CLOUDFRAMEWORK · JOINT WHITE PAPER

Co-authored · CLOUDFRAMEWORK + LAWORATORY

How to build governable AI systems under the EU AI Act

A practical guide for CEOs, CTOs, DPOs and compliance officers who want to deploy AI seriously within the European regulatory framework — from **inventory** to **operational controls**.

Edition: May 2026 **Co-authorship:** CLOUDFRAMEWORK (technical layer) + LAWORATORY (legal layer)

Scope: Companies operating in the European Union

1 · REGULATORY CONTEXT

Regulation (EU) 2024/1689 and the risk-based approach

Regulation (EU) 2024/1689 sets harmonized rules on artificial intelligence and adopts a **risk-based approach**. It distinguishes, among others, between AI system providers, deployers (those responsible for use), providers of general purpose AI models (GPAI), importers and distributors.

Within this framework, an organization that develops, integrates, configures or puts AI-based solutions into service may take on **different regulatory obligations depending on its role in the value chain**. Misjudging one's own role is the most expensive starting mistake: it determines virtually every obligation that will end up applying.

CLOUDFRAMEWORK's role

CLOUDFRAMEWORK acts as a platform that enables its clients to **develop, integrate, govern and operate AI systems** connected to third-party general purpose AI models. CLOUDFRAMEWORK therefore positions itself as a **technical layer of governance, security, traceability and operational control** that helps organizations manage AI systems in accordance with the Regulation's requirements.

