



OPERATIONS  
MANAGEMENT  
SUMMIT



THE LINUX FOUNDATION  
OPEN SOURCE SUMMIT  
NORTH AMERICA

# Accountability Taxonomy for AI Software Bill of Materials

Arthit Suriyawongkul, ADAPT Centre, Trinity College Dublin



#ossummit

@bact

16 April 2024



Registration

set surveillance authority in that  
in 30 days, the testing in real world  
be understood as approved. In cases

Information to be submitted upon the registration of high-risk AI systems in accordance with

TITLE VII

EU DATABASE FOR HIGH-RISK AI SYSTEMS LISTED IN  
ANNEX III

Article 60

EU database for high-risk AI systems listed in Annex III

1. The Commission shall, in collaboration with the Member States, set up and maintain a EU database containing information referred to in paragraphs 2 and 2a concerning high-risk AI systems referred to in Article 6(2) which are registered in accordance with Articles 51 and 54a. When setting the functional specifications of such database, the Commission shall consult the relevant experts, and when updating the functional specifications of such database, the Commission shall consult the AI Board.
2. The data listed in Annex VIII, Section A, shall be entered into the EU database by the provider or where applicable the authorised representative.
- 2a. The data listed in Annex VIII, Section B, shall be entered into the EU database by the deployer or where applicable the authorised representative or bodies, according to articles 54a(5) and 54a(6).
3. With the exception of the information referred to in Article 54a(5), the information referred to in Article 51 shall be accessible and publicly available in a user friendly manner. The information should be easily navigable and machine-readable. The information registered in accordance with Article 54a shall be accessible only to market surveillance authorities and the Commission, unless the prospective provider or provider has given consent for making this information also accessible to the public.
4. The EU database shall contain personal data only insofar as necessary for collecting and processing information in accordance with this Regulation. That information shall include the names and contact details of natural persons who are responsible for registering the system and have the legal authority to represent the provider or the deployer, as applicable.
5. The Commission shall be the controller of the EU database. It shall make available to providers, prospective providers and deployers adequate technical and administrative support. The database shall comply with the applicable accessibility requirements.

From this

Article 51

N A - Information to be submitted by providers of high-risk AI systems in accordance with Article 51(1)

Information shall be provided and thereafter kept up to date with regard to AI systems to be registered in accordance with Article 51(1):

Address and contact details of the provider;

Submission of information is carried out by another person on behalf of the provider, the name, address and contact details of that person;

Address and contact details of the authorised representative, where applicable;

Trade name and any additional unambiguous reference allowing identification of the AI system;

Intended purpose of the AI system and of the components and functions of the AI system through this AI system;

Concise description of the information used by the system (data, inputs) and its logic;

Location of the AI system (on the market, or in service; no longer placed on the market/in service);

2. URL for additional information (optional).

SECTION B - Information to be submitted by deployers of high-risk AI systems in accordance with Article 51(1b)

The following information shall be provided and thereafter kept up to date with regard to high-risk AI systems to be registered in accordance with Article 51:

1. The name, address and contact details of the deployer;

2. The name, address and contact details of the person submitting information on behalf of the deployer;

3. A summary of the findings of the fundamental rights impact assessment conducted in accordance with Article 29a;

4. The URL of the entry of the AI system in the EU database by its provider;

5. A summary of the data protection impact assessment carried out in accordance with Article 29a.

1. Before placing on the market or putting into service a high-risk AI system, the provider or, where applicable, the authorised representative shall register the system in the EU database referred to in Article 60.

AG\1296003EN.docx

145/245

- 1a. Before placing on the market or putting into service an AI system, the provider or, where applicable, the authorised representative shall conclude that it is not high-risk in application of the criteria set out in Article 6(2) and that system in the EU database referred to in Article 60.

- 1b. Before putting into service a high-risk AI system, the provider or, where applicable, the authorised representative shall select the system to be tested in accordance with the criteria set out in Article 6(2) and that system in the EU database referred to in Article 60.

Testing of high-risk AI systems in accordance with Article 60

1. Testing of AI systems in real world conditions shall be conducted by providers or prospective providers or, where applicable, the authorised representative. The detailed elements of the testing shall be adopted by the Commission in accordance with Article 74(2). This provision shall be without prejudice to the testing in real world conditions of high-risk AI systems referred to in Annex II.

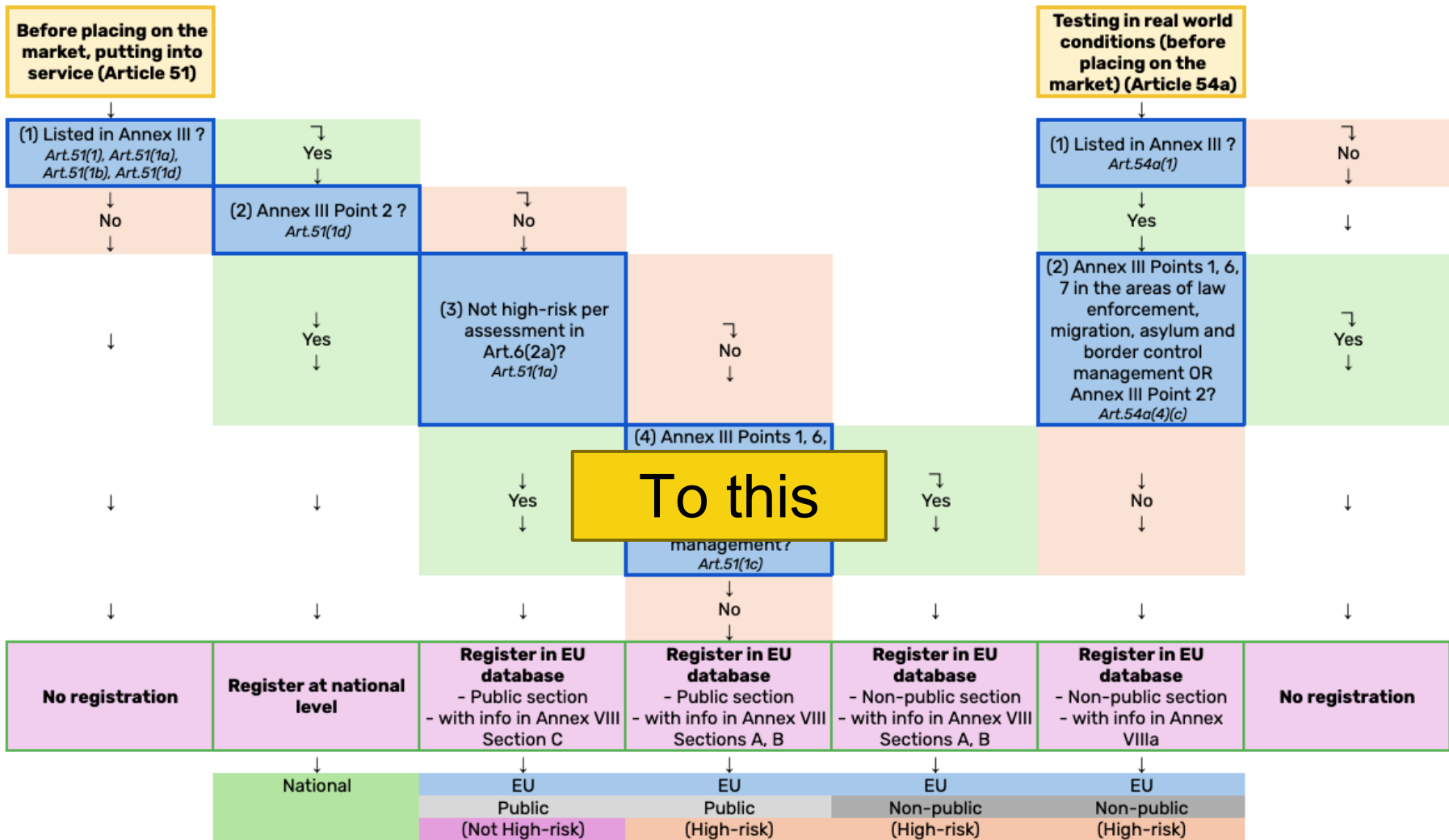
- 1c. For high-risk AI systems, the provider or, where applicable, the authorised representative shall ensure that the system is accessible and publicly available in a user friendly manner, in accordance with the criteria set out in paragraphs 3 and 4 of Article 51.

