

Supervision of the AI Act

CFA Risk event

1 October 2026

DeNederlandscheBank

EUROSYSTEEM



Who are we?

Gerard Kolenbrander

Senior Policy Officer



Tessa Sprokkel

Senior Supervisor Asset Management



Introduction to the AI Act



EUROSYSTEM

Question

What risks do you see in the use of AI within your organization?

The essence of the AI act

- To ***promote the uptake of human centric and trustworthy*** artificial intelligence
- To ensure a high level of protection of health, safety, ***fundamental rights***
- To ***protect against the harmful effects*** of AI systems in the Union
- To ***support innovation***

What the EU does

Artificial Intelligence (AI) is transforming how businesses operate, reshaping public services, and revolutionising science. As AI develops, it can offer even **more benefits** to citizens and businesses across Europe.

The EU is focused on maintaining its place as one of the **global leaders** in AI. To achieve this, we are putting in place initiatives that harness the untapped potential of our researchers and industries and support European startups and SMEs.

A cautionary tale about the possible negative effects of biased algorithms in practice comes from the Netherlands. In 2020, it came to light that the Dutch tax authorities had used algorithms that mistakenly labelled around 26,000 parents as having committed fraud in their childcare benefit applications. Many of these parents had an immigration background. They were required to pay back large sums, which led to great financial and psychological difficulties for the families concerned. The data protection authority concluded that the processing of data by the AI system in use was discriminatory.¹

An overview of the AI act

Prohibited AI practices	High-risk AI systems		AI sandbox
	Requirements on the system	Providers and deployers	
◦ Impairing the ability to make an informed decision by deploying subliminal, manipulative or deceptive techniques ◦ Exploitation of vulnerabilities of a person or group due to age, disability or specific social or economic situation ◦ Social scoring leading to detrimental or unfavourable treatment of natural persons or groups ◦ Predictive policing by using an AI system to predict the risk of a natural person committing a criminal offence ◦ And more (but less relevant for financial sector)	◦ Risk management system as a continuous iterative process ◦ Data governance and management practices that are appropriate ◦ Technical documentation is kept up-to-date ◦ Record keeping with automatic recording of events (logs) ◦ Transparent information for deployers ◦ Human oversight by natural persons ◦ Accuracy, robustness and cybersecurity at appropriate levels	◦ Compliance with requirements on the high-risk AI system by provider ◦ Quality management system by provider in line with EU financial services law (with some additions) ◦ Keeping of event logs by provider in line with EU financial services law ◦ Notification when fundamental rights risks are identified to MSA by deployer or provider ◦ Technical and organizational measures by deployer in line with EU financial services law ◦ Impact assessment for fundamental rights by deployer ◦ Conformity assessment based on internal control by provider ◦ Registration of high-risk and assessed as non-high risk AI systems in the EU database by provider ◦ Right of person to explanation by deployer on how the AI system affected the decision making regarding their case.	◦ National AI regulatory sandbox ◦ May include testing in real world conditions
			Testing in real world outside AI sandbox
			◦ Real-world testing and testing plan approval by MSA ◦ Subjects to provide informed consent
			Transparency
			◦ Transparency obligation for systems that interact directly with natural persons

High risk in the financial sector

- AI systems intended to be used to evaluate the **creditworthiness of natural persons** or establish their credit score, with the exception of AI systems used for the purpose of detecting financial fraud
- AI systems intended to be used for **risk assessment and pricing in relation to natural persons in the case of life and health insurance**

Supervision of the AI Act



EUROSYSTEEM

Show of hands

It is generally clear to me what I can expect from the supervision of DNB and the AFM

The three pillars of AI Act supervision

Planned supervision

Our 'standard' risk-based supervision: inclusion in risk analysis, supervisory planning, thematic reviews, deep dives, et cetera.

Trigger-based supervision

Formal complaints of customers, serious incidents, suspected risks, misclassification, non-compliance.

