AI Act, GDPR, DORA & the 'Digital Omnibus':

Regulatory convergence or a compliance burden for the European insurance sector?

Insurance & AI
November 2026

STRICTLY CONFIDENTIAL
The content of this document must not be disclosed to third parties without prior consent from Alpha FMC.

Executive Summary

The four frameworks do not contradict one another. They overlap on the same objects, the same data, models, suppliers and controls, which duplicates assessments, registers and reporting. Fragmentation, not contradiction, is the risk.

The AI Act has been in force since 1 August 2024, the AI Omnibus amending it entered into force on 27 July 2026, and the Annex III high-risk requirements apply from 2 December 2027. That gap is the time to prepare.

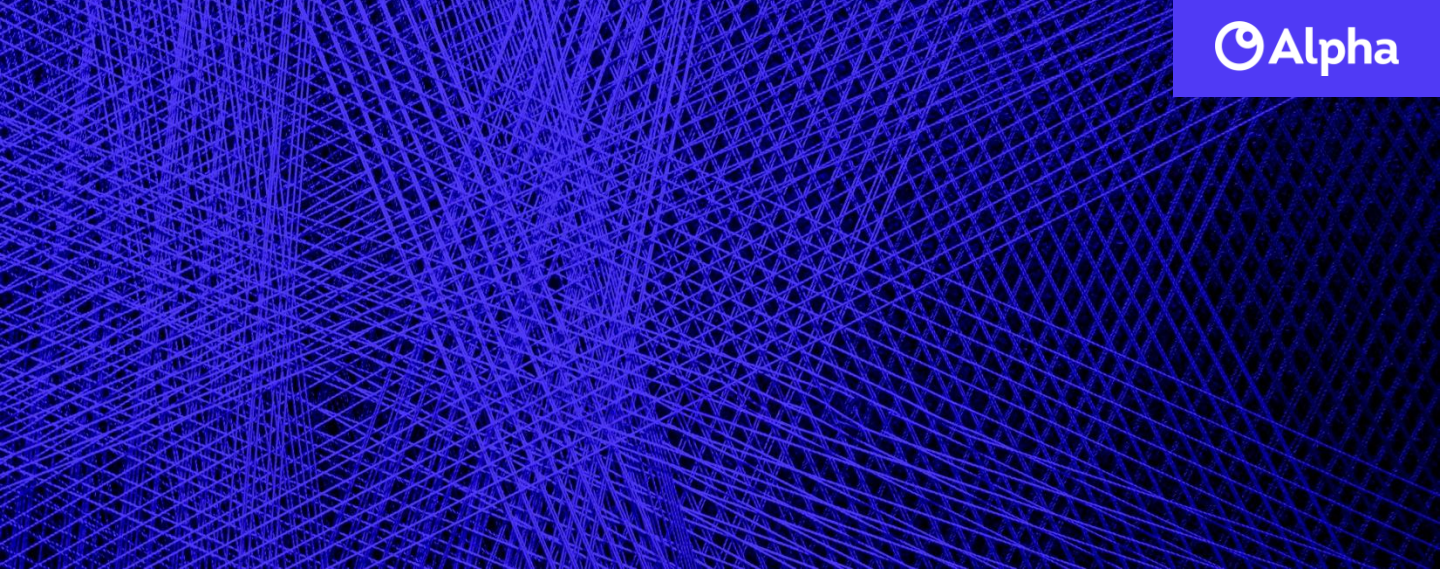
Four actions, all of which can start now

A1. Merge the governance forums. One cross-functional Digital Risks and Compliance committee replacing sequential Data Protection Officer (DPO), Chief Information Security Officer (CISO), risk and AI sign-offs.

A2. Classify every AI use case against Article 6. Distinguish genuinely high-risk systems from the rest before documentation costs are incurred.

A3. Unify supplier governance. One contractual and oversight framework covering AI Act provider duties, General Data Protection Regulation (GDPR) processing, Digital Operational Resilience Act (DORA) Information and Communication Technology (ICT) third parties and Solvency II outsourcing.

