# Operational Resiliency in the Age of AI Regulation: A Strategic Briefing for Banking Leadership on the EU AI Act

## I. Executive Summary

The European Union's Artificial Intelligence Act (Regulation (EU) 2024/1689) represents a watershed moment in global technology regulation. As the world's first comprehensive, binding legal framework for AI, it establishes a risk-based approach that will have profound and lasting implications for the financial services sector.1 This briefing provides senior leadership with a detailed analysis of the Act's impact on AI model operational resiliency, translating complex legal mandates into strategic and operational imperatives for large, multinational banking institutions.

The key findings of this analysis are stark: the Act explicitly designates core banking systems, most notably those used for credit scoring and creditworthiness assessment, as "high-risk." This classification triggers a suite of stringent new operational resiliency requirements that extend far beyond traditional IT availability and business continuity. The legislation mandates auditable proof of a model's accuracy, robustness against errors and malicious attacks, cybersecurity, transparent data governance, and effective human oversight throughout its entire lifecycle.

These new obligations necessitate a fundamental evolution of existing internal governance structures. The traditional paradigm of Model Risk Management (MRM), heavily focused on pre-deployment validation, must be augmented with a robust framework for continuous, post-deployment monitoring and *ex-post* risk management. Similarly, Third-Party Risk Management (TPRM) and internal audit functions must integrate new, AI-specific controls and capabilities.

Critically, the Act possesses a significant extraterritorial reach, mirroring that of the General Data Protection Regulation (GDPR). US-based operations of multinational banks will be directly impacted if AI models developed or hosted in the US produce outputs that are used within the EU. This creates an urgent need for a cohesive, transatlantic compliance strategy.

This briefing concludes that immediate, decisive action is required. Leadership must prioritize the creation of a comprehensive AI systems inventory, initiate a gap analysis of current governance frameworks against the Act's mandates, and begin developing a unified, cross-border compliance roadmap. Proactive engagement with these requirements is not merely a matter of legal compliance; it is a strategic necessity for maintaining operational resilience, customer trust, and competitive leadership in an increasingly AI-driven financial landscape.

## II. High-Risk AI Systems in Banking: Classification and Resiliency Mandates

The AI Act's most direct and significant impact on the banking sector stems from its classification of specific AI use cases as "high-risk".4 This designation is not a discretionary risk assessment but a legal classification that automatically subjects these systems to the Act's most stringent requirements.

### Defining the High-Risk Perimeter

Annex III of the Act enumerates the specific AI systems that are, by definition, considered high-risk. For a large banking institution, the following categories are of paramount importance 6:

* **Access to Essential Private Services:** The Act explicitly targets AI systems intended to be used "to evaluate the creditworthiness of natural persons or establish their credit score".6 This provision captures a wide array of models at the heart of retail and commercial banking, including those for mortgage origination, personal loans, credit card approvals, and small business lending. Any system that influences an individual's access to credit falls squarely within this high-risk perimeter.
* **Critical Infrastructure:** Also designated as high-risk are AI systems intended to be used as "safety components in the management and operation of critical digital infrastructure".6 Within a banking context, this can be interpreted to include AI systems that manage the stability and security of core banking platforms, high-value payment processing systems, liquidity management tools, and critical cybersecurity infrastructure like advanced threat detection. A failure in these systems could pose a risk to the bank's operational integrity and, potentially, systemic stability.

A crucial distinction within the Act provides a degree of operational clarity: AI systems "used for the purpose of detecting financial fraud" are explicitly exempted from the high-risk category under the "essential services" provision.6 While this is a significant exemption, it also introduces a critical operational boundary. In practice, models that detect fraud can directly impact a customer's ability to transact or access funds, blurring the line with systems that evaluate eligibility for a service. Therefore, institutions must establish and maintain rigorously documented "intended purpose" definitions for each model to justify its classification and avoid applying a lower standard of care to a system that is, in effect, performing a high-risk function.8

