Just in Time

Digital Omnibus

AI Act

June 2026

iason ESSENTIAL SERVICES FOR FINANCIAL INSTITUTIONS

Executive Summary

- The **Digital Omnibus** constitutes a targeted regulatory initiative intended to simplify the implementation, by the other things, of the **AI Act** within the broader EU **digital framework**, without modifying its fundamental structure or risk-based logic.
- The proposed adjustments primarily concern implementation **timelines**, conformity **assessment** procedures, documentation **requirements**, relief measures for **SMEs** and small mid-caps, and a more structured supervisory role for the AI Office at EU level.
- The overall objective is to reduce legal uncertainty and **regulatory fragmentation**, while making compliance more proportionate, operational, and consistent, without undermining the core principles of **safety**, **transparency**, and **fundamental rights protection**.

At a Glance

Keywords: Digital Omnibus, AI Act, Technology

01

Introduction on the Digital Omnibus

Regulatory Framework of the Digital Omnibus Package

The Fundamental Intervention of the Digital Omnibus

Implementations Problems to Solve – AI Act

Introduction on the Digital Omnibus 1/3

Regulatory Framework of the Digital Omnibus Package

On 19 November 2025, the European Commission introduced the **Digital Omnibus**, a long-anticipated initiative aimed at **streamlining** and **updating** key components of the **EU's digital regulatory framework**, including the *Data Act*, *GDPR*, and the ***AI Act***. This **package** includes regulations on **AI**, **data governance**, **digital markets**, and **cybersecurity**.

01 The Artificial Intelligence Act introduces the **first EU-wide** framework for AI, based on a **risk-based approach**. It regulates **high-risk** AI systems, **strengthens** transparency and **bans harmful** uses such as AI-generated **non-consensual intimate** content (effective from 2 December 2026). As recently stated in the publication of the *Council of the European Union* of May 2026, **compliance deadlines** for high-risk AI obligations extend to **2 December 2027** and **2 August 2028**, while **reducing administrative burdens, maintaining continuous** risk management and strong data **governance obligations**.

02 The Digital Markets framework aims to **ensure** fair and **contestable** digital markets by targeting **large platforms** identified as **gatekeepers**. It imposes **interoperability** obligations, restricts **self-preferencing** practices, and regulates data use between platforms and third parties. The regulation also enhances transparency across digital services.

03 The Data Governance Act establishes a framework for **safe** data sharing across the EU. It introduces certified data intermediaries and promotes data altruism. The Act supports the **development** of sectoral European data **spaces** and builds trust in **data exchange** between organizations. It sets rules for the reuse of protected public-sector data, improves data availability for **innovation** and research, and **supports** a federated approach to **data governance**.

04 The Data Act regulates access to and use of **data generated** by IoT devices. It **promotes** data sharing between **economic actors**, strengthens **access right**s for both users and businesses, and reduces contractual lock-in in cloud and **digital services**. It aims **to boost the EU** data **economy** by fostering fair competition, setting rules for data sharing between the public and **private sectors**, and introducing requirements for data portability and i**nteroperability.**

05 The Data Governance Act regulates **access** to IoT-generated data and promotes data sharing **across economic** actors. It strengthens user and **business access** rights, reduces cloud and **digital service** lock-in, and supports fair competition **through rules** on data sharing, portability, and interoperability.

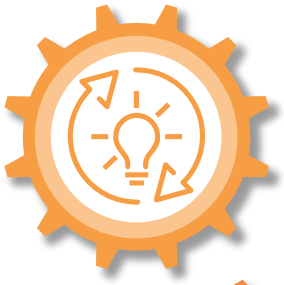
06 The NIS2 Directive strengthens EU cybersecurity by **expanding coverage** to more **critical sectors** and requiring **risk management**, incident reporting, and **security measures**. It also **increases** management responsibility and improves **digital infrastructure** resilience.

07 The General Data Protection Regulation (GDPR) regulates personal data protection in the EU, ensuring accountability, strong user rights, secure processing, and **clear rules** on **consent**, data breaches, and lawful data use**.**

Introduction on the Digital Omnibus 2/3

The Fundamental Intervention of the Digital Omnibus

In recent years, the European Union has developed an **extensive** and **ambitious** digital regulatory framework. However, the rapid expansion of legislation has led to increasing **complexity** for businesses, public authorities, and regulators, with **significant overlaps** between key regulations. This context has highlighted the need for a more **streamlined** and **coordinated** approach to digital regulation.