A4. Build one evidence repository. Article 27(4) allows an existing data protection impact assessment to inform a fundamental rights impact assessment, enabling teams to reuse existing evidence and avoid duplicating documentation across regulatory frameworks.



Introduction

Building an Integrated Compliance Framework for AI in Insurance

More and more players in the insurance sector are developing AI solutions, and there is no shortage of use cases. Predictive underwriting, fraud detection, claims automation, customer relations: AI now touches every part of the value chain. One key question remains for compliance and risk management teams: how to move forward in practical terms within a regulatory landscape that is still taking shape.

The challenge does not lie in any contradiction between these regulations, but in their overlap regarding the same subjects (data, models, suppliers, control mechanisms), leading to redundancies in assessments, registers and reporting. Feedback from the sector is clear: the risk of duplication of effort is real, particularly regarding impact assessments and documentation.

This white paper offers a comparative analysis of four sets of rules: the AI Act, the GDPR and DORA, which the Digital Omnibus amends or proposes to amend rather than replace, and Solvency II, the insurance rulebook they all build on. The aim is to help build an integrated compliance framework. With the AI Act already in force since 1 August 2024 and its requirements applying progressively, insurers must distinguish obligations already applicable from the forthcoming requirements for high-risk systems. Two steps are essential: understanding precisely what lies ahead and then drawing up a realistic roadmap.

Alpha supports insurance industry players throughout this process, from analyzing the obligations to implementing them, to ensure every deadline is met.

The Regulatory Pillars

Applies Since 27 July 2026.
Delays certain obligations for high-risk AI systems, facilitates bias detection, clarifies supervisory responsibilities and facilitates AI testing.

OMNIBUS ON AI
Harmonization

Applies Since 25 May 2018.
Supervisor National data protection authorities, the "Commission nationale de l'informatique et des libertés" in France (CNIL).

GDPR
Privacy

Asks A lawful basis under Article 6 and, for health data, a condition under Article 9, with a Data Protection Impact Assessment (DPIA), breach notification within 72 hours and safeguards on automated decisions.

DIGITAL FINANCE REGULATION
EU regulatory ecosystem

Applies In force since 1 August 2024, amended by the AI Omnibus on 27 July 2026, Annex III duties from 2 December 2027.
Supervisor Market surveillance authorities, the "Autorité de contrôle prudentiel et de resolution" (ACPR) for high-risk AI in French finance.

AI ACT
Governance

Asks Classify systems by risk and, for high-risk, maintain risk management, data governance, documentation, human oversight and a Fundamental Rights Impact Assessment (FRIA).

DORA
Resilience

Applies Since 17 January 2025.
Supervisor National supervisors for entities, the European Supervisory Authorities (ESAs) for critical ICT providers.
Asks ICT risk management and governance, incident reporting, resilience testing and third-party ICT risk management. Not every AI failure is a reportable major incident.

AI Omnibus applicable since 27 July 2026, supervised by market surveillance authorities (the in French finance)

In November 2025, the European Commission presented the 'Digital Omnibus' package, which aims to streamline the requirements set out in several European digital regulations to improve their consistency, clarity and operational effectiveness for businesses.

This initiative aims to address similar issues covered by different pieces of legislation, with a view to reducing administrative burdens and strengthening the international competitiveness of European players.