### The Pillars of Operational Resiliency under the Act

For systems classified as high-risk, the AI Act mandates a comprehensive set of lifecycle requirements detailed primarily in Articles 9 through 15. These form the new pillars of AI operational resiliency.9 An AI system can be fully operational from an IT perspective (i.e., online and processing data) yet be fundamentally non-compliant and non-resilient under the Act if it fails to meet these behavioral and governance standards. This represents a paradigm shift from traditional IT resiliency, which focuses on uptime and recovery (as governed by regulations like DORA), to a new concept of *model integrity* resiliency.10

The core mandates include:

* **Accuracy, Robustness, and Cybersecurity (Article 15):** This is the technical foundation of AI resiliency. High-risk systems must be designed and developed to achieve an appropriate level of performance and to perform consistently throughout their lifecycle.12
  + **Accuracy:** The system's levels of accuracy and its relevant metrics must be clearly declared in its instructions for use, creating a benchmark for ongoing performance monitoring.12
  + **Robustness:** Systems must be resilient to errors, faults, or inconsistencies. This requires the implementation of technical redundancy, such as backup or fail-safe plans.12 For adaptive systems that learn after deployment, specific measures are required to prevent biased outputs from creating negative feedback loops that degrade performance over time.12
  + **Cybersecurity:** The system must be resilient against attempts by unauthorized third parties to alter its use, outputs, or performance by exploiting vulnerabilities. The Act specifically calls for technical solutions to prevent and control AI-specific attacks, such as training data manipulation (data poisoning), model poisoning, and the use of adversarial inputs designed to cause the model to misclassify outputs.4
* **Risk Management System (Article 9):** Providers must establish, implement, document, and maintain a risk management system. This is not a one-time assessment but a "continuous iterative process" that runs throughout the AI system's entire lifecycle, requiring regular review and updates.15 The process must include the identification of known and foreseeable risks, the adoption of mitigation measures, and comprehensive testing.4
* **Data and Data Governance (Article 10):** Recognizing that data is the foundation of any AI system, the Act mandates stringent governance practices. Training, validation, and testing datasets must be "relevant, representative, free of errors and complete".4 This requires robust processes for data collection, preparation, and a thorough examination of possible biases that could lead to discriminatory outcomes.7
* **Record-Keeping and Logging (Articles 12 & 19):** High-risk systems must be designed with the capability to automatically record events ("logs") while the system is in operation. This is to ensure a level of traceability of the system's functioning and to facilitate post-incident investigation and monitoring by both the deployer and regulatory authorities.9
* **Transparency and Human Oversight (Articles 13 & 14):** High-risk systems cannot be opaque "black boxes." They must be designed to be sufficiently transparent to allow deployers (the bank) to interpret the system's output and use it appropriately. Providers must supply clear instructions for use, detailing the system's capabilities and limitations.7 Crucially, systems must be designed to facilitate effective human oversight. This means a designated person must be able to monitor the system's behavior and have the authority and ability to intervene, decide not to use the system's output, or interrupt or disable the system entirely.4

The following table summarizes these new mandates for key banking functions.

**Table 1: High-Risk AI Systems in Banking and Corresponding Resiliency Requirements**

|  |  |  |  |
| --- | --- | --- | --- |
| **High-Risk Banking Use Case (Annex III)** | **Key Resiliency Requirement** | **Operational Mandate under the AI Act** | **Relevant Article(s)** |
| AI for Credit Scoring of Natural Persons | Accuracy | Must achieve a declared level of accuracy and perform consistently. | Article 15 |
| AI for Creditworthiness Evaluation | Robustness | Must be resilient to errors and faults, with documented fail-safe plans. Must mitigate risks of biased feedback loops. | Article 15 |
| AI for Managing Critical Payments Infrastructure | Cybersecurity | Must be protected against unauthorized alteration of use or performance, including data poisoning and adversarial attacks. | Article 15 |
| All High-Risk Banking Systems | Risk Management | Must be subject to a continuous, iterative risk management process throughout the entire model lifecycle. | Article 9 |
| All High-Risk Banking Systems | Data Governance | Training, validation, and testing data must be high-quality, representative, and scrutinized for biases. | Article 10 |
| All High-Risk Banking Systems | Logging | Must automatically record events (logs) to ensure traceability of the system's functioning and decisions. | Articles 12, 19 |
| All High-Risk Banking Systems | Human Oversight | Must be designed to allow for effective human monitoring, intervention, and the ability to override or disable the system. | Article 14 |