Growing number of regulations and the complexity of the EU's digital framework

The AI Act is part of a **broader** and **highly complex** EU digital **regulatory framework** that also includes the ***GDPR***, ***Data Act***, ***DSA***, ***DMA***, ***CRA***, and ***NIS2***. While each regulation has specific objectives, their coexistence creates a **dense** and **interconnected legal environment**. This raises **concerns** about overall **coherence** and the cumulative impact on **competitiveness** and **innovation** within the European AI ecosystem.

Overlaps between regulations (AI Act, GDPR, NIS2)

The AI Act significantly **overlaps** with **several existing EU regulatory frameworks**, creating potential duplication and **uncertainty** in **compliance**. The most relevant interaction is with the ***GDPR***, where AI-specific requirements such as FRIAs overlap with DPIAs, leading to **redundant obligations** and **unclear management** of **data subjects' rights**. Similar overlaps arise with the ***Data Act***, where entities may simultaneously face data access obligations and AI compliance duties, and with cybersecurity frameworks like the CRA and NIS2, which introduce **parallel risk management** and **incident reporting requirements**.

Implementation challenges for businesses and government agencies

The increasing complexity and fragmentation of the EU technology regulatory framework generate **substantial legal uncertainty** and **regulatory pressure** for **innovators**. Consequently, **companies** operating in Europe are **subject** to **significant administrative** and **compliance burdens** stemming from a **highly fragmented** and overlapping **set of rules**. This environment complicates regulatory implementation and **raises** the **overall cost** of **compliance** across multiple legal regimes. Ultimately, it **limits firms' capacity** to effectively **invest in**, develop, and deploy **new technologies** and **products** within the European market.

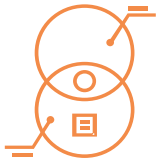
Introduction on the Digital Omnibus 3/3

Implementations Problems to Solve – AI Act

As the **AI Act** moved into its early implementation phase, a number of practical challenges began to emerge. These **issues** highlighted the need for a more **workable** and **proportionate framework**, creating stronger momentum for targeted **simplification**.

Delayed Standards and Guidance

In the early implementation phase, several **AI Act** obligations risked becoming applicable before the relevant **harmonised standards**, technical specifications, and detailed guidance were fully available. This **timing gap** created uncertainty for organisations that were willing to comply but lacked clear reference points on how to do so in practice.



Overlaps with Other EU Rules

Many **stakeholders** pointed to significant **overlaps** between AI Act obligations and existing **EU rules** on data protection, product **safety**, **cybersecurity** and **platform regulation**. These interactions made it difficult to understand which requirements applied in specific scenarios and raised the risk of duplicated assessments and documentation for the same AI system.

Disproportionate Burden on SMEs

The initial compliance model was perceived as particularly demanding for **SMEs**, start-ups and less mature organisations, both in terms of cost and internal resources. For many of these actors, the combination of complex obligations, limited legal certainty and high fixed compliance costs threatened to act as a barrier to entry rather than an incentive to develop trustworthy **AI**.

Unclear Supervision and Implementation Pathways

Uncertainty also emerged around how **supervision** would work in practice, including the allocation of **responsibilities** between **national authorities**, notified bodies and EU-level structures. This lack of clarity on roles, processes and enforcement tools made it harder for organisations to anticipate expectations and plan a coherent compliance strategy.

