systemic risk from compute, high-impact capability or Commission designation, but the stored classification is not systemic. It does not change the classification automatically and does not require the uses-GPAI answer.

Legal context: Art. 51.

GPAI Systemic Cybersecurity Required

Identifier: GpaiSystemicCybersecurityRequired

Effect: Blocks submission.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: The stored GPAI classification is systemic and both the model-protection and infrastructure-protection descriptions are blank. Either description alone passes this check. It does not require the uses-GPAI answer.

Legal context: Art. 55(1)(d).

GPAI Authorised Representative Missing

Identifier: GpaiAuthorisedRepresentativeMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: The first model-document record identifies a third-country provider, no open-source/non-systemic exception applies, and there is no representative-party reference. It does not require the uses-GPAI answer.

Legal context: Art. 54.

26 / Transitional provisions

A recorded transition and deadline support planning. Establish the actual legal conditions, applicable dates and system history independently.

Transitional Provision Deadline Missing

Identifier: TransitionalProvisionDeadlineMissing

Effect: Advisory calculated; not displayed in the current editor.

Scope: Non-prohibited tiers, including the Section B branch; apply the specific condition below.

Finding: Transitional-provision answer yes, deadline absent.

Legal context: Art. 111.