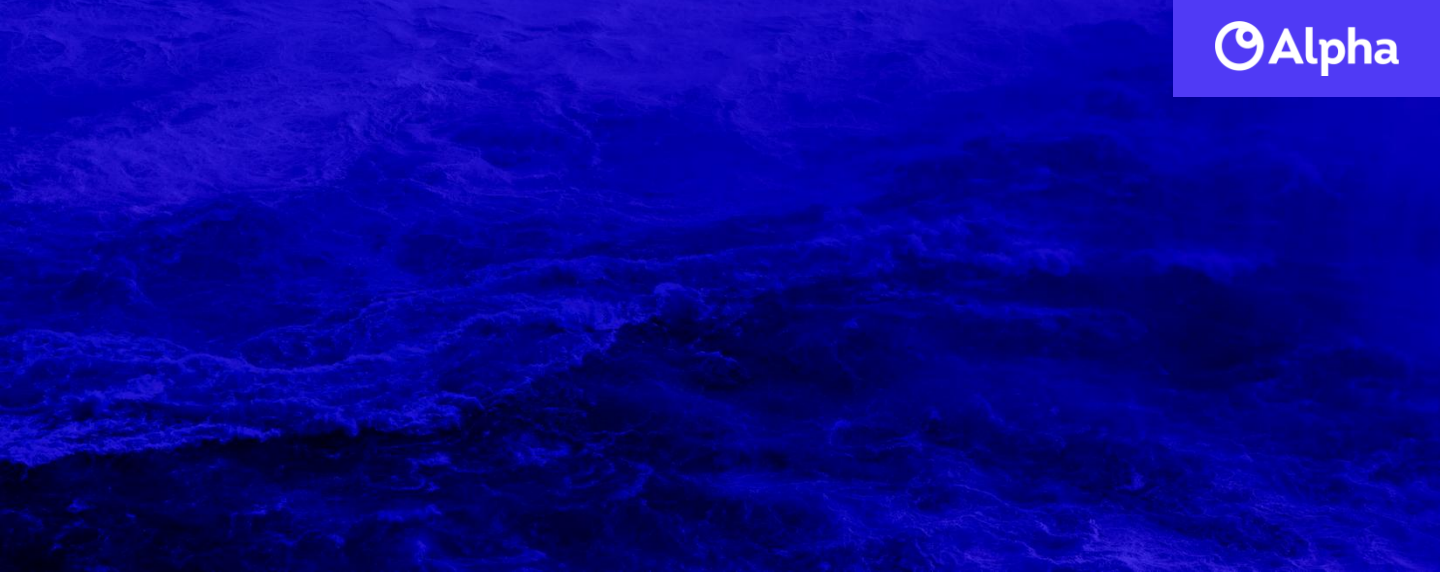
The AI Omnibus amending the AI Act was adopted and entered into force on 27 July 2026; the measures affecting data and cybersecurity legislation remain proposals. Key points to note include:

Annex III, 2 December 2027: AI systems classified as high-risk because of their intended use. This covers creditworthiness assessment and credit scoring of natural persons, as well as risk assessment and pricing in life and health insurance. AI tools used by a bank or insurer to recruit or evaluate its own employees are also concerned. From this date, an insurer using AI to price or assess risks in life and health insurance will have to comply with all high-risk obligations (risk management, human oversight, traceability, fundamental rights impact assessment, etc.).

- Annex I, 2 August 2028: AI systems embedded in products already covered by EU product safety legislation. These benefit from a longer transition period.
- Article 50, 2 August 2026: People must be informed when they are interacting with an AI system, such as a customer service chatbot. AI-generated content must also be disclosed. Systems already on the market before that date have until 2 December 2026 to apply technical marking to such content.
- Article 4a, 27 July 2026: insurers may now, on an exceptional basis, process special categories of personal data to detect and correct bias, subject to strict necessity and safeguards. This possibility extends to specified deployers and to other AI systems and models. This is not a general permission to reuse customer data.

Whilst these changes represent a first step towards simplifying the regulatory framework, many questions remain across all economic sectors. For players in the insurance sector, the challenges are primarily operational. Will the Digital Omnibus enable the pooling or simplification of regulatory reporting channels? Will it lead to the harmonization of definitions, particularly regarding personal data? Will it promote alignment between the various existing registers, such as outsourcing registers, the ICT asset inventories required by DORA and the AI system inventories provided for by the AI Act? Finally, will it clarify the division of responsibilities between the various supervisory authorities? The proposed European Union Agency for Cybersecurity (ENISA) single entry point for incident reporting would not merge AI system inventories, ICT asset inventories and outsourcing registers.