02

Key Amendments to the AI Act Framework

Implementation Timelines and Regulatory Readiness

Procedures and Compliance

Sensitive Data and AI Literacy

Governance and AI Office

Key Amendments to the AI Act Framework 1/4

Implementation Timelines and Regulatory Readiness

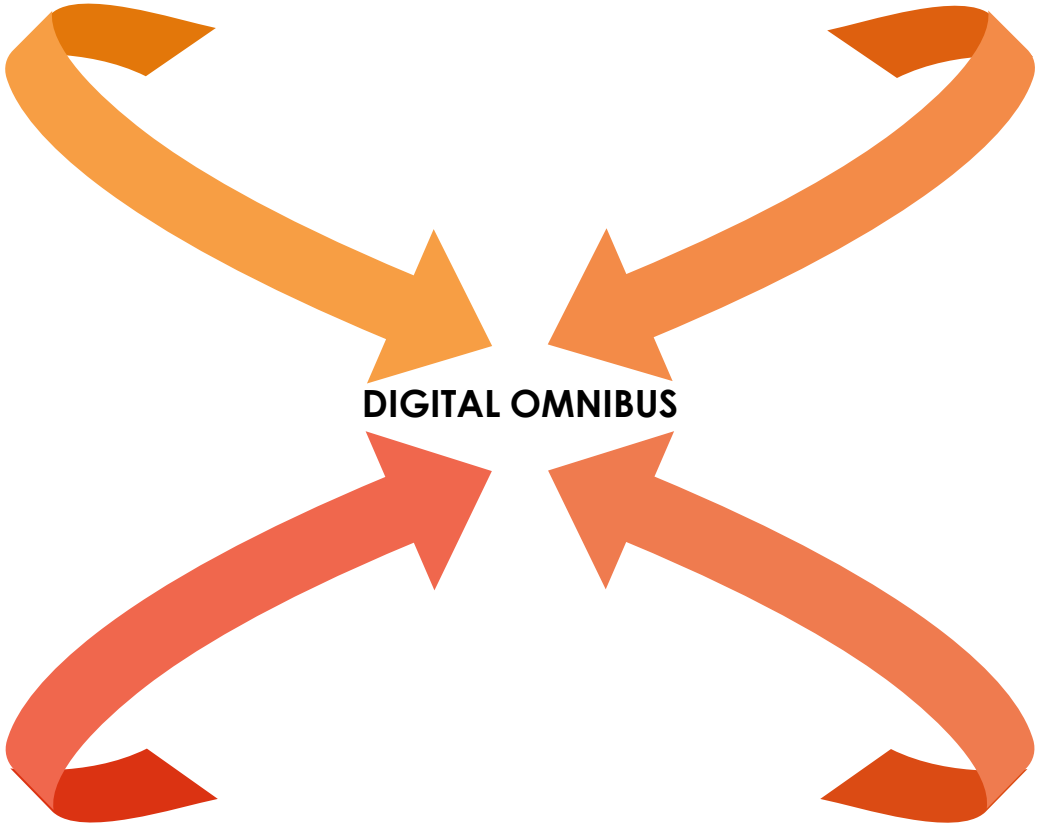
One of the most relevant **changes** concerns the **timing** of **compliance** obligations under the AI Act, especially for **high-risk systems**. The Digital Omnibus seeks to align **regulatory** deadlines with the actual availability of standards, guidance, and other tools needed for effective implementation.

Readiness-based timelines instead of rigid deadlines

The Digital Omnibus introduces a more **flexible approach** to **timing**, linking some obligations to the actual readiness of the regulatory **framework**. This helps avoid situations where companies are expected to comply before the necessary tools are available.

More realistic planning for compliance and governance

Harmonised standards, technical specifications and Commission guidance play a key role in turning **legal obligations** into practical requirements. Without them, the risk increases that compliance remains too vague or uneven across the **market**.



High-risk systems require clearer support tools

High-risk AI systems are the area where implementation pressure is strongest, because the obligations are more demanding. For this reason, clearer support tools are needed to make compliance realistic and consistent.

Standards and guidance are central to implementation

A more gradual timeline gives organisations time to organise internal processes, documentation and governance structures properly. It also makes the **overall implementation** path more predictable for **businesses** and **regulators**.

Key Amendments to the AI Act Framework 2/4

Procedures and Compliance

The Digital Omnibus aims to streamline the **AI Act compliance process** and make it more practical, particularly in cases where an AI system is also subject to other European **harmonisation standards**.

Streamlining of conformity assessment

The Commission aims to make the process more consistent, so that providers do **not have** to **manage** parallel or **overlapping procedures** when a system falls under multiple EU regulatory frameworks. This is particularly relevant for high-risk systems, for which the AI Act already provides for structured conformity assessment procedures.

Greater clarity on standards and documentation

The Digital Omnibus also aims to clarify the operational **framework** for **harmonised** standards, common specifications, and technical documentation. In practice, the Commission has tied the application of certain obligations to the availability of adequate technical tools and guidance, to avoid requiring operators to fully comply before the implementation framework is in place.

Single Procedure

the possibility of avoiding **duplication** where the AI system is already subject to another EU harmonisation regime. The rationale is to build on the work already carried out under sector-specific legislation, thereby **reducing** the **risk** of having to repeat checks, audits or documentation that are essentially similar.

Impact on post-market monitoring

Simplification does not only apply to the initial stage of market access, but also to the subsequent phase of monitoring and maintaining compliance. The idea is that providers can **manage** post-market **obligations** in a more organised and less fragmented manner, **reducing duplication** of documentation and uncoordinated reporting processes.

