Engaging Content
Engaging People

A World Leading SFI Research Centre

Science Foundation Ireland sfi For what's next

AI Act, Interoperability and the Semantic Web

Dave Lewis, TCD

With thanks to Delaram Golpayegani (TCD) and Harsh Pandit (DCU)

ADAPT Centre

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

HOST INSTITUTION
DCU

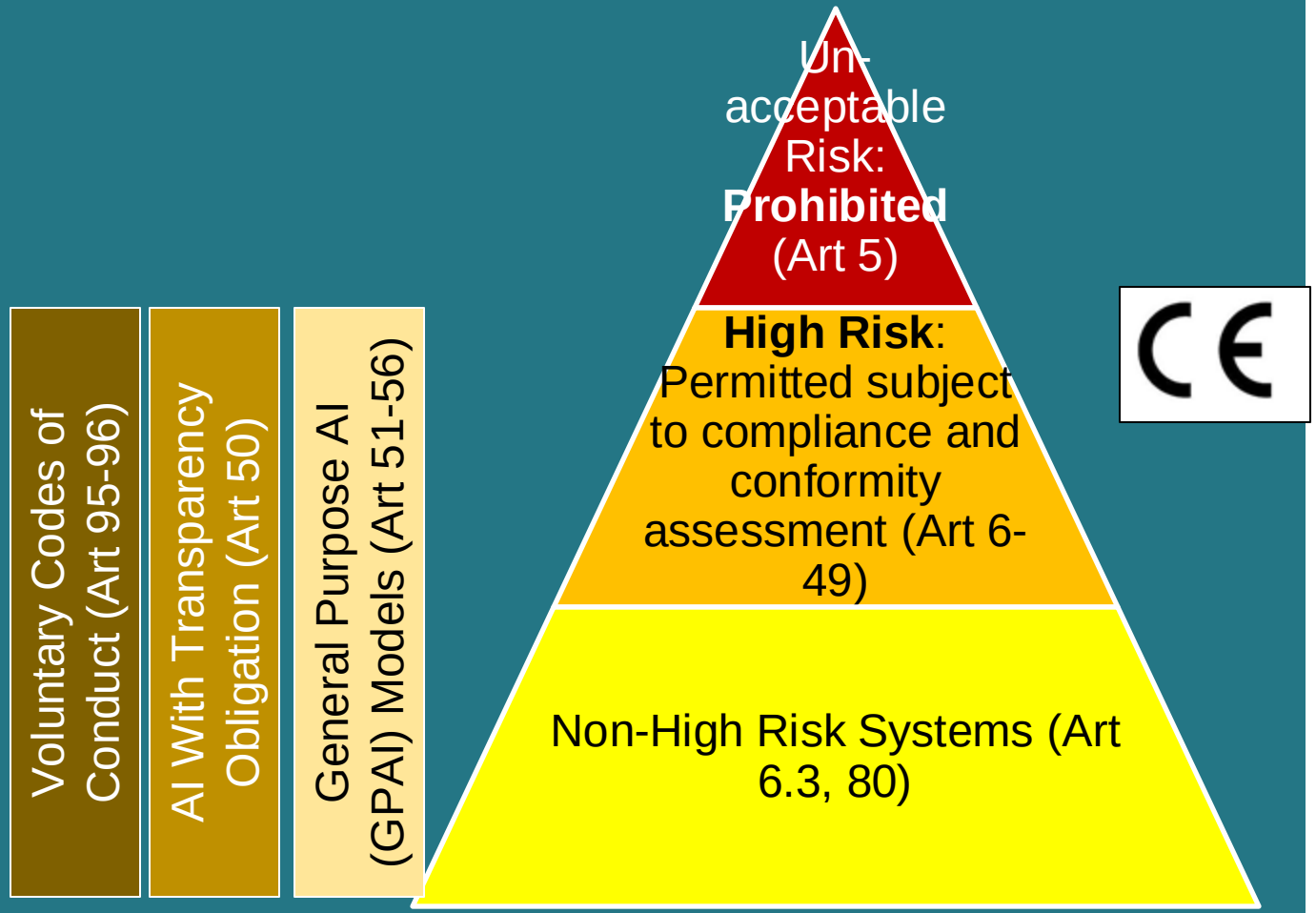
PARTNER INSTITUTIONS
TU Dublin
University College Dublin
An Coláiste Ollscoile, Baile Átha Cliath
Ireland's Global University
MTU
Ollscoil Teicneolaíochta na Mumhan
Munster Technological University
TUS
Maynooth University
National University of Ireland Maynooth
Ollscoil na Gaillimhe
University of Galway

EU “Digital” Jurisprudence

Engaging Content
Engaging People

Law	Enforcement	Area	Rights & Freedoms
GDPR	MAY-2018	personal data	transparency, autonomy, fiduciary
Digitial Services Act	NOV-2022	service	transparency, autonomy, fiduciary
Digital Marget Act	MAY-2023	market	autonomy
Data Governance Act	SEP-2023	market	fiduciary
AI Act	AUG-2024	technology	fiduciary
ePrivacy Reg	draft	communication	transparency, autonomy, fiduciary
Data Act	JAN-2024	data	autonomy
Health Data Space	Autumn ‘24	health data	autonomy, fiduciary
Interoperable Europe Act	APR-2024	data, software	autonomy

EU AI Act



- Aims to protect **health, safety** and **fundamental rights**
- Enable access to **EU single market** for AI products/services
- Part of New Legislative Framework for product health and safety harmonization across EU single market

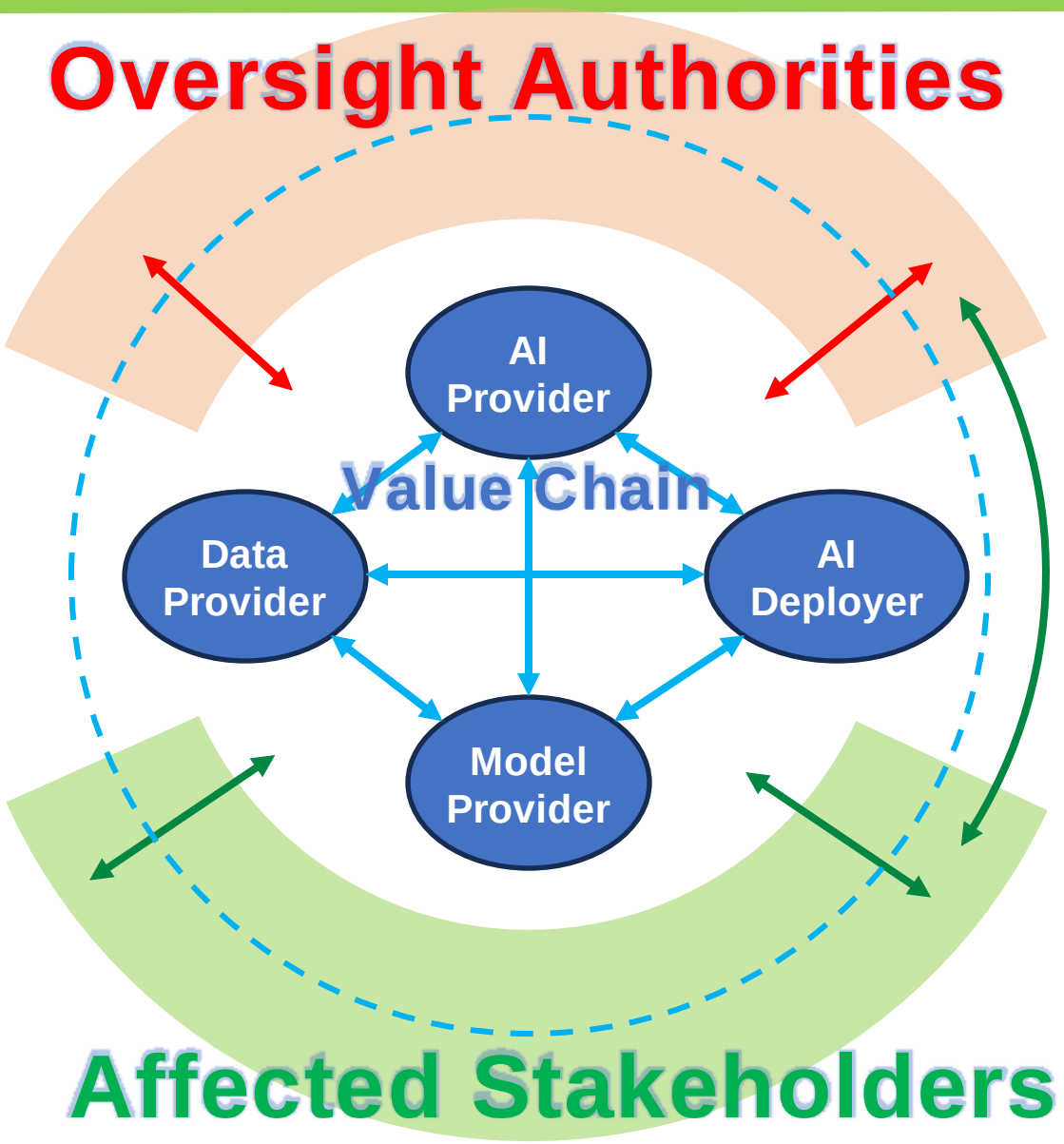
- A **Risk-based** approach to regulating AI
- Requires **product certification & surveillance** for high-risk AI system
- Separate direct regulation of **General Purpose AI Systems**

Impact/Risk Assessment : Three little words ….
“and fundamental rights"

- Reference to European Fundamental Rights
- Broad expansion in scope of EU product certification
- Requires understanding of legislation that protect these rights
- Introduces Legal Uncertainities
- A ‘Regulatory Turn’ in AI ethics?

https://commission.europa.eu/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en

