protiviti®
Global Business Consulting

Understanding the Impact of the EU AI Act: A Primer for Financial Institutions

By Carol M. Beaumier

The EU AI Act (Act) is arguably the most significant and wide-reaching AI regulation to date issued by any jurisdiction. It offers an integrated approach aimed at both promoting the beneficial uses of AI and managing the risks identified in the Act, while ensuring its ethical and responsible use. The Act has extraterritorial application and impacts any company that provides or uses AI services or products in the EU, including companies that offer B2B AI services that are provided to or used by EU citizens, regardless of where a company is headquartered. For both EU-domiciled and multinational financial institutions, therefore, understanding the requirements of the Act is a business imperative.

What should all companies know about the EU AI Act?

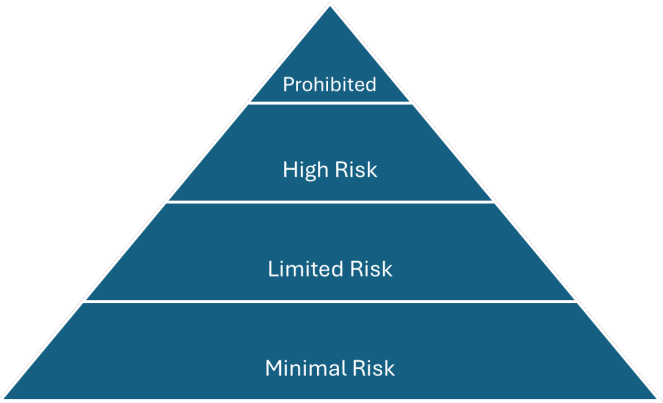
Underpinning the Act are a number of important principles including proportionality based on risk, transparency and accountability, fairness and non-discrimination, prevention of harm, data privacy and security, safety and trustworthiness, and the need for human oversight.

> *AI system*: a machine-based system designed to operate with varying levels of autonomy; may exhibit adaptiveness after deployment; infers from the input it receives; generates outputs such as content, predictions, recommendations, or decisions; and can influence physical or virtual environments.
>
> **As defined by the EU AI Act**

The Act adopts a risk-based approach to categorising AI systems:

- **Unacceptable**: Systems that pose a clear threat to the safety, livelihood or rights of people.
- **High**: Systems with significant implications that need stringent oversight due to their potential impact.
- **Limited**: Systems with lesser implications but that still require some level of transparency to ensure users know they are interacting with an AI system.
- **Minimal**: Systems that pose negligible risks to users' rights or safety.

EU AI Act levels of risk



Examples of AI Systems
Social scoring system[1]
Credit scoring/credit assessment system
Customer service chatbot
Email spam filter

The Act relies on the partnership of providers and deployers to foster and maintain the safety and trustworthiness of AI. Deployers are users of a system. Providers develop AI systems or have AI systems developed and placed on the market under their names or trademarks, whether for payment or free of charge.

All AI systems must be risk-assessed and included in an AI inventory. Providers are responsible for ensuring that AI systems comply with the Act before they are placed on the market or put into service. For high-risk systems that are subject to the strictest requirements, this means conducting a conformity assessment to ensure the system meets the requirements of the Act, maintaining comprehensive technical documentation that demonstrates the system's compliance with regulatory requirements, developing and maintaining a risk management system throughout the lifecycle of the AI system, maintaining system-generated logs to ensure traceability of the system's functioning, ensuring clear and accurate information (including system limitations) is provided to users, performing post-deployment monitoring to assess the system's performance throughout its lifecycle, and reporting any malfunctions or serious incidents to the appropriate authorities. In addition, providers of certain types of high-risk AI are required to register their systems in an EU database before deployment.

Deployers are responsible for using high-risk AI systems in accordance with their intended purpose as stipulated by providers and managing the risks that may result from misuse or malfunction; ensuring that relevant, representative bias-free data is used by the system and that usage of data complies with data protection regulations, as needed; ensuring human oversight, when required; and monitoring and reporting immediately any malfunctions or significant abnormalities that affect health, safety or fundamental rights. A deployer may be reclassified as a provider if it makes significant modifications to an AI system that is or becomes high-risk.

[1] Social scoring AI systems use data points like social behavior, personality characteristics, and other data to evaluate people and determine their access to benefits like education, healthcare, and public transportation. People with good scores receive advantages, while those with bad scores may be punished or denied benefits.

Limited-risk AI applications must be designed so users know they are interacting with a machine and not with a human being. Minimal risk AI systems are not subject to specific requirements under the Act, although they are still expected to conform to the fundamental principles of responsible AI under voluntary codes of conduct.

The Act entered into force on August 1, 2024, with provisions phasing in over the next three years. Rules related to high-risk systems start coming into play on August 2, 2026. National authorities within the EU are afforded enforcement authority under the Act, which sets fines for non-compliance up to 7% of global annual turnover or €35 million, whichever is greater.

For additional information about the Act, read about what business leaders should know.

How will the EU AI Act affect the financial services industry?

> In the rapidly evolving world of finance, artificial intelligence (AI) stands out as a transformative force reshaping the landscape of financial services.
>
> **The Transformative Impact of AI On Financial Services** (forbes.com)

Fraud and money-laundering detection systems, customer due diligence and customer rating systems, credit scoring systems, algorithmic trading systems, investment optimisation/asset management decisioning, insurance underwriting systems, and robo-advisors – these are just a sample of AI systems used by financial institutions that fall under the purview of the AI Act. While the Act applies broadly to all industries, its impact on the financial services industry may be greater as financial services is a heavy user of AI and because it is such a highly regulated industry where multinational firms often need different compliance strategies for different markets.