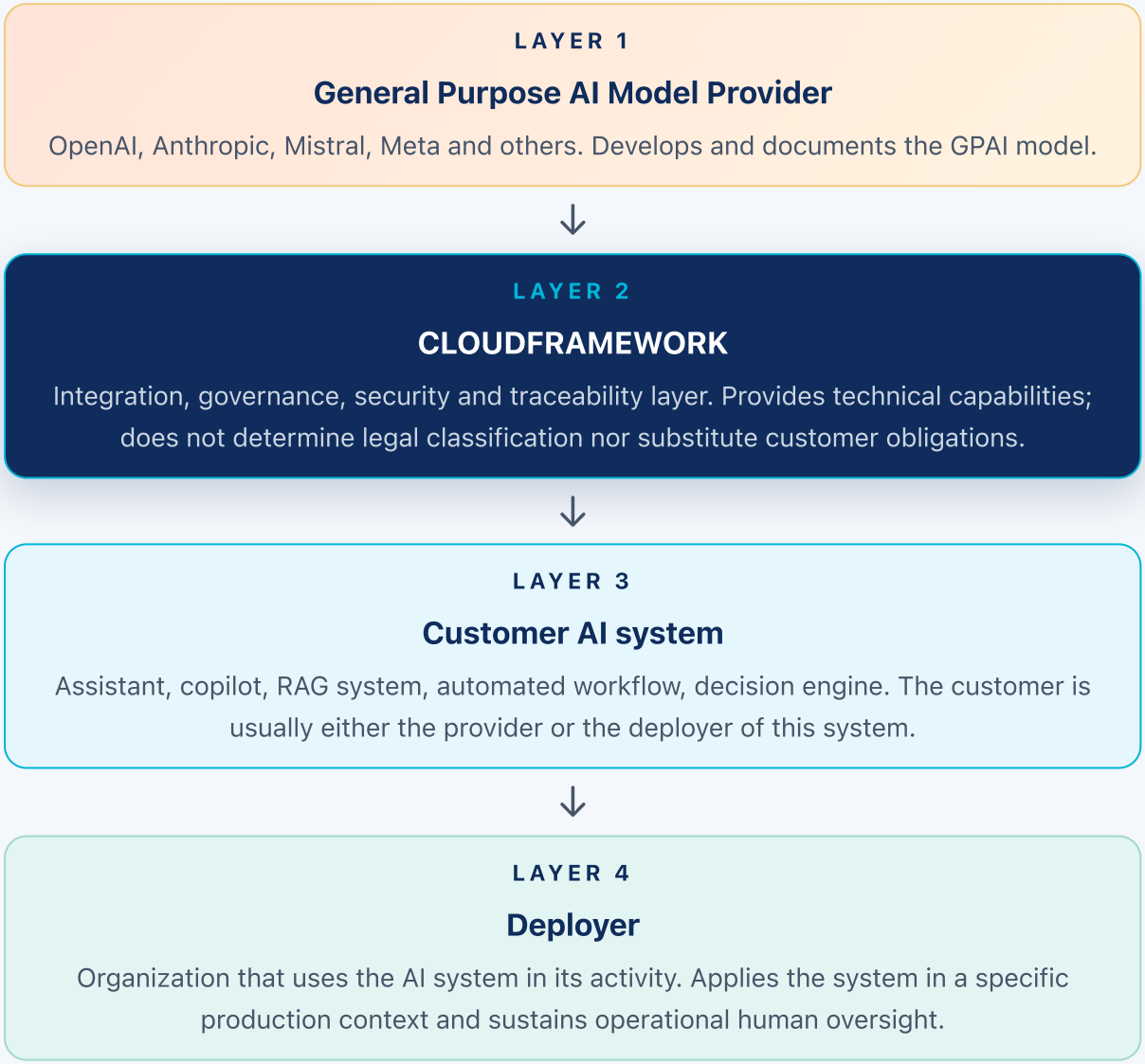
LAWORATORY's role

LAWORATORY, led by Óscar López, contributes the **complementary legal layer**: regulatory classification of each AI system, DPIA and FRIA assessments, contracts with AI providers, corporate AI governance and support before regulatory authorities. Both layers — technical and legal — operate in a coordinated manner over the same perimeter, avoiding the usual seams between legal consultancy and technology provider.

2 · SHARED RESPONSIBILITY

Shared responsibility model — who answers for what

Enterprise AI is usually built across several layers. Each layer has an actor with its own responsibilities. Identifying them clearly before deployment avoids contractual ambiguity and unnecessary regulatory exposure.



Indicative distribution of responsibilities

Actor	Main responsibility
GPAI Model Provider	Development and documentation of the general purpose AI model.
CLOUDFRAMEWORK	Technical capabilities for integration, governance, security, traceability and control.
Customer	Intended purpose, risk classification, configuration, data, use and applicable compliance.
Deployer	Use of the AI system in accordance with instructions, supervision and operational control.

> **Important.** CLOUDFRAMEWORK **does not substitute** the legal obligations of the AI system's provider or deployer. The platform facilitates technical and organizational controls, but the **final legal assessment depends on the use case, the context, the data processed and the intended purpose**. That assessment belongs to the customer and its legal counsel — LAWORATORY can accompany it when contracted to do so.

3 · LIFECYCLE

AI system lifecycle governance

Compliance with the Regulation must not be addressed solely as pre-launch documentation. It must be integrated **throughout the entire lifecycle** of the AI system, from design to retirement — and evidence must be generated at each stage, not reconstructed afterwards.

Phase	Relevant capabilities
Design	Definition of intended purpose, policies and restrictions.
Development	Versioning, testing, evaluation and traceability.
Integration	Connection with general purpose AI models and enterprise systems.
Deployment	Access controls, secure configuration and supervision.
Operation	Records, monitoring and usage control.
Oversight	Human intervention, review and escalation.
Post-market monitoring	Follow-up, incidents and corrective measures.
Retirement	Decommissioning, evidence retention and historical traceability.

CLOUDFRAMEWORK enables these controls to be incorporated systematically within the enterprise operation of AI systems, integrated with the rest of corporate governance and not in parallel to it.

4 · AI ACT OBLIGATIONS ⇔ CAPABILITIES

Mapping AI Act obligations to CLOUDFRAMEWORK capabilities

The following matrix translates the Regulation's obligations into concrete platform capabilities. **The availability of a capability does not in itself equate to compliance** — the customer must still configure, operate and document it correctly in its use case.