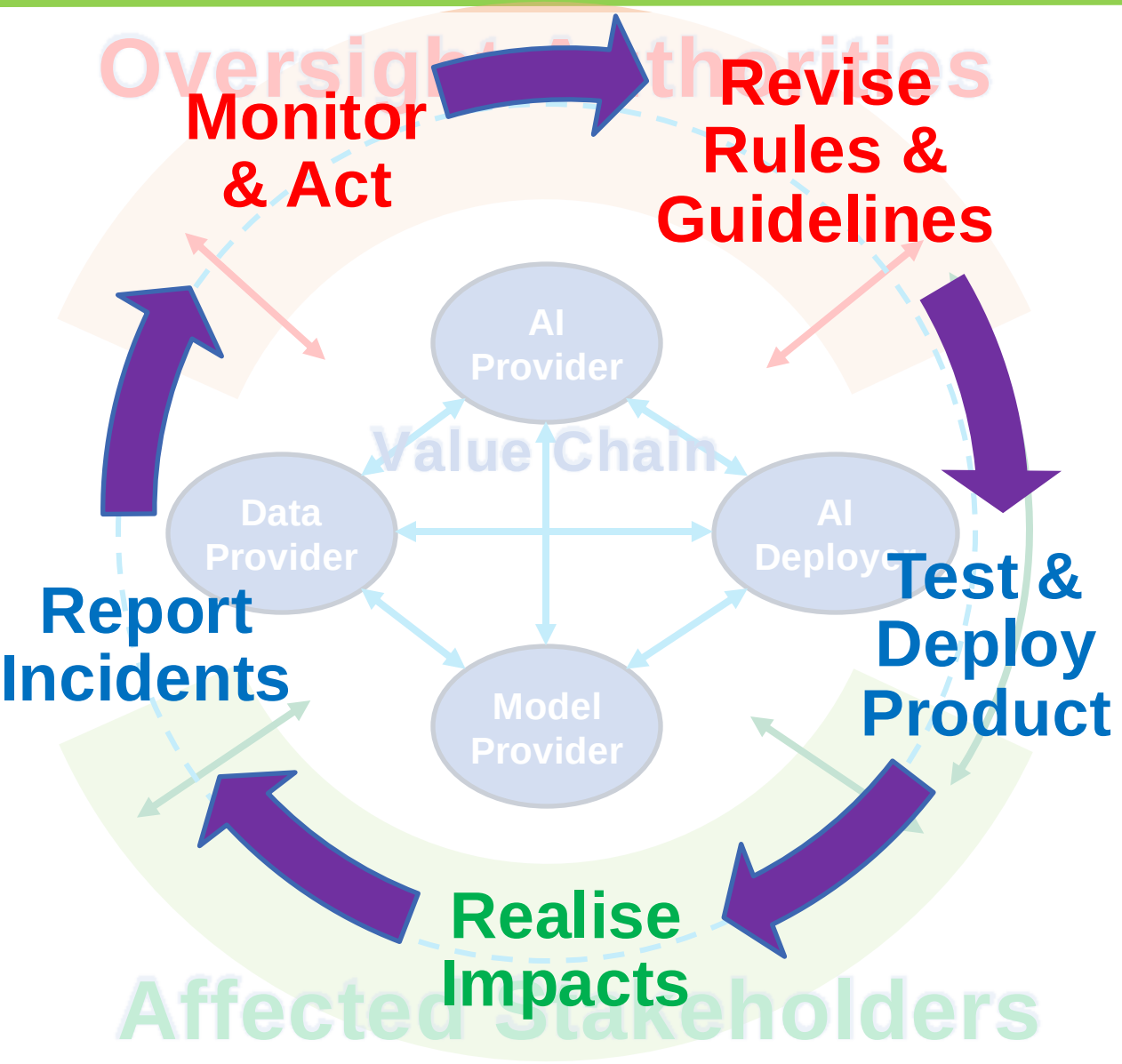
Types of Roles in the AI Act



AI Act is a Co-regulation Model

- Risk Management& Documentation Obligations on **AI value chain actors**
- Member States and EU appoint **Oversight Authorities**
- Some monitoring role for **Affected Stakeholders**: citizens and NGOs

AI Act as a Learning Loop



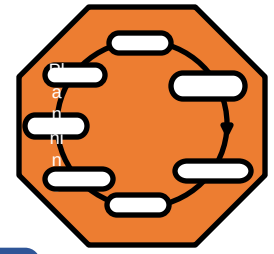
AI Act is a <u>Regulatory Learning Framework</u>

- Providers must assess and treat risks
- For severe risks with known treatments – external certification required
- Otherwise providers can self-certify
- If Risks materialize post-deployment, products can be removed, correctives demanded and fines levied
- Learning on new risks shared across market & authorities
- Regulator Leaning via **Sandboxes and Human Trials** accelerate learning and sharing knowledge on risks

AI Act: Requirements on High Risk AI System Providers

Determine if classified as High Risk

Ensure Design and Development are in compliance with Reg: risk management, data quality, transparency, traceability, auditability, robustness, accuracy, cybersecurity, human oversight



Quality Management System

Third Party or Internal Conformity assessment procedure

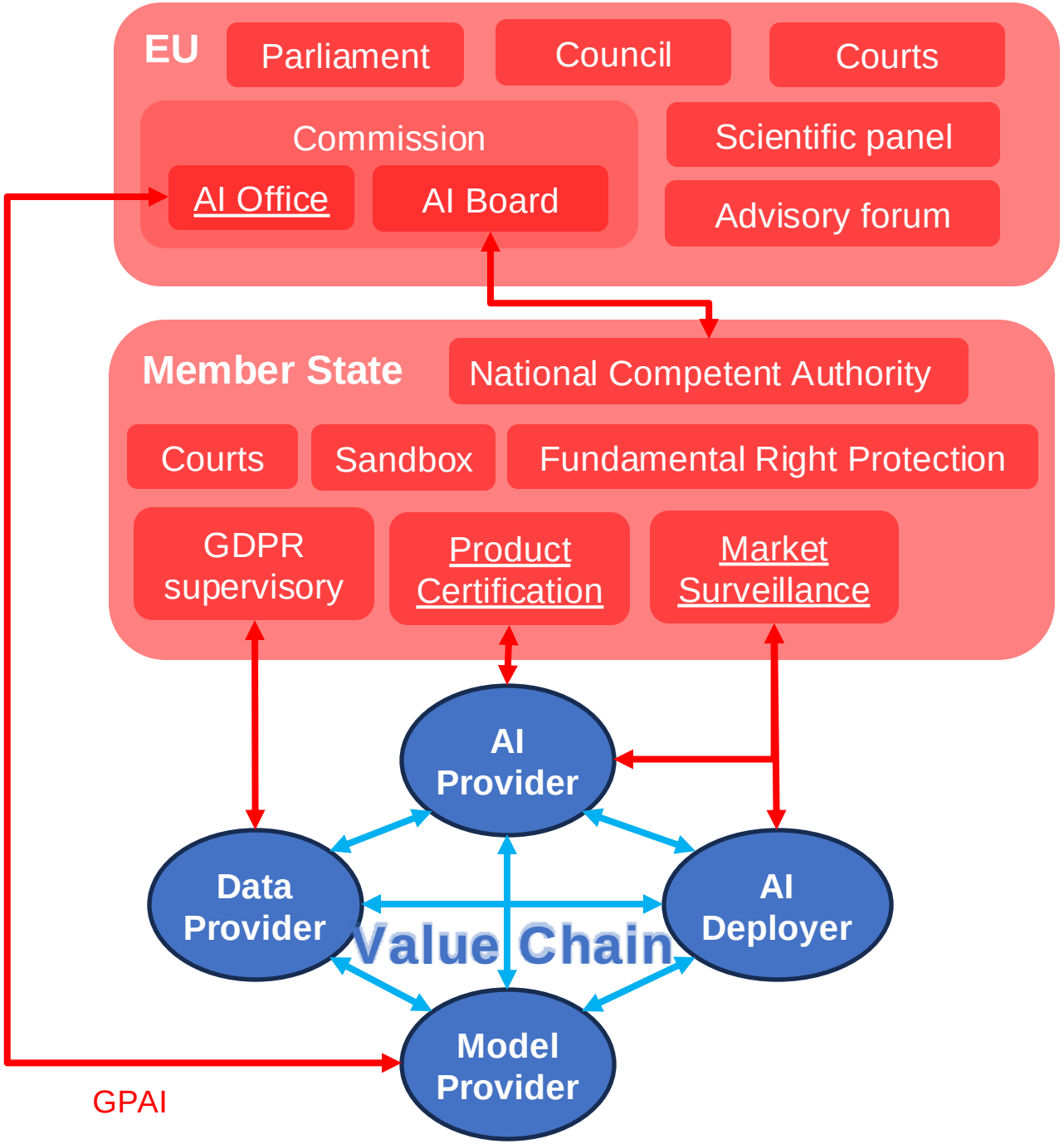
Affix CE mark

CE

Put on Market/into Service

Source: European Commission

Oversight Authorities



- Sectorial **product certification bodies**
- Sectorial **market surveillance authorities** in each Member State
- **AI Office** provides guidelines, coordination and GPAI oversight
- **European AI Board** representing **national competent authorities**
- Advisory forum and scientific panel
- Commission empowered to change certain AI system type definitions, derogations and documentation requirements

Complex network of authorities across sectors and member states –
Coordination and Knowledge Sharing are key to consistent enforcement

AI Act Annex II: AI areas already subject to Harmonised Legislation & Certification e.g. existing IE authorities