- points 1 to 9 of Annex II
- points 1 to 3 of Annex II
- points 1 to 9 of Annex II
- points 1 to 5 of Annex II

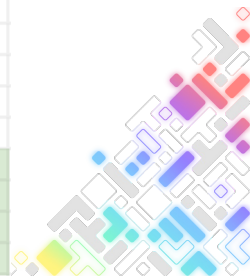
Only the Commission shall be responsible for these restricted systems.

AG\1296003EN.docx

- 1d. High risk AI systems



	Before placing on the market, putting into service (Article 51)			Testing in real world conditions (Article 54a)
	↓	↓	↓	↓
	with info in Annex VIII Section C	with info in Annex VIII Sections A, B	with info in Annex VIII Sections A, B	with info in Annex VIIIa
	↓	↓	↓	↓
	EU	EU	EU	EU
	Public	Public	Non-public	Non-public
	(Not High-risk)	(High-risk)	(High-risk)	(High-risk)
1 Name and contact details of the provider	Provider	Provider	Provider	Provider
4 AI system trade name	Provider	Provider	Provider	
5 Traceable ID	Provider	Provider	Provider	Provider
6 Intended purpose	Provider	Provider	Provider	Provider
7 Components and functions supported through this AI system;		Provider	Provider	
8 Information used by the system (data, inputs) and its operating logic;		Provider		
10 Summary of the grounds for considering the AI system as not high-risk	Provider			
11 Status of the AI system (on the market, or in service; no longer placed on the market/in service, recalled);	Provider	Provider	Provider	
13 Type, number and expiry date of the certificate issued by the notified body		Provider		
15 A copy of the EU declaration of conformity		Provider		
16 Instructions for use		Provider		
18 Name and contact details of the deployer		Deployer	Deployer	
20 A summary of the findings of the fundamental rights impact assessment		Deployer		
21 The URL of the entry of the AI system in the EU database by its provider		Deployer		
22 A summary of the data protection impact assessment		Deployer		
23 Union-wide unique single identification number of the testing				Provider
24 Name and contact details of users involved in the testing				Provider
26 A summary of the main characteristics of the plan for testing				Provider
27 Information on the suspension or termination of the testing				Provider



# The 8 LFAI Principles for Trusted AI – (R)REPEATS

Reproducibility

Robustness

Equitability

Privacy

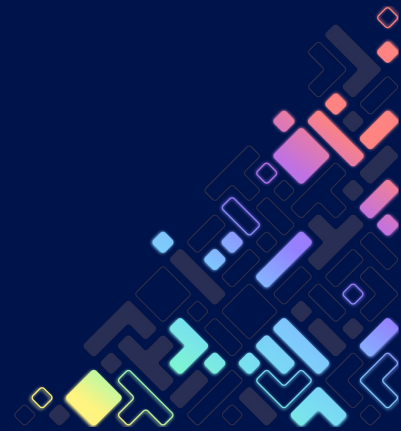
Explainability

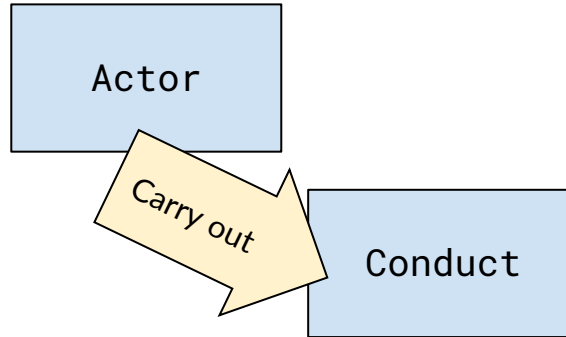
Accountability

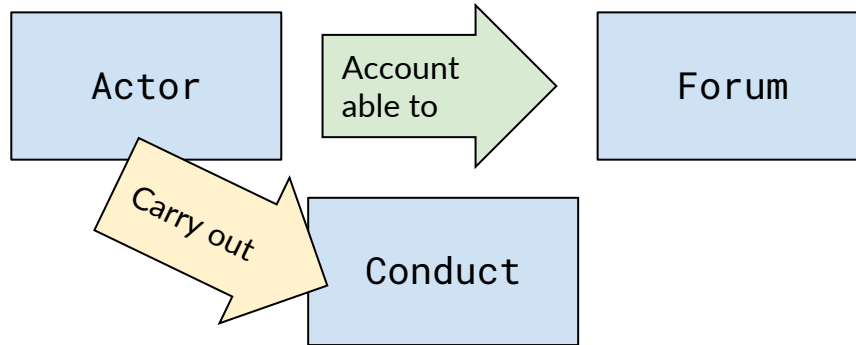
Transparency

Security

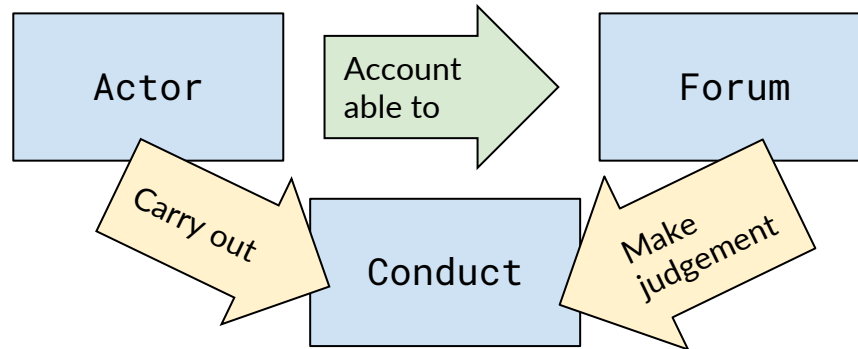
# Accountability?

