COORDINATEF

Boosting European AI innovation, together.

From risk to reliability: RISE's risk assessment analysis of AI Systems and CitCom's proposed TEF Label

25th November 2025

Funded by the European Union

Webinar Agenda

Time	Session	Presenter
11.30-11.35	Welcome and Introduction	***David Brunelleschi, Pablo Ivankovich*** *Intellera Consulting*
11.35-11.50	Risk assessment analysis of AI systems	***Kateryna Mishchenko*** *RISE (CitCom.ai)*
11.50-12.05	CitCom.ai label for building trust among partners and clients	***Alessio Buscemi*** *Luxembourg Institute of Science and Technology (CitCom.ai)*
12.05-12.25	Q&A Session	*Moderated by* ***Alberto Venditi*** *Intellera Consulting*
12.25-12.30	Closing remarks & Next steps	***Pablo Ivankovich*** *Intellera Consulting*

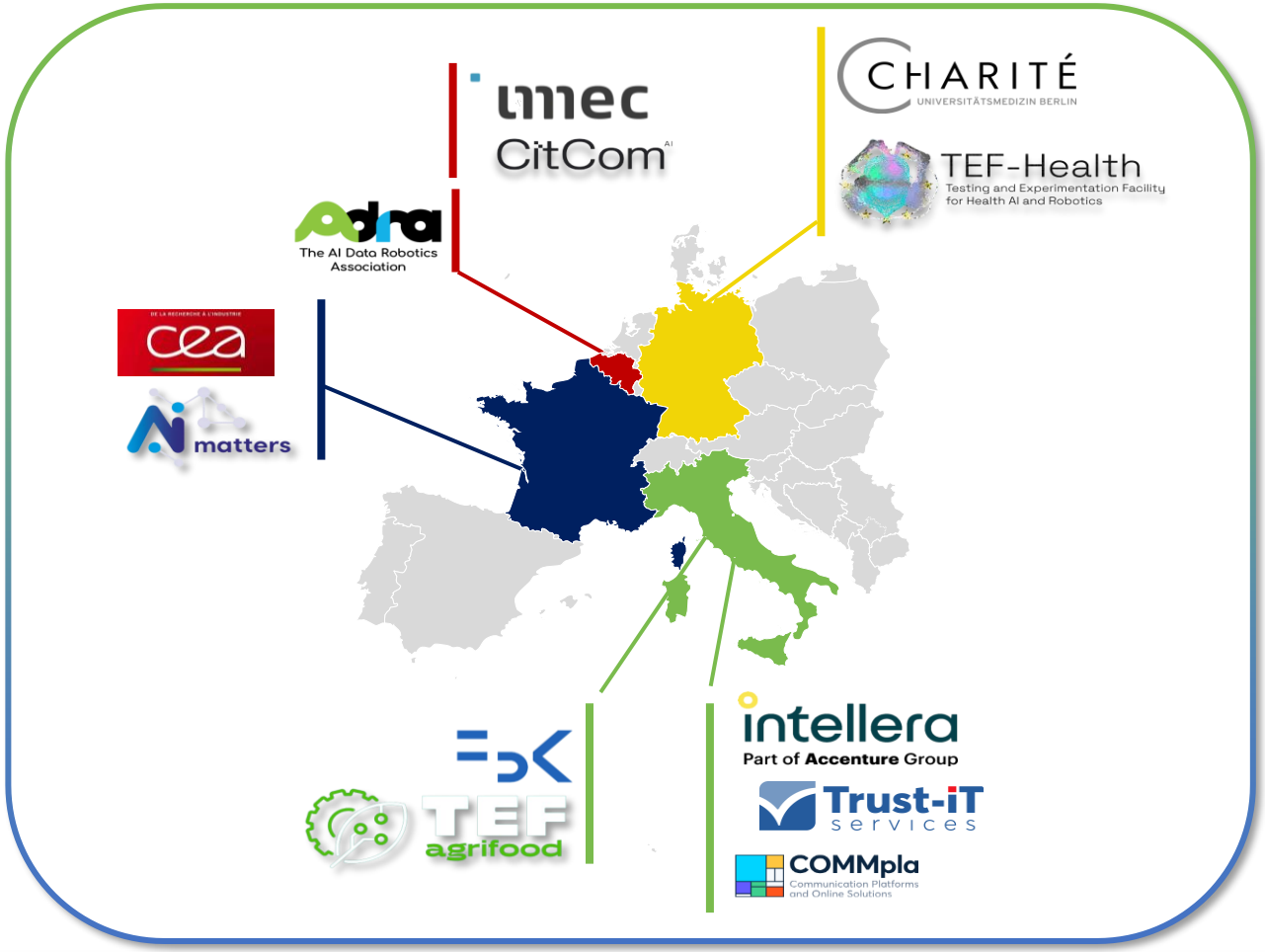
Please, be aware that the webinar will be recorded for the purpose of further dissemination