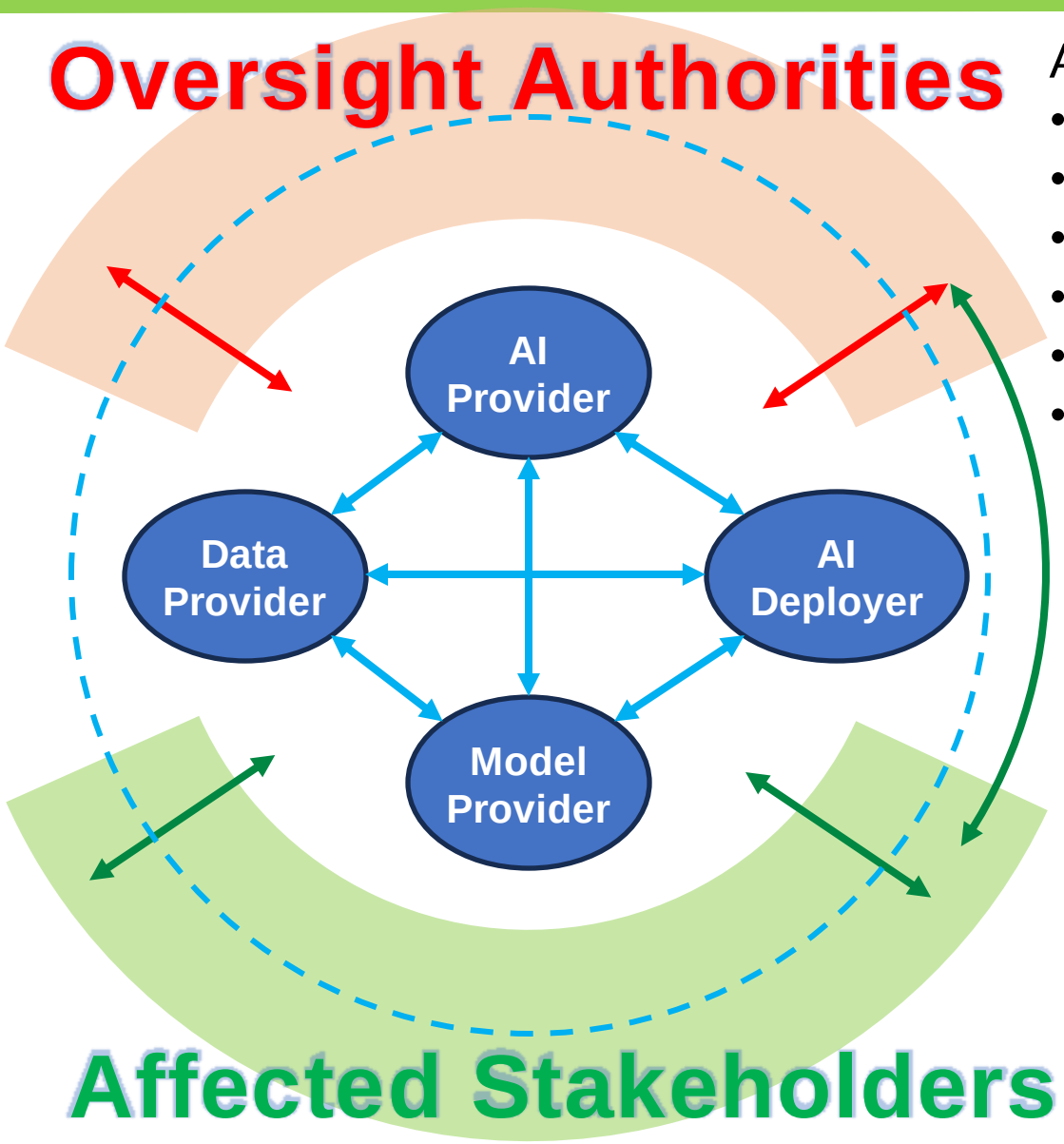
Area	Harmonised legislation	Responsible Irish Body
machinery	2006/42/EC	Health and Safety Authority
toys	2009/48/EC	Competition and Consumer Protection Commission
recreational/personal watercraft	2013/53/EU	Dept of Transport
lifts	2014/33/EU	Health and Safety Authority
explosive gasses	2014/34/EU	Health and Safety Authority
radio equipment harmonised legislation	2014/53/EU	ComReg
pressure equipment harmonised legislation	2014/68/EU	Health and Safety Authority
cableway installation harmonised legislation	2016/424	Commission for Railway Regulation
personal protective equipment harmonised legislation	2016/425	Health and Safety Authority & Competition and Consumer Protection Commission
burning gaseous fuels harmonised legislation	2016/426	Health and Safety Authority & Competition and Consumer Protection Commission
medical devices harmonised legislation	2017/745	Health Products Regulatory Authority
in vitro diagnostic medical devices harmonised legislation	2017/746	Health Products Regulatory Authority
civil aviation harmonised legislation	300/2008	Irish Aviation Authority
two- or three-wheel vehicles and quadricycles harmonised legislation	168/2013	Under consideration
agricultural and forestry vehicles harmonised legislation	167/2013	Minister for Agriculture, Food and the Marine
marine equipment harmonised legislation	2014/90	Department of Transport. Marine Survey Office
rail systems harmonised legislation	2016/797	Commission for Railway Regulation
motor vehicles and their trailers and components harmonised legislation	2018/858	Road Safety Authority of Ireland
civil aviation safety harmonised legislation	2018/1139	Irish Aviation Authority

High-risk AI System Types

High risk applications identified in Annex III:

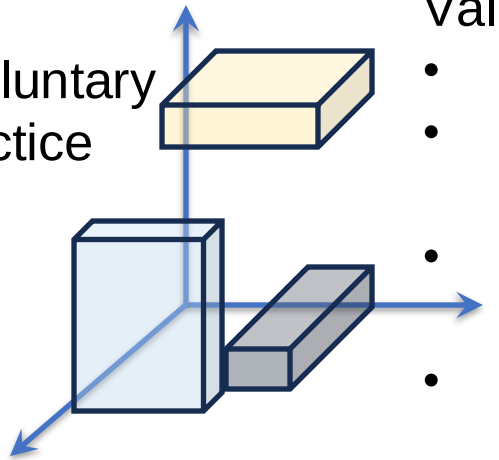
- Biometric identification and categorisation of natural persons (externally certified)
- Management and operation of critical infrastructure
- Education and vocational training
- Employment and workers management, access to self-employment
- Access to and enjoyment of essential private services and public services and benefits
- Law enforcement
- Migration, asylum and border control management
- Administration of justice and democratic processes

Mapping the Act's Regulatory Learning Space



AI System Types

- Prohibited
- Annex I
- Annex III
- Non-High Risk
- GPAI
- Subject to voluntary codes of practice



Areas of Protections

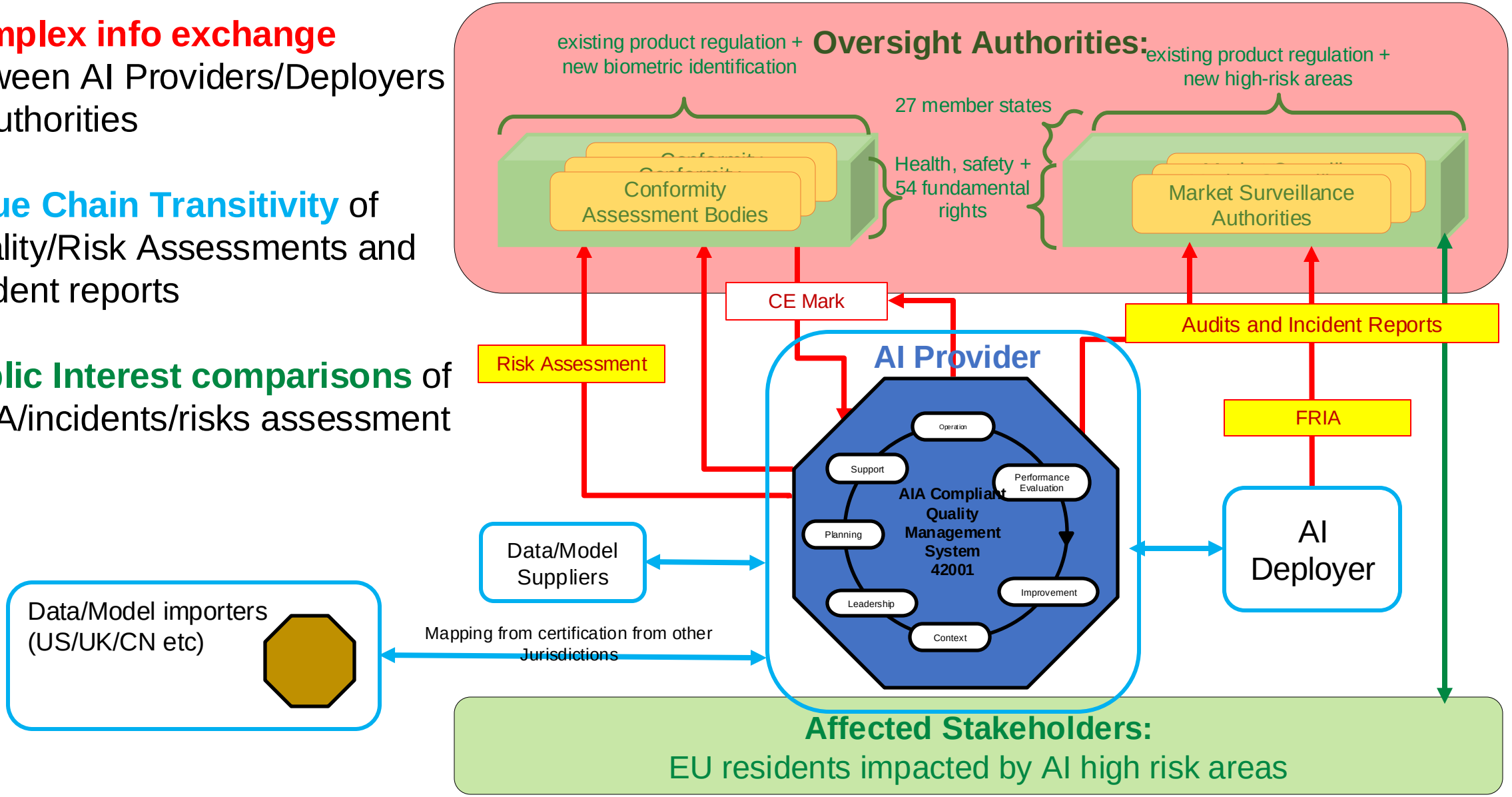
- Safety
- Health
- Fundamental Rights
- Democracy
- Environment

