

EU AI Act & ISO/IEC 42001 Governance Decision Map



IG-Smart Ltd · Practical Guide Collection · 25 October 2026

General information and original working aids; not legal advice, certification, clinical authorisation or regulatory approval.
NHS identity appearing in retained illustrative artwork does not imply NHS approval or endorsement.

Use this guide to make a better-evidenced decision. This is general information and an original working aid, not a client-specific legal opinion, certification, clinical safety authorisation or regulatory approval. Apply the relevant jurisdiction, current requirements and competent professional review to your circumstances. Examples are illustrative unless expressly attributed.

Your first three steps

1. Describe one real AI use, its users and the role your organisation performs.
2. Record the applicable law and effective date rather than assuming all AI has the same duties.
3. Use the seven gates and companion workbook to identify missing evidence and accountable decisions.

An enterprise guide to AI Act applicability, operator responsibilities, AI management systems, evidence readiness and board decisions

Executive answer: one AI programme, multiple distinct legal and governance questions

A UK organisation can have a credible AI management system and still be unable to demonstrate that a particular EU-facing product meets the EU AI Act. Conversely, a product team may complete a specific AI Act conformity process without establishing a sufficiently mature enterprise-wide governance system for all its other AI uses.

The distinction matters because the two instruments have different purposes:

- **The EU AI Act** is a legal regime. Whether particular duties apply depends on the system or model, intended purpose, operator role, territorial facts, relevant risk or use category, exceptions, transitions and the date each provision applies. Some duties already apply in October 2026 while certain high-risk system requirements have later application dates. [S1][S2]
- **ISO/IEC 42001:2023** specifies requirements for establishing, implementing, maintaining and improving an artificial intelligence management system (AIMS). An organisation can adopt it to govern AI development, supply and use, and may seek voluntary third-party certification. The standard does not itself grant an AI Act exemption, legal approval, product conformity or a CE mark. ISO does not issue organisations' certificates. [S4][S5]
- **Privacy, cyber security, clinical safety and sector-specific regimes** may apply in parallel. A GDPR data protection impact assessment, an AI Act fundamental-rights impact assessment and an AI management-system impact assessment can inform one another but do not become the same statutory document merely by sharing a risk register. [S6][S7][S8]

The critical buyer question: For this specific AI system, organisation, jurisdiction and point in time, what legally applies; who is responsible; what evidence exists; and what decision remains open? Enterprise AIMS governance should help the organisation answer and monitor those questions, not replace them.

Inside this guide: The original IG-Smart Seven-Gate AI Governance Decision Map; the October 2026 legal timeline; provider/deployer/GPAI role matrix; risk classification and territorial applicability pathways; practical legal-to-AIMS evidence crosswalk; GDPR/DPIA/FRIA distinctions; 16-check evidence register; supplier due-diligence questions; board briefing; six applied scenarios; buyer FAQs; source register and an editable companion assessment worksheet.

1. Read the current application timeline and verify the operative law

Regulation (EU) 2024/1689 entered into force on 1 August 2024. The European Commission's current implementation timeline reports revised application dates of 2 December 2027 for Annex III high-risk systems and 2 August 2028 for Annex I product-related high-risk systems, taking account of Digital Omnibus amendments. These dates are a guidance-based planning reference: confirm the applicable final legal text, commencement, transitional provisions and operator role before treating a date as a legal deadline for a particular system. [S1][S2][S3]

Milestone	Position at 24 October 2026	Practical question for the buyer
1 Aug 2024	AI Act entered into force	Is the product, business unit or contract within the Act's potential territorial and material scope?
2 Feb 2025	General definitions, prohibited-practice provisions and AI literacy provisions started applying	Have prohibited uses and relevant AI literacy measures been assessed? Verify the applicable current AI literacy duties.
2 Aug 2025	General-purpose AI (GPAI) model-provider obligations began applying, subject to transitions and exceptions	Is the organisation actually a GPAI model provider , as distinct from a user of a model or an AI system provider?
2 Aug 2026	Commission-reported milestone for further provisions, including transparency; verify operative applicability	Do chatbots, synthetic content or specific biometric/emotion systems trigger transparency measures?
2 Dec 2026	Commission-reported milestone for new prohibitions; verify operative provisions and case applicability.	Are near-term remediation and communication controls required?
2 Dec 2027	Commission-reported planning date: applicable Annex III high-risk AI system provisions	Is an Annex III use case in scope, and what must be implemented by the relevant date?
2 Aug 2028	Commission-reported planning date: Annex I product-related high-risk provisions	Does AI form part of a product subject to listed EU harmonisation legislation, such as a potentially qualifying medical device?

