



ISITC
EUROPE CIC



AI PRODUCT SAFETY IN CAPITAL MARKETS: FROM REGULATORY OBLIGATION TO BUSINESS IMPERATIVE

An ISITC Europe/AIRTA Systems White Paper

Abstract

Capital markets firms operating in or serving the EU can no longer treat AI product safety as optional: it is a non-negotiable condition of market access, effective governance, and liability control. This paper shows how the EU AI Act and revised Product Liability Directive compel firms to establish accountable ownership, rigorous testing, technical documentation, human oversight, incident response, and post-market monitoring across the AI lifecycle, or face regulatory, financial, operational, and reputational consequences.

AIRTA
SYSTEMS

Contents

1. Executive Summary	2
2. Key Risks for Capital Markets Businesses	3
2.1 Legal and Regulatory Liability	3
2.2 Financial and Litigation Exposure	3
2.3 Reputational Damage	3
2.4 Operational and Compliance Risk.....	3
2.5 Consumer and Market Harm.....	3
3. AI Product Safety Components	3
3.1 What Makes a Safe AI Product?.....	3
3.2 Stakeholder first Product Safety.....	4
4. The Business Case for AI Product Safety.....	5
4.1 AI as a Product.....	5
4.2 The EU AI Act (AIA)	6
4.3 The Product Liability Directive (PLD)	6
4.4 International and Industry Standards	7
5. Conclusions	8
6. About ISITC Europe CIC.....	8
7. About AIRTA Systems	8

Disclaimer

The authors and publishers have checked the information in this document to the best of their ability. Although the facts are believed to be correct at the time of publication, their accuracy cannot be guaranteed.

The findings, conclusions, and recommendations are based on information gathered in good faith from primary and secondary sources. ISITC Europe, AIRTA Systems, and the authors cannot guarantee the accuracy or completeness of every source.

Where information is identified as having been supplied by a third party, ISITC Europe and AIRTA Systems have not independently verified it, and it does not necessarily reflect their views. Accordingly, they accept no liability for actions taken in reliance on information that later proves inaccurate or for losses arising from decisions based on that information.

Any opinions expressed are those of the authors and editors.

1. Executive Summary

Capital markets firms connected with the EU market should treat AI product safety as an immediate market-access, governance, and liability priority. Their obligations depend on the role they perform, such as provider, importer, distributor, integrator, or deployer. The system's risk classification, and the applicable implementation date. The EU AI Act and the revised Product Liability Directive create distinct but connected requirements, making early system mapping and role classification essential.

The immediate management priority is to determine which AI systems fall within scope, identify the firm's role for each system, and assign accountable owners for classification, testing, approval, documentation, monitoring, and incident response. Firms that wait for a single compliance deadline risk discovering too late that different obligations apply at different stages.

This paper helps capital markets firms determine where AI product safety obligations and liability exposure may arise. It explains how responsibilities vary among firms that develop, procure, integrate, or deploy AI systems connected with the EU market; distinguishes regulatory obligations under the EU AI Act from potential liability under the revised Product Liability Directive; and sets out a practical implementation sequence. It provides a strategic overview rather than legal advice.

Throughout the paper, references to firms should be read by reference to the role performed for each AI system, rather than by organisation type alone. A single firm may perform different roles across its AI portfolio and may perform more than one role for the same system, so scope, duties, evidence requirements, and potential liability should be assessed system by system.

The policy shift responds to tangible harms from unsafe or deceptive AI, including physical and psychological injury, fraud, unlawful discrimination, infringements of fundamental rights, and manipulation. The EU AI Act addresses these risks through role and risk-based regulatory duties, including requirements concerning risk management, transparency, human oversight, documentation, accuracy, robustness, and cybersecurity where applicable.

The Product Liability Directive addresses a different question: whether a defective product caused covered damage for which a relevant economic operator may be strictly liable. The two instruments therefore interact, but they do not impose the same duties or establish liability in the same way.

Firms should respond with an end-to-end AI product safety programme that:

- assigns accountable ownership.
- inventories and classifies relevant systems.
- applies proportionate testing and approval controls.
- maintains technical documentation and meaningful human oversight; and
- connects incident response with post-market monitoring.

The paper first examines the principal risks for capital markets businesses, then defines the components of a safe AI product. It next explains how the EU AI Act, the revised Product Liability Directive, and international standards shape the regulatory and commercial case for action. It concludes with a practical implementation sequence.

2. Key Risks for Capital Markets Businesses

2.1 Legal and Regulatory Liability

AI systems used in trading, risk management, compliance, and client services may bring capital markets firms within the EU AI Act, the revised Product Liability Directive, or both. Exposure depends on the firm's role, the system's intended purpose and classification, and the conduct or product at issue; it should not be assumed that every deployer is automatically liable for every failure. Under the Product Liability Directive, a claimant need not prove negligence, but must establish defect, covered damage, and causation, subject to the Directive's disclosure rules and rebuttable presumptions.