Value Chain Use Cases

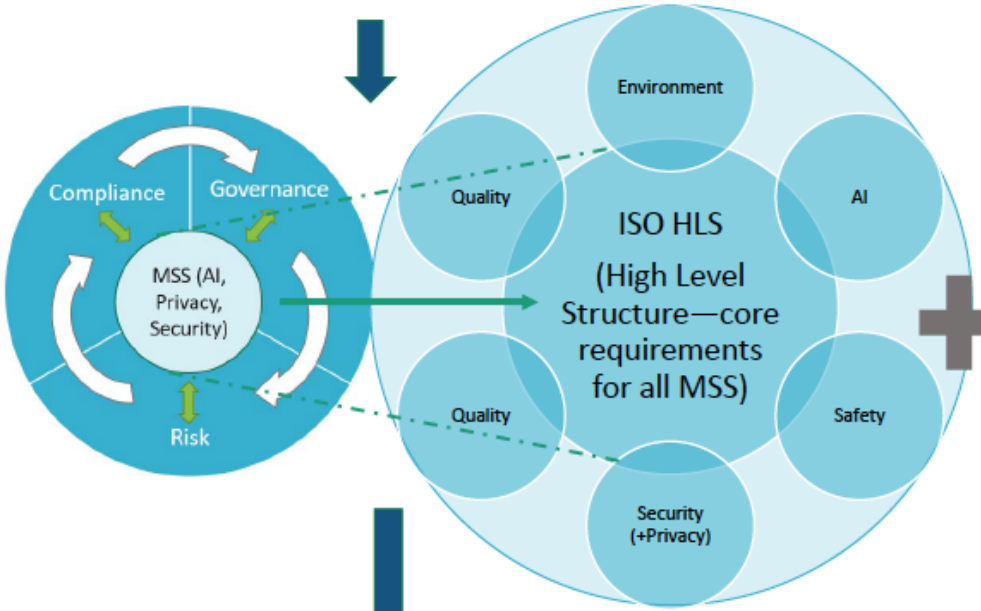
- Deployer FRIA
- HRAI Provider-Deployer
- Public Procurement of HRAI
- GPAI Provider-HRAI Provider
- GPAI Provider—HRAI Deployer
- HRAI Deployer Substantial Change
- Risk Materialisation/ Incident Reporting

Standardisation and Interoperability Challenges for the AI Act

- **Complex info exchange** between AI Providers/Deployers & Authorities
- **Value Chain Transitivity** of Quality/Risk Assessments and incident reports
- **Public Interest comparisons** of FRIA/incidents/risks assessment



Role of Standards in Product Certification: Presumption of Conformity



GRC Standards

Created by:
Standards Committees (e.g. SC42)

Used by:
Organizations globally

Certification/Accreditation Standards

Created by:
CASCO

17021 Requirements for certification bodies for MSS

17065 Requirements for certification bodies for products/services

Used by:
Accreditation bodies

Schemes

Created by:
Governments, regulatory bodies, certification bodies, industry, trade organizations, etc.

Certification Schemes

Used by:
Certification bodies

Certification

Issued by:
Accredited Certification Body

Certificate

Used by:
Organizations
For:
Customers, supply chain, regulatory compliance, competition

Standards and the AI Act

Requirement for European Standard https://ec.europa.eu/growth/tools-databases/enorm/mandate/593_en	Candidate SC42 standards
Risk Management Systems for AI systems	**ISO/IEC 23894** - Ai Risk Management
Governance and quality of datasets used to build AI systems	**ISO/IEC 5259** - Data quality for analytics and machine learning
Record keeping through logging capabilities by AI systems	ISO/IEC 24970 — AI system logging
Transparency and information provisions for users of AI systems	ISO/IEC DIS 12792 - Transparency taxonomy of AI systems
Human oversight of AI systems	ISO/IEC AWI 42105 - Guidance for human oversight of AI systems
Accuracy specifications for AI systems	ISO/IEC AWI TS 25223 - Guidance and requirements for uncertainty quantification in AI systems & ISO/IEC AWI 23282 - Evaluation methods for accurate NLP systems
Robustness specifications for AI systems	ISO/IEC TR 24029 Assessment of the robustness of neural networks
Cybersecurity specifications for AI systems	ETSI
Quality management systems for providers of AI systems, including post-market monitoring processes	**ISO/IEC 42001** AI management system & **ISO/IEC 27001:2013** Information security management systems
Conformity assessment for AI systems	**ISO/IEC DIS 42006** - Requirements for bodies providing audit and certification of AI management systems

- EC Request for Harmonized Standards from ESO
- Compliance by Providers conveys presumption of conformity
- But Provider would remain responsible for satisfying Act requirement and harmonized standard remain under review
- If unsuccessful, EC can define Common Specifications
- Preference to use existing international standards (e.g. SC42 - but these cannot address national legal requirements)

https://publications.jrc.ec.europa.eu/repository/handle/JRC132833

AI Act Interoperability Challenges & Sem Web

Interoperability Challenges	Semantic Web Benefits	
AI Act is a Learning Framework	Provisional, extensible, progressively specific semantic vocabularies	Mappable & comparable Parallel development through name spaces
SC42 Standards focus on process vs info exchange	Semantic mapping from Act and standards concepts	Serialisation and Web API integration
Complex value chains	Upper layer models for flexible semantic interoperability with permissionless innovation	Serialisation, API and access control
Need for broad stakeholder engagement	Open access availability, especially for SME, NGO, public sector	Open tools for queries, constraints, rules, catalogues & user interfaces

Experiences: Open Legal Compliance Vocabularies – Community driven, EU aligned

Input

- Open data for GDPR compliance
- Open provenance, queries, constraints

Output

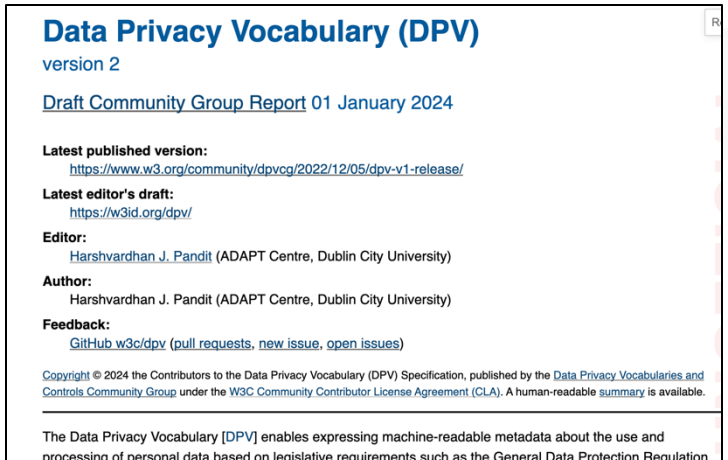
- Semantic GDPR models - Legal Text, Consent & Provenance
- Series of Publications

Outcomes

- W3C Data Privacy Vocab
- EU Legal Data prize
- EU Pub Office Engagement
- IE and EU funding

Impact

- International leadership – open data privacy vocabulary
- Industrial DPV adoption
- Consent Receipt ISO/IEC TS 27560



Data Privacy Vocabulary (DPV)

version 2

Draft Community Group Report 01 January 2024

Latest published version:
https://www.w3.org/community/dpvcg/2022/12/05/dpv-v1-release/

Latest editor's draft:
https://w3id.org/dpv/

Editor:
Harshvardhan J. Pandit (ADAPT Centre, Dublin City University)

Author:
Harshvardhan J. Pandit (ADAPT Centre, Dublin City University)

Feedback:
GitHub w3c/dpv (pull requests, new issue, open issues)

The Data Privacy Vocabulary [DPV] enables expressing machine-readable metadata about the use and processing of personal data based on legislative requirements such as the General Data Protection Regulation