CoordinaTEF at a glance

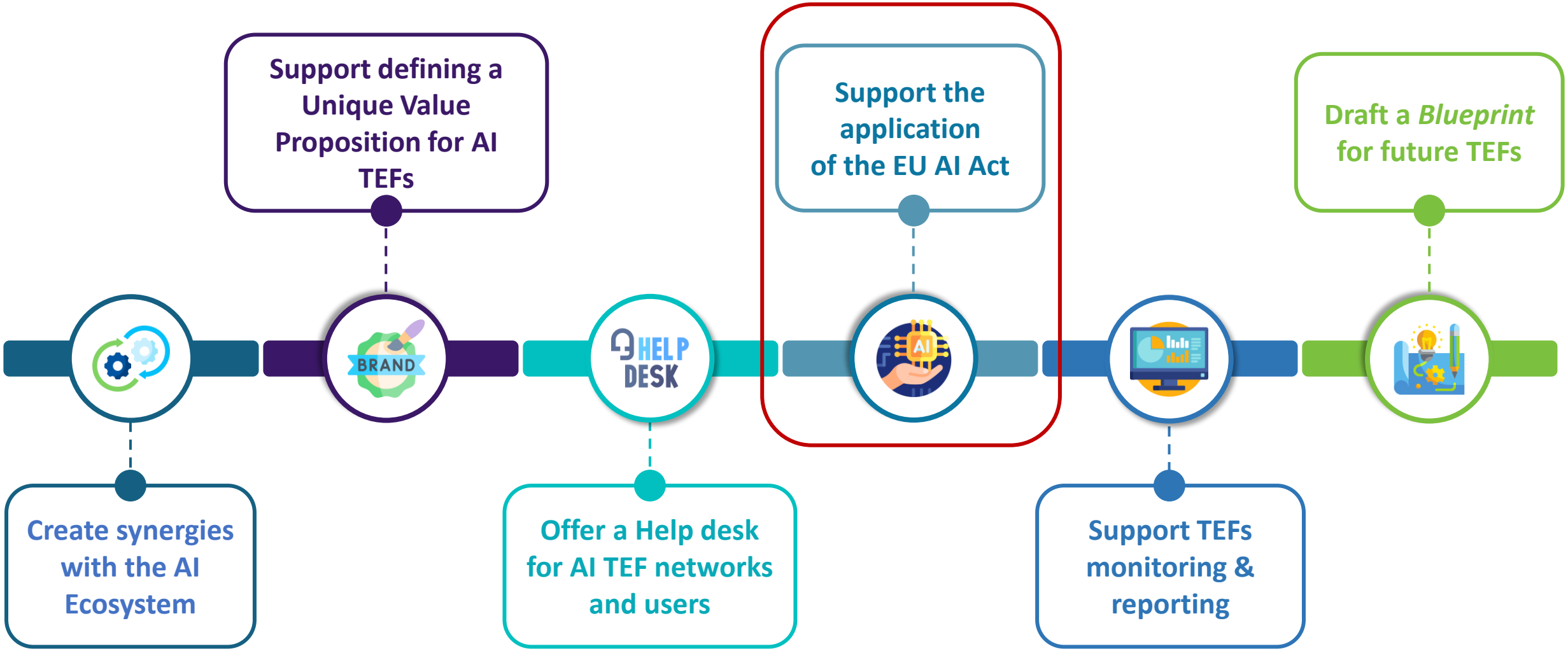
CoordinaTEF strengthens Europe's commitment to ethical AI and innovation by **uniting and coordinating AI sectorial TEFs,** amplifying their visibility, impact, and collective reach

Coordination and Support Action under the **Digital Europe Programme**

Consortium composed of AI sectorial TEFs coordinators and organisations providing specialised expertise to **foster synergies and drive joint efforts**



CoordinaTEF key objectives



COORDINATEF
Boosting European AI innovation, together.

Risk assessment analysis of AI systems

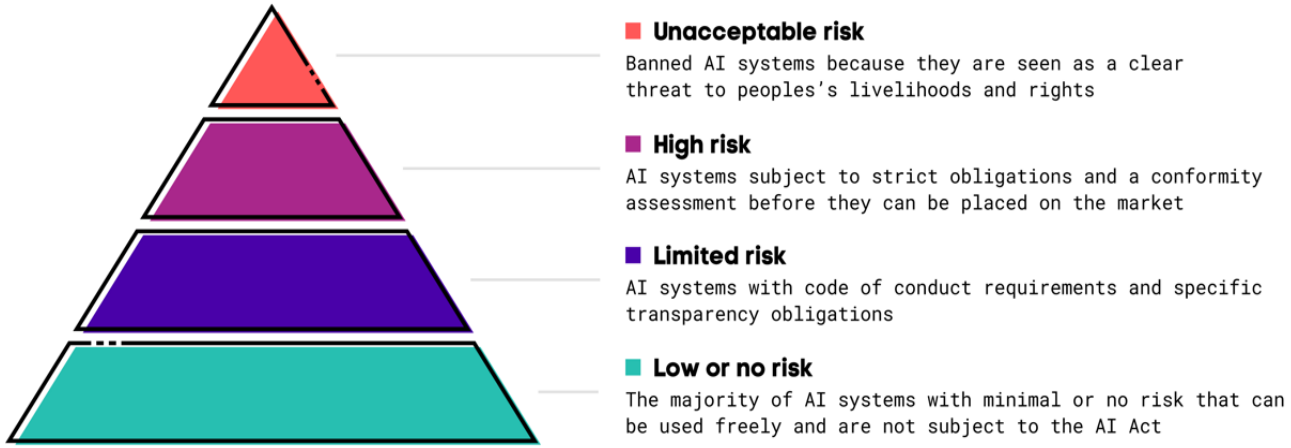
Kateryna Mishchenko
RISE (CitCom.ai)

Funded by
the European Union

Short introduction on AI Act requirements

EU Artificial Intelligence Act (Reg. 2024/1689)

Establishes harmonised rules on AI systems on a risk-based approach.



Title I. General Provisions (Art. 1–4): Defines scope, key terms, and promotes AI literacy.

Title II. Prohibited Practices (Art. 5): Bans AI that exploits vulnerabilities, enables social scoring, or biometric ID in public.

Title III. High-Risk AI (Art. 6–43):

Requirements include:

- Risk management, data governance, documentation, transparency, human oversight, accuracy, cybersecurity,...
- Also covers provider obligations and conformity assessment.

Title IV .Transparency (Art. 50–52): AI must inform users when interacting with humans, using biometrics, or generating content.