Key Amendments to the AI Act Framework 3/4

Sensitive Data and AI Literacy

Identifying and **correcting** biases in AI models often requires the use of **sensitive data**, raising concerns regarding compliance with **GDPR data protection** rules. At the same time, fostering AI literacy poses a challenge for businesses with limited resources. The package introduces proportionate measures to facilitate these processes, whilst maintaining a balance between innovation, fairness and the protection of fundamental rights.

Expanded legal basis for sensitive data

The package **extends** the **legal basis** for **processing** special categories of data (Article 9 of the GDPR) in bias detection and correction, not only for high-risk AI but potentially for **GPAI** as well. This allows for the use of sensitive data where synthetic or anonymised data are insufficient, subject to justified and documented exceptions.

Term of Use

The exceptions are limited: **processing restricted** to what is strictly necessary, a ban on disclosure to third parties, immediate deletion following corrections, a complete audit trail, and verification of necessity and proportionality. The Commission is thus strengthening Article 10(5) of the original AI Act, addressing the tension between data quality and privacy.

Enhanced documentation and accountability

Providers must document every instance of the use of **sensitive data** in internal records and **technical documentation**, subject to national and European oversight. This ensures accountability, with **GDPR** penalties applicable in the event of misuse, but makes the process more predictable for those acting in good faith.

AI literacy

With regard to **AI literacy requirements** (Article 4 of the AI Act), the focus is shifting from the direct responsibility of businesses to public support measures: sector-specific guidelines, free courses, EU certifications and national programmes. This facilitates staff upskilling without imposing fixed costs on SMEs.

Balancing innovation, inclusion and privacy

The amendments strike a delicate balance between three **key factors**:

- model effectiveness (reduced bias)
- inclusivity (representative data)
- the protection of rights (GDPR compliance).

The Digital Omnibus Act brings the AI Act into force, preventing innovation from being stifled.

Key Amendments to the AI Act Framework 4/4

Governance and AI Office

With the **Digital Omnibus**, the governance of the **AI ACT** becomes more clearly anchored at **EU level**. The proposal strengthens the **AI Office** as a centre of expertise, supervision, and coordination, especially for **GPAI-based systems** and **cross-border cases**. This responds to early **implementation frictions**, including uneven **national readiness** and limited availability of **standards** and **guidance**. The aim is to reduce **fragmentation across member states** and make **enforcement** more coherent. In this sense, **simplification** also concerns **institutions**, not only companies.

AI Office

The **Digital Omnibus** further **reinforces** the **AI Office** as the **EU's main centre of competence** for the implementation of the **AI Act**. Its role becomes more **operational** and more visible, particularly in relation to **general-purpose AI models** and to **AI systems built on those models**. This means that the **AI Office** is not only a **policy** and **coordination body**, but increasingly a practical **supervisory actor** within the **European governance.**

Oversight

The proposal also moves towards more **centralized oversight** in cases considered more significant from a **market** and **risk perspective**. In particular, the **AI Office** would supervise **AI systems** integrated into **very large online platforms** or **search engines**, as well as systems based on **GPAI** where both the **model** and the **system** are provided by the same entity. This reflects a clear intention to place the most impactful and **cross-border cases** under stronger **EU-level scrutiny.**

Coordination

Another core objective is to improve **coordination** between the **European** and **national levels of enforcement**. The **Omnibus** seeks to reduce **divergent interpretations** and uneven **supervisory practices** across **Member States** by clarifying **competences** and embedding **national authorities** within a more structured **EU framework**. In practice, this supports a model in which **national regulators** remain important, but operate within a **stronger coordination system** led by the **AI Office** and supported by the **AI Board**.