This table is a **high-level planning aid**, not a complete transition analysis. Article 111 and other transitional provisions, exceptions, and the precise role or system category may change the answer. Dates should be verified from the updated EU AI Act Service Desk immediately before client use. [S1][S2][S3]

Governance implication: Different cohorts may require immediate action, future-readiness work, or monitoring rather than identical 'EU AI Act compliant by August 2026' programmes. A current readiness assessment should clearly label obligations as applicable now, applicable later, outside scope on established facts, or legal clarification required.

2. The IG-Smart Seven-Gate AI Governance Decision Map

This is an **original IG-Smart practitioner framework**, not the European Commission's classification tool or an ISO-prescribed assessment. It turns a vague question—'Are we AI compliant?'—into a traceable management decision. A separately editable worksheet follows the same steps.

Gate	Decision to establish	Evidence to retain	Stop / escalation trigger
G1 – System identity	What is the AI system/model, intended purpose, configuration, deployment context and material change history?	AI inventory, owner, architecture summary, intended-use statement, vendor chain	Unknown system purpose or undocumented consequential use
G2 – Operator role	Are we provider, deployer, importer, distributor, product manufacturer, authorised representative or GPAI model provider? Could we hold more than one role?	Role rationale, product branding, licences, contractual responsibility map	'We only use a vendor' asserted despite substantial modification/rebranding
G3 – Territorial scope	Why might EU AI Act apply, even if a party is UK-based? What exclusions apply?	Market, establishment, customer, output-use and jurisdiction record	EU use/output nexus not analysed
G4 – Legal classification	Are prohibited practices implicated? Is it Annex I or Annex III high-risk, or subject to distinct transparency/GPAI provisions?	Classification memo, purpose, Annex checks, exceptions and legal reviewer	Potential prohibited practice or disputed high-risk classification
G5 – Effective obligations	Which article-level duties apply now, later or not at all, including transitions?	Dated obligation register, commencement source, accountable owner	Wrong deadline, reliance on superseded law, or material unknown
G6 – Evidence architecture	Can an AIMS and system-level evidence demonstrate the relevant requirements without conflating them?	Risk log, controls, impact assessments, documentation, monitoring and supply-chain records	Policy exists but operational proof is absent; certification substituted for product conformity
G7 – Executive decision	Who approves continued deployment, remediation, escalation, procurement or withdrawal; what triggers re-review?	Decision paper, signed risk ownership, exceptions, next review triggers	Unresolved material safety/fundamental-rights issue or unowned obligation

Outputs: (1) applicability position with uncertainties, (2) legal and voluntary-control register, (3) evidence readiness view, (4) role-specific remediation programme, (5) defensible executive decision and trigger-based review schedule.

The seven gates are **not a maturity score or compliance grade**. Do not convert 'seven gates passed' into a claim of legal compliance, accredited ISO certification or regulatory approval.

Accessible decision-tree reading path

- 1. Can you identify the system and its intended use?** If not, stop and establish inventory, purpose and owner.
- 2. Does an EU AI Act territorial connection exist?** If uncertain, obtain legal classification; the UK location of a supplier is not decisive by itself.
- 3. What is your legal role?** A single corporate group can have multiple roles for different products, deployments and models.
- 4. Do any prohibited practices apply?** Escalate immediately; do not treat a policy waiver or ISO control as permission to carry out a prohibited activity.
- 5. Does the system satisfy Article 6 Annex I or Annex III routes?** Record any exclusions, filters and source of classification; if neither, still assess applicable transparency and other obligations.

6. **Are GPAI model-provider obligations implicated separately?** If yes, use that branch, even if the same undertaking also provides an AI system.
7. **Which requirements are in force and what evidence supports each?** Map controls to legal duties, ownership and real implementation records.
8. **Is the organisation prepared to make an accountable decision?** Record limitations, mitigations, approvals and reassessment triggers.

The companion worksheet follows the same decision sequence and provides fields for recording the evidence, reviewer and decision at each gate.

3. First determine what is being governed: model, system or use case

The AI Act distinguishes a **general-purpose AI model** from an **AI system** and defines different operator obligations. Calling every generative application a 'GPAI provider' obscures the obligations of the underlying model developer, downstream AI system provider and deployer. [S1][S9]

A minimal AI inventory should capture:

- The business process and decision influenced by AI; intended purpose and reasonably foreseeable use or misuse.
- Whether the subject is an AI system, an underlying general-purpose model, or an ordinary software component that may not meet the statutory AI-system definition.
- Legal entity, customer and users; EU market/access/output use; affected individuals.
- Build-versus-buy and contractual chain; model and system versions; hosting, data transfers, suppliers and integrations.
- Whether the system is used for employment, education, credit, healthcare, law enforcement or another context with potentially heightened obligations.
- Human oversight arrangements, impact assessment position, change controls and date of first market placement/use.
- Who can suspend operation when evidence is inadequate.