Risk assessment analysis framework: about the service

Purpose

Help organisations determine whether their AI systems may fall under the **High-Risk** category of the **EU AI Act** and support early preparation for compliance, https://citcomtef.eu/services/ai-act-risk-level-evaluation

Scope

Applies to industrial automation, energy and utilities, critical infrastructure, mobility, agrifood, healthcare, and public-sector AI. Focus on classification triggers described in Articles 5 and 6, Annex I and Annex III.

What does the service provide

- A structured methodology that translates AI Act requirements into a practical assessment, supported by relevant international and sectoral standards.
- Initial screening of model type, use case, deployment domain, risk indicators, testing approaches, and role-based obligations.
- Early insights into classification outcomes, compliance gaps, and readiness for conformity assessment.
- A foundation for informed decision-making and strategic planning for AI-based products and services.

Service foundations

Two-Path High-Risk Assessment Logic

Article 6 (High-Risk AI Systems)
Path A – Product-Based (Art. 6(1)(a)(b))
"AI systems that are safety components of products, or which are themselves products, covered by the Union harmonization legislation listed in Annex I, and that are subject to a third-party conformity assessment under that legislation."
Path B – Use-Based (Art. 6(2))
"AI systems that are intended to be used in any of the areas listed in Annex III."

Standards & Reference Frameworks

Interim: ISO/IEC 23894, ISO/IEC 42001, ISO 12100,

AI Act: prEN 18286 (emerging harmonized standard)

Complementary: NIST AI RMF, JRC AI Watch

Service Workflow, Tools and Deliverables

Process Flow

Tools and Inputs:

- Assessment Questionnaire (system purpose, context of use, technical design, deployment patterns, and potential regulatory triggers)
- Screening Matrix (Article 5) (prohibited use)
- Legal Mapping Template (Article 6) (high-risk identification)
- Compliance Gap Table (missing elements as RM, fundamental rights assessment, oversight mechanisms, etc)
- Actor-Role Identification Template (Provider, Deployer, Importer, or Distributor, etc)

Deliverables:

- Preliminary Risk Classification Report summarising outcomes, rationale, regulatory references, and contextual considerations.
- Validated Questionnaire and Evidence Record including clarifications and assumptions.
- Compliance Gap Table highlighting missing or partial measures required under the EU AI Act.
- Optional Testing and Compliance Roadmap presenting further recommendations.

Risk assessment analysis framework: Use Cases

Visual Quality Inspection (Manufacturing)

Deep-learning defect detection (approve/reject).

Deployment via PLCs, robotic integration, semi-automated or automated modes.

Results:

Path A may apply if the AI acts as a safety function under Machinery Regulation (EU) 2023/1230.

Path B applies only in specific critical-infrastructure contexts.

For now: Minimal-Risk (Article 52 transparency obligations)

https://citcomtef.eu/news/gimic-first-to-undergo-rises-new-ai-risk-assessment-service

District-Heating Forecasting (Energy Infrastructure)

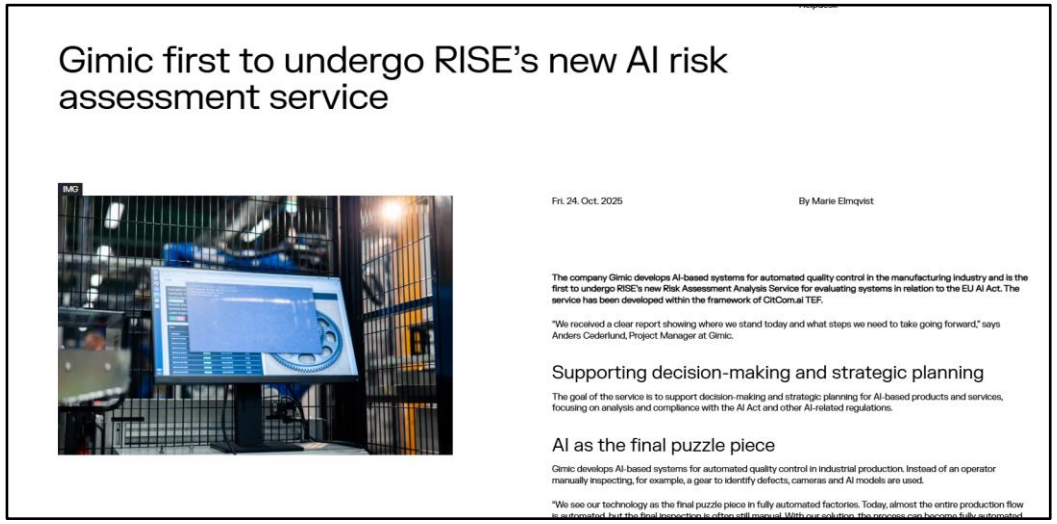
Forecasts heat demand, indoor temperature, and distribution delays.

Integrated with SCADA and PLCs (operator-in-the-loop).

Results:

Path B applies: Confirmed High-Risk under Annex III.2 (critical infrastructure).

Path A may apply if future versions execute autonomous control functions.



Gimic first to undergo RISE's new AI risk assessment service

Fri. 24. Oct. 2025 By Marie Elmqvist

The company Gimic develops AI-based systems for automated quality control in the manufacturing industry and is the first to undergo RISE's new Risk Assessment Analysis Service for evaluating systems in relation to the EU AI Act. The service has been developed within the framework of CitCom.ai TEF.

"We received a clear report showing where we stand today and what steps we need to take going forward," says Anders Cederlund, Project Manager at Gimic.

Supporting decision-making and strategic planning

The goal of the service is to support decision-making and strategic planning for AI-based products and services, focusing on analysis and compliance with the AI Act and other AI-related regulations.

AI as the final puzzle piece

Gimic develops AI-based systems for automated quality control in industrial production. Instead of an operator manually inspecting, for example, a gear to identify defects, cameras and AI models are used.