03

Impacts on Businesses and Market – AI Act

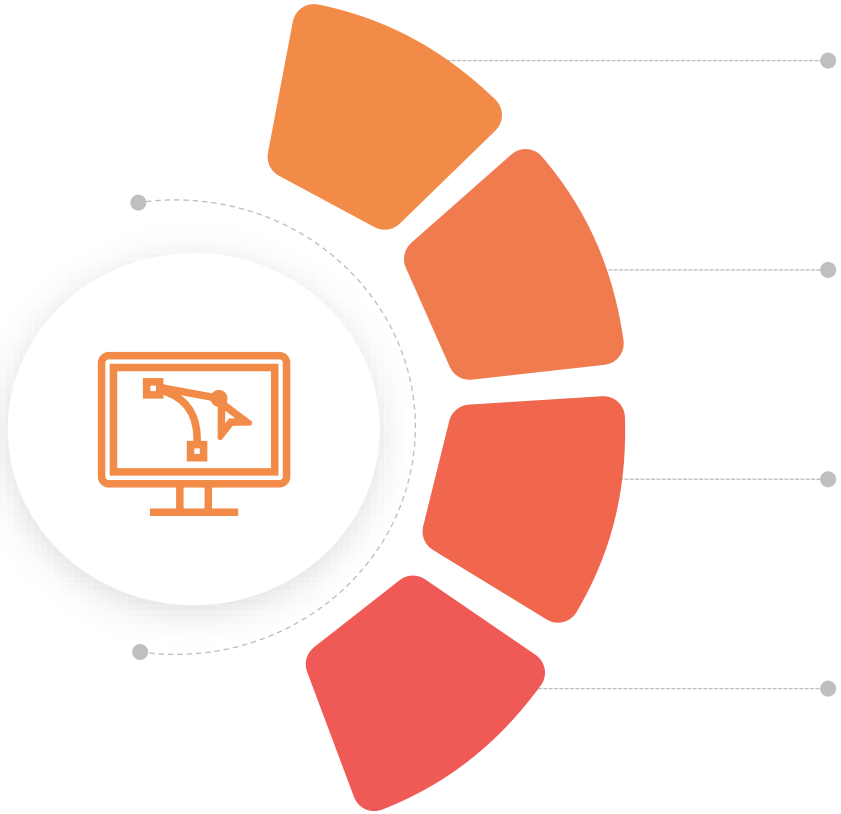
From Abstract Obligation to Manageable Compliance

Simplification or Weakening? The Real Trade-Off

Impacts on Businesses and Market – AI Act 1/2

From Abstract Obligation to Manageable Compliance

For companies, **the Digital Omnibus** aims to make **compliance** under the **AI Act** more operational and less fragmented. It revises **timelines, documentation requirements, conformity assessment procedures**, and the interaction with other **EU rules**. A key objective is to avoid forcing firms into full compliance before the necessary **standards, guidance**, and **compliance tools** are in place. The result is a more **phased** and realistic **implementation path**. In practice, the proposal aligns legal obligations more closely with companies' actual **capacity to comply**.



Timing

High-risk AI obligations are no longer treated as purely **calendar-driven**. Instead, the **Digital Omnibus** links key **compliance milestones** to the actual availability of **harmonized standards**, **common specifications**, and other **supporting tools**. This should reduce the risk of companies being required to comply before the **regulatory framework** is technically ready.

Assessment

The proposal simplifies **conformity assessment** by making it more coordinated and less duplicative. In practice, this means a clearer and more efficient process for businesses whose **AI systems** may also fall under other **EU harmonized legislation**. The aim is to reduce **procedural overlap** and make the **compliance route** more predictable.

Relief

SMEs and **small mid-caps** benefit from more proportionate **obligations** and **lighter documentation requirements**. The **Digital Omnibus** recognizes that smaller operators often lack the same **legal** and **organizational resources** as large incumbents. The objective is to avoid imposing the same **administrative burden** on businesses with very **different capacities**.

Clarity

For companies developing or **deploying AI**, the main benefit is greater **operational certainty**. Less **duplication**, more **proportionality**, and more consistent **sequencing of obligations** make the **compliance journey** easier to manage. This is especially relevant for **scale-ups, fintechs** and other operators integrating **AI into core business processes**.

Impacts on Businesses and Market – AI Act 2/2

Simplification or Weakening? The Real Trade-Off

The most **sensitive issue** in the **Digital Omnibus** is how to simplify **implementation** without weakening the **safeguards** established by the **AI Act**. The proposal has therefore triggered debate among **EU institutions, academics, consumer groups, and privacy bodies**. While **simplification** is broadly supported, several **stakeholders** argue that some **amendments** may go too far. The real question is not whether **simplification** is needed, but how far it can go without undermining **rights, transparency, and regulatory credibility.**

Safeguards

A more **gradual application** of **high-risk obligations** can give businesses greater **legal certainty** and more time to prepare, but it may also delay the effective **protection** that those rules were designed to provide. Several critics argue that if **graduality** becomes a substantive **postponement** rather than a technical adjustment, the result could be a weakening of the **AI Act's original protective function**.