Practitioner warning: A model's marketing label ('low-risk', 'explainable', 'responsible', 'EU-ready') does not establish legal classification. Classification follows the Act's definitions, intended purpose, factual deployment and relevant exceptions, not a vendor badge.

4. Operator responsibilities: one organisation may occupy several roles

Role / position	Indicative situation	Core questions and likely evidence	Do not infer
AI system provider	Develops or has developed a system placed on the EU market or put into service under its name or trademark	Purpose, risk classification, product documentation, applicable high-risk duties and conformity pathway	That contracting out development transfers all provider obligations
AI system deployer	Uses an AI system under its authority in a business context	Instructions, input-data responsibility, competent oversight, monitoring, incident handling, data protection	That vendor certification fully discharges local deployment responsibilities

Role / position	Indicative situation	Core questions and likely evidence	Do not infer
Importer / distributor	Makes a qualifying system available in the Union through relevant supply arrangements	Chain of supply, declarations, provider records, procedural requirements	That reseller status necessarily eliminates all responsibility
Product manufacturer	Markets a product incorporating a relevant AI system or safety component under its own brand	Annex I legislation, product conformity integration and AI component role	That every medical AI feature is automatically high-risk under Annex I
GPAI model provider	Places a qualifying general-purpose AI model on the EU market	Model documentation, downstream information, copyright policy, training-content summary, systemic-risk assessment where applicable	That a company merely calling an LLM API is the model provider
Authorised representative	Accepts a relevant written mandate for an in-scope non-EU provider	Nature and limits of mandate; applicable documentation/cooperation duties	That a DPO or EU GDPR Article 27 representative is automatically the AI Act representative
Downstream system provider	Integrates a general-purpose model into its own marketed system	Both contract and statutory role allocation; own system risks and user information	That upstream documentation proves downstream system conformity

A deployer, importer, distributor or third party can become the **provider of a high-risk AI system** in specified circumstances, including certain changes of intended purpose, substantial modifications or marketing under its own name/trademark. Article 25 requires a facts-and-role analysis rather than reliance on the contract's label. [S10]

Contracting rule of thumb: Put legal roles and practical evidence-delivery duties in a supplier responsibility schedule. A vendor may promise help with records and incidents, but its contract cannot make a statutory duty disappear.

5. Territorial scope: UK incorporation is not a blanket exemption

The Act reaches, among others, relevant providers placing AI systems or general-purpose models on the EU market, EU-based deployers and certain third-country providers/deployers where AI-system output is used in the EU. It also addresses specified supply-chain and representative roles. Exceptions and context matter. [S11]

Scenario	First-pass position	Required follow-up
UK SaaS supplier markets an AI-enabled decision tool to EU customers	Potentially in scope	Determine actual AI-system status, intended purpose, provider role, market facts and relevant obligations
UK company uses AI internally; outputs are used only in UK	EU AI Act may be outside scope on known facts	Test third-country output use, EU presence, other roles, changes and UK law; do not claim global exemption
UK employer applies AI recruitment ranking to EU-located candidates	Strong territorial and Annex III classification questions	Legal and HR review, purpose and role analysis, safeguards, effective dates
EU affiliate deploys a third-party AI system	Deployers in EU can have direct obligations	Determine high-risk status and specific deployment duties; supplier obligations remain separate

Scenario	First-pass position	Required follow-up
UK developer offers a model through EU channels	GPAI model-provider scope requires examination	Distinguish model versus system, exceptions, documentation and EU representation where relevant
EU hospital uses UK-supplied AI in a medical device	May engage the AI Act and separate medical-device/clinical-safety regimes	Establish Annex I route and applicable product classification, certification and transitional rules

Escalation condition: If a cross-border interpretation materially changes go-live, financing or a procurement submission, obtain a documented, appropriately qualified legal determination instead of resolving uncertainty through an internal risk score.

