

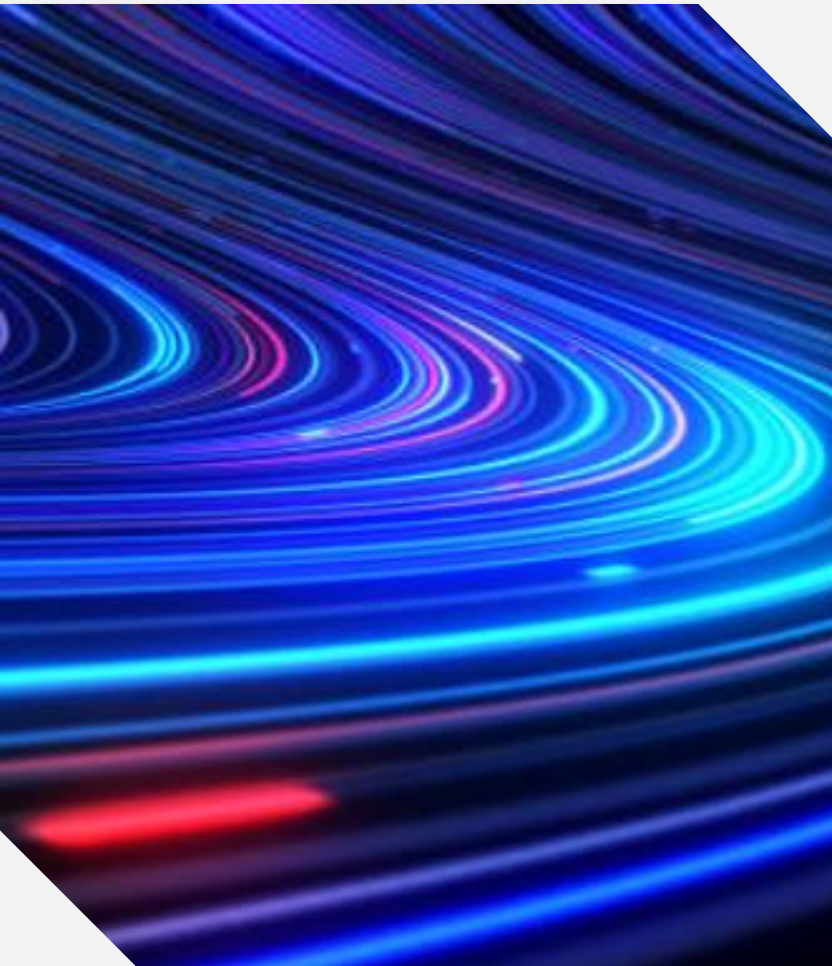
# Third-Party Technology

Key Considerations for Firms

*March 2024*



- Artificial intelligence (“AI”) systems are the core regulatory target of the upcoming European Union Artificial Intelligence (“AI”) Act (the “EU AI Act”), whether they are built in-house or procured from a third-party.
- When firms are procuring third-party AI systems, especially those classified as high-risk under the EU AI Act, several critical considerations emerge from the legislation. These considerations are pivotal for ensuring compliance with the Act and maintaining operational integrity and legal accountability.
- Ahead of the EU AI Act’s scheduled entry into force in 2024, this document looks at key considerations for firms thinking of using third-party technology (“T-PT”) (i.e. off-the-shelf) AI systems, based on data from the Financial Conduct Authority’s (“FCA”) guidance document in regard to T-PT banking solutions produced in July 2014, as the recent technology boom has seen firms procuring a large number of AI systems from T-PT providers (e.g. OpenAI) (see **Slide 9**).
- For example, **Article 28 (Responsibilities Along the AI Value Chain)** of the EU AI Act requires firms to be aware that if they, as distributors, importers, deployers, or other third parties, put their name or trademark on a high-risk AI system already on the market, make substantial modifications to it, or modify its intended purpose in a way that it becomes a high-risk AI system, they will be considered the provider of that AI system and subject to the obligations of the provider under Article 16. This includes ensuring compliance with the conformity assessment of high-risk AI systems.



## Evaluate the Business Case

- Before engaging third parties for critical technology services, thoroughly assess whether there is a clear business case or rationale for doing so.
- Determine if outsourcing these services aligns with the strategic objectives and needs of the organization.