https://w3id.org/dpv/

Protect ITN

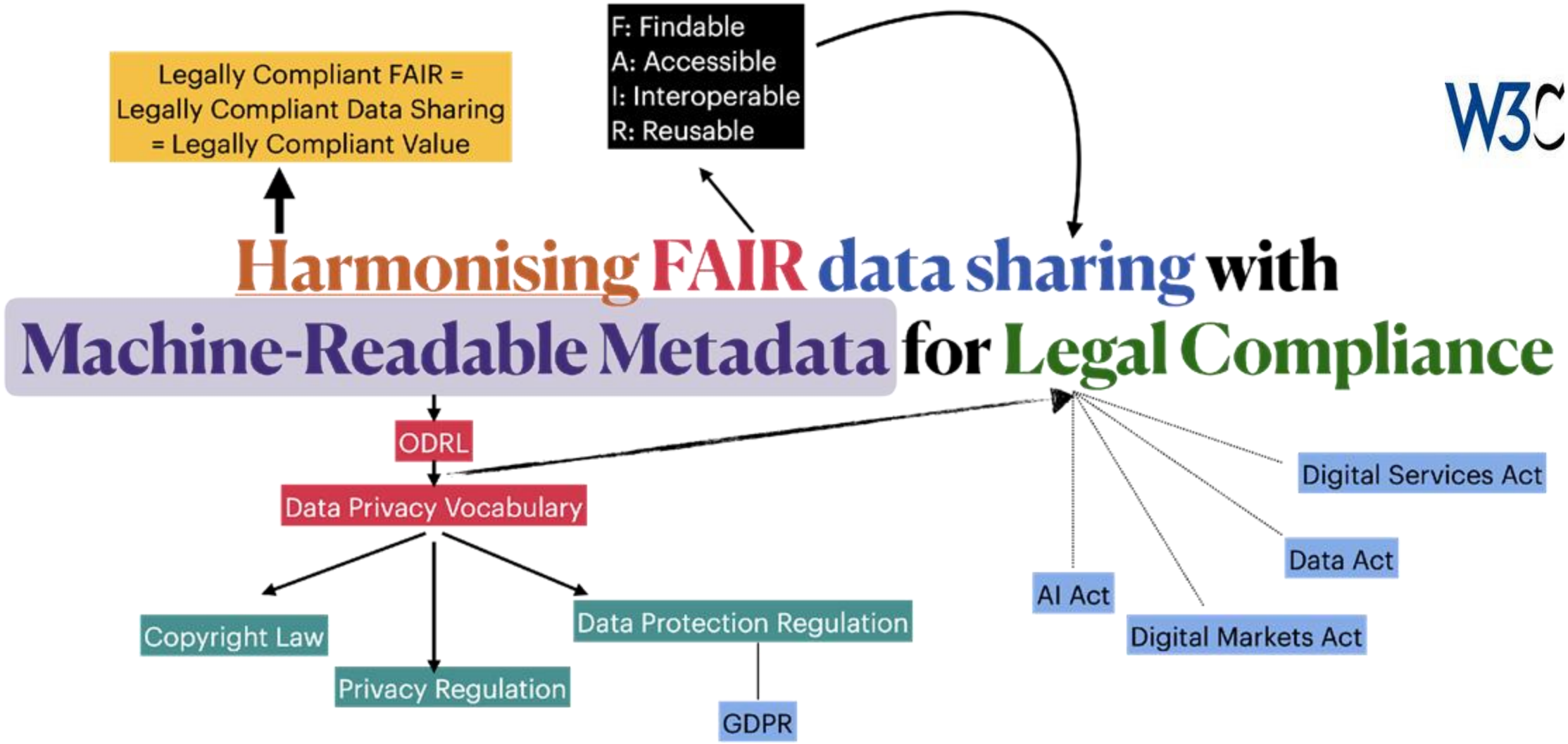
NGI TRUST

IRISH RESEARCH COUNCIL
An Chomhairle um Thaighde in Éirinn

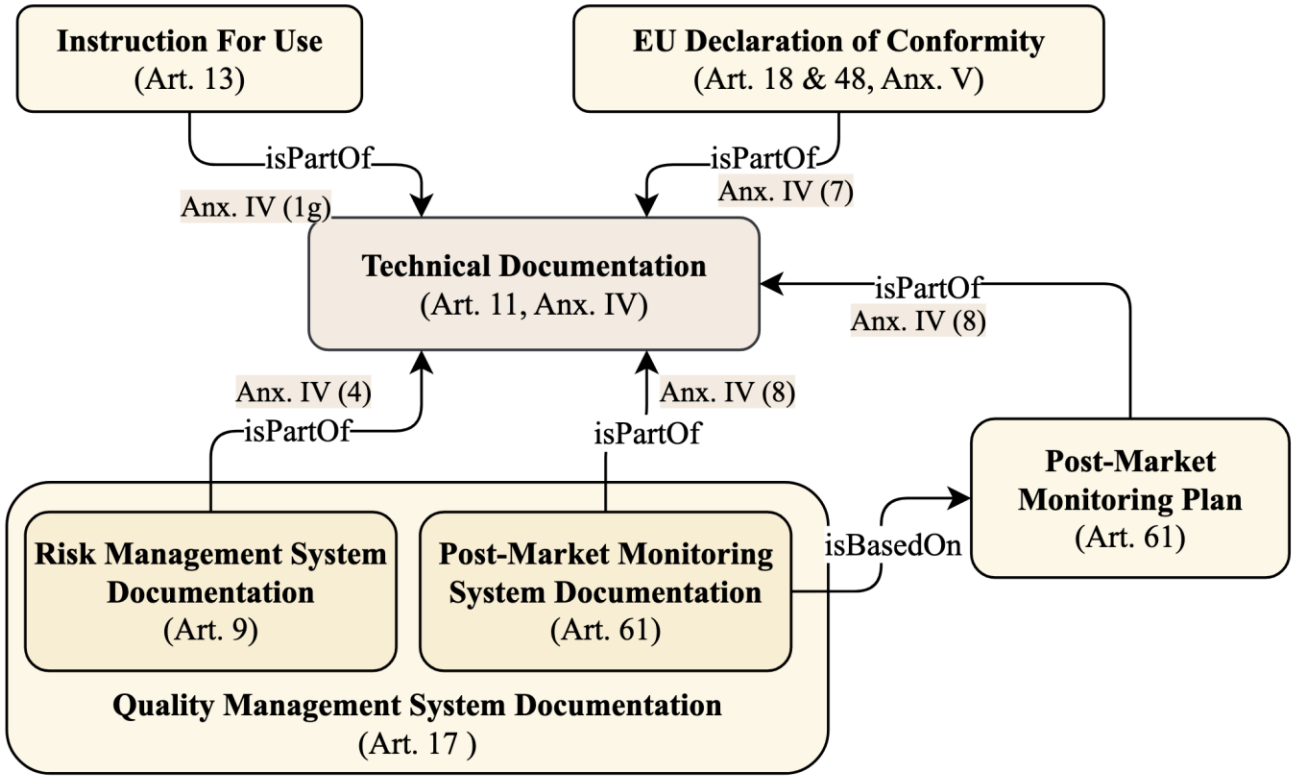
Focus:

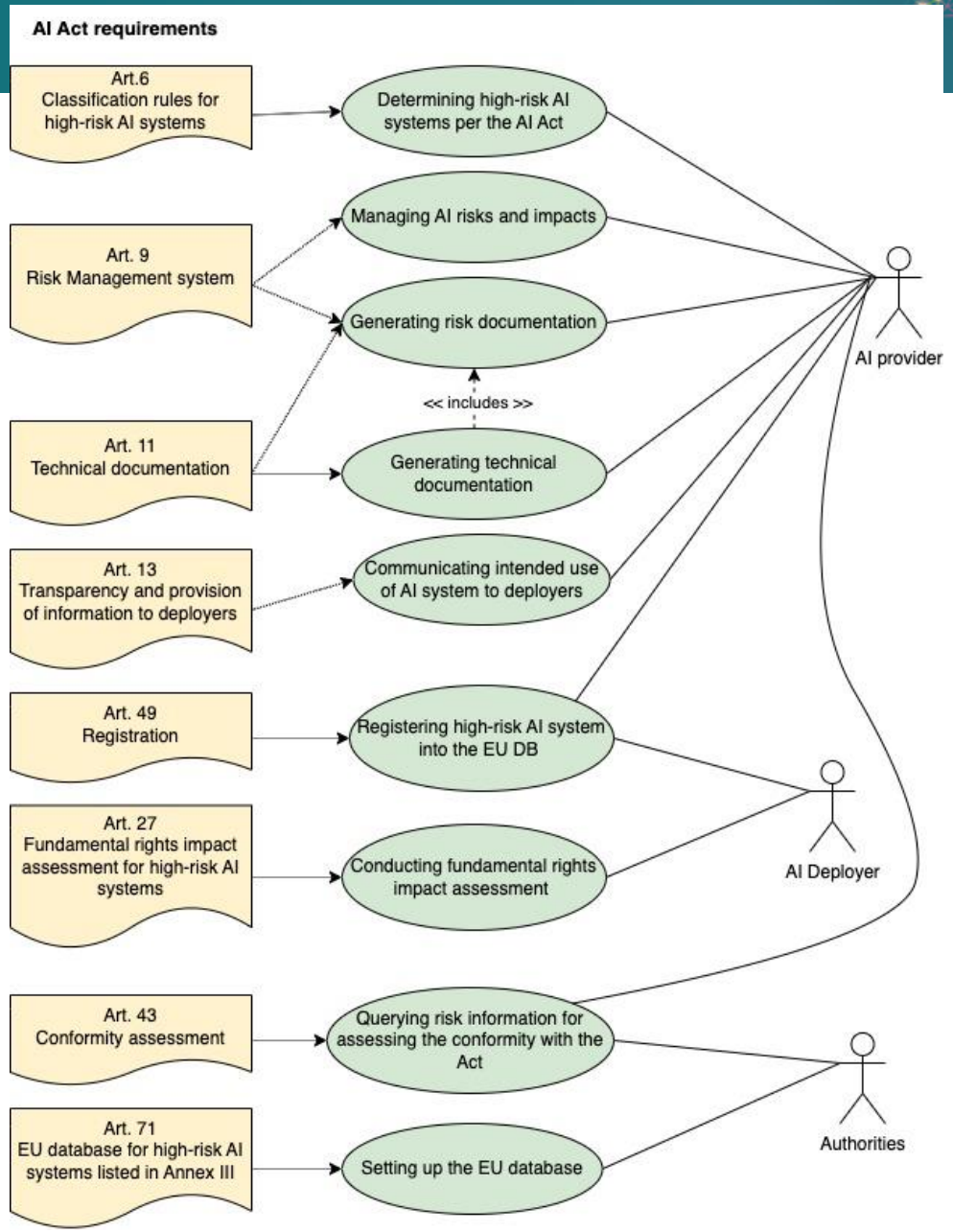
- Informal, multi-stakeholder
- Deep legal compliance knowledge
- Open access, machine readable specs