## III. Adapting Governance Frameworks for AI Resiliency

The AI Act's mandates require more than just new technology; they demand a significant evolution of the bank's internal governance frameworks. While the Act acknowledges that heavily regulated entities like banks can leverage existing structures, the unique nature of AI challenges the efficacy of traditional, siloed approaches to risk management.5

### The Evolution of Model Risk Management (MRM)

For years, MRM has focused primarily on *ex-ante* validation—ensuring a model's theoretical soundness through careful design, backtesting, and documentation before deployment.5 While this remains necessary, it is no longer sufficient. The capacity of AI models for self-engineering and adaptation means that a model approved at launch can "drift" over time as it encounters new data, rendering the initial validation obsolete.5

The AI Act compels a shift toward a more balanced approach with a greatly enhanced emphasis on ex-post risk management and continuous monitoring.5

Recommendations:

* MRM teams must expand their mandate from a pre-deployment gatekeeper to a lifecycle supervisor. This requires developing new capabilities and tools for real-time performance monitoring, ongoing bias and fairness testing, and continuous validation of model explainability.
* MRM policies must be fundamentally updated. New policies should define clear thresholds for performance degradation, data drift, or changes in output distribution that automatically trigger a formal model review, re-validation, or, if necessary, deactivation.
* This evolution will require a significant investment in talent. The skills needed to monitor adaptive AI systems and diagnose novel risks like adversarial vulnerability are distinct from those of traditional quantitative analysts. The Act's 'AI literacy' requirement is not just for front-line users but is a critical imperative for all three lines of defense, especially MRM.5

### Third-Party Risk Management (TPRM) for the AI Supply Chain

Many banks will act as "deployers" of AI systems developed by third-party vendors. The AI Act is unequivocal that responsibility is shared across the value chain; a bank cannot outsource its compliance obligations.24 The Act defines clear roles and responsibilities for providers, deployers, importers, and distributors, creating a chain of accountability.15

**Recommendations:**

* TPRM frameworks must be augmented with a dedicated AI risk assessment module. Due diligence on potential AI vendors must now go beyond financial stability and cybersecurity posture to include a deep dive into their compliance with the AI Act's provider obligations.
* Contractual agreements with AI vendors must be overhauled. New contracts must include explicit clauses that:
  + Clearly allocate responsibilities for AI Act compliance.
  + Guarantee the bank access to all necessary technical documentation to verify compliance.
  + Provide the bank with robust rights to audit and test the vendor's AI system.
  + Establish clear protocols and timelines for the vendor to report serious incidents or performance issues.25

### The Enhanced Role of Internal Audit and Compliance

The second line (Compliance) and third line (Internal Audit) are critical for providing independent assurance over the bank's AI governance framework. While their role is not explicitly prescribed in the same detail as that of providers or deployers, their involvement is essential for demonstrating a robust control environment to regulators.20

**Recommendations:**

* The Compliance function must integrate the AI Act's requirements into the bank's enterprise-wide compliance risk management program. This includes developing policies, conducting training, and monitoring the firm's adherence to the new rules.
* The Internal Audit function must design and execute a new, specialized audit program focused on AI risk and AI Act compliance. This program should independently test the effectiveness of the updated MRM framework, the adequacy of TPRM controls for AI vendors, the integrity of automated logging systems, and, critically, the real-world efficacy of human oversight mechanisms.26

### Integrating Data Governance and IT Resiliency (The DORA-AI Act Nexus)

The AI Act operates in concert with the Digital Operational Resilience Act (DORA).10 It is crucial to understand their relationship: they are complementary, not duplicative.11 DORA ensures the resilience of the underlying ICT infrastructure (e.g., servers, networks, cloud environments). The AI Act ensures the resilience of the AI model *itself*—its logic, its data, and its outputs. A bank could be fully DORA-compliant but fail its AI Act obligations if a cyber-attack successfully poisons its training data without causing a system outage.