6. Risk classification is not a single four-colour label

The EU AI Act includes prohibited practices, high-risk system obligations, transparency obligations for specified systems and separate GPAI model-provider duties. An enterprise governance programme should record these **distinct applicability pathways**. A single 'low/medium/high' enterprise risk matrix may help management prioritisation, but it is not itself an Article 6 legal classification. [S1][S12]

6.1 Prohibited-practice screen

Review Article 5 against the actual use case and applicable amendments. If a prohibited practice is plausibly triggered, the decision is not merely whether mitigations reduce a numerical risk rating; legal permissibility must be addressed. The Commission reports a **2 December 2026** milestone for new prohibitions; verify operative provisions and case applicability. [S2][S3]

6.2 Annex I product route

Article 6(1) looks to specified product/safety-component uses covered by listed Union harmonisation legislation, including relevant third-party product conformity assessment conditions. The precise device/product facts matter. It would be inaccurate to treat every clinical AI application as automatically high-risk under this route. The Commission timeline reports **2 August 2028** for applicable Annex I high-risk requirements; verify operative provisions and transitions. [S2][S12]

Check the operative Article 6 product/safety-component conditions, any exclusions and relevant third-party assessment requirements against the actual product and consequences of failure. Do not infer classification from its marketing description. [S12]

6.3 Annex III use-case route

Article 6(2) and Annex III identify sensitive-use categories. Check the full wording, including the Article 6(3) filter and exceptions, rather than deciding based on a sector label alone. An AI tool used by a hospital for appointment scheduling may differ materially from one making consequential patient-care recommendations. The Commission timeline reports **2 December 2027** for applicable Annex III high-risk requirements; verify operative provisions and transitions. [S2][S12]

6.4 Transparency and GPAI are separate branches

Certain AI systems face disclosure/marketing obligations under Article 50 even if they are not classified high-risk. Distinct Article 53 obligations apply to qualifying GPAI model providers; additional measures may apply to systemic-risk GPAI models under Article 55. Do not import those duties wholesale onto every organisation that licenses an external model. [S9][S13]

Minimum classification memorandum: Product, intended purpose, operator roles, territory, statutory route, applicable article, exceptions/filter, transition, approving legal reviewer, supporting material and next review trigger.

7. What ISO/IEC 42001 contributes — and where it stops

ISO/IEC 42001:2023 provides an AIMS through which an organisation can structure responsibilities, policy, objectives, assessment of AI risks and impacts, lifecycle controls, monitoring, internal review and continual improvement. It is designed for organisations providing or using AI-based services and products. [S4][S5]

Its advantage is **management-system continuity**: an enterprise can apply repeatable governance beyond a single product or regulation, connecting system-level risk ownership to board oversight and the organisation's broader controls.

Its limitation is equally important: **ISO/IEC 42001 adoption or certification is not EU AI Act conformity assessment, CE marking or proof that any particular AI system complies with all applicable legal duties**. Certification is a voluntary choice except insofar as a buyer, contract or other independent arrangement imposes expectations. The legal effect of standards in a specific regulatory conformity mechanism must be separately verified; ISO 42001 should not automatically be described as an EU-harmonised standard giving an AI Act presumption of conformity. [S4][S5][S14]

7.1 AIMS evidence that is genuinely worth retaining

- Approved AI governance policy and scope; inventory and ownership.
- Objectives and decision rights covering AI development, procurement and deployment.
- Methodology for identifying and assessing AI risks, impacts, opportunities and relevant legal/contractual requirements.
- Control selection and implementation records covering data, transparency, human oversight, change and supplier dependencies.
- Competence/AI literacy measures and relevant training evidence.
- Monitoring, internal evaluation, incidents, corrective action and management review.
- Documented exceptions, owners and reassessment triggers.

Evidence threshold: A template or policy document is not the same as proof that a specific deployed model has been tested, monitored or lawfully placed on the EU market.

8. AI Act-to-AIMS governance evidence crosswalk

The following is IG-Smart's **non-normative interpretative crosswalk**, designed to help evidence owners organise work. It is not a reproduction of ISO/IEC 42001's licensed requirements and not a clause-by-clause legal equivalence table. SMEs must validate detailed cross-references against the current legal text and licensed standard before using it for an assessment.

Assurance domain	EU AI Act question, if applicable	Potential AIMS contribution	System-level evidence still needed
Leadership and accountability	Who holds provider/deployer/model-provider obligations?	Roles, objectives and escalation governance	Approved role determination, RACI, decisions
System inventory and purpose	What system and uses are being assessed?	AI asset inventory, use policy	Model/system version and intended-use specification
Territorial/legal applicability	Which jurisdictions, roles, dates and articles apply?	Legal-obligations identification and change monitoring	Signed, dated applicability analysis
High-risk classification	Does Article 6/Annex I/III apply?	Consistent classification workflow	Product/use-case legal memo, exceptions and evidence
Risk management	What foreseeable harms require control under Article 9?	Risk methodology, owners and mitigation cycle	System-specific hazards, tests, residual-risk decision
Data governance	Are data governance requirements relevant under Article 10?	Data controls, stewardship and quality	Dataset provenance, suitability, bias/quality tests
Technical documentation	What documentation must provider maintain?	Document control and review	Appropriate Article 11/Annex IV product file
Logging and traceability	Can relevant events be recorded and reviewed?	Operational logging policy	System logs, retention and access evidence
Transparency/instructions	What disclosures and instructions are mandated?	Communications and procurement controls	Actual notices, marking, operator instructions
Human oversight	Can authorised people effectively supervise and intervene?	Accountability, competence and escalation	Human factors evaluation, override/stop tests
Accuracy, robustness and cyber	Are performance and security requirements met?	Test governance, monitoring, incident response	Test protocols, measured performance, security evidence
Supplier/model chain	Is there usable assurance from upstream vendors?	Supplier selection and monitoring	Model cards, licences, integration limits, incident commitments
FRIA/DPIA and other impacts	Which legally required assessments apply?	Impact-review processes and traceability	Approved distinct statutory assessments as applicable
Change/incident monitoring	How will drift or material change be controlled?	Corrective action, management review	Version-trigger logs, monitoring, regulatory reporting evidence
Conformity/registration	Has the correct statutory conformity path been completed?	Programme and evidence management	Appropriate assessment, declaration, CE/registration evidence where required