Creating “Scalable Compliance” upon Machine Readable Metadata

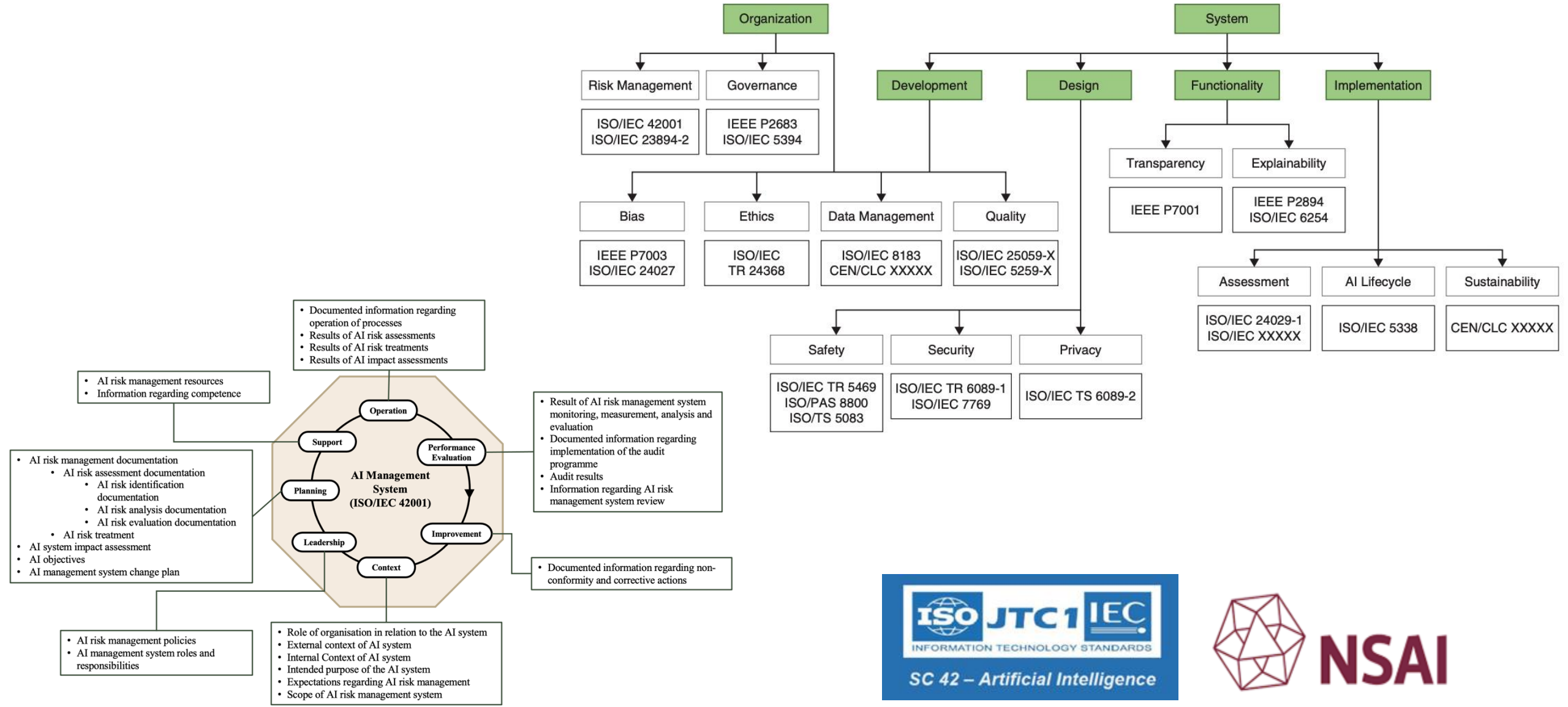


AI Act: Risk Management and Documentation Use Cases





Harmonised Standards for Technical Requirements

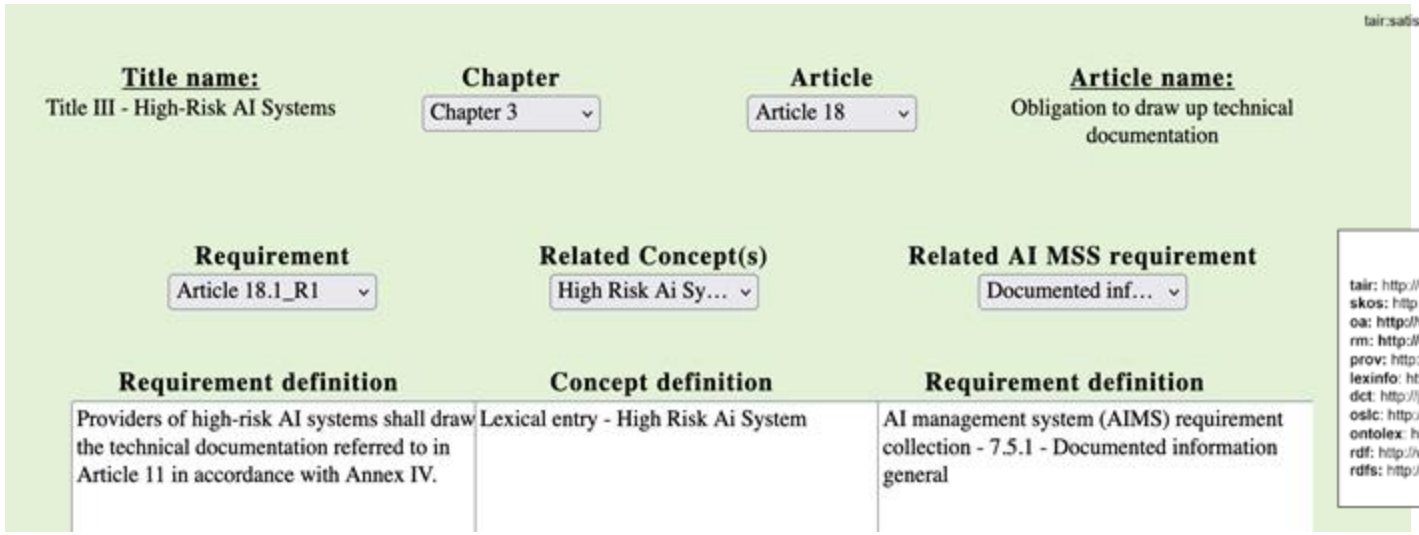


ISO JTC 1 IEC
INFORMATION TECHNOLOGY STANDARDS
SC 42 – Artificial Intelligence

NSAI

Mapping AI Act Requirements to AIMS Requirements

- TAIR demo: The demo explores the Title III of the Draft AI Act mapped to High-Risk AI System requirements (ISO 42001)



Title name: Title III - High-Risk AI Systems

Chapter Chapter 3

Article Article 18

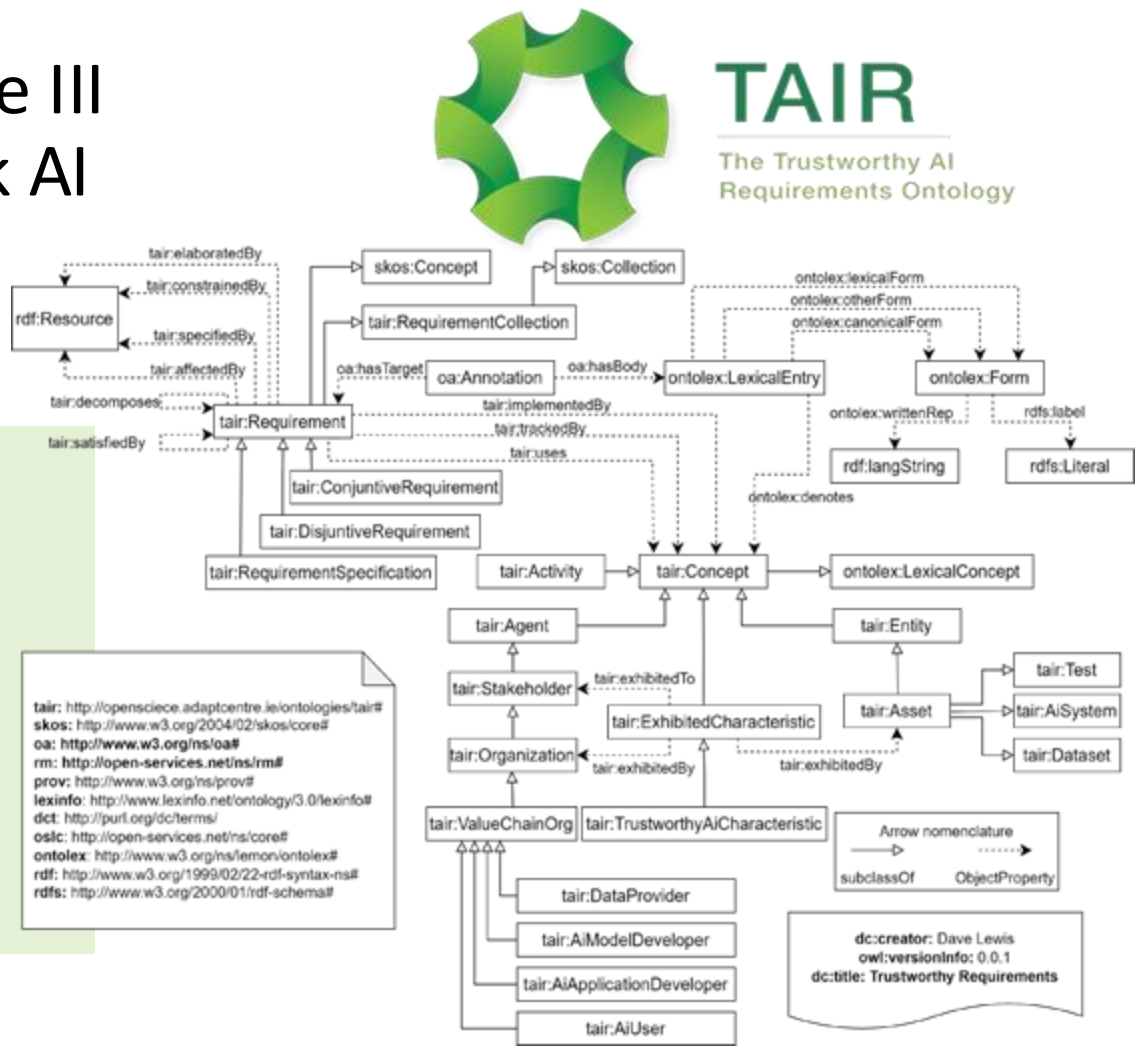
Article name: Obligation to draw up technical documentation