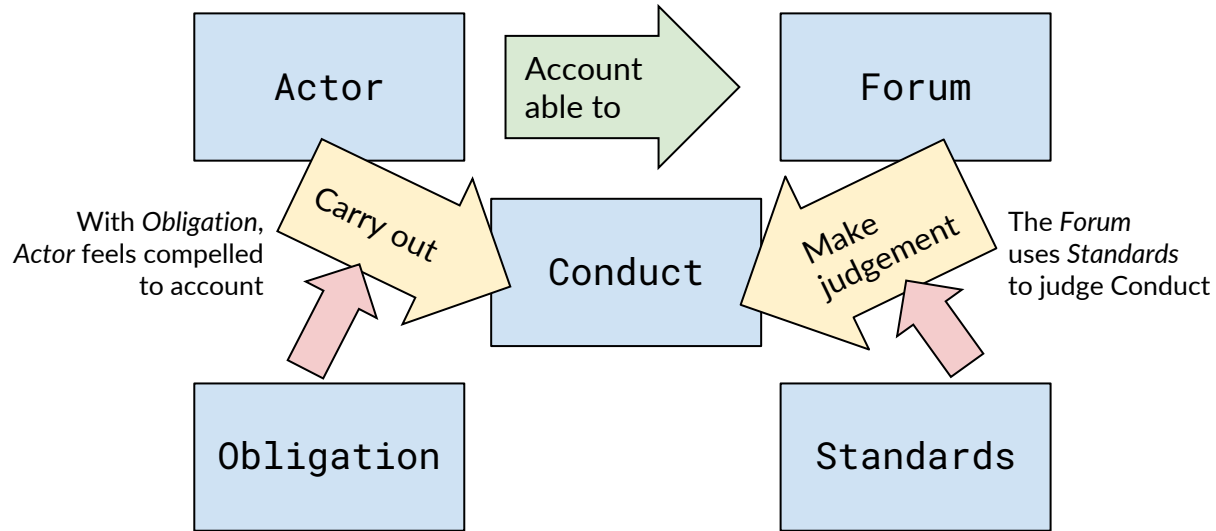




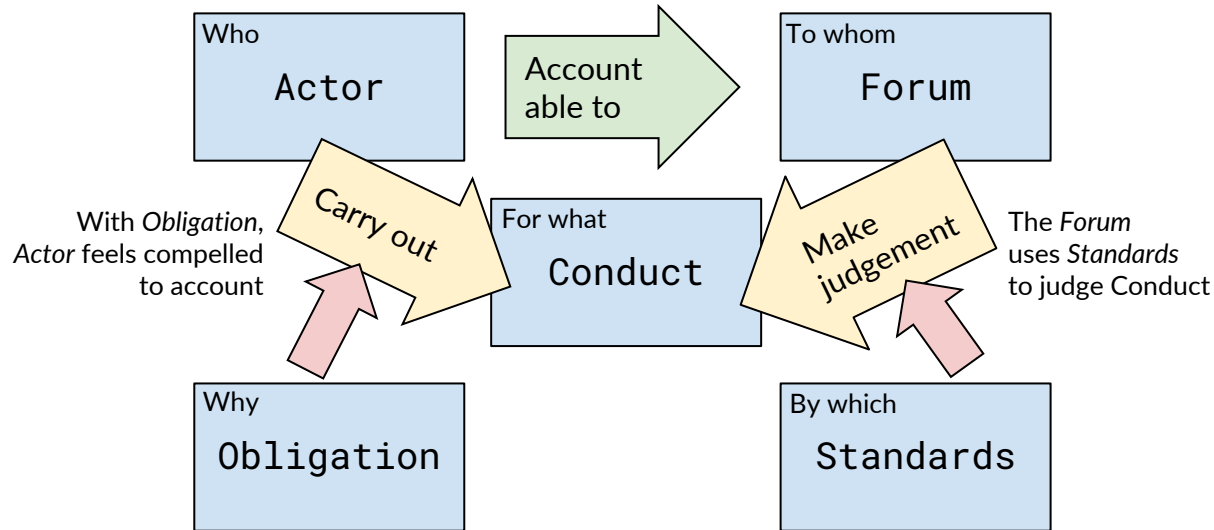




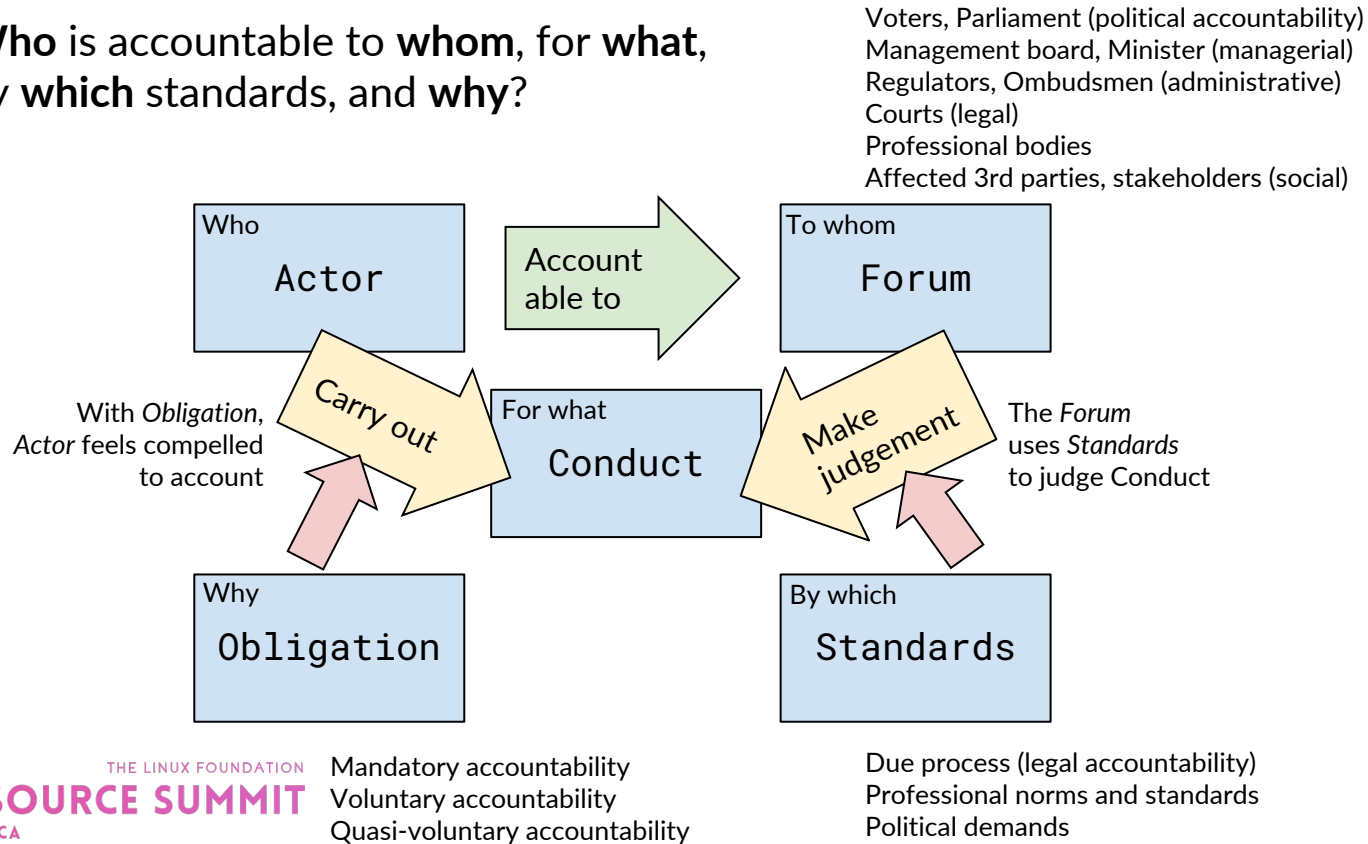




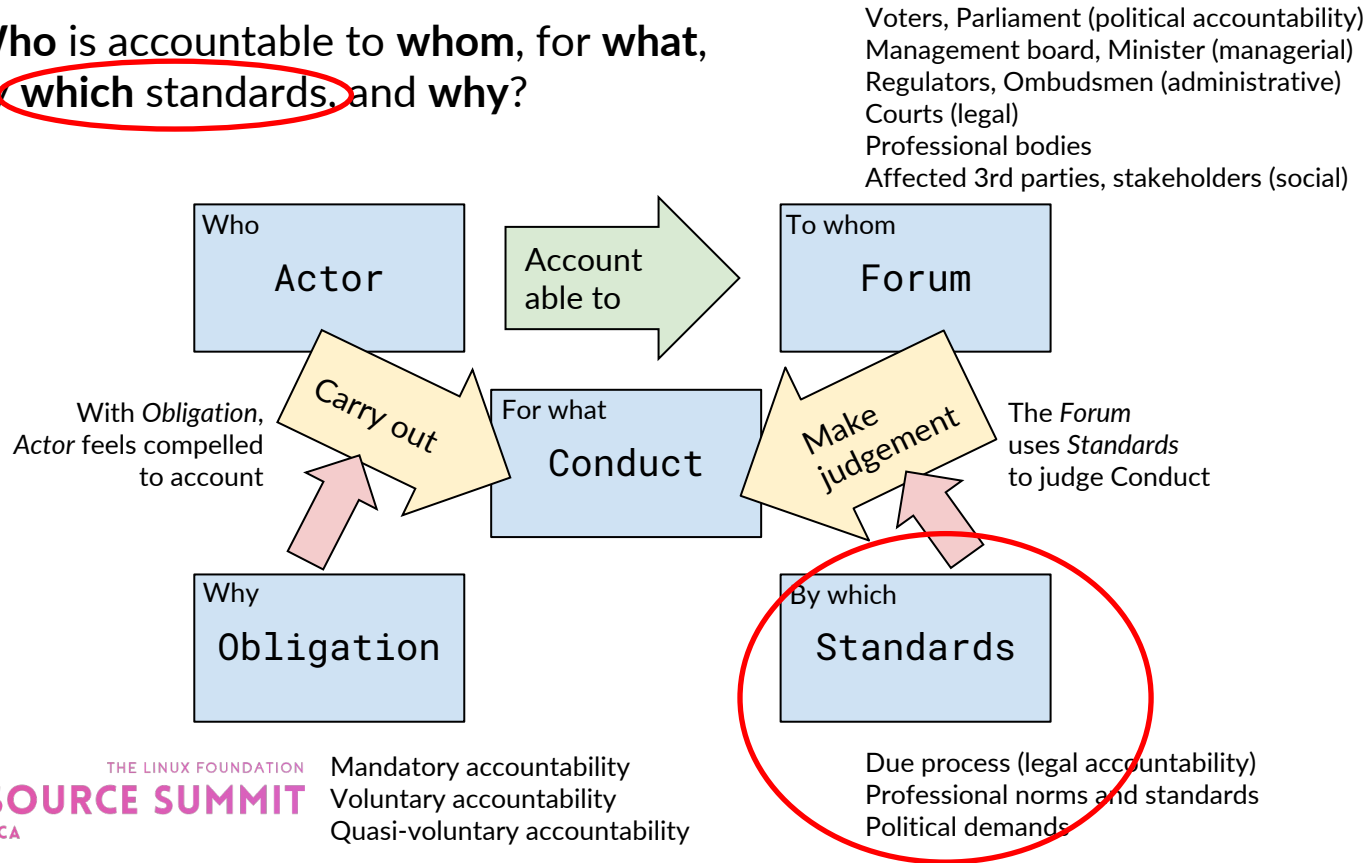
**Who** is accountable to **whom**, for **what**,  
by **which** standards, and **why**?



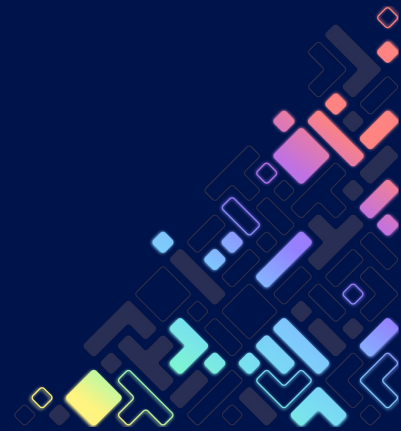
**Who** is accountable to **whom**, for **what**,  
by **which** standards, and **why**?



Who is accountable to whom, for what,  
by which standards, and why?



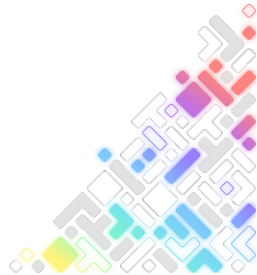
# A working definition of accountability.



# “Accountability” definition

“A set of mechanisms, practices and attributes that sum to a governance structure which involves committing to legal and ethical obligations, policies, procedures and mechanism, explaining and demonstrating ethical implementation to internal and external stakeholders and remedying any failure to act properly”.

Derived from Felici et al. 2013. Used in [IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems](#) and in [“A governance framework for algorithmic accountability and transparency”](#) study report by European Parliamentary Research Service.



# Purposes of Public Accountability

(adapted from Bovens et al. 2010)

## Democratic perspective

Popular control