"We see our technology as the final puzzle piece in fully automated factories. Today, almost the entire production flow is automated, but the final inspection is often still manual. With our solution, the process can become fully automated

Risk assessment analysis framework: Challenges and Lessons Learned

1 **Limited Information Visibility and Documentation**
Providers often hesitate to share technical or deployment details, even under NDA.
Deployment information is frequently incomplete or undocumented, making classifications conditional and dependent on actual use cases.

2 **Uncertainty in Applying Article 6 (Path A / Path B)**
Determining whether AI is a **safety component** under the Machinery Regulation (Path A) or falls within **critical-infrastructure domains** under Annex III (Path B) remains difficult.
Ambiguous Annex III wording complicates borderline cases, especially for industrial control systems.

3 **Strong Dependence on Deployment Context**
Classification outcomes rely more on **where and how** the AI system is used than on its core function.
Technical integration into robotics or control systems can elevate risk under **Article 6(2)**.

4 **Lack of Harmonised Standards and Compliance Pathways**
Harmonised AI Act standards are not yet available and providers struggle to demonstrate compliance (e.g., robustness, accuracy, cybersecurity).
Interim reliance on **ISO 23894**, **ISO 42001**, **IEC 62443** offers procedural support, and the forthcoming **prEN 18286** will be central for conformity.

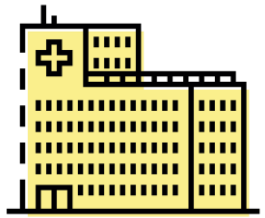
5 **Questionnaire and Methodology Practicalities**
Designing universally applicable questions is challenging; many items cannot be answered with simple yes/no choices.
The structured, stepwise process (screening → classification → obligations mapping) improves traceability but requires time and customer engagement.

6 **Customer Awareness, Expectations, and Sensitivity**
Many organisations remain unaware of the AI Act and underestimate their likelihood of falling into the High-Risk category.
Customers expect not only classification results but also practical guidance on compliance.
Risk classification reports can be sensitive, especially in critical sectors, requiring attention to confidentiality and contractual arrangements.

Conclusions and TEFs at RISE

- CitCom TEF continues to develop the Risk Classification Analysis Service, extending it into new application sectors.
- The service will be adapted to upcoming harmonised standards, new secondary legislation, and related EU directives.
- Expansion to other TEFs (Health, AgriFood) is planned, requiring additional work on identifying and integrating sector-specific standards.
- The full report on Risk Classification has been prepared at CitCom.
- A scientific article on the challenges of risk classification for industrial and ICS-related AI systems is under development.

TEFs at RISE



Health

AgriFood

Smart and sustainable cities and societies

CitCom AI

Please, reach out to us for any further details concerning the service!

COORDINATEF
Boosting European AI innovation, together.

CitCom.ai label

Alessio Buscemi
Luxembourg Institute of Science and Technology (CitCom.ai)

Funded by
the European Union

A testing use case within Citcom

- The municipal administration of Luxembourg City was experimenting with a third-party provider a citizen-facing chatbot to operate as the first line of interaction between residents and municipal services.

- Before releasing the chatbot, the administration requested LIST to perform an assessment of social biases, focusing on whether the system treats different groups equitably and avoid harmful stereotypes
- a
- The goal was to verify that the chatbot behaves consistently across equivalent prompts, does not make group dependent assumptions, and provides accurate, neutral, and actionable guidance to all citizens.

- Therefore, using our AI Sandbox, we conducted an extensive bias assessment of the chatbot using use case relevant challenges co-designed with the City administration

- We initially identified a few issues, which were solved with the addition of safety guardrails

Good, but...

1. How can the City ensure that the positive results of this one-off bias assessment can be reproduced consistently in future updates or in other municipal chatbots?

2. How can third-party providers and municipalities demonstrate to citizens that such bias testing meets a recognised, minimum standard rather than relying on an ad-hoc evaluation?

3. How can policymakers and administrators communicate transparently that the chatbot has passed a trustworthy and independently verifiable assessment, beyond simply stating that “the issues were fixed”?

The importance of AI labels

AI labels are a way solve the communication gap between technical and non-technical stakeholders [1]:

Make AI understandable

Translate complex technical details into clear, visual summaries for non-experts.

Bridge communication gaps

Help technical and non-technical stakeholders make shared, informed decisions.

Increase transparency and trust

Show key performance, data, and robustness indicators clearly.

Promote responsible use

Highlight ethical and sustainability aspects like fairness and energy efficiency.

Support better governance

Offer insights that complement detailed AI documentation.

[1] K. Poitz, R. Fischer, "AI Labels – How They Can Provide Guidance and Build Trust", LAMARR Institute, 2025

CitCom.ai: where cities and AI innovators find each other …… and create mutual trust

City Journey

a concrete challenge to perform one of the city missions and processes…

…find / define a concrete use case..

… find relevant AI solutions…

… ready for cities? ready for my city?

…easier to buy & adopt AI solutions from innovators

AI Innovator Journey

AI solution…

…applied to smart city use cases…

…how to convince cities that it is "city ready" ?

…how to adapt it to each city?

…easier to sell AI solutions to cities

Perform a CitCom.ai experiment

Citcom Label

Citcom AI Solution Catalog

A design thinking approach

Name: Thomas De Meester
Organization: imec
Role: Innovation manager

AI and AI assessment-related assets and activities: Belgian node coordinator
Expectations about the AI Assessment club: Looking to contribute imec expertise and use outcomes of assessment club to develop services in the Belgian node.