Regulation obligation	CLOUDFRAMEWORK capability
Risk management system	Policy engine, configurable controls and review workflows.
Data governance	Source traceability, access controls and minimization.
Technical documentation	Configuration registry, versions, policies and evidence.
Record keeping	Traceability of requests, responses, models and actions.
Transparency and user information	Metadata, notices, interaction logs and information mechanisms.
Human oversight	Approval workflows, human review and operational intervention.
Accuracy, robustness and cybersecurity	Monitoring, security controls and anomaly detection.
Post-market monitoring	Continuous observability, incident management and evidence.
Serious incident notification	Event capture, trace reconstruction and documentary support.

5 · RUNTIME ARCHITECTURE

Runtime governance architecture

The main challenge of enterprise AI is not only accessing general purpose AI models, but **governing how they are used in real systems**. CLOUDFRAMEWORK acts as an intermediate layer between GPAI models, enterprise applications, users, internal systems and corporate policies.

Main capabilities

Model orchestration

- Connection with multiple GPAI models
- Model selection by policy
- Substitution or provider switch
- Fallback routes when models are unavailable
- Control by region, customer or use case

Policy enforcement

- Instruction validation
- Input and output filtering
- Restrictions by user, role or purpose
- Blocking of unauthorized uses
- Security and compliance rules

Operational security

- Role-based access control
- Isolation between customers or environments
- Secure credential management
- Connection control
- Data segregation

Observability and logging

- Request retention
- Response retention
- Identification of model used
- Version traceability
- Usage, latency and error metrics

Governance controls

- Human approval
- Result review
- Incident escalation
- Configuration rollback
- Change control

6 · TRACEABILITY

Traceability and auditability

The Regulation requires certain AI systems to be able to **retain records and demonstrate how they have operated**. Without a living documentary substrate there is no defense possible before an inspection, an auditor or a sectoral authority.

What traceability must cover

OPERATION

What was executed

- Inputs
- Outputs
- Instructions
- System versions
- Model used

GOVERNANCE

How it was governed

- Policies applied
- User or process that executed the operation
- Human approvals
- Incidents
- Configuration changes

Evidence by design

CLOUDFRAMEWORK enables generating and retaining technical evidence related to:

- Usage logs
- Instruction traceability
- Model traceability
- Configuration history
- Routing decisions
- Controls applied
- Approvals and reviews
- Incidents and corrective measures

These capabilities facilitate **internal audits, compliance reviews and preparation for requirements from authorities or third parties**.

7 · HUMAN OVERSIGHT

Human oversight and operational control

For high-risk AI systems, the Regulation requires **adequate human oversight measures**. The discourse "a human always supervises" is not enough: operational human oversight requires an interface to review, intervene and revert; roles assigned with effective authority; and a record of interventions.

What human oversight must enable

The Regulation requires that a person with sufficient competence and authority can:

- Understand the general functioning of the system
- Interpret its results
- Intervene when necessary
- Stop or modify use
- Review relevant results
- Avoid or mitigate risks

Mechanisms provided by CLOUDFRAMEWORK

- Approval workflows
- Pre- or post-review by humans
- Escalation controls
- Review queues
- Manual intervention
- Operation blocking
- Reversal of decisions or configurations

8 · GPAI GOVERNANCE

Governance of third-party general purpose AI models

Many enterprise systems are built on top of GPAI models provided by third parties. This introduces **specific risks** that the organization must manage explicitly, not assume resolved by default.

Specific risks of using third-party GPAI

OPERATIONAL

- Provider dependency
- Model changes
- Availability
- Performance variations

VISIBILITY AND DATA

- Lack of visibility
- Data transfer
- Data residency
- Contractual policy differences

How CLOUDFRAMEWORK helps manage these risks

- Authorized model registry
- Version control
- Allow/deny model lists
- Policy-based model selection
- Geographic restrictions
- Separation by environment or customer
- Traceability of the model used in each operation
- Controlled provider substitution

9 · RISK CLASSIFICATION

Risk classification support

Classifying an AI system under the Regulation depends mainly on its intended purpose, the sector, the context of use, the data processed, the potential impact on natural persons, the degree of autonomy and the legal or similarly significant effects. **It is not a single technical decision: it is a comprehensive legal assessment.**