Requirement Article 18.1_R1

Related Concept(s) High Risk Ai Sy…

Related AI MSS requirement Documented inf…

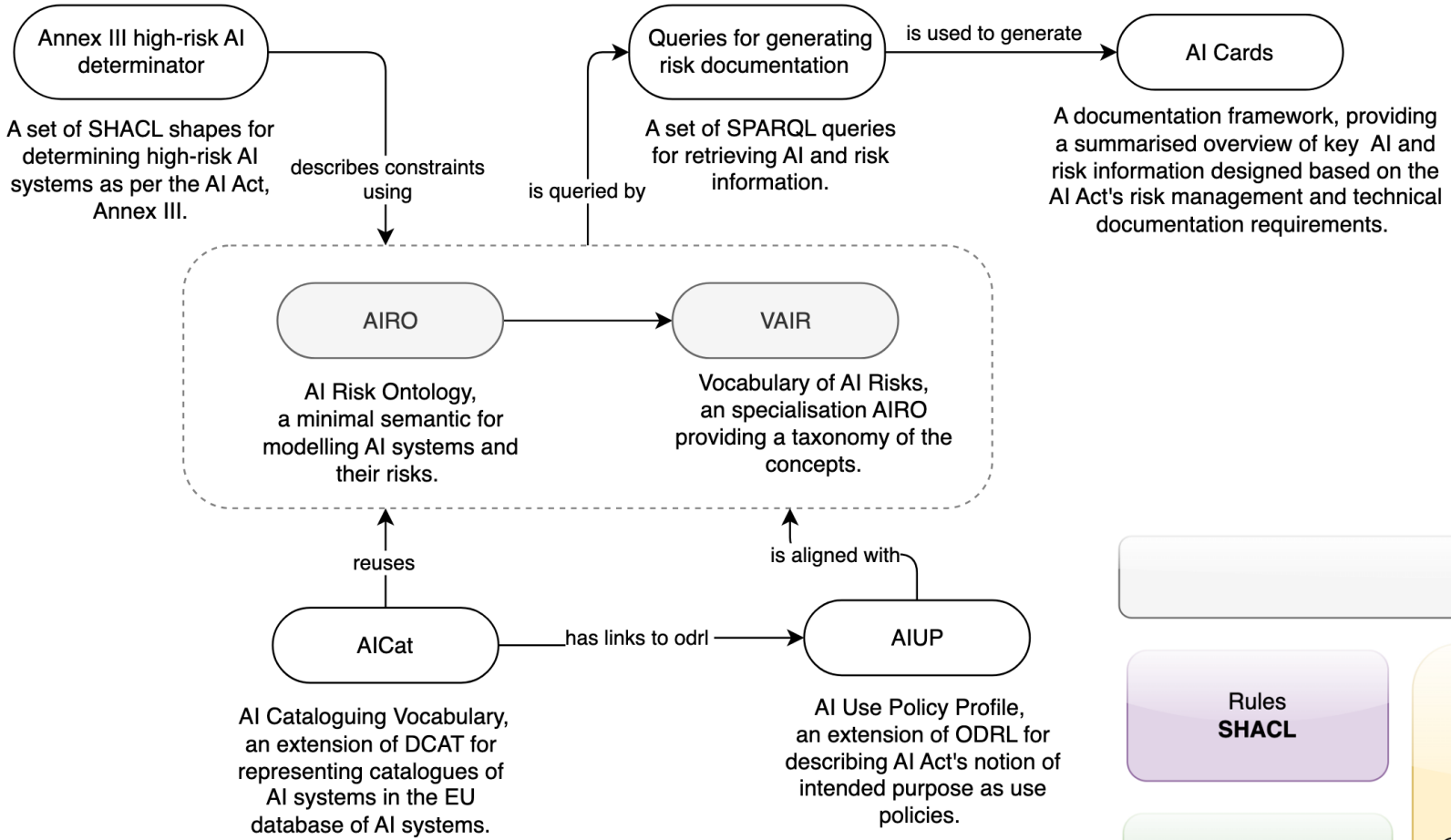
Requirement definition	Concept definition	Requirement definition
Providers of high-risk AI systems shall draw the technical documentation referred to in Article 11 in accordance with Annex IV.	Lexical entry - High Risk Ai System	AI management system (AIMS) requirement collection - 7.5.1 - Documented information general

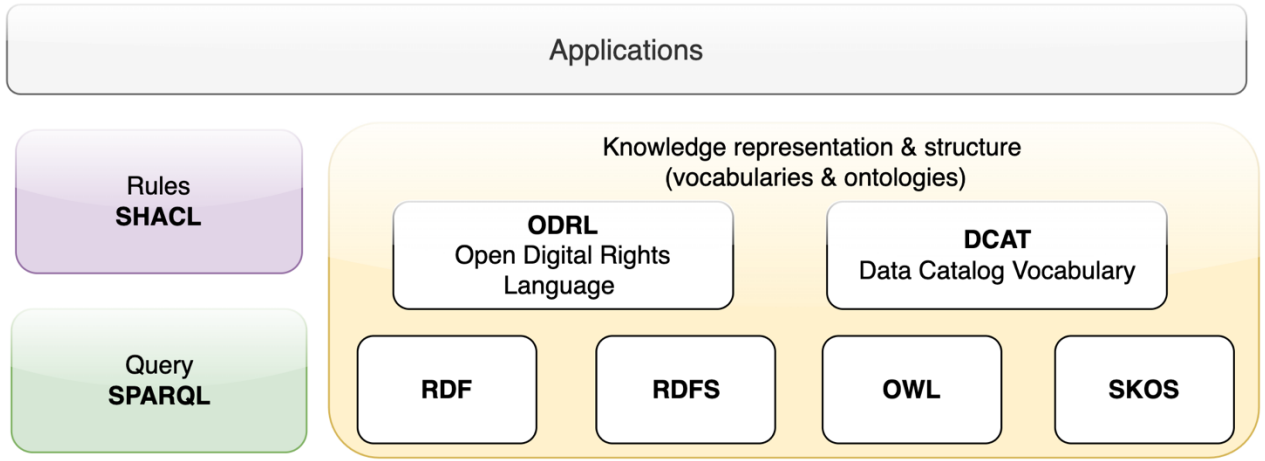


https://tair.adaptcentre.ie

This project has received funding as a research gift from Meta and is supported by the Science Foundation Ireland under Grant Agreement No 13/RC/2106_P2 at the ADAPT SFI Research Centre and the European Union's Horizon 2020 Marie Skłodowska-Curie grant agreement No 813497 for the PROTECT ITN.

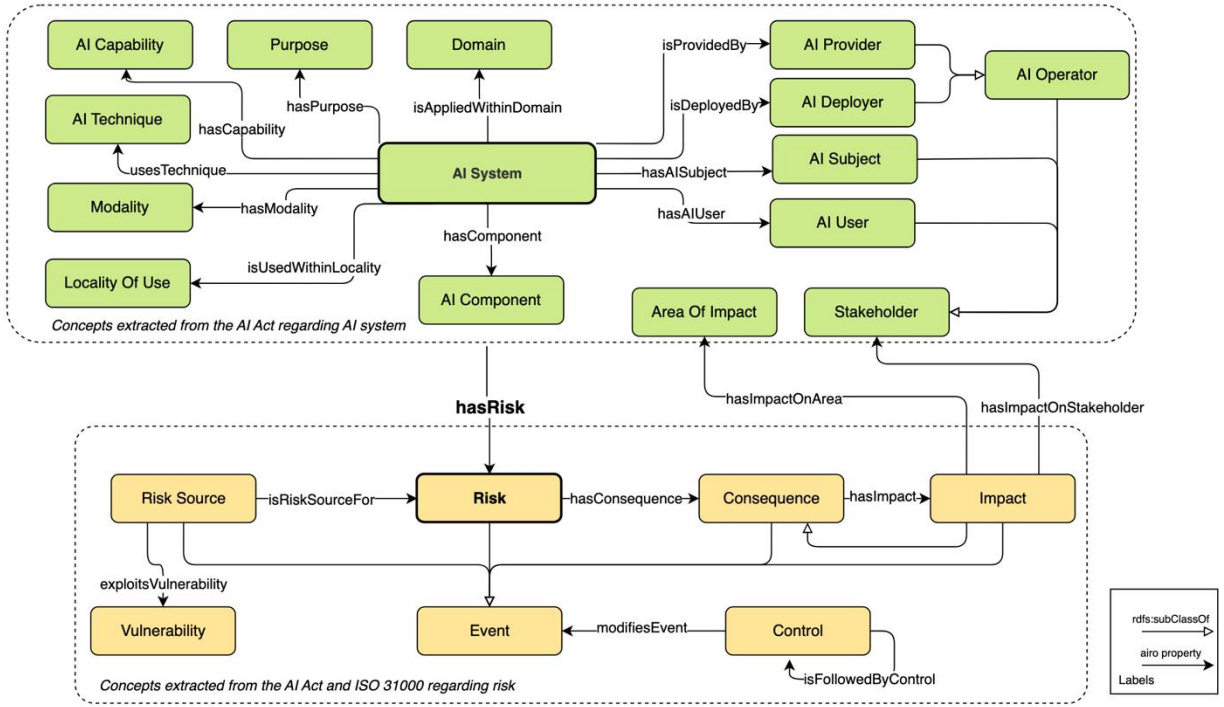
Semantic Web Framework for AI Act Risk Management & Documentation