These questions remain open and will be crucial to the operational implementation of the new regulatory requirements within insurance companies.



AI Act, Risk-based compliance for AI systems

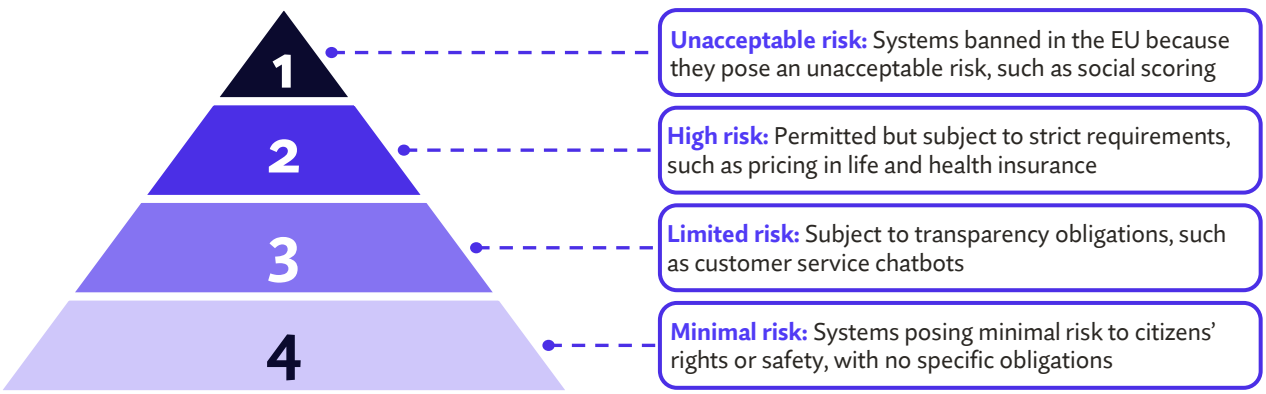
In force since 1 August 2024

The AI Act is the first legislative framework adopted by the European Union aimed at regulating the development, marketing and use of artificial intelligence systems. Its objective is to ensure that these systems respect fundamental rights, safety and European values whilst promoting innovation. It entered into force on 1 August 2024 and applies in phases.

In practical terms, the AI Act is based on a risk-based approach. It classifies AI systems according to their level of risk: unacceptable risk, high risk, limited risk and minimal risk. High-risk AI systems are subject to stricter regulatory requirements. The higher the level of risk, the more onerous the applicable obligations.

These requirements relate in particular to the implementation of a risk management system, governance and data quality, technical documentation and traceability, transparency towards users, human oversight, as well as the accuracy, robustness and cybersecurity of the systems. A conformity assessment must also be carried out before they are placed on the market or put into service.

Classification under the AI Act:



Source: AI Act — Regulation (EU) 2024/1689 on artificial intelligence

For the insurance sector, a key point of concern is that AI systems used for risk assessment and pricing concerning natural persons in life and health insurance are classified as high-risk AI systems. Not all insurance AI is high-risk: classification depends on the system's intended purpose and on the conditions set out in Article 6.

For example, an insurance company that deploys an AI model to automatically adjust health insurance premiums based on the medical, behavioral or socio-economic characteristics of policyholders would be subject to all the obligations applicable to high-risk AI systems.

Furthermore, prior to the deployment of a high-risk AI system, deployers subject to Article 27 must carry out a Fundamental Rights Impact Assessment in accordance with Article 27 of the AI Act. The obligation covers the relevant life and health insurance category, but not every high-risk deployment. The results must be notified to the competent market-surveillance authority (the for the relevant French financial-sector cases).

Finally, it should be emphasized that the obligations set out in the AI Act apply both to providers, who are responsible for the design and placing on the market of the systems, and to deployers, who use them in the course of their business. Software providers are therefore responsible for ensuring the product itself complies with the provider's obligations, whilst insurers remain responsible for the way in which they use the solution.