*Explainability (legitimacy) + Human oversight (lawful + ethical)*

## Constitutional perspective

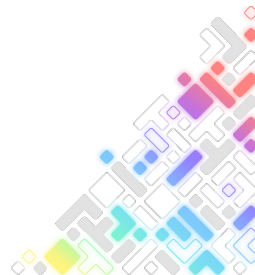
Prevention of corruption and abuse of power

*Bias and drift detection (technically robust + ethical)*

## Learning perspective

Maximising public value

*Information that allow the improvement of the system  
(technically robust, organizational learning)*

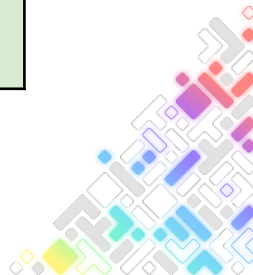




# Accountability as a virtue and as a mechanism

Accountability as a virtue	Accountability as a mechanism
<b><u>Focus on Behaviour</u></b>	<b><u>Focus on governance of behaviour</u></b>
Focus on actual performance of agencies	Focus on institutional relation or arrangement in which an agent can be held to account by another agent or institution
Accountability is dependent variable; accountability has effect on behaviour	Accountability is independent variable; accountability may or may not have effect on behaviour
Virtue is more domain-specific	Mechanism is less domain-specific
In AI context: How the AI system performs (accuracy, drift, etc.)	In AI context: How the AI system get built and served
<b>AI regulations: Post-market monitoring</b>	<b>AI regulations: Quality management system, Technical documentation</b>