Do not publish a green 'compliant' badge based only on this crosswalk. Requirements and implementation may differ by role, system and effective date. The legal and technical assessor must judge sufficiency.

9. Who must produce which evidence?

Evidence or activity	Typical owner	Other contributors	Important boundary
AI inventory and intended use	Accountable product/business owner	Engineering, procurement, AI governance	Inventory is not legal classification

Evidence or activity	Typical owner	Other contributors	Important boundary
EU AI Act role/scope analysis	Legal/regulatory lead	Product, privacy, commercial, local EU counsel	Must be facts-specific and dated
Enterprise AIMS policy and governance	Executive management	AI governance officer, risk, security, DPO	Certification is optional and separate from statutory conformity
High-risk provider technical file	Qualifying AI system provider	Engineering, test, safety, legal	Deployers need relevant information but do not automatically own provider technical documentation
Human oversight in deployment	Deployer, where obligations apply	Provider instructions, business lead, safety	Real operational authority and training matter
GPAI model documentation	Qualifying GPAI model provider	Model engineering, legal, downstream providers	Using a GPAI API does not automatically confer model-provider status
Fundamental-rights impact assessment	In-scope Article 27 deployer	Legal, business, equality/fundamental-rights experts	Article 27 applies to specified deployers/use cases, not every AI user
GDPR DPIA	Relevant controller under applicable GDPR	DPO, privacy, processors and affected teams	Not replaced by an ISO AI impact assessment
Medical-device/clinical safety assurance	Applicable manufacturer and deployer entities	Clinical safety, quality, privacy and technical experts	Preserve sectoral legal and safety responsibilities
Deployment decision	Accountable executive or authorised governance forum	Regulatory, technical, privacy, safety	Advisers do not accept management risk on the client's behalf

10. GDPR DPIA, AI Act FRIA and an AI impact assessment: related, not identical

Organisations often attempt to save time by producing one document labelled 'AI DPIA'. That can obscure different statutory triggers, subjects and ownership.

Assessment	Primary focus	Legal trigger / applicability	Decision owner
GDPR DPIA	High-risk processing of personal data; data-subject rights and freedoms	Where the relevant GDPR Article 35 criteria apply; UK and EU GDPR positions must be assessed separately	Data controller, advised by DPO where applicable
EU AI Act Article 27 FRIA	Impacts on fundamental rights from specified high-risk AI deployments	Specified public/public-service and certain other deployers of specified Annex III high-risk systems, subject to exceptions	Relevant deployer
Enterprise AI impact assessment	Wider safety, ethics, operational, societal, strategic and business impacts	Internal governance standard, contractual requirement or chosen methodology; not by itself a single universally mandated EU form	Accountable business and AI governance owner
ISO/IEC 42001 governance review	Adequacy and operation of an organisation's AIMS	Organisation's adopted AIMS scope and certification arrangements	AIMS management and independent reviewer where appropriate

Relevant GDPR DPIA evidence may inform an applicable FRIA, but **does not automatically eliminate remaining FRIA elements**. The Article 27 assessment applies to specified categories of deployers and systems rather than all 'high-risk AI' in every context. UK ICO guidance remains relevant where processing of personal data triggers a UK GDPR DPIA. [S6][S7]

A practical combined evidence schedule

1. Create a **common facts register**: identity, actors, purpose, architecture, data flows and affected people.
2. Maintain **separate applicability decisions**: EU AI Act, EU GDPR, UK GDPR, clinical/product/sector rules.
3. Reuse verified common evidence by reference rather than copy uncontrolled versions across documents.
4. Record the **distinct legal questions** each assessment must answer and any assessment-specific consultation or notification.
5. Put unresolved risks before the authorised decision-maker; do not treat positive performance testing as legal authorisation.