Key date: the relevant Annex III high-risk requirements for life and health insurance risk assessment and pricing apply from 2 December 2027.

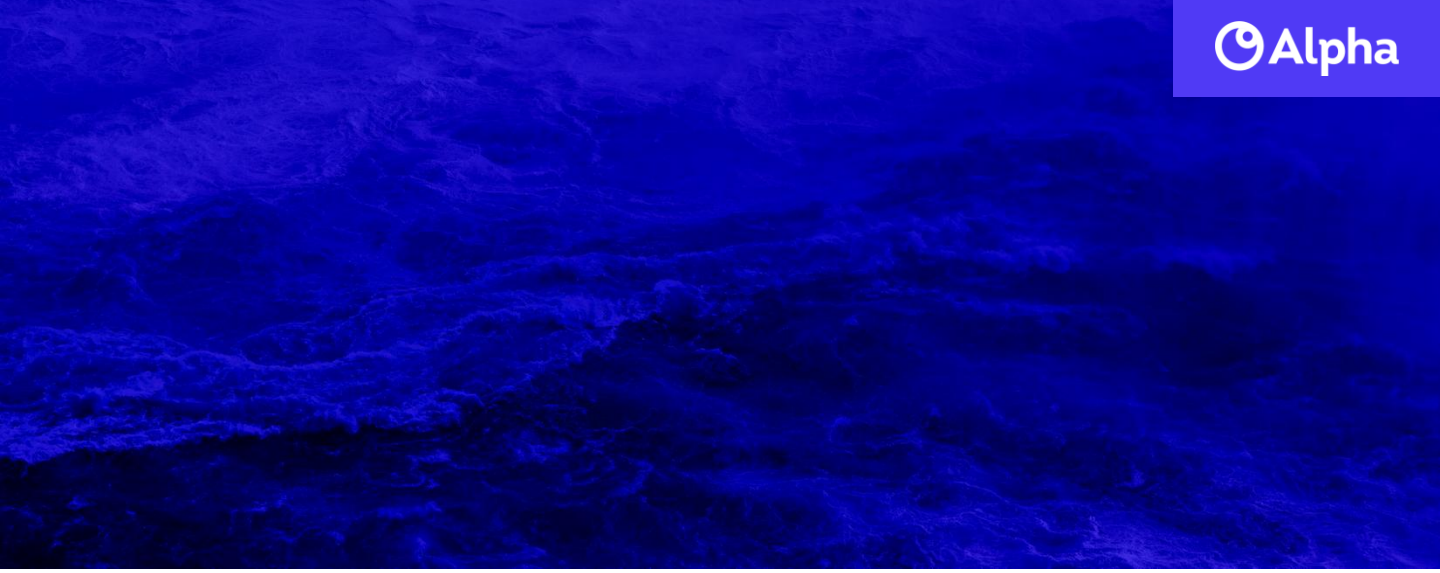
DORA Regulation (EU) 2022/2554, Operational resilience as a 'single regulatory framework'

Applicable since 17 January 2025

The DORA Regulation (EU) 2022/2554, applicable since 17 January 2025, harmonizes requirements for digital operational resilience across the financial sector, covering ICT risk management and governance, incident reporting, digital operational resilience testing, third-party ICT risk management and information sharing. It applies to in-scope financial entities, as certain exclusions exist.

In the insurance sector, the DORA Regulation applies to the governance and control framework. European Insurance and Occupational Pensions Authority (EIOPA) describes EU-level supervision of critical third-party ICT providers (CTPPs) as complementary to, rather than a substitute for, the third-party risk management carried out by financial institutions themselves and the application of national supervisory measures (EIOPA, Supervision under DORA).

Regarding incident reporting, the supervisory documents outline a phased reporting process for major ICT-related incidents (initial notification, interim report(s), final report), as well as the voluntary reporting of significant cyber threats (EIOPA, slides on incident reporting). Regarding the risk of technological concentration, the 'Lead Overseer' model and Joint Examination Teams (JETs) create a new center of gravity for the supervision of critical service providers (EIOPA, DORA Supervision).