This interconnectedness demands a unified governance approach. An AI model's risk profile is a function of its training data (Data Governance), its algorithmic design (MRM), its operational environment (Cybersecurity under DORA), and its provenance if from a vendor (TPRM). A failure in one domain is a failure of the whole system.

**Recommendations:**

* Banks should streamline their compliance efforts by creating a single, well-documented risk management framework that explicitly addresses both ICT risks under DORA and the AI-specific risks mandated by the AI Act.11
* A cross-functional AI Governance Council should be established, with senior representation from MRM, TPRM, Cybersecurity, Data Governance, IT, Legal, and Compliance, to break down traditional silos and provide holistic oversight of high-risk AI systems.

## IV. A Phased Compliance Roadmap for High-Risk AI Systems

Achieving compliance with the AI Act's resiliency mandates is a complex, multi-year endeavor that requires a structured, phased approach. The following roadmap outlines critical, actionable steps structured around the model lifecycle, aligning with the Act's staggered implementation deadlines.29 This is not merely a legal or compliance project; it is a foundational data and technology infrastructure program that requires significant investment in MLOps platforms and tooling to automate the required monitoring and logging at scale.18

### Phase 1: Foundation and Scoping (Immediate Actions: 0-6 Months)

1. **Establish AI Governance:** Formally designate a cross-functional team or council responsible for overseeing AI Act compliance, with clear mandates and executive sponsorship.31
2. **Conduct AI Inventory:** Create and maintain a comprehensive, enterprise-wide inventory of all AI systems currently in use, in development, or procured from third parties. This inventory is the bedrock of the entire compliance program.15
3. **Risk Classification:** For each system in the inventory, perform a legal classification based on the AI Act's risk tiers (unacceptable, high, limited, minimal). This is a legal determination based on the system's intended purpose, not a traditional risk assessment.15 Prohibited systems must be identified and decommissioned immediately to meet the February 2025 deadline.23
4. **Gap Analysis:** Conduct a thorough gap analysis comparing the bank's existing governance, risk management, and control frameworks against the specific requirements for high-risk systems under the Act. This will identify key deficiencies and inform the remediation plan.7

### Phase 2: Pre-Deployment - Fortifying Validation and Testing (6-18 Months)

Before any new high-risk AI system is deployed, or before existing systems are re-certified, a new set of validation gates must be established.

1. **Conformity Assessment:** High-risk systems must undergo a formal conformity assessment procedure to demonstrate compliance with all requirements of the Act.15 For banks, this will largely be an internal self-assessment process that leverages existing regulatory frameworks but must result in a new, auditable package of evidence.33 This package will become a critical artifact for both internal and external auditors.
2. **Fundamental Rights Impact Assessment (FRIA):** As deployers of high-risk systems, banks must conduct a FRIA prior to putting a system into use. This assessment evaluates the system's potential impact on individuals' fundamental rights and outlines mitigation measures.12
3. **Enhanced Data Validation:** Implement rigorous, documented procedures for testing training, validation, and testing datasets for quality, completeness, relevance, and potential biases before a model is trained or retrained.17
4. **Structured Real-World Testing:** Where appropriate, leverage the mechanism under Article 60 of the Act, which allows for testing high-risk systems in real-world conditions. This involves submitting a formal testing plan to the relevant national supervisory authority and provides a structured, supervised pathway for validating model performance before a full-scale launch.34

### Phase 3: Post-Deployment - Continuous Monitoring and Reporting (18-24+ Months)

The resiliency obligations of the Act are continuous and apply throughout a system's operational life.