Relevant factors for classification

- The intended purpose
- The sector
- The context of use
- The data processed

- The potential impact on natural persons
- The degree of autonomy
- Legal or similarly significant effects

Indicative examples

Use case	Possible classification
Internal document assistant	Limited or minimal risk
General corporate copilot	Limited or minimal risk
Candidate screening	High risk
Credit scoring	High risk
Medical triage	High risk
Biometric identification	High risk or prohibited, depending on the case
Legal assistant	Variable depending on purpose and use

> **CLOUDFRAMEWORK can help document, control and monitor the system, but does not by itself determine the final legal classification.** That determination belongs to the customer and its legal counsel — LAWORATORY can accompany it with case-by-case analysis when contracted to do so.

10 · SECURITY AND SOVEREIGNTY

Security, sovereignty and data residency

Enterprise AI systems can generate **new security risks** that did not exist before the massive adoption of third-party GPAI models. The deploying enterprise inherits those risks and must articulate concrete controls to mitigate them.

New risks to consider

- Exposure of confidential information
- Personal data leakage
- Unauthorized model use
- International data transfer
- Loss of control over instructions or responses
- Use of non-approved tools

Capabilities provided by CLOUDFRAMEWORK

- Environment isolation
- Access control
- Secure credential management
- Encryption
- PII masking
- Region restriction
- Residency policies
- Authorized provider control
- Traceability of transfers and access

These capabilities are **especially relevant for regulated organizations, public administrations, healthcare, financial services and critical infrastructure**, where the combination of sector-specific regulation, GDPR, NIS2 and the AI Act requires a defensible technical architecture from day one.

11 · POST-MARKET

Post-market monitoring

Conformity **does not end with the deployment**. AI systems must be monitored during their operation to detect deviations, misuse, performance degradation and risks not foreseen in the initial design.

What must be detected during operation

- Errors
- Deviations
- Misuse
- Performance degradation
- Incidents
- Policy violations
- Unforeseen risks

Monitoring capabilities provided by CLOUDFRAMEWORK

- Continuous monitoring
- Anomaly detection
- Alerts
- Event review
- Incident follow-up
- Usage analysis
- Evidence retention
- Support for corrective measures

12 · EVIDENCE AND AUDIT

Evidence generation and audit readiness

One of the main challenges of complying with the Regulation is **demonstrating in a verifiable way** that effective controls exist. Having procedures is not enough: one must be able to show material, dated, integrity-protected evidence traceable back to its origin.

On what evidence is consolidated

- System configuration
- Intended purpose
- Models used
- Versions
- Policies applied
- Usage logs
- Human reviews
- Incidents
- Corrective measures
- Relevant changes

What this evidence is for

- Audit preparation
- Internal reviews
- Contractual compliance
- Responses to authorities

- Certifications
- Provider evaluations
- Continuity of AI system governance

13 · LIMITATIONS

Limitations and responsibilities

CLOUDFRAMEWORK provides a technical platform to **integrate, govern, operate and monitor** enterprise AI systems. It is important to precisely delimit what it does not do — and what always belongs to the customer and its legal counsel.

What CLOUDFRAMEWORK does not do

- **Does not provide legal advice.**
- **Does not substitute conformity assessment** where required.
- **Does not automatically determine risk classification.**
- **Does not by itself guarantee compliance with the Regulation.**
- **Does not replace the obligations of the provider** or deployer.

What each organization must evaluate in its case

Each organization must evaluate its specific case considering:

- Intended purpose
- Data processed
- Sector
- Affected users

- Potential impact
- Degree of autonomy
- Integration with other systems
- Applicable sector-specific obligations

How LAWORATORY fits in. When the client requests it, LAWORATORY assumes that layer of legal assessment: regulatory classification of the system, DPIA, FRIA, contracts with AI providers, corporate governance, support before authorities. The technical layer and the legal layer work over the same evidence perimeter.