GDPR

Applicable since 25 May 2018

The General Data Protection Regulation is a European regulation that sets out strict rules on the collection, processing and protection of personal data for all individuals, including those in the insurance sector. Its aim is to ensure that customers' data is used transparently, securely and on an appropriate lawful basis under Article 6 and, for special-category data such as health data, an applicable condition under Article 9.

In the insurance sector, this means that insurance companies, brokers and other industry players must handle customers' personal information with care, such as their identity details, health data, financial information or claims history.

For example, when a customer takes out health or home insurance, the insurer must clearly inform them of the data being collected (such as medical information or claims history) and the purposes for which it is processed (pricing, contract management, fraud prevention).

The insurer must also protect this data against unauthorized access by using secure IT systems and applying strict internal procedures. In the event of an incident, such as a data breach resulting from a cyberattack, notification to the supervisory authority (such as the CNIL in France) is required without undue delay and, where feasible, within 72 hours of becoming aware of the breach, unless it is unlikely to result in a risk to the rights and freedoms of individuals; the individuals concerned must generally be informed where the breach is likely to result in a high risk, subject to the exceptions in Article 34.

Where underwriting or pricing decisions are taken solely by automated means with legal or similarly significant effects, Article 22 GDPR also applies: permitted only on limited grounds and with suitable safeguards, including human intervention. AI Act compliance does not replace this assessment.

The texts overlap in four places

The difficulty is not a conflict of rules but a collision of the same objects: data, models, suppliers and controls. Solvency II, the insurance rulebook, joins the three digital texts here. Each zone is analyzed in the following pages and resolves into one action.

Overlap 1 - Governance Solvency II, DORA, GDPR, AI Act

The overlap Four texts each require a governance system over the same processes, with separate policies, committees and sign-off chains.

The risk Parallel forums and sequential approvals slow every AI decision.

Analyzed on page 10, resolved by action A1.

Overlap 2 - Risk taxonomy AI Act, Solvency II

The overlap The AI Act ranks risk by impact on fundamental rights, Solvency II by financial significance, so a system can be high-risk in one and immaterial in the other.

The risk Effort lands on the wrong systems, and the two registers never reconcile.

Analyzed on page 11, resolved by action A2.

Overlap 3 - Suppliers and outsourcing All four texts

The overlap AI arrives through vendors and cloud platforms, four regimes govern the same contract, and modification can turn an insurer into a provider.

The risk Contractual gaps surface only at the incident, and the same supplier is reviewed several times over.

Analyzed on page 11, resolved by action A3.

Overlap 4 - Supervision and evidence , CNIL, ESAs

The overlap The mandates overlap rather than divide, so two or three authorities examine the same AI process on unsynchronized cycles.

The risk The same control ends up documented three times, in three formats.

Analyzed on page 12, resolved by action A4.

At the crossroads of conceptual frameworks

Overlaps in governance

Four texts impose governance duties over the same processes. The question is not which one applies, but whether an insurer runs four arrangements or one.

Solvency II sets the enterprise frame. Article 41 requires an effective governance system, proportionate to the nature, scale and complexity of the business, with written policies covering risk management, internal control and outsourcing. Article 44 requires a risk management system integrated into decision-making; Article 46 an internal control system including compliance (Directive 2009/138/EC).

The GDPR underpins it. Any use of personal data rests on it, and it sets the reference framework the other regimes build on.

DORA adds the ICT layer. Documentation, testing, third-party management and ICT governance (Regulation (EU) 2022/2554). EIOPA withdrew its ICT security and cloud-outsourcing guidelines in January 2025 to remove duplication, so those expectations now sit within DORA.

The AI Act does not require a fifth layer. Articles 17(4), 18(3), 19(2) and 26(5)–(6) allow the quality management system, technical documentation, logging and monitoring duties to be discharged through arrangements already required under sectoral financial legislation. Its reach is nonetheless wider than operational risk: discrimination and lack of transparency fall outside the Solvency II prudential frame.