Name: Ross Lowette
Organization: City of Mechelen
Role: Citcom.ai project coordinator

AI and AI assessment-related assets and activities: TEF site in Citcom, real life testing in the city of Mechelen.
Expectations about the AI Assessment club:

Name: Benjamin Vermeulen
Organization: City of Mechelen
Role: CitCom.ai data analist

AI and AI assessment-related assets and activities: Sensor data/platform expert - Sensor solutions and their applications in policy making.
Expectations about the AI Assessment club:

Name: Vicent Botti
Organization: VRAIN - UPV
Role: Full Professor

AI and AI assessment-related assets and activities: member of the AI Safety Institute Consortium (AISIC), member of the project 'Foundations of Trustworthy AI - Reasoning, Learning and Optimization (TAILOR)', expertise in explainable AI and AI Evaluation
Expectations about the AI Assessment club:

Design thinking session (35 Min)

To be compiled offline + 10 min discussion

Have you/your TEF site conducted or required assessments of AI solutions?

YES - Please share a high-level overview, key learnings, open questions, and future directions.

NO - Please explain the reasons, where you believe assessments could be integrated, and your thoughts on future directions.

25 min = 10 min post-its + 15 min discussion

Who are the personas we aim to serve with AI assessments?
What is the value of AI assessment solutions within Citcom?
What kind of AI assessments should be included in the Citcom.ai assessment catalogue?

Target Personas

Project sponsor / owner (RoBs)

SMEs, public authorities

Value of AI assessment within Citcom

Trustworthy AI models

Ethical and legal license to operat (RoBs)

Type of Assessment Services / Catalogue

Prioritization, wrap-up and next steps (15 Min)

- Summary
  - Current state in Citcom
  - Towards an AI assessment catalogue
    - Target personas
    - Value Proposition
    - Type of assessments in the catalogue
    - Catalogue format
- Lead-in to the next session
  - Categorization of different AI assessment approaches.
  - Evaluation of the feasibility and value of a common AI assessment framework.
  - Establishment of asset-sharing mechanisms and defining cross-TEF collaborations for test development.

Expected outcomes

- We have identified key deliverables to guide the next phase of development:
  - **Launch of the AI Assessment catalogue**
  - **Formalisation of Guidelines and Evaluation Reports**
  - **Creation of the Citcom Label**
  - **Pilot Implementation**

Launch of the AI assessment catalogue

- A fundamental step before the actual creation of the catalogue, is the identification of categorisation guidelines for testing solutions, in a way that allows easy matching with the use cases requiring the assessment

- This are the criteria we identified:

Current assessment capabilities across Citcom

Solution name	Provider	Licensing Type	Project Phase/ TRL	Domain of Application	Ethical Dimensions	Security & Securitization of Data	Assessment Type	Example of use case	Resources

Citcom experiments requiring AI Assessment

Experiment	City	Description	AI Innovator	Project Phase/ TRL	Assessment requirements	AI Risk Category	Ethical Dimensions	Security & Securitization of Data	Assessment Type	Resources

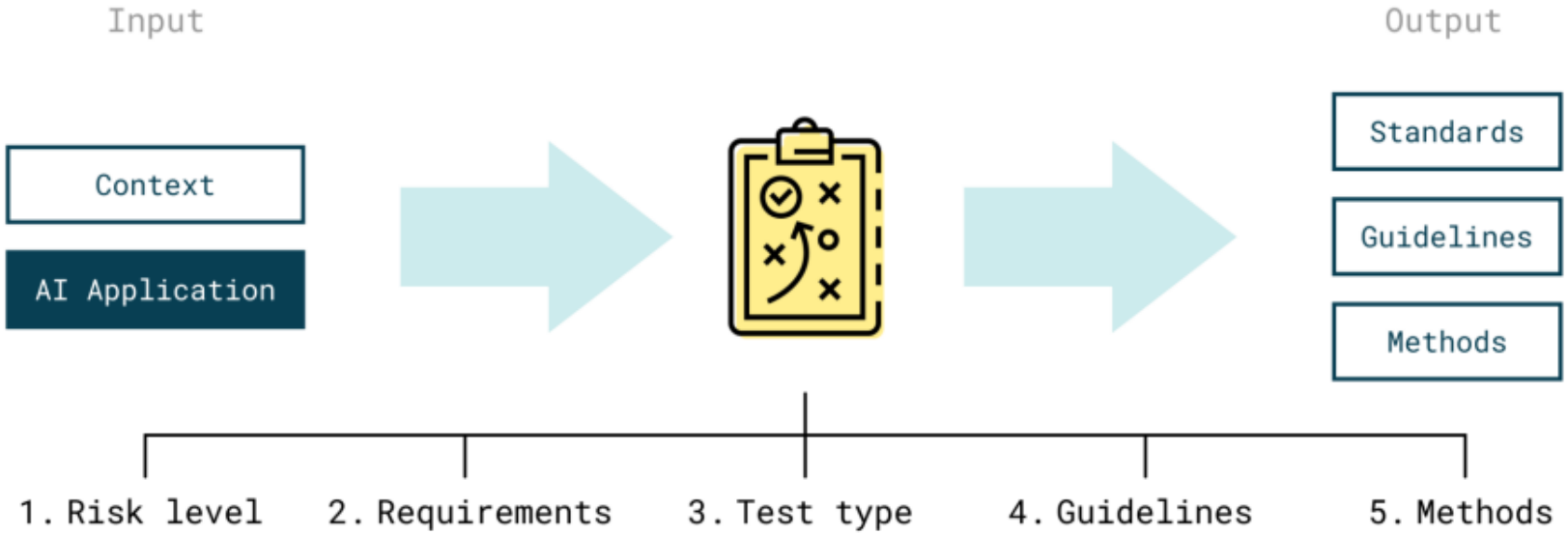
- The next step is to create the actual catalogue collecting all assessment solutions operated by Citcom partners

Expected outcomes

- We have identified key deliverables to guide the next phase of development:
  - **Launch of the AI Assessment catalogue**
  - **Formalisation of Guidelines and Evaluation Reports**
  - **Creation of the Citcom Label**
  - **Pilot Implementation**

Methodology

- LIST and RISE started the mapping from legal requirements to methods, based on RISE's methodology*



- In our soon-to-be-released paper, we work on identifying:

Requirements | Sources | Assessment Dimensions

*Mowla, N. et al., (2024). *From AI Act to structured testing of AI systems*. RISE Research Institutes of Sweden.