Adapted from Bovens, M., Schillemans, T., Goodin, R.E., 2014. Public Accountability, in: The Oxford Handbook of Public Accountability. Oxford University Press, Oxford, New York, pp. 1–20. <https://doi.org/10.1093/oxfordhpb/9780199641253.013.0012>

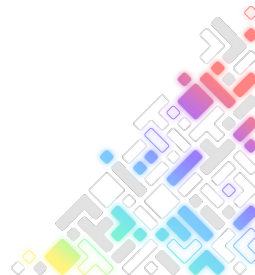


# “Non-algorithmic” accountability

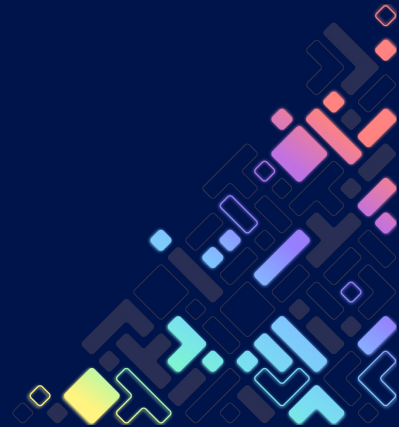
“Technical issues in algorithmic accountability are largely a question if the system behaves **according to specifications**.”

Accountability issues such as redress are beyond the technical challenges of the algorithm; these are more a question about the actions **implied by the specifications.**”

European Parliament. Directorate General for Parliamentary Research Services. "A Governance Framework for Algorithmic Accountability and Transparency."



# Information obligations as accountability mechanism

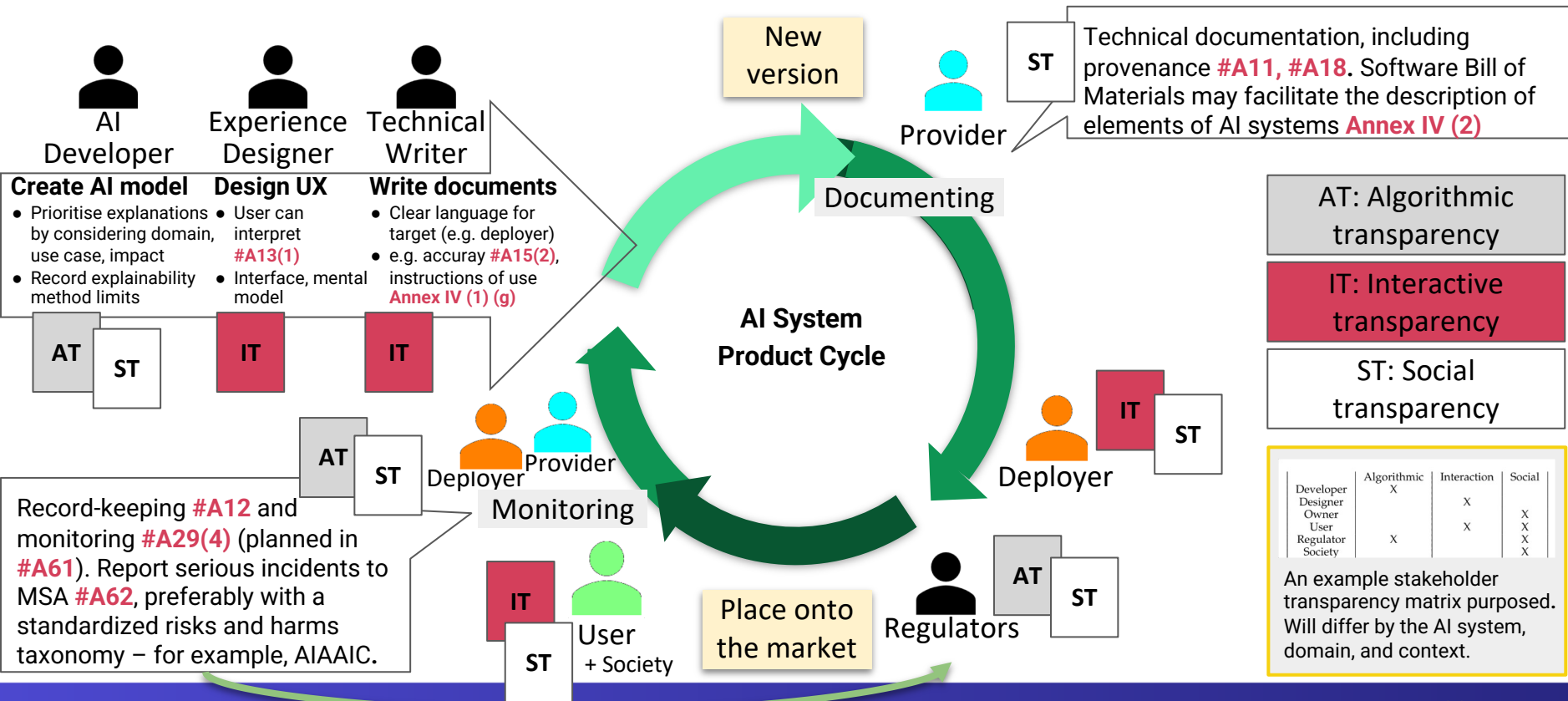


# Information obligations in EU AI Act that can support accountability (partial)

For high-risk AI systems
Provider name, registered trade name
Intended purpose
Instruction for use
Design choices
Standards applicable
Data origin, Collection original purpose
Possible biases, Measures to detect

For general purpose AI models
Intended tasks, Limitations
Instruction for use
Model design specification
Training process, Testing process
Information on the data used
Copyright protection policy
Acceptable use policies applicable

# Ensuring Transparency in AI Life-Cycle



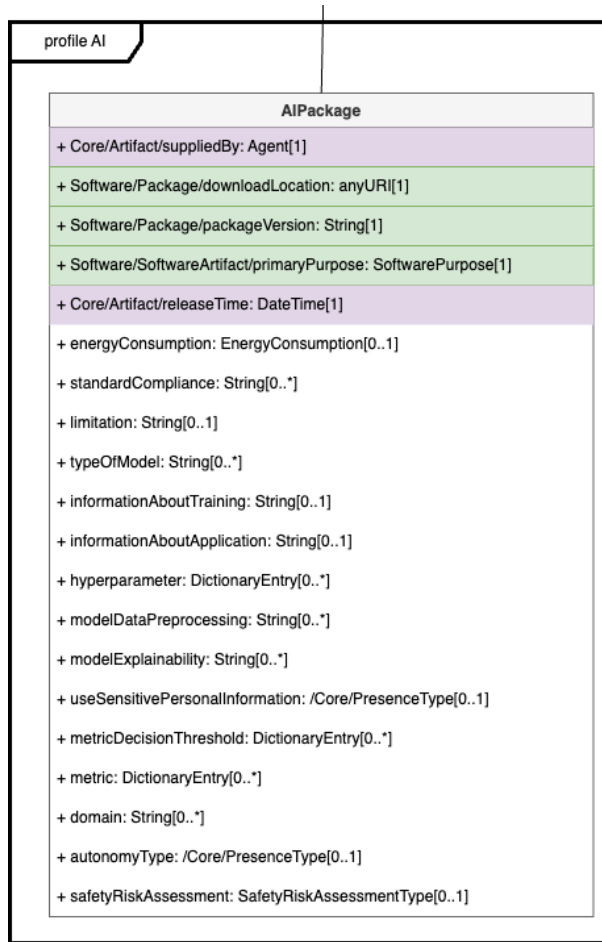
# Software Bill of Materials

“formal record containing the details and supply chain relationships of various components used in building software” – **Executive Order on Improving the Nation’s Cybersecurity (EO 14028)**