## Assess Risks and Mitigation Strategies

- Conduct a comprehensive evaluation of the business risks associated with using third parties for critical technology services.
- Identify potential risks such as data breaches, service disruptions, or loss of intellectual property.
- Develop robust mitigation strategies to address and manage these risks effectively.

## Consideration of Key Factors

- Ensure that the decision-making process includes consideration of key factors such as cost-effectiveness, expertise of third-party providers, and scalability of services.
- Evaluate the potential impact on the organization's reputation, compliance requirements, and regulatory obligations.

## Customisation and Tailoring to Domestic and Firm Requirements

- Ensure that any proposed solution can be tailored to meet both domestic regulatory requirements and the specific needs of the firm.
- Assess the feasibility and flexibility of the solution to accommodate necessary adjustments to comply with local regulations and internal policies.

## Validation of Solution Usage

- Investigate whether the proposed solution is already in use by other firms in the UK.
- Seek references or case studies from existing users to understand their experiences and the suitability of the solution for similar needs.

## Assessment of Required Changes

- Evaluate the degree of customization or modification needed to tailor the solution to meet the firm's specific needs.
- Prioritize requirements and assess the impact of changes on functionality, integration, and usability.

## Retained Accountability and Oversight

- Acknowledge that the regulated firm retains full accountability for fulfilling its responsibilities under the regulatory system and cannot delegate this to a service provider.
- Develop a robust oversight framework to monitor the services provided by an Outsourced Service Provider (OSP) and ensure compliance with regulatory requirements.

## Responsibility Allocation

- Define clear lines of responsibility for overseeing the day-to-day and strategic management of the service supplier within the firm's organizational structure.
- Assign dedicated personnel or teams with the appropriate skills and expertise to perform oversight functions effectively.

## Management Information Requirements

- Define the management information requirements necessary to support the oversight and management of the service provider.
- Ensure that relevant data and performance metrics are available in a timely fashion to facilitate informed decision-making.

## Establishing Target Quality of Service

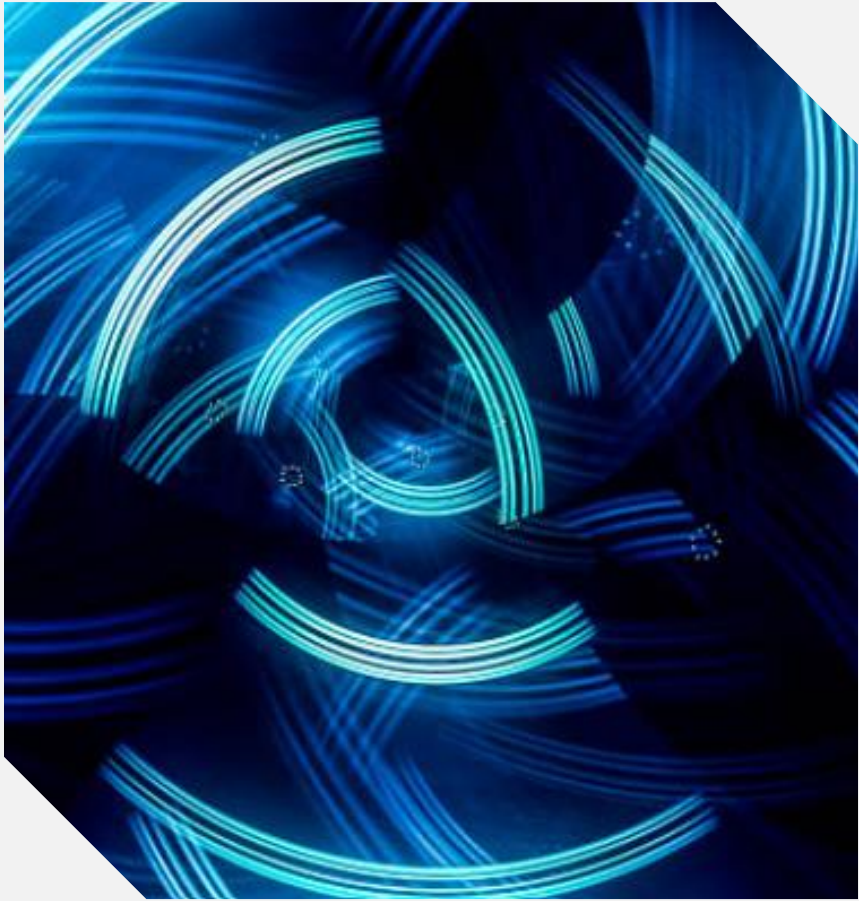
- Begin by defining clear and measurable targets for the quality of service expected from third-party arrangements.
- Ensure these targets align with the firm's overall quality objectives and are realistic and achievable.