Requirements

- We identified 11 categories of requirements that capture the key dimensions of AI trustworthiness & compliance

- The starting point was the 7 principles of Trustworthy AI defined by the European Commission's HLEG:

🔎 **Human agency and oversight**

🛡 **Robustness and safety**

🔒 **Privacy and data governance**

🔳 **Transparency**

✅ **Accountability**

🤲 **Fairness, diversity & non-discrimination**

🌱 **Societal and environmental well-being**

- To complement these ethical foundations with more operational and procedural dimensions, we added 4 additional categories corresponding to key obligations introduced by the AI Act:

🏅 **Quality management**

⚠️ **Risk Management**

📄 **Technical Documentation**

🗂 **Record-keeping**

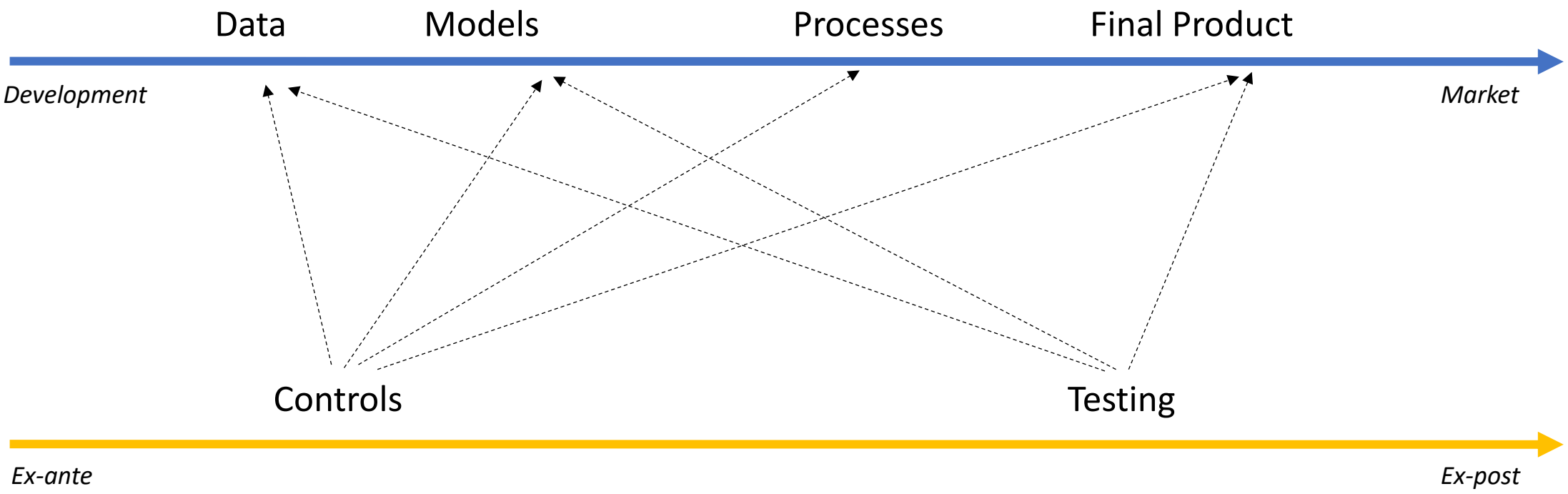
Sources for controls and testing methods

Binding or quasi binding regulatory sources (AI Act, GDPR etc.)

International standards or authoritative guidance (ISO, GPAI Code of Practice, ISACA etc.)

Recognised and highly cited scientific work

Dimensions of Assessment



Expected outcomes

- We have identified key deliverables to guide the next phase of development:
  - **Launch of the AI Assessment catalogue**
  - **Formalisation of Guidelines and Evaluation Reports**
  - **Creation of the Citcom Label**
  - **Pilot Implementation**

Proposed Citcom Label

- **Value proposition:** Independent third-party assessment of AI trustworthiness, with **non-binding compliance recommendations** to guide cities and procurement officers.

- **Badging system:** Result-specific badges awarded to innovators, with granularity based on market needs.

- **Credibility & thresholds:** Consistent credibility across badges ensured by harmonised guidelines andcase-by-case expert evaluation.

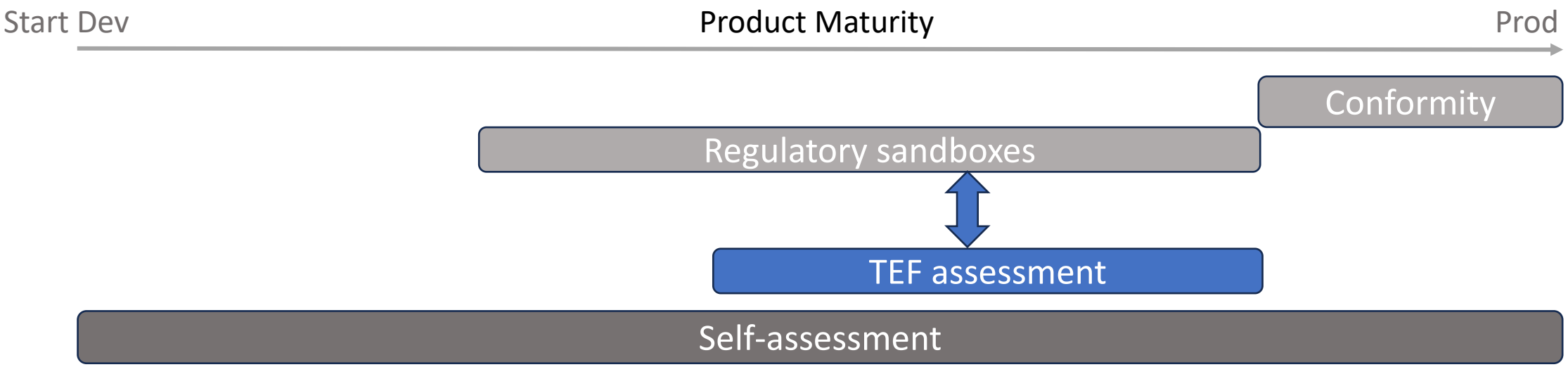
- **Badge infrastructure:** Timestamped, tamper-proof badges linked to the Citcom Hub for verification,transparency, and metadata access.