1. **Implement Continuous Monitoring:** Deploy the necessary tools and processes to continuously monitor the performance of high-risk AI systems in production. This must track accuracy, robustness, and data drift against the metrics declared in the conformity assessment.18
2. **Activate Automated Logging:** Ensure that the automatic logging capabilities of all high-risk systems are enabled, configured correctly, and that the logs are securely retained for a period appropriate to the system's purpose. These logs are essential for traceability and incident investigation.18
3. **Establish Incident Response and Reporting:** Develop and operationalize clear procedures for identifying, escalating, and responding to serious incidents involving high-risk AI systems. This includes protocols for taking immediate corrective actions (e.g., human override, system shutdown) and reporting such incidents to the relevant national authorities as required.18

The table below provides a high-level project plan for executing this roadmap.

**Table 2: Phased Compliance Roadmap**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Compliance Phase** | **Critical Action Item** | **Primary Ownership** | **Target Completion** | **Relevant AI Act Deadline** |
| **Phase 1: Foundation** (0-6 months) | Establish AI Governance Council | CCO / CRO | Q1 2025 | N/A |
|  | Complete Enterprise AI Inventory & Risk Classification | CDO / Head of MRM | Q2 2025 | 6 months (Prohibited Systems) |
|  | Conduct Gap Analysis of Governance Frameworks | Head of MRM / Head of TPRM | Q3 2025 | N/A |
| **Phase 2: Pre-Deployment Build-Out** (6-18 months) | Update MRM, TPRM, and Data Governance Policies | CRO / CCO | Q4 2025 | 24 months (High-Risk Systems) |
|  | Develop Conformity Assessment & FRIA Procedures | Head of MRM / Compliance | Q1 2026 | 24 months (High-Risk Systems) |
|  | Procure/Build MLOps & Continuous Monitoring Tools | Head of AI/IT Strategy | Q2 2026 | 24 months (High-Risk Systems) |
| **Phase 3: Post-Deployment & Ongoing Compliance** (18-24+ months) | Conduct First Conformity Assessment for a New System | Business Line / MRM | Q3 2026 | 24 months (High-Risk Systems) |
|  | Operationalize Incident Reporting Procedures | CCO / Head of Operations | Q3 2026 | 24 months (High-Risk Systems) |
|  | Roll Out AI Literacy Training Program | Chief Human Resources Officer | Q4 2026 | 6 months (AI Literacy) |

## V. The Act’s Extraterritorial Reach: Implications for US-Based Banking Operations

The EU AI Act is designed with a significant extraterritorial scope, ensuring that its protections apply to individuals within the Union regardless of where an AI system is developed or hosted.2 This has direct and unavoidable consequences for the US-based legal entities and operations of any multinational bank.

### Understanding the Global Impact

The critical trigger for the Act's extraterritorial application is found in Article 2, which states that the regulation applies to providers and deployers located in a third country (such as the US) "where the output produced by the AI system is used in the Union".36 This "use of output" nexus means that a bank's global AI strategy must be viewed through the lens of EU law. The operational reality for multinational banks is that maintaining two divergent and costly governance frameworks for AI is untenable. The most prudent and efficient path forward will be to adopt the high standards of the EU AI Act as the global baseline for all high-risk systems, an example of the "Brussels Effect" in practice.

### Scenario Analysis

To clarify the practical implications, consider the following common scenarios:

* Scenario 1: Model Developed and Hosted in the US, with Outputs for EU Branches/Clients.  
  A US-based entity that develops a credit scoring model hosted on US servers, but which provides decisions or scores to an EU-based branch for underwriting loans to EU clients, falls squarely within the Act's scope. In this situation:
  + The US entity is acting as a "provider" of a high-risk AI system.8 The physical location of the hardware and development team is irrelevant.37
  + The US entity must comply with all provider obligations under the Act, including conducting a conformity assessment, preparing extensive technical documentation, establishing a quality management system, and registering the system in the central EU database.19
  + Critically, as a provider not established in the EU, the US entity is legally required under Article 22 to appoint an EU-based "authorised representative." This representative is the designated point of contact for EU supervisory authorities and is responsible for verifying the provider's compliance documentation.32
* Scenario 2: Models Trained on Global Data Including EU Citizen Data.  
  The Act's primary trigger is the use of the output in the EU, not the geographic origin of the training data.36 However, if that model is deemed high-risk because its output is used in the EU, then the data governance requirements of Article 10 apply to the entire dataset used for training, validation, and testing. The bank must be able to demonstrate that its global dataset is relevant, representative, and has been examined for biases that could affect EU citizens.4 Furthermore, Recital 106's requirement for General-Purpose AI models to comply with EU copyright law regardless of where training occurs sets a strong precedent that the EU expects its data-related rules to apply to the inputs of systems affecting its market.40 The parallel application of GDPR to any personal data of EU citizens further strengthens these obligations.36

### Framework for Transatlantic Compliance Coordination

Effective compliance requires seamless coordination between US and EU-based teams. A robust framework should include:

1. **Centralized AI Governance:** Establish a single, enterprise-wide AI governance body with senior representation from both US and EU legal, compliance, risk, and technology functions. This body should be responsible for setting the global AI risk appetite and overseeing compliance with all relevant regulations, using the AI Act as the high-water mark.
2. **Unified AI Inventory and Risk Framework:** The AI inventory and risk classification process must be global in scope. A model's risk classification should be consistent across the enterprise to ensure a single, high standard of governance is applied everywhere.
3. **Empowering the Authorised Representative:** The EU-based authorised representative is a substantive role with legal responsibilities, not a mere mailbox. This entity (whether an internal subsidiary or a third-party firm) can terminate its mandate and inform regulators if it believes the US provider is non-compliant.40 US-based legal and development teams must establish clear, documented communication and information-sharing workflows with this representative to ensure they can fulfill their duties and respond to regulatory inquiries effectively.

## VI. Strategic Recommendations and Conclusion

The EU AI Act is a paradigm-shifting regulation that moves the management of AI from a set of best practices to a domain of hard legal requirements. For a multinational banking institution, compliance is a significant undertaking, but it is also an opportunity to build a foundation of trustworthy, resilient, and responsible AI that can serve as a competitive advantage. The following strategic imperatives are directed to the institution's senior leadership.

* **For the Chief Risk Officer (CRO):** The immediate priority is to recognize that AI introduces a new and distinct category of risk that requires a fundamental evolution of existing frameworks. The CRO should commission a cross-functional task force to integrate the AI Act's requirements into the bank's Enterprise Risk Management (ERM) framework. A top priority must be overseeing the transformation of the Model Risk Management (MRM) function to build the necessary capabilities for continuous monitoring and the management of novel AI-specific risks.
* **For the Chief Compliance Officer (CCO):** The CCO must initiate and champion a global AI compliance program, beginning with the foundational steps of a comprehensive AI inventory and a formal gap analysis. This program must establish the framework for transatlantic coordination between US and EU teams. The CCO should also oversee the critical process of selecting and formally mandating the EU-based authorised representative, ensuring this entity is adequately resourced to perform its substantive oversight duties.
* **For the Head of AI/IT Strategy:** The technology and data infrastructure is the bedrock of compliance. The Head of AI/IT Strategy must partner closely with Risk and Compliance to ensure that the bank's technology roadmap and MLOps capabilities can support the Act's demanding requirements for continuous monitoring, automated logging, and robust cybersecurity. This leader must also champion the "human oversight by design" principle, ensuring that all new AI systems are built from the ground up with the necessary interfaces and controls to allow for effective human governance.

In conclusion, the EU AI Act presents a formidable compliance challenge. However, it also provides a clear and comprehensive roadmap for mitigating the profound risks associated with high-impact AI systems. By proactively embracing the Act's principles, banking institutions can not only ensure regulatory compliance but also enhance operational resiliency, strengthen customer and public trust, and solidify their position as leaders in the responsible and innovative use of artificial intelligence.