## Alignment of Third-Party Arrangements

- Review arrangements with third parties to ensure they are aligned with the firm's quality of service objectives.
- Verify that contracts, service level agreements (SLAs), and other agreements explicitly support the realization of these objectives.

## Assigning Responsibility for Quality of Service

- Clearly designate responsibility for overseeing and ensuring the quality of service within the firm's organizational structure.
- Assign specific individuals or teams accountable for monitoring and maintaining service quality standards.



## Specifying Service Availability Requirements

- Clearly define and agree upon service availability requirements with each service supplier.
- Ensure that these requirements are documented in service level agreements (SLAs) to establish expectations for uptime and availability.

## Preventing Service Outages

- Take proactive steps to prevent service outages by implementing robust monitoring, maintenance, and redundancy measures.
- Invest in infrastructure redundancy, failover systems, and continuous monitoring to minimize the risk of disruptions.

## Implementing Disaster Recovery Plans

- Develop comprehensive disaster recovery plans for both the firm and each service supplier.
- Ensure that these plans include procedures for data backup, system recovery, and business continuity in the event of service disruptions or disasters.

## Segregation of Data

- Ensure that the firm's data is appropriately segregated to maintain confidentiality, integrity, and availability.
- Implement access controls and data segregation measures to prevent unauthorized access and data leakage.

## Encryption During Transmission

- Encrypt data during transmission to protect it from interception or unauthorized access.
- Utilize secure communication protocols such as SSL/TLS to encrypt data in transit over networks.

## Data Jurisdiction Considerations

- Evaluate the jurisdiction where data is held and processed to ensure compliance with regulatory requirements and data protection laws.
- Ensure that data is stored and processed in jurisdictions with adequate legal protections for privacy and data security.



# Examples

Purpose

Writing

Uses

Third-Party Tool



Imagery

Uses



Data

Uses



# Contact Details



AI  
AI & Partners

Amsterdam - London - Singapore



Email

[contact@ai-and-partners.com](mailto:contact@ai-and-partners.com)



Phone

+44(0)7535 994 132



Website

<https://www.ai-and-partners.com/>



Social Media

LinkedIn: <https://www.linkedin.com/company/ai-&-partners/>

Twitter: [https://twitter.com/AI and Partners](https://twitter.com/AI_and_Partners)



AI  
AI & Partners

**Amsterdam - London - Singapore**

**Thank You!**

# Disclaimer

This Presentation may contain information, text, data, graphics, photographs, videos, sound recordings, illustrations, artwork, names, logos, trade marks, service marks, and information about us, our lines of services, and general information may be provided in the form of documents, podcasts or via an RSS feed (“the Information”).

Except where it is otherwise expressly stated, the Information is not intended to, nor does it, constitute legal, accounting, business, financial, tax or other professional advice or services. The Information is provided on an information basis only and should not be relied upon. If you need advice or services on a specific matter, please contact us using the contact details for the relevant consultant or fee earner found on the Presentation.

The Presentation and Information is provided “AS IS” and on an “AS AVAILABLE” basis and we do not guarantee the accuracy, timeliness, completeness, performance or fitness for a particular purpose of the Presentation or any of the Information. We have tried to ensure that all Information provided on the Presentation is correct at the time of publication. No responsibility is accepted by or on behalf of us for any errors, omissions, or inaccurate information on the Presentation. Further, we do not warrant that the Presentation or any of the Information will be uninterrupted or error-free or that any defects will be corrected.

Although we attempt to ensure that the Information contained in this Presentation is accurate and up-to-date, we accept no liability for the results of any action taken on the basis of the Information it contains and all implied warranties, including, but not limited to, the implied warranties of satisfactory quality, fitness for a particular purpose, non-infringement, compatibility, security, and accuracy are excluded from these Terms to the extent that they may be excluded as a matter of law.

In no event will we be liable for any loss, including, without limitation, indirect or consequential loss, or any damages arising from loss of use, data or profits, whether in contract, tort or otherwise, arising out of, or in connection with the use of this Presentation or any of the Information.