“analogous to a list of ingredients” “can help organisations or persons avoid consumption of software that could harm them.” – **Wikipedia**

“communicating a release: name, version, components, licenses, copyrights, and useful security references.” – **SPDX**

**ISO/IEC 5962:2021 Software Package Data Exchange (SPDX) Specification V2.2.1**



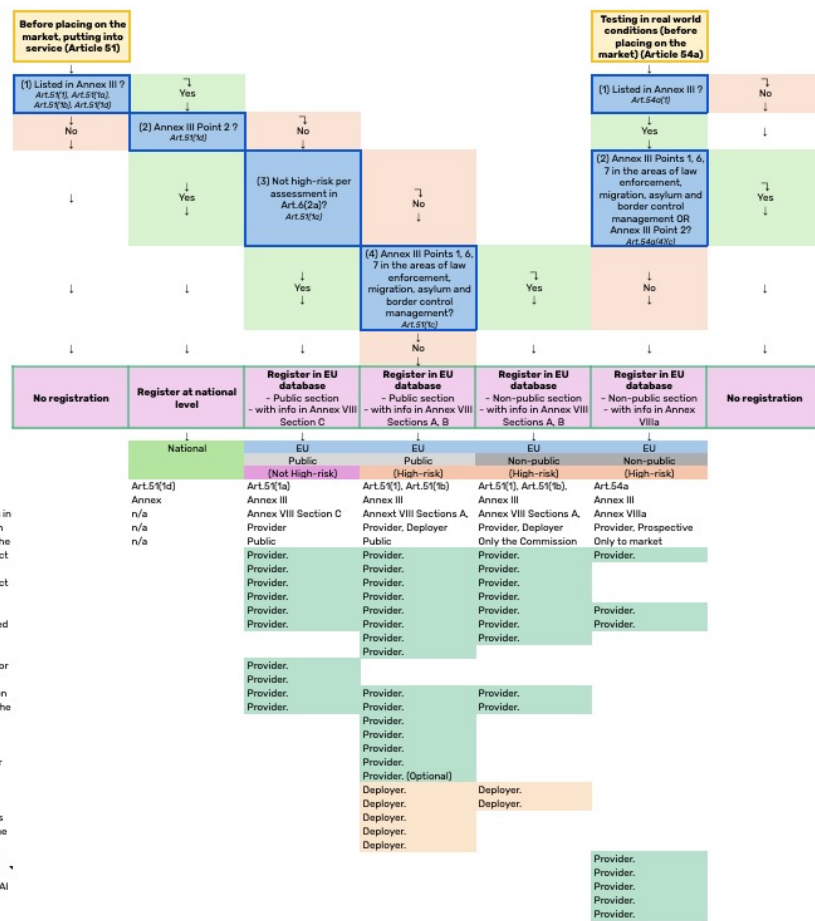
# Use cases

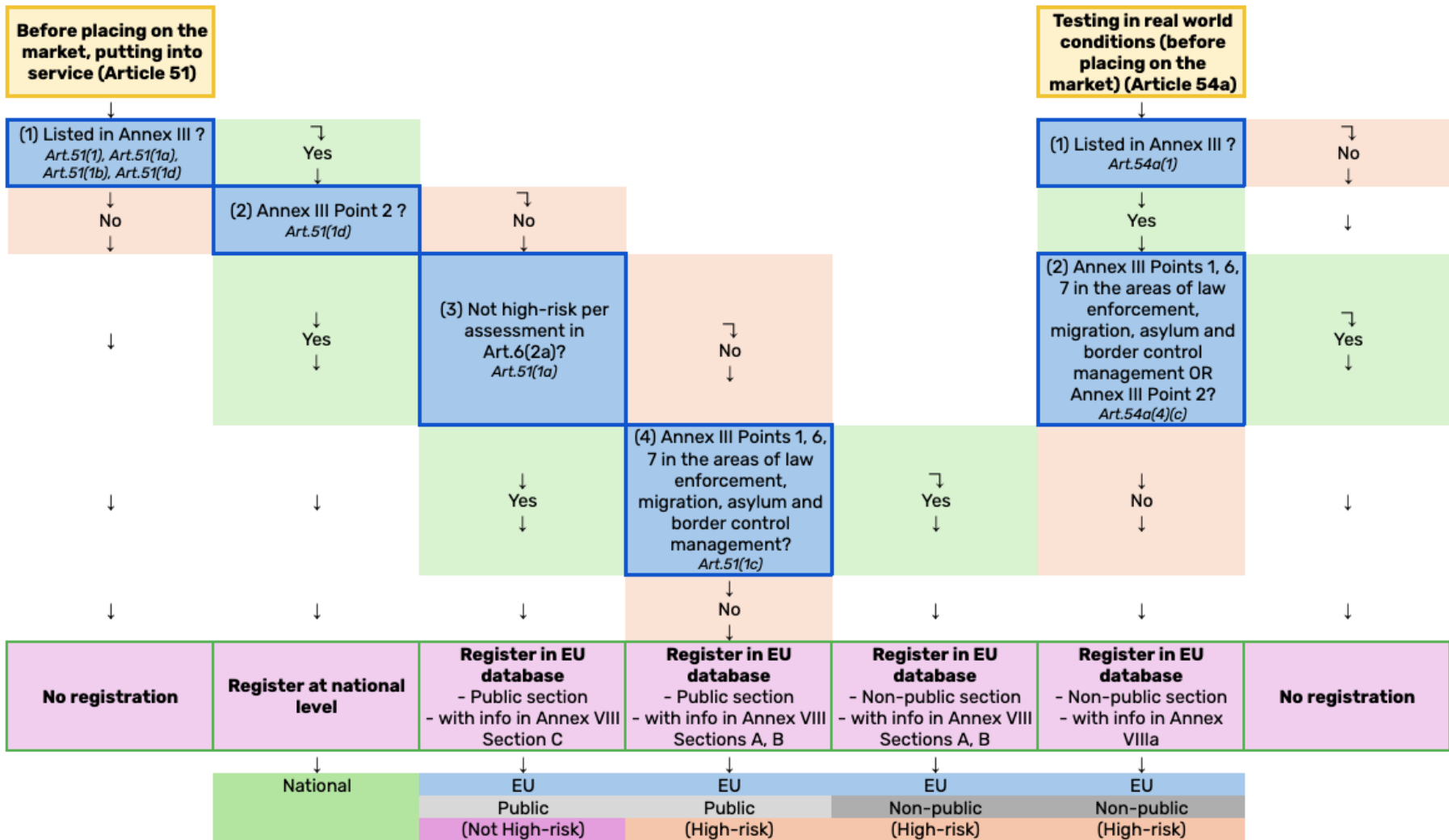
For AI providers/deployers

- To register in national/supranational database
- To get permission for testing in real-world conditions
- To get the declaration of conformity
- To report serious incident post-market
- To estimate remaining information obligations to fulfil to enter a new market