EIOPA takes the same position: the AI Act creates specific duties for high-risk systems while providing for integration with existing sector rules (EIOPA Opinion on AI governance and risk management, EIOPA-BoS-25-007, 6 August 2025).

Alpha's Advice A1 - Merge the governance forums:

Replace the sequential DPO, CISO, risk and AI sign-off chain with a single cross-functional Digital Risks and Compliance committee. It reviews each AI use case once, against all four regimes (Solvency II, DORA, GDPR, AI Act), and issues one decision. The DPO, CISO, risk and AI functions sit on the committee as members rather than as successive approvers.

Owner: Risk

Risk taxonomy and supplier governance

Overlap 2 · Risk taxonomy. The AI Act and Solvency II rank the same AI system differently, because they protect different things.

	AI Act	Solvency II
Ranks by	Impact on fundamental rights	Financial significance
Protects	Access to essential services, non-discrimination	Solvency (Directive 2009/138/EC, Article 44)
In insurance	High-risk for life and health pricing of natural persons (Article 6)	Operational risk and governance requirements

The gap. A system can be high-risk under the AI Act and immaterial under Solvency II, so the two registers never reconcile.

Alpha's Advice A2 - Classify every use case against Article 6:
Run one intended-purpose test per AI use case and map it onto the Solvency II taxonomy, so both registers share one classification.
Owners: Data science and Compliance

Overlap 3 · Suppliers. AI reaches insurers through vendors and cloud platforms, so one contract can sit under four regimes at once.

Regime	What it requires
AI Act	Duties split between providers and deployers; building or modifying a system can make the insurer a provider
GDPR	Personal data used by AI is strictly governed; outsourced processing needs specific contract terms
DORA	ICT third-party risk governance and EU oversight of critical providers (EIOPA cloud guidelines withdrawn, Jan 2025)
Solvency II	An outsourcing policy; the insurer stays responsible for outsourced functions

The gap. The same supplier is reviewed four times against four sets of criteria, and contractual gaps surface only at the incident.

Alpha's Advice A3 - Unify supplier governance:
One contractual and oversight framework for all four regimes: each supplier is reviewed once and gaps close at signature.
Owner: Procurement and Risk



Convergence in supervision

The supervisory mandates overlap rather than divide, so one AI process can face two or three control points.

Prudential supervisors assess governance, operational risk management and outsourcing controls.

Market surveillance authorities enforce the AI Act through a product-compliance approach. The has confirmed its designation for high-risk AI systems in the French financial sector.

The ESAs oversee critical ICT providers under DORA, with national implementation for entities (Regulation (EU) 2022/2554; EIOPA, 'DORA Oversight').

Why it matters operationally. The same AI-based process can draw a prudential finding under Solvency II, a product-compliance finding under the AI Act and an ICT finding under DORA, on review cycles that are not synchronized and with evidence requested in three different formats. Article 27(4) already permits a FRIA to rely on cross-references to an existing DPIA, so reuse is available today, but it needs a repository to reuse from.

Alpha's Advice A4 - Build one evidence repository:

Document each control once, in a single repository, and map it to every authority that examines it. Each review then draws on the same evidence instead of a new file in a new format. The repository also lets a FRIA cross-reference an existing DPIA under Article 27(4).

Owner: Compliance

Everything on the critical path starts before the 2027 deadline

The regulatory milestones are fixed, so the four actions are sequenced against them. The two that cost nothing to start begin immediately, and the window closes when the Annex III requirements apply.

Now, through end 2026
Stand up the Digital Risks and Compliance committee and the shared dashboard, since it is the forum every later decision runs through, and classify the existing estate of AI use cases against Article 6. Neither step requires a new budget line: one reorganizes forums, the other classifies what already exists.

First quarter 2027
Rewrite the supplier framework so a single contractual and oversight approach satisfies all four regimes, and stand up the evidence repository, reusing the DPIA content for the first FRIA. These two carry the build cost, which is why they start a full year ahead.