2.2 Financial and Litigation Exposure

Defective AI can generate direct losses through erroneous trades, flawed risk calculations, service disruption, and remediation costs. Litigation exposure may also increase because courts can require disclosure of relevant technical evidence and, in defined circumstances, apply rebuttable presumptions. Firms therefore need records that show how systems were designed, tested, approved, changed, and monitored.

2.3 Reputational Damage

AI driven errors can erode trust when they affect clients, investors, market participants, or regulators. Biased decisions, manipulative outputs, or failures to detect fraud may attract public scrutiny and raise doubts about a firm's controls. In capital markets, those doubts can damage client relationships, increase regulatory attention, and weaken confidence in the firm long after the immediate incident has been addressed.

2.4 Operational and Compliance Risk

Weaknesses in accuracy, robustness, fairness, cybersecurity, or human oversight can disrupt markets, trigger regulatory action, and undermine business continuity. Compliance is therefore not a one-off approval exercise: controls must continue through deployment, change management, incident handling, and post-market monitoring.

2.5 Consumer and Market Harm

Unsafe or deceptive AI products can cause direct harm to consumers and market participants, including:

- Financial loss due to algorithmic errors or manipulation
- Unfair or discriminatory outcomes in lending, onboarding, or trading
- Violation of privacy or fundamental rights through unlawful surveillance or data misuse

Taken together, these exposures make AI product safety a core business control discipline rather than a stand-alone compliance exercise.

3. AI Product Safety Components

3.1 What Makes a Safe AI Product?

A safe AI product is one for which the organisation can demonstrate, with evidence proportionate to its intended purpose and risk, that the system performs reliably, remains robust under foreseeable conditions, avoids unjustified discriminatory outcomes, supports effective human oversight, and is governed by accountable

owners throughout its lifecycle. These characteristics provide a practical basis for design requirements, testing, approval, monitoring, and remediation.

- **Validity and Reliability:** The system must function as specified and do so consistently. Validity asks if the AI system is accurate in its conclusions. Reliability asks if it produces those conclusions consistently over time and under a range of conditions.
- **Robustness:** The system must maintain its specified function and performance, even when faced with unexpected inputs, edge cases, or adversarial attempts to make it fail.
- **Fairness and Bias Mitigation:** The system should be designed, tested, and monitored to identify and mitigate inequitable, discriminatory, or unjust outcomes. NIST treats fairness with harmful bias managed as a characteristic of trustworthy AI, making documented evaluation and remediation important components of safety and reliability.
- **Accountability:** Ownership of each AI system, its impacts, and its outputs must be unambiguous throughout the lifecycle. Governance records should identify who approved material design decisions, including trade-offs between performance and explainability, what evidence informed those decisions, and when they were made. Accountability must operate proactively through prevention and control, and reactively through proportionate incident response and remediation.

3.2 Stakeholder first Product Safety

The clearest answer to “Who needs AI product safety?” is the people and organisations affected by AI enabled decisions, including customers, investors, employees, counterparties, and other market participants. The priority is not confined to speculative or existential risk; it includes immediate, real-world harm arising from financial decisions, client interactions, market operations, and supporting business processes. Product safety programmes should therefore begin by identifying affected stakeholders, foreseeable harms, and the controls required to prevent or mitigate them.

For organisations doing business in the EU, the EU AI Act is the central cross sector regulatory framework. Its risk-based obligations place consumer protection and fundamental rights at the centre of AI development and use.

AI related harm can arise within capital markets and across the wider economy. In capital markets and adjacent financial services, the most relevant examples include financial loss from erroneous or manipulated decisions; discriminatory outcomes in lending, onboarding, employment, or access to financial services; privacy and fundamental rights violations arising from unlawful surveillance or data misuse; fraud enabled by synthetic content or impersonation; and harm to vulnerable customers through deceptive or exploitative interactions. The wider examples below illustrate the breadth of product safety risks that firms may also encounter through suppliers, clients, investments, or embedded technologies.

- **Physical Harm or Danger:** Medical misdiagnosis, autonomous vehicle malfunctions, unsafe industrial controls
- **Psychological Harm:** Suicide encouragement, harassment, traumatic content, targeting vulnerable individuals.
- **Fraud and Impersonation:** AI-generated deepfakes and voice cloning tools are enabling fraud and sophisticated impersonation scams at scale.

- **Illegal Discrimination:** AI tools can perpetuate illegal discrimination. This is most dangerous when AI products make decisions in high-risk contexts, determining whether a consumer gets medical help, a place to live, a job, or a loan.
- **Fundamental Rights Violations:** Unlawful surveillance, censorship, denial of benefits or essential services.
- **Harm to Vulnerable Groups:** Unsafe child interactions, exploitative targeting of minors or elderly.
- **Manipulative Techniques:** Subliminal nudging, deceptive conversations, undue influence causing harm.