For regulators

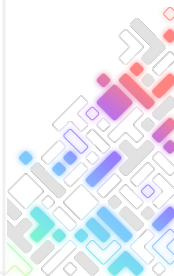
- To estimate resource for regulatory compliance



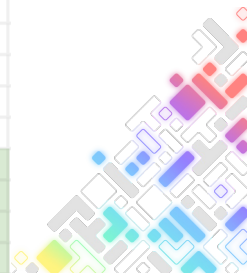





	Register at national level	Register in EU database - Public section - with info in Annex VIII Section C	Register in EU database - Public section - with info in Annex VIII Sections A, B	Register in EU database - Non-public section - with info in Annex VIII Sections A, B	Register in EU database - Non-public section - with info in Annex VIIIa
	↓	↓	↓	↓	↓
	National	EU	EU	EU	EU
		Public	Public	Non-public	Non-public
		(Not High-risk)	(High-risk)	(High-risk)	(High-risk)
Classification Articles	Art.51(1d)	Art.51(1a)	Art.51(1), Art.51(1b)	Art.51(1), Art.51(1b), Art.51(1c)	Art.54a
Classification	Annex III Point 2	Annex III Points 1, 3, 4, 5, 6, 7, 8	Annex III Points 3, 4, 5, 8 AND Annex III 1, 6, 7 that is not in the areas of law enforcement, migration, asylum and border control management	Annex III Points 1, 6, 7 in the areas of law enforcement, migration, asylum and border control management	Annex III Points 3, 4, 5, 8 AND Annex III 1, 6, 7 that is not in the areas of law enforcement, migration, asylum and border control management
Information requirements in the EU database	n/a	Annex VIII Section C	Annex VIII Sections A, B	Annex VIII Sections A, B with Exceptions in Art.51(1c)	Annex VIIIa
Information obligations on	n/a	Provider	Provider, Deployer	Provider, Deployer	Provider, Prospective provider
Who can have access to the information	n/a	Public Art.60(3)	Public Art.60(3)	Only the Commission and national authorities referred to in Art. 63(5) (Market surveillance authorities) Art.51(1c)	Only to market surveillance authorities and the Commission, unless the prospective provider or provider has given consent for making this information also accessible the public. Art.60(3)

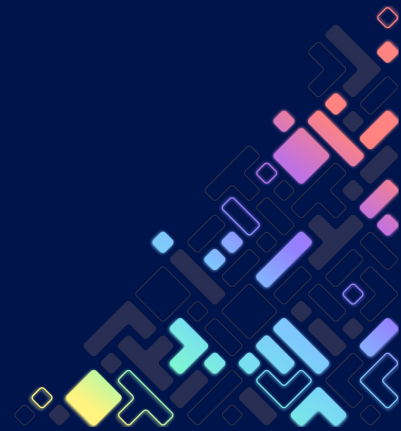


	Before placing on the market, putting into service (Article 51)			Testing in real world conditions (Article 54a)
	↓	↓	↓	↓
	with info in Annex VIII Section C	with info in Annex VIII Sections A, B	with info in Annex VIII Sections A, B	with info in Annex VIIIa
	↓	↓	↓	↓
	EU	EU	EU	EU
	Public	Public	Non-public	Non-public
	(Not High-risk)	(High-risk)	(High-risk)	(High-risk)
1 Name and contact details of the provider	Provider	Provider	Provider	Provider
4 AI system trade name	Provider	Provider	Provider	
5 Traceable ID	Provider	Provider	Provider	Provider
6 Intended purpose	Provider	Provider	Provider	Provider
7 Components and functions supported through this AI system;		Provider	Provider	
8 Information used by the system (data, inputs) and its operating logic;		Provider		
10 Summary of the grounds for considering the AI system as not high-risk	Provider			
11 Status of the AI system (on the market, or in service; no longer placed on the market/in service, recalled);	Provider	Provider	Provider	
13 Type, number and expiry date of the certificate issued by the notified body		Provider		
15 A copy of the EU declaration of conformity		Provider		
16 Instructions for use		Provider		
18 Name and contact details of the deployer		Deployer	Deployer	
20 A summary of the findings of the fundamental rights impact assessment		Deployer		
21 The URL of the entry of the AI system in the EU database by its provider		Deployer		
22 A summary of the data protection impact assessment		Deployer		
23 Union-wide unique single identification number of the testing				Provider
24 Name and contact details of users involved in the testing				Provider
26 A summary of the main characteristics of the plan for testing				Provider
27 Information on the suspension or termination of the testing				Provider



	Before placing on the market, putting into service (Article 51)			Testing in real world conditions (Article 54a)	
	↓	↓	↓	↓	
	with info in Annex VIII Section C	with info in Annex VIII Sections A, B	with info in Annex VIII Sections A, B	with info in Annex VIIIa	
	↓	↓	↓	↓	
	EU	EU	EU	EU	
	Public	Public	Non-public	Non-public	
	(Not High-risk)	(High-risk)	(High-risk)	(High-risk)	
1 Name and contact details of the provider	Provider	Provider	Provider	Provider	<div>  </div> <div>Agent.name</div> <div>AIPackage.name</div> <div>Y</div> <div>intendedUse</div> <div>Y</div>
4 AI system trade name	Provider	Provider	Provider		
5 Traceable ID	Provider	Provider	Provider	Provider	
6 Intended purpose	Provider	Provider	Provider	Provider	
7 Components and functions supported through this AI system;		Provider	Provider		supportLevel
8 Information used by the system (data, inputs) and its operating logic;		Provider			
10 Summary of the grounds for considering the AI system as not high-risk	Provider				
11 Status of the AI system (on the market, or in service; no longer placed on the market/in service, recalled);	Provider	Provider	Provider		
13 Type, number and expiry date of the certificate issued by the notified body		Provider			<div> Agent.name </div> <div> standardCompliance </div> <div> packageUri? </div> <div> standardCompliance </div> <div> Y </div>
15 A copy of the EU declaration of conformity		Provider			
16 Instructions for use		Provider			
18 Name and contact details of the deployer		Deployer	Deployer		
20 A summary of the findings of the fundamental rights impact assessment		Deployer			<div> Agent.name </div> <div>standardCompliance</div> <div>packageUri?</div> <div>standardCompliance</div> <div>Y</div>
21 The URL of the entry of the AI system in the EU database by its provider		Deployer			
22 A summary of the data protection impact assessment		Deployer			
23 Union-wide unique single identification number of the testing				Provider	
24 Name and contact details of users involved in the testing				Provider	
26 A summary of the main characteristics of the plan for testing				Provider	
27 Information on the suspension or termination of the testing				Provider	