11. Six representative scenarios: use facts, not categorical labels

These scenarios are **fictional illustrations** and not client case studies, legal opinions or claims of previous IG-Smart delivery.

Scenario A — UK HealthTech company selling an AI clinical system into the EU

The company supplies software that may inform clinical decisions. The first task is to establish whether this product falls under applicable medical-device law, whether it contains a qualifying AI system or safety component, what EU market activity occurs and which Annex I/Annex III route is relevant. An AIMS can support governance, but medical-device conformity, clinical risk management, privacy and relevant AI Act obligations require specific evidence and professional review. **Do not label every clinical system high-risk without testing Article 6.**

Scenario B — EU hospital deploys a third-party clinical AI product

The hospital may have **deployer-side** duties and local patient-safety, clinical governance and privacy responsibilities. Supplier documents are necessary but cannot substitute for safe integration, workforce oversight and deployment-specific risk decisions. Assess whether a statutory FRIA is triggered rather than assuming it is always mandatory for healthcare.

Scenario C — UK enterprise deploys a general-purpose chatbot

The organisation uses a vendor's external model to draft customer replies. The firm is not necessarily the GPAI **model provider**. Examine its own operator role, EU nexus, Article 50 transparency where applicable, UK GDPR/privacy and operational safeguards. ISO/IEC 42001 can provide broader enterprise oversight even where no Annex III high-risk classification arises.

Scenario D — HR supplier changes an AI recruitment tool for EU customers

Recruitment may engage Annex III rules, depending on the intended use and exclusions. Record whether the modification changes the system's intended purpose or creates Article 25 provider consequences. Maintain discrimination and data-protection analysis; do not use the extended 2027 application date to justify ignoring already-applicable prohibitions or other laws.

Scenario E — Financial services group procures credit-scoring AI

Credit-related Annex III classification and financial-sector responsibilities require careful checking. The group must distinguish the model provider, system provider and deployer, then identify whether specific Article 27 FRIA or related rules apply. Financial regulatory governance and privacy requirements continue in parallel; ISO/IEC 42001 is supportive but not a substitute.

Scenario F — Enterprise changes an LLM model version after go-live

The company changes the underlying model, retrieval data and prompt controls. Re-open intended-use assumptions, testing, bias/quality, privacy, cybersecurity, human oversight and supplier arrangements. Reassess whether the organisation's legal role or relevant classification has changed. Retain a reproducible change/decision trail rather than assuming the old vendor statement covers the new system.

12. Sixteen-check evidence readiness checklist

Use status: Present / Partial / Missing / Not applicable (with reason). Each evidence item needs an accountable owner, source, date and review trigger.

A. Inventory, roles and classification

- [] A1. Unique AI system/model identifier, intended purpose, owner and version.
- [] A2. Provider/deployer/GPAI/supply-chain role assessment for each relevant legal entity.
- [] A3. EU territorial nexus and exceptions analysis supported by facts.
- [] A4. Dated Article 5, Article 6 and transparency/GPAI applicability review.

B. Governance, risk and people

- [] B1. AI policy, scope and accountable executive decision forum.
- [] B2. Risk and impact assessment method applied to this use case.
- [] B3. Human oversight, competence and intervention arrangements tested.
- [] B4. AI literacy measures and any applicable role-specific training recorded.

C. Technical and supplier assurance

- [] C1. Data governance, provenance, rights and representative-testing records.
- [] C2. Model/system performance, robustness and cybersecurity evidence suitable for purpose.
- [] C3. Supplier documentation, intended-use constraints and contractual responsibilities retained.
- [] C4. Change, incident, monitoring, logging and post-market processes mapped to the actual role.

D. Law and defensibility

- [] D1. Article-by-article applicability and effective-date register reviewed.
- [] D2. GDPR DPIA, FRIA and sectoral assessments completed where genuinely required.

- [] D3. Conformity, marking, registration or model-provider records retained where applicable.
- [] D4. Board or delegated executive acceptance, open risks, dependencies and review triggers documented.

The **companion worksheet** expands these into a 36-check, owner-assigned evidence register with an accountability and review record. Neither checklist is a statutory certificate.