Data Use

The proposal to allow, on an **exceptional basis**, the use of **special categories of personal data** for **bias detection and correction** is one of the most contested elements of the package. Supporters see it as necessary to improve **fairness and model quality**, while critics warn that it could normalise broader processing of highly **sensitive data**. This creates a particularly delicate trade-off between **anti-bias objectives** and **data protection guarantees.**

Pressure

Some **amendments** are seen as reducing **regulatory pressure** on potentially **sensitive** or **borderline uses of AI**. In particular, criticism has focused on the easing of **AI literacy obligations** and on the removal of **registration requirements** for certain systems that providers classify as **non-high-risk**. According to several **stakeholders**, these changes could reduce **transparency**, **limit accountability**, and make **supervisory visibility** weaker in practice.

Dependence

A more **flexible framework** also increases reliance on future **guidance, harmonized standards, and supervisory practice**. Much of the real balance between **simplification** and **protection** will depend on how these tools are developed and applied over time. This means that the **credibility** of the **Omnibus** will ultimately rest not only on the **legal text** itself, but also on the quality of **implementation and enforcement**.

04

Conclusions & Takeaways

Key Takeaways

Next Steps

Conclusions & Takeaways 1/2

Key Takeaways

The **Digital Omnibus** does not replace the AI Act, but seeks to make its implementation more workable, **coherent**, and **proportionate**. Its overall direction is to reduce regulatory friction while preserving the core objectives of **safety**, **transparency**, and **fundamental rights protection**.

1. **Not a new AI Act, but a targeted refinement:**
The Omnibus **preserves** the original **structure** and **risk-based logic** of the AI Act, while introducing targeted adjustments in those areas that proved more difficult to apply in practice during the early implementation phase.

2. **Stronger focus on practical compliance:**
The reform **aims** to make **obligations clearer**, better sequenced over time, and easier to manage in practice for both companies and regulators, especially in those areas where implementation has proved more complex and fragmented.

3. **More proportionate and coordinated implementation:**
The proposal seeks to **reduce overlaps across EU digital rules**, ease compliance burdens on smaller operators, and promote a more consistent and proportionate application of requirements across the broader European regulatory framework.

4. **More visible EU-level governance model:**
The stronger **role** of the **AI Office** points to a more **coordinated** and **structured approach** to supervision and enforcement, with the aim of reducing fragmentation across Member States and ensuring more consistent implementation at EU level.

5. **Simplification remains a delicate balancing exercise:**
The main **challenge** is to **improve** the practical **feasibility** of the **framework** without weakening rights protection, accountability, and the level of trust that the regulatory system is meant to ensure over time.

Conclusions & Takeaways 2/2

Next Steps

The practical **impact** of the Digital Omnibus will depend not only on the **legal text**, but also on how **implementation tools**, **standards**, and **supervisory practices** evolve over time. The next phase will therefore be shaped by both legislative developments and operational readiness across the EU.

Standards and guidance will be critical for real implementation:
Much of the **framework's** effectiveness will depend on how obligations are translated into practical **tools** and supervisory expectations.

The EU digital rulebook will likely continue to evolve:
The **Omnibus** should be seen as part of a broader **regulatory** adjustment process rather than a final settling point.

Further changes may emerge during the legislative process:
The final **balance** of the reform will depend on how **EU institutions** refine the proposal in the next stages.

Companies will need to adapt their compliance models over time:
Simplification **reduces friction**, but it does not remove the need for robust governance, documentation, and oversight.

ESSENTIAL SERVICES FOR FINANCIAL INSTITUTIONS

iason is an international consulting firm that has been supporting both financial institutions and regulators in topics related to Risk Management, Finance and ICT since 2008

Strategy

Strategic advisory on the **design** of **advanced frameworks** and **solutions** to fulfil both **business** and **regulatory needs** in Risk Management and IT departments

Methodology & Governance

Implementation of the designed **solutions** in bank departments **Methodological support** to both **systemically important financial institutions** and **supervisory entities**

Solution

Advanced **software solutions** for **modelling, forecasting, calculating** metrics and **integrating** risks, all on cloud and distributed in Software-as-a-Service (**SaaS**)

KEEP IN TOUCH

iason

Company Profile

iason is an international firm that consults Financial Institutions on Risk Management. **iason** integrates deep industry knowledge with specialised expertise in Market, Liquidity, Funding, Credit and Counterparty Risk, in Organisational Set-Up and in Strategic Planning.

Fabrizio Gentalavigna

Gaspare Campaniolo

Vincenzo Marano

Gabriele Donadoni

Amal Ben Abdallah

www.iasonltd.com