Innovation support

Regulatory sandbox and real-world testing

Supervisory pilot and other supervisory research

- Realistic test of methodologies to supervise AI act requirements
- How much information is gathered at which cost and what specialist knowledge requirement?
 - Interviews
 - Document analysis
 - Bias testing
 - Data quality assessment
 - Calibration testing
- Supervision of AI in the context of our regular supervision

Preliminary conclusions

- Qualitative analysis works: it is not always needed to dive into the numbers
- No simple cut-off values: discrimination is not easily caught in a statistical test
- AI literacy required: end-users of the model need a thorough understanding of how the outcome of the model can/should be interpreted
- Models use data that is insignificant for the predictions: considerations regarding model complexity
- Model calibration required: ensure predicted probabilities match actual outcomes

What is always a good idea?



Stocktaking

Map all existing and planned AI systems.



Responsibilities

Assign clear internal responsibilities for AI Act compliance.



Classification

Conduct a risk analysis to determine which systems (potentially) qualify as 'high risk'.



Training

Start setting up AI literacy programs to comply with Art. 4.



Gap Analysis

Evaluate existing governance and risk processes (especially data, model validation and oversight) against the requirements.



Contracts

Evaluate contracts with third-party AI vendors to ensure they can provide the necessary information and assurances for compliance.

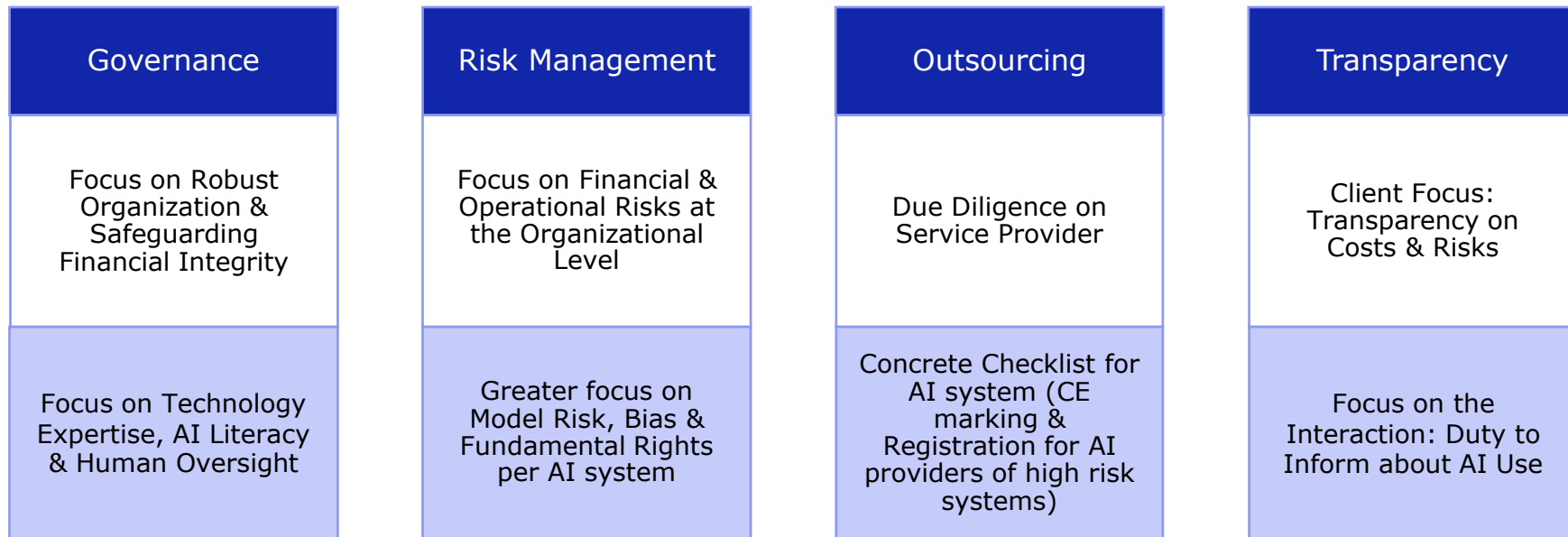
Supervision in addition to the AI Act

DeNederlandscheBank

EUROSYSTEEM



The AI Act adds a specific dimension – existing standards continue to apply



Fundamental principles

Transparency	Governance & ownership
Explainability	Robustness
Human responsibility	Verifiability
System-level control	Proportionality

Questions?