- **Reporting & visibility:** Harmonised evaluation reports with **legal disclaimers**; public list of participating AI innovators hosted on the Citcom Hub.

Expected outcomes

- We have identified key deliverables to guide the next phase of development:
  - **Launch of the AI Assessment catalogue**
  - **Formalisation of Guidelines and Evaluation Reports**
  - **Creation of the Citcom Label**
  - **Pilot Implementation**

TEF assessment in the broader EU innovation ecosystem



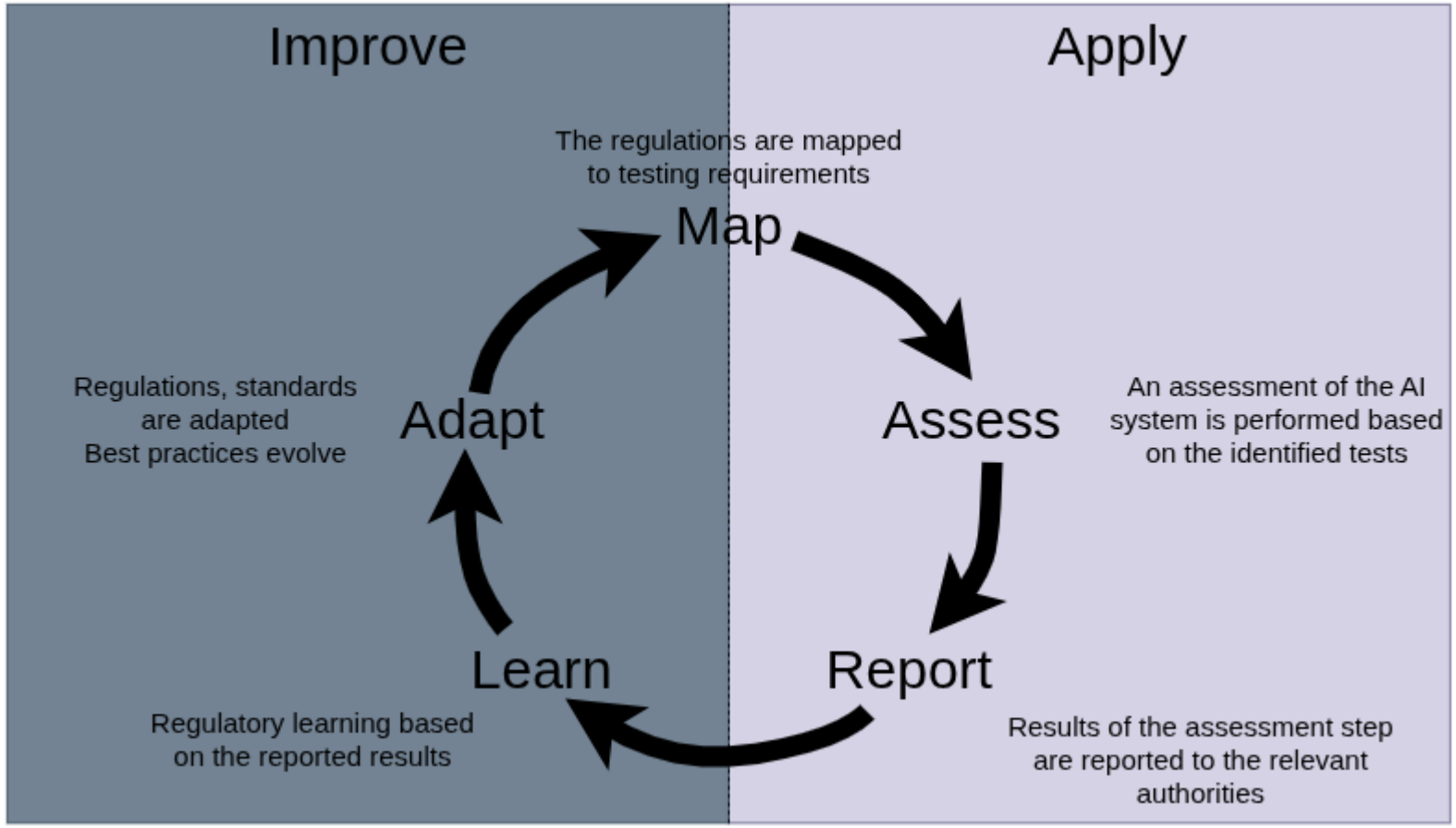
- We believe that TEF assessment could be also valuable with respect to AI Regulatory Sandboxes (AIRSes)
- The AI Act (Art. 58(2)(i)) explicitly mandates that AIRSes should *"facilitate the development of tools and infrastructure for testing, benchmarking, assessing and explaining dimensions of AI systems [..]"*
- Testing tools, thresholds, and result interpretations must be adapted to the specific sector and use case
- TEFs could serve as preferred partners for Competent Authorities seeking external technical expertise to carry out assessments in Regulatory Sandboxes within their respective domains

MARLA

- Drawing from discussions and personal experience with regulators and legal experts, fostering effective communication between technical and legal professionals remains a major challenge.