4. The Business Case for AI Product Safety

AI product safety protects consumers and strengthens the commercial resilience of organisations that develop or deploy AI. For capital markets firms, effective controls do more than support regulatory compliance: they preserve market access, strengthen client and regulator confidence, reduce the likelihood and impact of failures, and create defensible evidence when systems, decisions, or incidents are challenged.

4.1 AI as a Product

Historically, European product liability frameworks did not always apply clearly to intangible software. Software failures were often treated as contractual or service issues rather than product defects. The revised Product Liability Directive changes that position by expressly bringing software, including AI systems, within the definition of a product.

The Directive expressly covers software, digital manufacturing files, and standalone AI systems. By reducing the ambiguity that previously surrounded intangible digital products, it aligns product liability rules more closely with the harms that software and AI can cause.

An AI chatbot, algorithm, or embedded system can be assessed within the product liability framework where it falls within the Directive's scope. If an AI product is defective and causes covered damage, the relevant economic operator may be liable under the applicable rules. Organisations placing AI enabled products on the EU market should therefore identify whether they act as providers, manufacturers, importers, distributors, or deployers and determine the obligations attached to each role. Potential defects may include unsafe generated content, biased decision making, inadequate cybersecurity, or harmful autonomous behaviour.

Two complementary instruments shape this framework:

- **The EU AI Act** sets mandatory, risk-based requirements for systems within scope, including risk management, technical documentation, transparency, human oversight, accuracy, robustness, and cybersecurity. Non-compliance with applicable safety requirements may be relevant when a court assesses whether a product was defective.
- **The Product Liability Directive** provides a strict liability cause of action. A claimant need not prove negligence, but must establish defect, damage, and causation, subject to the Directive's disclosure rules and rebuttable presumptions.

4.2 The EU AI Act (AIA)

The European Union has adopted a comprehensive and mandatory approach to AI product safety. The EU AI Act, which entered into force in 2024, establishes a cross sector, risk-based framework for artificial intelligence in the European Union:

Unacceptable Risk (Prohibited Practices): The Act prohibits specified AI practices that are considered incompatible with fundamental rights and Union values. These include certain manipulative or exploitative techniques, specified forms of social scoring, and particular uses of real-time remote biometric identification in publicly accessible spaces, subject to the detailed definitions, conditions, and exceptions in the legislation.

High Risk Systems (Strictly Regulated): High risk classification is central to the Act. Broadly, it covers certain AI systems used as safety components of products governed by specified EU product safety legislation and certain systems used for purposes listed in the Act's high-risk categories. In capital markets and adjacent financial services, classification must be based on the system's intended purpose and the detailed conditions and exceptions in the legislation; a system is not high risk merely because it supports a financial activity.

1. AI is used as a safety component in products already covered by EU product safety laws.
2. AI systems used for specified purposes in sensitive areas listed by the Act, including certain uses involving critical infrastructure, education and vocational training, employment and worker management, access to essential services, law enforcement, migration, and the administration of justice. Whether a system is high risk depends on its intended purpose and the detailed conditions and exceptions in the legislation.

Obligations for High-Risk Systems: Providers (developers) of these systems are subject to strict, mandatory obligations before the product can be put on the market. These include conducting adequate risk assessments, using high-quality training data to minimize bias, logging all activity for traceability, providing clear instructions for use, and ensuring appropriate human oversight, robustness, and cybersecurity.

General Purpose AI (GPAI): General purpose AI models, including models used in services such as ChatGPT, are subject to transparency and documentation obligations, including requirements concerning information for downstream providers and policies for compliance with EU copyright law. Additional duties apply to general purpose AI models classified as presenting systemic risk. AI systems built on or incorporating those models may also be subject to separate obligations, including transparency requirements for specified AI generated or manipulated content.

Although the AI Act is already in force, its obligations apply in stages between 2025 and 2027. Organisations should map each relevant system and organisational role to the applicable commencement date rather than treating compliance as a single deadline.

4.3 The Product Liability Directive (PLD)

The updated Product Liability Directive provides a route to compensation for covered damage caused by defective products. Adopted in 2024, it modernises the European Union's product liability framework for the digital age by addressing software and AI expressly. It complements the EU AI Act but serves a different function: the AI Act establishes regulatory obligations, while the Directive governs claims for compensation.

- **Expanded Definition of Product:** The PLD expressly includes software, AI systems, and digital manufacturing files within the concept of a product. This removes much of the previous uncertainty

about whether intangible software can fall within product liability rules. The economic operator potentially liable in a particular case depends on the roles and conditions defined by the Directive; an AI developer should not be assumed to be the liable manufacturer in every circumstance.