One of the challenges that financial institutions will face is ensuring that they can evidence that both new and existing AI systems comply with the rigorous standards of the Act related to, among other considerations, transparency, fairness, accountability and oversight. The number of AI systems used by financial institutions varies significantly based on factors such as size of the institution, the geographic regions in which the institution operates, and where the institution is on its digital transformation journey. For larger financial institutions, the number of AI systems used may be in the hundreds. Financial institutions that developed or deployed AI systems prior to the effective date of the Act will need to reassess whether these systems meet the criteria of the Act. With the consumer protections embedded in the Act, for example, this may require financial institutions to modify existing systems. It may also require additional steps to inform customers impacted by high-risk systems on how their data is being used and how AI systems are formulating recommendations and decisions.

The Act also applies to the use of third-party AI systems. Under the shared responsibility model, this means if a financial institution uses a third-party AI system that falls under the high-risk category, both the provider of that AI system (the third party) and the deployer (the financial institution) have specific responsibilities to ensure compliance. Where a financial institution has significantly modified or customised a third-party system – not an uncommon practice – additional effort may be required to evidence compliance.

Call to action

As part of effectuating the strategic AI core principles listed above, there are a number of steps financial institutions should be taking now to ensure compliance with the Act. These include, but are not limited to:

- Conducting an impact assessment of the Act and mapping its requirements to existing policies, procedures and programs (e.g., Model Risk Management, Data, Third Party Risk Management) where there may be dependencies or overlaps.
- Training staff on the ethical use of AI and the specific requirements of the AI Act.
- Identifying all AI systems (including third-party systems) used in the EU and grouping them into the risk categories established by the Act.
- Reviewing/supplementing AI system documentation to ensure it meets the standards of the Act, given the financial institution's role as a provider or deployer.
- For non-EU domiciled financial institutions, determining differences between the EU requirements and those of the financial institution's home country (and other host countries in which it operates) and developing and implementing a strategy for complying with all applicable requirements which should be documented in an institution's AI Use Policy.
- Evaluating the datasets used by AI systems to understand how they are sourced and to ensure they are accurate and complete, fair and free of bias, and that usage complies with applicable data protection requirements.
- Determining what changes need to be made to operational procedures, e.g., data controls or system logs, to ensure ongoing compliance with the Act.
- Identifying the need for additional customer communications and developing a communications plan.
- Considering how steps taken to comply with the Act align with the company's global AI program, i.e., can the company support that it has a cohesive and uniform application of AI standards across the organisation?

Proponents of the Act believe that its strict standards will lead to increased customer trustworthiness and acceptance of AI systems. Detractors claim the Act may stifle innovation as a result of these strict standards. In time, we will know which view is correct. Indisputable for now is that all companies, including financial institutions, which provide or use AI services or products in the EU, must comply with the Act or face the potentially significant penalty of non-compliance.

How Protiviti can help

Whether your organisation is just getting started with AI technologies or is far along on its journey to explore advanced use cases, Protiviti can provide support and guidance to help lead your organisation to successful outcomes along the entire lifecycle of AI adoption, all while ensuring compliance with the EU AI Act. We can assist with:

- **Considering AI**: Protiviti can assist with the identification of potential areas where AI can bring value to operations, products, or services, and outline a deployment plan. Considerations include Business Value Definition, Data Accessibility, Operational Readiness, Strategic Alignment and Governance.
- **Implementing AI**: Protiviti can help the successful development and deployment of AI solutions that address specific business challenges or opportunities. Considerations include proving initial hypotheses and technical challenges, defining clear objectives for AI projects, selecting appropriate AI techniques and allocating resources, ensuring close collaboration between all relevant stakeholders, and designing and effectuating strong governance.
- **Monitoring AI**: Protiviti can aid the measurement of the effectiveness and impact of AI solutions on operations and/or goals. Considerations include establishing relevant performance metrics, revising risk management taxonomies and processes to cover AI holistically, conducting thorough testing and validation of the AI models, and creating feedback loop and continuous monitoring.
- **Securing AI**: Protiviti can help organisations protect AI systems and data from potential threats and ensure their ethical and responsible use. Considerations include implementing robust cybersecurity measures to safeguard AI models, addressing AI bias and fairness concerns, and adhering to ethical guidelines and regulatory requirements (e.g., transparency, privacy).

In summary, Protiviti can not only help empower your organisation's AI journey but ensure such is being achieved with adherence to all aspects and considerations of the EU AI Act.

The author wishes to thank Protiviti New York Managing Director Constantine Boyadjiev and Protiviti Frankfurt Director Denis Lippolt for their contributions to this article.

About the author

Carol Beaumier is a senior managing director in Protiviti's Risk and Compliance practice and leader of the firm's APAC Financial Services practice. Based in Metro D.C., she has more than 30 years of experience in a wide range of regulatory issues across multiple industries. Before joining Protiviti, Beaumier was a partner in Arthur Andersen's Regulatory Risk Services practice and a managing director and founding partner of The Secura Group, where she headed the Risk Management practice. Before consulting, Beaumier spent 11 years with the U.S. Office of the Comptroller of the Currency (OCC), where she was an examiner with a focus on multinational and international banks. She also served as executive assistant to the comptroller, as a member of the OCC's senior management team and as liaison for the comptroller inside and outside of the agency. Beaumier is a frequent author and speaker on regulatory and other risk issues.