LAWORATORY · INTEGRATED PARTNER

LAWORATORY — part of our LegalTech solution and governance partner

CLOUD LEGALTECH · INTEGRATED PARTNER

Legal knowledge and governance within the CLOUDFRAMEWORK ecosystem itself

LAWORATORY, founded by **Óscar López**, is part of the **CLOUDFRAMEWORK LegalTech solution**: it runs on the same EaaS platform as the rest of the verticals (CLOUD Hipotech, CLOUD HRMS...) and shares architecture, data governance and CloudIA integration. It is not an associated third party: it is a native piece of the ecosystem.

Óscar is also **a partner at CLOUDFRAMEWORK and the compliance lead** of the company itself — the same standard we apply to our customers we sustain internally. The legal co-authorship of this joint whitepaper is signed by him.

The combination delivers, for each client: **AI Act system classification, DPIA and FRIA assessments, contracts with AI providers, a documented shared responsibility model, AI corporate governance and support before regulatory authorities**, all connected to the technical substrate of the platform — not in a separate Word document.

Result for the customer: a single counterpart for both the technical and legal dimension of compliance — without the usual seams between legal consultancy and technology provider, and with responsibilities clearly assigned to each actor in the shared responsibility model described in section 2.

Operating principle. Compliance is not added *after* enterprise AI — it is built *with* it from the start. CLOUDFRAMEWORK provides the technical governance and compliance enablement layer; LAWORATORY provides the legal knowledge and classification of each system. Together they ensure that regulation stops being the brake on AI projects and becomes the ground from which they take off — without the false promise to the customer that "using the platform = compliant".

14 · CONCLUSION

Enterprise AI as a continuous governance discipline

The EU AI Act transforms enterprise AI into a **continuous discipline of technical, legal and operational governance**. Organizations that develop, integrate or use AI systems will need permanent capabilities — not one-off projects.

Permanent capabilities the company must sustain

- Control the use of general purpose AI models
- Retain records
- Document configurations
- Supervise results
- Manage risks
- Apply policies
- Monitor incidents
- Generate evidence

CLOUDFRAMEWORK positions itself as a **governance and operation layer** for enterprise AI systems, designed to help organizations deploy AI in a **traceable, secure, auditable manner aligned** with the requirements of the European regulatory framework. LAWORATORY brings the legal layer that complements that operation with the conformity assessment required in each case.

Regulation application timeline

Regulation (EU) 2024/1689 came into force on 1 August 2024 and applies in phases. The prohibitions are already in application (February 2025) and the obligations for general purpose models (August 2025). In August 2026, the obligations for high-risk systems become applicable. The rest is completed from August 2027 onwards.

✓ Feb 2025
Prohibited practices (Art. 5) in application

✓ Aug 2025
Obligations for **GPAI** (Chapter V)

Aug 2026
Obligations for **high-risk systems** (Ch. III, Sec. 2)

2027
Sector-specific regulated systems and remaining obligations

New timeline for high-risk systems — Digital Omnibus Regulation

The **Digital Omnibus Regulation on Artificial Intelligence** postpones the application of the rules for high-risk systems, in order to allow better technical preparation:

2 DEC 2027

High-risk standalone systems

Biometrics, infrastructure, education, employment. Applicable from **2 December 2027**.

2 AUG 2028

Systems embedded in products

Toys, lifts, medical devices. Applicable from **2 August 2028**.

Commercial reading. The Omnibus extension is an opportunity for preparation, not an excuse to delay AI governance. Organizations that start now will be ready — with evidence and with judgment — when it applies. Those that wait for the last quarter will arrive with incomplete documentation and no technical substrate.

Next step: a joint session CLOUDFRAMEWORK + LAWORATORY

A 60-minute conversation with your leadership, your CTO/CISO and your DPO/legal counsel. We map the AI systems in use or development, classify the probable role of your organization for each one, and propose — if it makes sense — a formal technical-legal diagnosis. No commitment required.

cloudframework.io/cloudia

CLOUDFRAMEWORK provides technical capabilities (governance, traceability, operational control). LAWORATORY provides legal assessment and regulatory classification. Both layers operate over the same perimeter.