- **Works with the AI Act:** The PLD operates alongside the AI Act. Non-compliance with applicable safety requirements may be relevant to a court's assessment of defectiveness. In the circumstances defined by the Directive, disclosure rules and rebuttable presumptions may assist a claimant, but non-compliance does not remove the need to establish the elements required for liability.
- **Easing the Burden of Proof:** The Directive addresses the evidential difficulty created by complex technical systems. National courts may order the disclosure of relevant evidence, subject to the Directive's conditions and safeguards. In defined circumstances, a failure to comply with a disclosure order or evidence of non-compliance with applicable safety requirements may support a rebuttable presumption concerning defectiveness or causation.
- **Strict Liability (No-Fault):** The PLD maintains the principle of strict liability. A claimant does not need to prove that the relevant economic operator was negligent or intended to cause harm, but must establish defect, covered damage, and causation, subject to the Directive's rules and presumptions.

4.4 International and Industry Standards

The United States has generally taken a more decentralised and sector specific approach than the European Union, combining legislation, agency enforcement, standards, guidance, and voluntary measures. Whereas the EU AI Act establishes a cross sector legal framework, responsibility in the United States is distributed across federal and state authorities and individual sectors. For multinational firms, the practical implication is that a common governance framework may still need jurisdiction specific controls, evidence, and escalation paths.

Between these models sits a growing body of international principles and industry standards. Although not all are legally binding, they are helping to define a global baseline for responsible AI governance.

- **International organisations:** The OECD, UNESCO, and G7 support interoperable AI governance approaches centred on human rights, fairness, safety, and accountability.
- **ISO/IEC 42001:2023:** This auditable standard provides a framework for establishing and operating an AI management system, covering governance, development, deployment, compliance, and continual improvement.

The global landscape reflects different regulatory structures rather than a single international model. Under the "Brussels Effect," the EU AI Act may influence practices beyond Europe because multinational organisations may choose to apply a demanding common standard across jurisdictions. International standards can provide a practical point of convergence by supporting interoperable controls while allowing firms to maintain jurisdiction specific evidence, governance, and escalation paths.

4.5 Practical Implementation

1. Create an inventory of AI systems that records each system's intended purpose, business owner, technical owner, deployment context, affected stakeholders, and the role or roles performed by the firm. The inventory should be maintained through procurement, development, deployment, material change, and retirement so that classification and control decisions remain current.

2. Classify each system by intended purpose, deployment context, regulatory scope, risk level, affected stakeholders, and potential harm. Record the basis for the classification, the applicable obligations and commencement dates, and the circumstances that would trigger reassessment.
3. Assign accountable business, technical, risk, and compliance owners.
4. Define proportionate testing, documentation, approval, and change control requirements.
5. Connect incident response, consumer reporting, and post-market monitoring.
6. Use independent assurance where risk, complexity, or market impact warrants additional scrutiny.

5. Conclusions

AI product safety is now an engineering, governance, and compliance discipline, not merely an ethical aspiration. For capital markets firms, effective controls protect consumers, support market access, reduce operational and litigation exposure, and strengthen confidence among clients and regulators.

For affected individuals and market participants, the shift addresses immediate harms ranging from discriminatory financial or employment decisions to fraud, physical injury, and psychological manipulation. For businesses, it requires AI enabled products to be governed with the same lifecycle discipline applied to other products capable of causing material harm. This alignment of consumer protection and business control is the central case for treating AI product safety as an operational discipline.

The EU AI Act defines risk-based obligations for systems within scope, while the revised Product Liability Directive provides a route to compensation where defective products cause covered damage. Together, they make evidence of sound design, testing, approval, oversight, and monitoring increasingly important.

Capital markets firms should now operationalise AI product safety as a lifecycle discipline. The immediate priorities are to assign clear ownership, classify systems and organisational roles, apply proportionate safety testing, maintain technical documentation, control approvals and changes, integrate incident response with post-market monitoring, and use independent assurance where risk, complexity, or market impact warrants it. These measures should be implemented through accountable business, technical, risk, and compliance owners rather than treated as a stand-alone legal exercise.

6. About ISITC Europe CIC

ISITC Europe CIC is a not-for-profit industry body that promotes education, innovation, and collaboration across global capital markets.

7. About AIRTA Systems

AIRTA Systems provides an AI product-safety platform designed to support EU market access, litigation defence, and consumer protection. Its Consolidated AI Product Safety Pipeline combines agentic and human-validated risk assessment, compliance documentation, continuous post-market monitoring, and incident-ready workflows. The platform also supports consumer reporting and Product Liability Directive assurance, helping organisations protect users and address risks to safety and fundamental rights.