# Demo



# Standardised logging

mlflow 2.11.3 Experiments Models

Default >  
flawless-bug-360

Overview Model metrics System metrics Artifacts

Run ID	Ocd3815a79cf4617924fdf80d604ffe
Duration	4.6s
Datasets used	—
Tags	InformationAboutTra... : Basic LR model for iris... AIProvider: Acme Corporation AutonomyType: No AIDeployer: Sirius Cybernetics UseSensitivePersonalInformation: No Hyperparameter: ('solver': 'lbfgs', 'max_iter': 1...
Source	ipykernel_launcher.py
Logged models	sklearn
Registered models	tracking-quickstart v7

Parameters (4)

Search parameters

Parameter	Value
random_state	8888
solver	lbfgs
max_iter	1000

Metrics (2)

Search metrics

Metric
TrainingEnergyConsumption
MetricsAccuracy

```
with mlflow.start_run():
    mlflow.set_tag(stav.INFO_TRAINING, "Basic LR model for iris data")
    mlflow.set_tag(stav.AI_PROVIDER, "Acme Corporation")
    mlflow.set_tag(stav.AI_DEPLOYER, "Sirius Cybernetics")
    mlflow.set_tag(stav.AUTONOMY_TYPE, "No")
    mlflow.set_tag(stav.USE_SENSITIVE_PERSONAL_INFO, "No")
    mlflow.set_tag(stav.HYPERPARAMETER, params)
    mlflow.log_params(params)

    mlflow.log_metric(stav.METRICS_ACCURACY, accuracy)
    mlflow.log_metric(stav.ENERGY_CONSUMPTION_TRAINING, 0.35)

# Infer the model signature
signature = infer_signature(X_train, lr.predict(X_train))

# Log the model
model_info = mlflow.sklearn.log_model(
    sk_model=lr,
    artifact_path="iris_model",
    signature=signature,
    input_example=X_train,
    registered_model_name="tracking-quickstart",
)
```



# Enable standardised query

Default ⓘ [Provide Feedback](#) [Add Description](#)

Q metrics.rmse < 1 and params.model = "tree" ⓘ

Time created ▾

params.random\_state

params.solver

Tags

tags.InformationAboutTraining

tags.AIProvider

tags.AutonomyType

tags.AIDeployer

tags.UseSensitivePersonalInformation

Q tags.UseSensitivePersonalInformation = "Yes" | ⓘ

Time created ▾

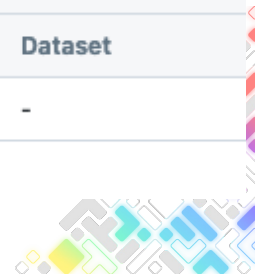
Sort: Created ▾

Columns ▾

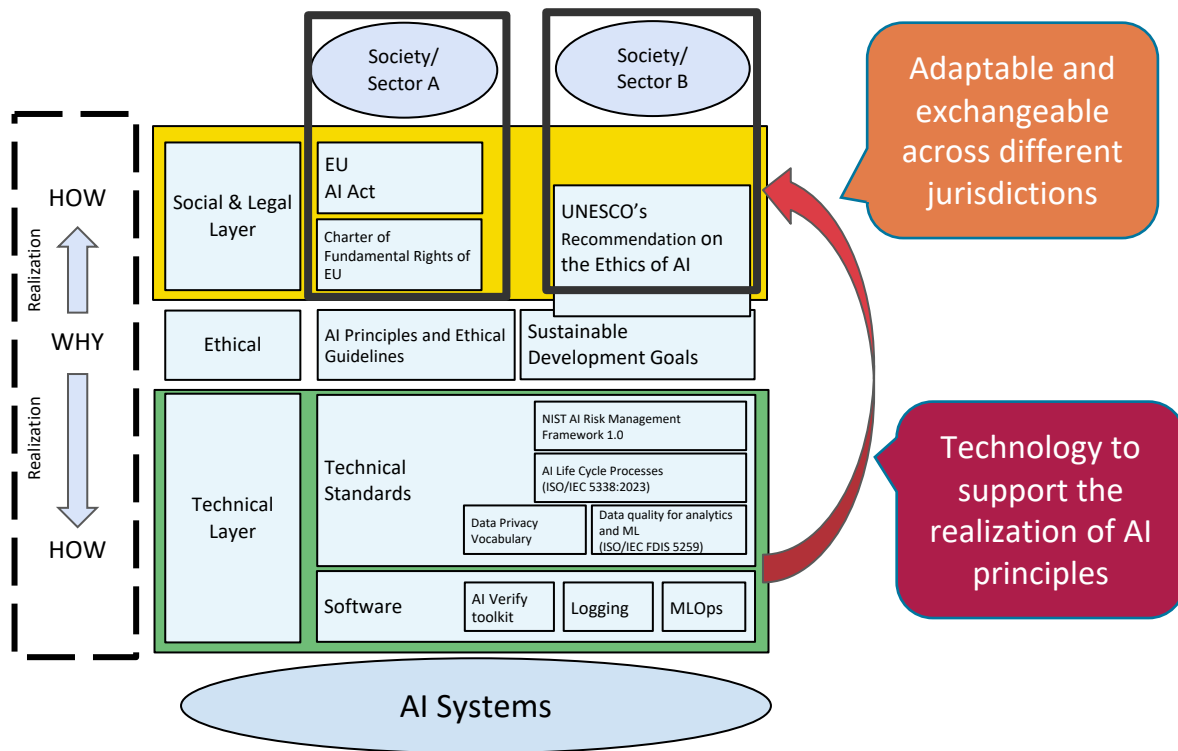
Group by ▾

Table Chart Evaluation **Experimental**

<input type="checkbox"/>		Run Name	Created	Dataset
<input type="checkbox"/>		luminous-grub-855	2 hours ago	-



# Bridging the gaps



Standard taxonomy to serve three accountability purposes:

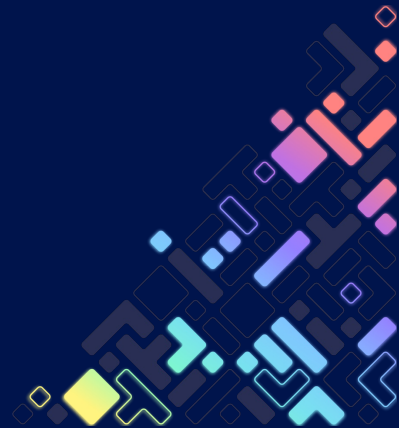
**Democratic**  
Technical documentation + database for informed popular control

**Constitutional**  
Continuous record keeping to minimize corruption or abuse of power

**Learning**  
Incident reporting to maximize public value and safety



regtech.adaptcentre.ie





# Thank you

Arthit Suriyawongkul  
suriyawa@tcd.ie



## HOST INSTITUTION



**Trinity College Dublin**  
Coláiste na Tríonóide, Baile Átha Cliath  
The University of Dublin

## PARTNER INSTITUTIONS



**DCU** City of  
Chesham  
Baile Átha Cliath  
Dublin City University



**University College Dublin**  
An Coláiste Ollscoile, Baile Átha Cliath  
Ireland's Global University



**OLLSCOIL NA GAILLIMHE**  
UNIVERSITY OF GALWAY



**OPEN SOURCE SUMMIT**  
NORTH AMERICA

THE LINUX FOUNDATION