13. Supplier procurement: 16 due-diligence questions boards should insist upon

1. Is the product an AI system under the Act, and what is its **intended purpose**? Show the basis of that determination.
2. Which party is provider, deployer, importer, distributor, model provider or authorised representative in each market?
3. What is the Article 2 territorial analysis for our actual EU/UK operations and output use?
4. Which Article 5 prohibitions were screened; when and by whom?
5. What supports the Annex I/III high-risk determination and any exclusion or Article 6(3) decision?
6. Which obligations apply now, in December 2026, in December 2027 or in August 2028?
7. What technical documentation, system descriptions, instructions and limitations can the supplier share?
8. Which training, validation, robustness and bias measurements are relevant to the proposed deployment?
9. How is human oversight implemented and can the deployer meaningfully suspend or override the system?
10. Which inputs and outputs are logged, for how long, and who has lawful access?
11. How do model changes, prompt updates, retrieval corpus changes and system integrations trigger reassessment?
12. Which personal-data, confidentiality, IP and cross-border transfer issues arise?
13. What provider/deployer notification and response commitments apply to serious incidents?
14. Is the vendor's ISO/IEC 42001 claim a documented AIMS adoption, valid independent certification or merely aspiration? What is its scope?
15. Where relevant, what statutory conformity/registration evidence exists or remains pending due to future applicability dates?
16. What exceptions, remediation commitments and unacceptable residual risks require our management decision before procurement or deployment?

Procurement rule: Do not accept 'EU AI Act compliant' as an unqualified sales statement. Require it to resolve into particular legal roles, articles, dates, systems and evidence.

14. Board briefing: a one-page decision record

Subject: [AI system / programme name and version] **Decision date / sponsor:** [date / accountable person]
Proposed activity: [develop / market / procure / deploy / substantially change / suspend] **Territorial footprint:** [EU countries / UK / output location / supply chain]

A. The legal position

- AI-system and GPAI model status: [documented / uncertain]
- Our relevant operator role(s): [list with legal entities]
- EU AI Act legal scope: [in / out on facts / unresolved]
- Potential prohibited practice: [no on checked facts / yes / uncertain — escalate]

- Classification: [Annex I / Annex III / Article 50 / GPAI / other / pending]
- Dates and transition rules: [actual article-level decisions, source date]

B. Evidence and controls

- AIMS governance record: [owner, policy, review]
- System-level technical and supplier evidence: [source and completeness]
- Privacy/FRIA/sectoral assessment: [applicability and status]
- Human oversight and suspension: [named roles, test evidence]
- Material gaps and residual risk: [high consequence first]

C. Management decision

- ☐ Proceed on documented basis ☐ Proceed only after specified conditions ☐ Defer ☐ Suspend / stop
- Conditions, owners and dates: ☐
- Formal legal/regulatory advice required? [yes/no; rationale]
- Accountable decision-maker and signature: ☐
- Trigger for reassessment: [new EU geography / provider rebrand / material model change / incident / enforcement guidance / new law milestone]

Board warning: A checked worksheet is not approval. The decision-maker must receive sufficient evidence and retain actual responsibility for the authorised action.

15. How to turn findings into an implementable AI governance programme

IG-Smart's approved sequence **Assess → Build → Manage → Assure → Improve** is a useful way to organise governance work, without promising that every phase is included in every engagement.

Phase	Governance decision	Illustrative outputs where contracted
Assess	What systems, roles, legal regimes and gaps exist?	Inventory review, applicability register, role matrix, evidence gap assessment
Build	Which accountabilities, policies and controls are missing?	AIMS governance architecture, supplier roles, risk and assessment workflows
Manage	Who maintains evidence and responds to change?	Review cadence, issue ownership, control monitoring and supplier assurance
Assure	What has actually been implemented and is it suitable for purpose?	Independent or appropriately separated evaluation, evidence scrutiny, board reporting
Improve	How will future versions, uses and regulations change the programme?	Corrective actions, revisions and reassessment triggers

Not every organisation needs ISO/IEC 42001 certification; not every AI Act regime is already in force; and no consultancy assessment substitutes for accredited certification or a legally mandated product conformity process.

Right next action by buyer circumstance

- **'We are unsure whether the EU AI Act applies.'** Commission a defined-scope role, territory and system applicability assessment, with legal escalation where required.

- **'Our board needs evidence before deploying AI.'** Identify existing AIMS, system testing, impact assessment, suppliers, human oversight and decision records.
- **'Our enterprise customer requires ISO 42001.'** Confirm whether the contract asks for alignment, an independently issued certificate, the scope of certification or specific controls.
- **'We use third-party LLM services.'** Separate model-provider assurances from your own governance and downstream product/deployer responsibilities.
- **'We have high-risk systems.'** Confirm Article 6 classification, operator role, applicable commencement, provider/deployer duties and conformity route without assuming all requirements were due in August 2026.

Discuss the next step: [AI Governance Assessment](#) addresses a defined organisational review; [AI Impact Assessment](#) focuses on a particular use. Discuss continuing governance needs separately with IG-Smart. Scope, practitioner competence, deliverables and any independent-assurance boundary are agreed before work begins. This guide does not claim completed ISO/IEC 42001-specific client engagements or certification outcomes.