Through 2027
Apply the supplier framework at each contract renewal and keep classification inside the intake of every new use case rather than running it as a one-off exercise.

Third quarter 2027
Dry-run the evidence pack against each authority's expectations, so the first real supervisory request is not the first time the repository is tested.

2 December 2027
The Annex III high-risk requirements apply. Bringing a system already in production into compliance retrospectively costs more than building the requirements in from the start.

Alpha's Perspective

The risk is not the theoretical overlap between regulations but the operational fragmentation it creates: distinct definitions, separate authorities and unaligned timetables. Three priorities carry the four actions into practice.

1 Break the silos in governance

Strengthen governance by breaking down the silos between the DPO, the CISO, risk management and the AI teams. A monthly cross-functional Digital Risks and Compliance committee gives one decision-making forum, and reviewing incidents, technology projects and regulatory change on a single shared dashboard replaces slow sequential approvals. It also brings compliance, cybersecurity and operational risk into the design phase rather than the review phase. On AI literacy, amended Article 4 requires measures supporting staff AI literacy, not a guaranteed individual level of competence.

2 Classify the estate before documenting it

Every AI model in use or under development should be categorized against the AI Act now. A health insurer using scoring algorithms to adjust premiums from connected-device data should already be documenting its model logic and formalizing human oversight. Compiling technical documentation from the design phase is a strategic necessity: bringing a high-risk system already in production into compliance retrospectively costs more, operationally and financially, than building the requirements in from day one.

3 Use the window before December 2027

The substance has been known since 2024: risk management, data governance, human oversight and the FRIA are set out in the regulation as amended by the AI Omnibus. The implementing detail, meaning harmonized standards, guidelines and the FRIA template, is arriving progressively ahead of the Annex III requirements. That lag is a window, not a reprieve: AI governance, system mapping and FRIA preparation can start now, and Solvency II and DORA already cover part of the framework.

How can Alpha help you?

Understanding the applicable regulatory framework and its recent amendments is an essential step, particularly given the growing use of AI to automate processes.

As use cases become more diverse, insurers must be able to comply with the regulatory requirements arising from DORA, the AI Act and its amendment by the AI Omnibus.

The main challenge lies in clearly and comprehensively mapping out the various obligations arising from these regulations, identifying both their commonalities and their specific features. This means distinguishing obligations that already apply, adopted amendments whose application dates fall in the future, and measures that remain proposals; the Digital Omnibus is not a standalone regime calling for a separate compliance program. Rather than creating regulatory silos, the aim is to establish a single governance and control framework that complies with all these rules.

Thanks to our combined expertise in business and IT, Alpha is ideally positioned to analyze your internal processes, identify redundancies and inefficiencies, propose improvements and successfully deliver compliance projects.

Contributors



Thomas Noël-Betrancourt | Director

Thomas is a Director in Alpha's MENA Insurance team with extensive experience in finance transformation, distribution and investment. Thomas has led engagements to adapt to changing regulatory environment, support M&A transactions, strengthen operating models, and leverage technology to enhance finance, investment and distribution ranging from reinsurance to brokerage.



Mohamed El Magri | Manager

Mohamed is a Manager in Alpha's Insurance practice with experience in resilience and finance transformation across EMEA region. He has supported engagements covering regulatory adaptation, operating model design, M&A transactions, and the application of technology to enhance finance and investment functions working across a broad range of insurance and reinsurance clients.



Pauline Ratajczak | Senior Consultant

Pauline is a Senior Consultant in Alpha's Insurance practice, with experience in business transformation across the insurance sector. Through the projects she has led, she has developed in-depth expertise in the regulatory frameworks applicable across Europe.



Confidence in the complex

For information or permission to reprint, please contact Alpha FMC at info@alphafmc.com. To find our latest content and insights, please visit alphafmc.com. Follow Alpha FMC on LinkedIn.

© Alpha Financial Markets Consulting. All rights reserved. 2026