- This dialogue is essential for practitioners to correctly interpret legal requirements and to foster regulatory learning, a key principle introduced by the AI Act.

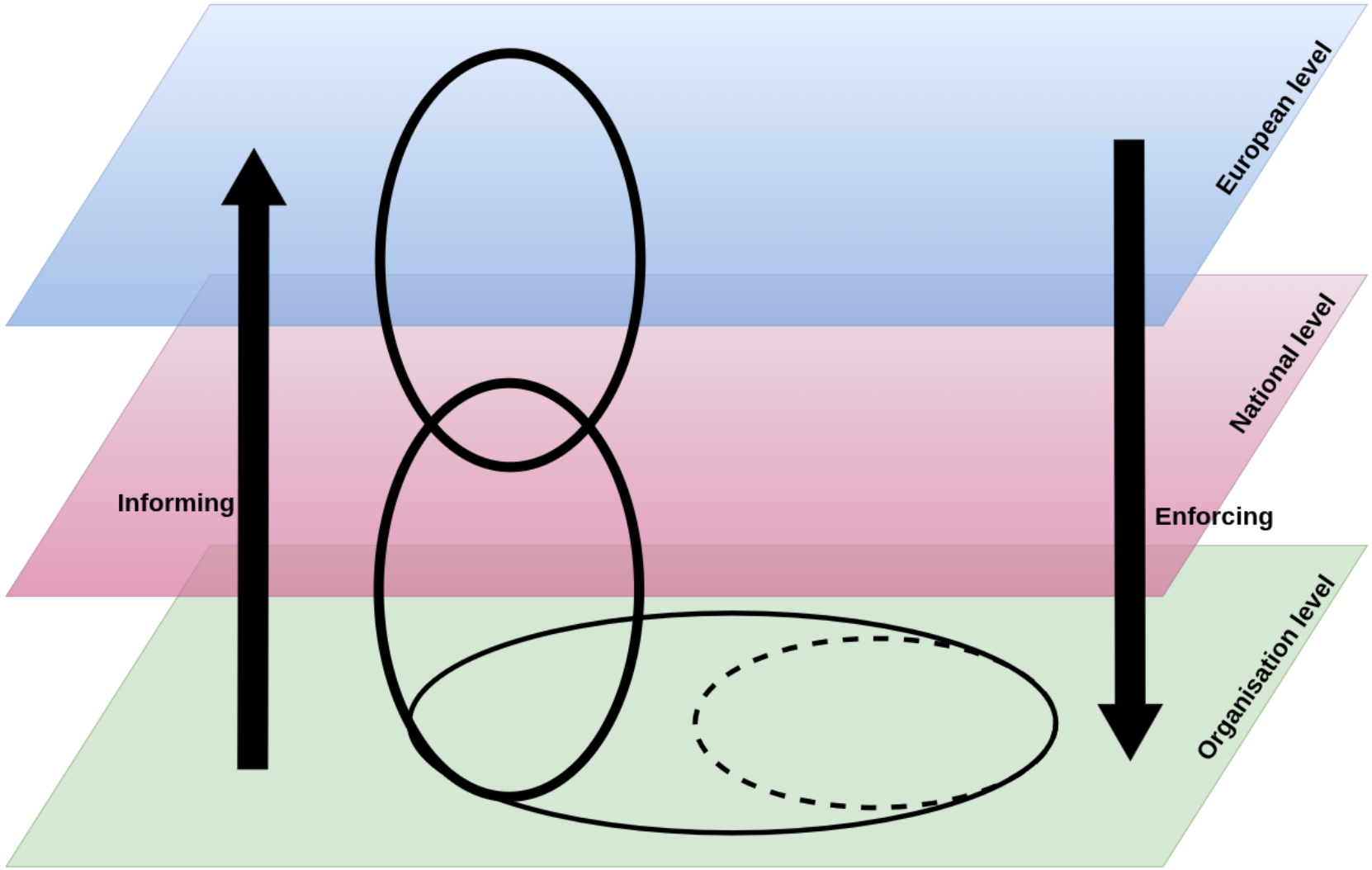
- For this reason, within the Luxembourg AI Factory, we developed **MARLA**, a high-level framework designed to identify and structure the various stages of this cycle.



Enabling dialogue between developers and regulators

MARLA can be implemented on three complementary levels:

- **Organisational level:** to support internal learning and continuous improvement within companies or institutions.
- **National level:** to enable regulatory learning and structured dialogue with competent authorities.
- **European level:** to promote alignment, knowledge exchange, and coherence across Member States.



Conclusion

- The Citcom label is conceived as an independent third-party evaluation of AI trustworthiness, offering non-binding compliance recommendations to guide cities and procurement officers in their decision-making.
- It can serve as a blueprint for other TEFs
- The assessments conducted within the TEFs can serve as a benchmark in the European AI landscape for the sectors they cover.
- To ensure coherence and complementarity across domains, other TEFs are encouraged to contribute to the refinement of the assessment guidelines.
- Where sector-specific regulations apply, their additional requirements can be mapped and integrated into the proposed methodology.

COORDINATEF
Boosting European AI innovation, together.

Q&A Session

COORDINATEF
Boosting European AI innovation, together.

Closing remarks & Next Steps

Next Steps

1. Set up of a **working group** on **AI Regulatory Sandboxes** to establish connections among AIRS & TEFs

2. Collection of **further TEF Consortia members compliance practices** thanks to the Workshop.
   Engage with us and share your practices!

3. Development of a **common compliance framework** for TEFs in order to ensure **compliance** with the AI Act

Visit our website and LinkedIn profile!

Subscribe to the CoordinaTEF LinkedIn channel!

Visit CoordinaTEF Project website!

COORDINATEF
Boosting European AI innovation, together.

Thank you!