#### Works cited

1. Artificial Intelligence Act - Wikipedia, accessed October 29, 2025, <https://en.wikipedia.org/wiki/Artificial_Intelligence_Act>
2. EU Adopts the AI Act: The World's First Comprehensive AI Regulation - Wiley Rein, accessed October 29, 2025, <https://www.wiley.law/alert-EU-Adopts-the-AI-Act-The-Worlds-First-Comprehensive-AI-Regulation>
3. EU AI Act: A New Regulatory Era for Banking AI Systems - Latinia, accessed October 29, 2025, <https://latinia.com/en/resources/the-eu-ai-act-is-now-in-force>
4. AI Act | Shaping Europe's digital future - European Union, accessed October 29, 2025, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>
5. Setting the ground rules: the EU AI Act - KPMG International, accessed October 29, 2025, <https://kpmg.com/xx/en/our-insights/ecb-office/setting-the-ground-rules-the-eu-ai-act.html>
6. Annex III: High-Risk AI Systems Referred to in Article 6(2) | EU ..., accessed October 29, 2025, <https://artificialintelligenceact.eu/annex/3/>
7. The EU AI Act and Its Implications for Credit Risk Models in Banking - Advisense, accessed October 29, 2025, <https://advisense.com/2025/03/19/the-eu-ai-act-and-its-implications-for-credit-risk-models-in-banking/>
8. Article 3: Definitions | EU Artificial Intelligence Act, accessed October 29, 2025, <https://artificialintelligenceact.eu/article/3/>
9. The AI Act Explorer | EU Artificial Intelligence Act, accessed October 29, 2025, <https://artificialintelligenceact.eu/ai-act-explorer/>
10. Digital Operational Resilience Act (DORA) | Updates, Compliance, Training, accessed October 29, 2025, <https://www.digital-operational-resilience-act.com/>
11. Financial services compliance with the EU AI Act and DORA can be streamlined, accessed October 29, 2025, <https://www.pinsentmasons.com/out-law/analysis/financial-services-compliance-eu-ai-act-dora-streamlined>
12. Article 15: Accuracy, Robustness and Cybersecurity | EU Artificial ..., accessed October 29, 2025, <https://artificialintelligenceact.eu/article/15/>
13. artificialintelligenceact.eu, accessed October 29, 2025, <https://artificialintelligenceact.eu/article/15/#:~:text=The%20EU%20AI%20Act%20states,ways%20to%20measure%20these%20qualities.>
14. How to Achieve Cybersecurity Compliance with the EU AI Act | Ankura - JDSupra, accessed October 29, 2025, <https://www.jdsupra.com/legalnews/how-to-achieve-cybersecurity-compliance-1330451/>
15. The EU AI Act: What it means for your business | EY - Switzerland, accessed October 29, 2025, <https://www.ey.com/en_ch/insights/forensic-integrity-services/the-eu-ai-act-what-it-means-for-your-business>
16. Top 10 operational impacts of the EU AI Act﻿ – Obligations on providers of high-risk AI systems - IAPP, accessed October 29, 2025, <https://iapp.org/resources/article/top-impacts-eu-ai-act-high-risk-ai-providers/>
17. High-level summary of the AI Act | EU Artificial Intelligence Act, accessed October 29, 2025, <https://artificialintelligenceact.eu/high-level-summary/>
18. AI governance: Navigating EU compliance standards - Moody's, accessed October 29, 2025, <https://www.moodys.com/web/en/us/insights/ai/ai-governance-navigating-eu-compliance-standards.html>
19. The EU's AI Act: Review and What It Means for EU and Non-EU Companies, accessed October 29, 2025, <https://www.pillsburylaw.com/en/news-and-insights/eu-ai-act.html>
20. Explainable AI for EU AI Act compliance audits, accessed October 29, 2025, <https://mab-online.nl/article/150303/>
21. kpmg.com, accessed October 29, 2025, <https://kpmg.com/xx/en/our-insights/ecb-office/setting-the-ground-rules-the-eu-ai-act.html#:~:text=The%20AI%20Act%20recognises%20that,model%20risk%20management%20and%20governance.>