16. Frequently asked enterprise questions

Does UK incorporation mean the EU AI Act does not apply?

No. The Act can apply to relevant third-country providers and deployers in specified circumstances, including EU market activity and AI-system outputs used in the Union. Establish the particular Article 2 facts and exceptions. [S11]

Does ISO/IEC 42001 certification prove EU AI Act compliance?

No. ISO/IEC 42001 certification concerns an AIMS with a defined scope; it is not the AI Act's product conformity assessment, declaration, marking or registration, nor a universal legal compliance opinion. [S4][S5][S14]

Is every AI system used in healthcare automatically high-risk?

No. Check the AI-system definition, intended use, relevant Annex I product conditions, Annex III use cases and any exceptions. Medical-device and clinical safety obligations may still apply independently. [S12]

Are the AI Act's high-risk requirements already in force in October 2026?

The Commission timeline reports Annex III and Annex I high-risk planning dates of **2 December 2027** and **2 August 2028**, respectively. Other AI Act obligations are already applicable. Transitional provisions and circumstances must be checked. [S2][S3]

Is a DPIA the same as a fundamental-rights impact assessment?

No. They have different scope and triggers. Where Article 27 applies, check the operative requirements separately; shared DPIA evidence does not eliminate remaining FRIA elements. [S6][S7]

Does use of an external LLM make us the model provider?

Not merely because the organisation is a customer or API user. However, own system-provider, deployer and contractual responsibilities must be assessed, and modifications may affect roles. [S9][S10]

What AI literacy measures should an organisation consider?

Assess and maintain relevant AI literacy measures for the actual people, roles and system context. Verify current Article 4 duties and any operative amendments; do not delay an applicable duty on the basis of a planning summary. [S15]

Must we certify to ISO 42001 before selling to the EU?

The AI Act does not impose a blanket ISO/IEC 42001 certification mandate. Buyers can separately stipulate contractual standards or certification expectations. Confirm the contract's language and who may certify. [S4][S5]

Does the AI Act replace GDPR, cyber requirements or medical-device law?

No. Applicable legal regimes interact. A rigorous programme maps responsibilities without claiming that one assessment discharges all the others. [S6][S7][S8]

What is the minimum useful output of an AI governance gap analysis?

A scoped inventory, factual role and territorial assessment, dated obligation register, specific evidence gaps, accountable owner, remediation priorities and a defensible executive decision. A generic red/amber/green dashboard is insufficient without its supporting basis.

17. Sources and regulatory currency

The citations above point to primary sources or regulator guidance. Source summaries are explanatory; **the current legislation takes precedence** over a guide, blog or vendor claim. Check the current legal text when making a new deployment or procurement decision, and retain the version used.

How to keep this decision current

Changes in law or guidance can leave older content with inaccurate dates or overstated legal requirements. For this topic, annual review alone is insufficient: set **event-triggered review** for EU law or Commission guidance changes, decisions affecting scope or use, and relevant standards revisions.

Sources

- [S1] EUR-Lex — Regulation (EU) 2024/1689; confirm operative amendments and transitions separately. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- [S2] European Commission - AI Act application dates (Article 113). <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-113>
- [S3] European Commission - AI Act regulatory framework and implementation. <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>
- [S4] ISO - ISO/IEC 42001:2023 catalogue and scope. <https://www.iso.org/standard/42001>
- [S5] ISO - ISO/IEC 42001 explained. <https://www.iso.org/insights/iso-42001-explained>
- [S6] European Commission - Article 27: fundamental rights impact assessment. <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-27>
- [S7] ICO - AI accountability and governance. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/what-are-the-accountability-and-governance-implications-of-ai>

- [S8] European Commission - Article 26: deployer obligations. <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-26>
- [S9] European Commission - Article 53: general-purpose AI model providers. <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-53>
- [S10] European Commission - Article 25: responsibilities along the value chain. <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-25>
- [S11] European Commission - Article 2: scope. <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-2>
- [S12] European Commission - Article 6: high-risk classification. <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-6>
- [S13] European Commission - Article 50: transparency. <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-50>
- [S14] European Commission - Article 16: provider obligations. <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-16>
- [S15] European Commission - Article 4: AI literacy. <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-4>
- [S16] European Commission - general principles for high-risk classification (references draft guidance). <https://ai-act-service-desk.ec.europa.eu/en/general-principles-classification-high-risk-ai-systems>
- [S17] European Commission - official EU AI Act implementation timeline, accounting for 2026 Digital Omnibus amendments. <https://ai-act-service-desk.ec.europa.eu/en/ai-act/eu-ai-act-implementation-timeline>