22. How generative AI can help banks manage risk and compliance - McKinsey, accessed October 29, 2025, <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/how-generative-ai-can-help-banks-manage-risk-and-compliance>
23. The roadmap to the EU AI Act: a detailed guide - Alexander Thamm, accessed October 29, 2025, <https://www.alexanderthamm.com/en/blog/eu-ai-act-timeline/>
24. The EU AI Act: The impact on financial services institutions - Consultancy.eu, accessed October 29, 2025, <https://www.consultancy.eu/news/11237/the-eu-ai-act-the-impact-on-financial-services-institutions>
25. Third-Party Risk Management for the EU AI Act | RadarFirst, accessed October 29, 2025, <https://www.radarfirst.com/blog/third-party-risk-management-for-the-eu-ai-act/>
26. The AI Act: Road to Compliance | ECIIA, accessed October 29, 2025, <https://www.eciia.eu/wp-content/uploads/2025/01/The-AI-Act-Road-to-Compliance-Final.pdf>
27. Governing AI's Rise: Internal Audit's Role in Risk & Accountability ..., accessed October 29, 2025, <https://www.stout.com/en/insights/article/governing-ai-rise-internal-audits-role-risk-accountability>
28. Digital Operational Resilience Act (DORA) - EIOPA - European Union, accessed October 29, 2025, <https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en>
29. EU AI Act Roadmap: What does the AI act mean for your organization? | EY - Netherlands, accessed October 29, 2025, <https://www.ey.com/en_nl/insights/ai/eu-ai-act-roadmap-what-does-the-ai-act-mean-for-your-organization>
30. EU AI Act Compliance: 5 Things to Know | TransPerfect, accessed October 29, 2025, <https://www.transperfect.com/blog/eu-ai-act-compliance-5-things-know>
31. The EU AI Act: 6 Steps to Take in 2024 - Orrick, accessed October 29, 2025, <https://www.orrick.com/en/Insights/2024/09/The-EU-AI-Act-6-Steps-to-Take-in-2024>
32. EU's AI Act: What regulators should know - Next Move - PwC, accessed October 29, 2025, <https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/tech-regulatory-policy-developments/eu-ai-act.html>
33. Implications of the EU AI Act on Risk Modelling - ADC Consulting, accessed October 29, 2025, <https://adc-consulting.com/insights/implications-of-the-eu-ai-act-on-risk-modelling/>
34. Article 60: Testing of High-Risk AI Systems in Real World Conditions Outside AI Regulatory Sandboxes | EU Artificial Intelligence Act, accessed October 29, 2025, <https://artificialintelligenceact.eu/article/60/>
35. Navigating the EU AI Act: a strategic approach for financial services | Insights | UK Finance, accessed October 29, 2025, <https://www.ukfinance.org.uk/news-and-insight/blog/navigating-eu-ai-act-strategic-approach-financial-services>
36. Article 2: Scope | EU Artificial Intelligence Act, accessed October 29, 2025, <https://artificialintelligenceact.eu/article/2/>
37. EU AI Act – Landmark Law on Artificial Intelligence Approved by the ..., accessed October 29, 2025, <https://www.mofo.com/resources/insights/240314-eu-ai-act-landmark-law-on-artificial-intelligence>
38. Understanding the Impact of the EU AI Act: A Primer for Financial Institutions, accessed October 29, 2025, <https://www.aba.com/news-research/analysis-guides/understanding-the-impact-of-the-eu-ai-act>
39. EU AI Act: Does It Affect Your Organization or Not? - cyber/data ..., accessed October 29, 2025, <https://cdp.cooley.com/eu-ai-act-does-it-affect-your-organization-or-not/>
40. A Practical Guide to the Extraterritorial Reach of the AI Act - WILLIAM ..., accessed October 29, 2025, <https://www.williamfry.com/knowledge/a-practical-guide-to-the-extraterritorial-reach-of-the-ai-act/>