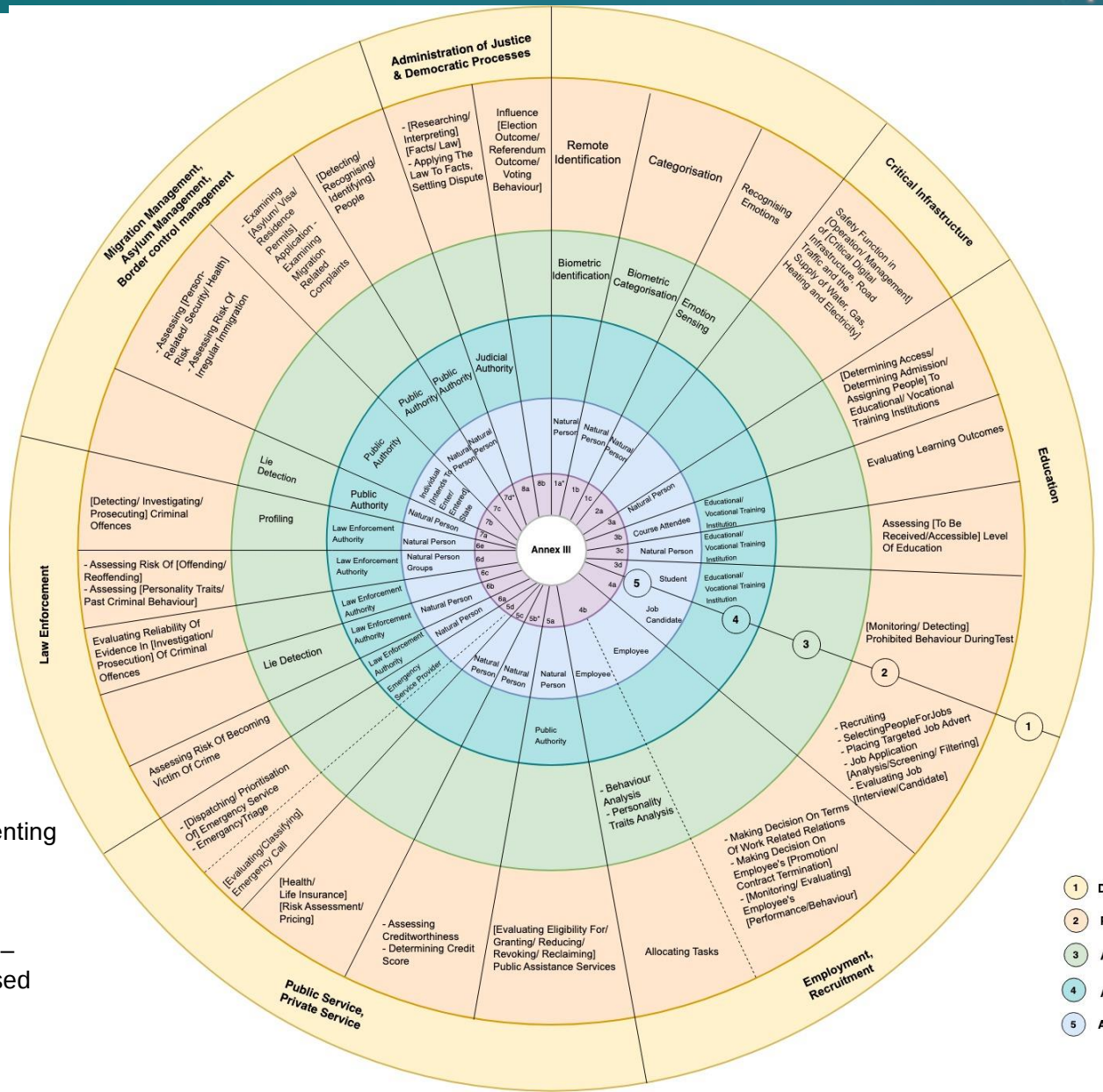




https://regtech.adaptcentre.ie

AI Risk Ontology & Vocabulary for AI Risk

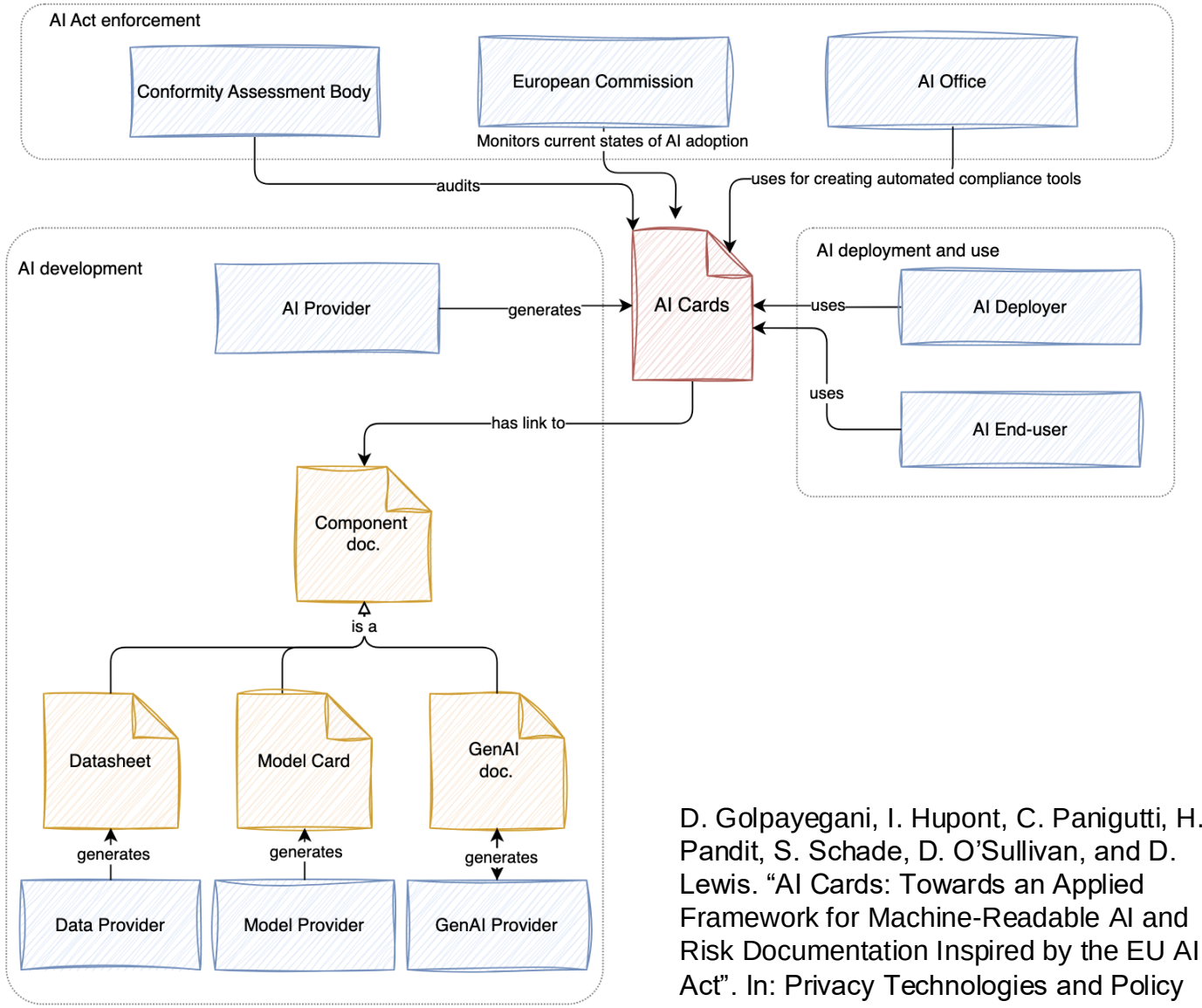




Delaram Golpayegani, Harshvardhan J. Pandit, and Dave Lewis. “AIRO: An ontology for representing AI risks based on the proposed EU AI Act and ISO risk management standards”. In: Towards a Knowledge-Aware AI. Vol. 55. IOS Press. 2022, pp. 51–65.

Delaram Golpayegani, Harshvardhan J Pandit, and Dave Lewis. “To Be High-Risk, or Not To Be–Semantic Specifications and Implications of the AI Act’s High-Risk AI Applications and Harmonised Standards”. In: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency. 2023, pp. 905–915

AI Card: Lightweight AI Act Documentation



D. Golpayegani, I. Hupont, C. Panigutti, H.J. Pandit, S. Schade, D. O'Sullivan, and D. Lewis. "AI Cards: Towards an Applied Framework for Machine-Readable AI and Risk Documentation Inspired by the EU AI Act". In: Privacy Technologies and Policy

AI Cards: Proctify

https://raw.githubusercontent.com/DelaramGlp/airo/main/usecase/proctify.ttl

Card's Version	1.2.3
Card's Date (Issued)	2024-04-23
Card's Language	Eng
Card's Publisher	AIEduX
Contact Info	proctify@aiedux.org

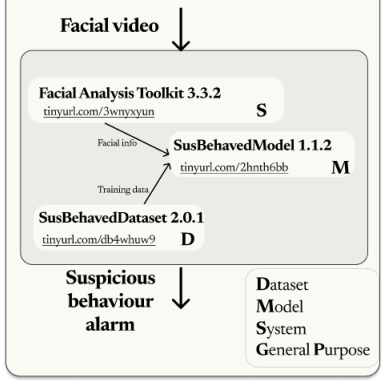
1. General Information

Version: 1.2
Modality: Software
AI Technique(s): ML>>ANN>>Deep learning
Provider(s): AIEduX
Developer(s): AIEduX

2. Intended Use

Domain: Education
Purpose: Detecting suspicious behaviour during online exam
Capability: Facial behaviour analysis, video analysis
Deployer: University within EU
AI Subject: Students

3. Key Components



4. Data Processing

	SusBehaved	Input data
Personal	✓	✓
Category	Facial>>Biometrics	Facial>>Biometrics
DPIA	✓	✗
Non-Personal	✓	✓
Anonymised	✓	✗
Licenced	✓	✗

5. Human Involvement

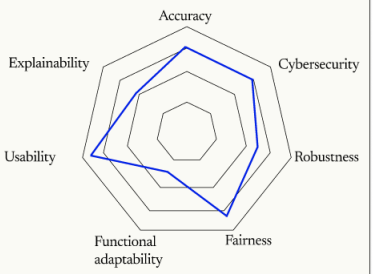
Level of Automation: Partial automation
Human Involvement: Human decision

	Intended	Active	Informed	Control
Student	✓	✓	✓	ex-post challenge
Occupant (of the room)	✗	✗	✗	No opt-out
Instructor	✓	✓	✓	No opt-out

6. Risk Profile

Impact on ↓	Risk			Measures					
	Likeli.	Severity	Residual	Org.	Tech.	Monit.	Secur.	Transp.	Log.
Health & Safety	Med.	V. High	Low	✓	✓	✓	✗	✓	✗
Fundamental Rights	High	V. High	Low	✓	✓	✓	✓	✓	✓
Society	Low	Med.	Med.	✓	✓	✓	✗	✓	✗
Environment	Low	Low	Low	✓	✗	✗	✗	✗	✗

7. Quality



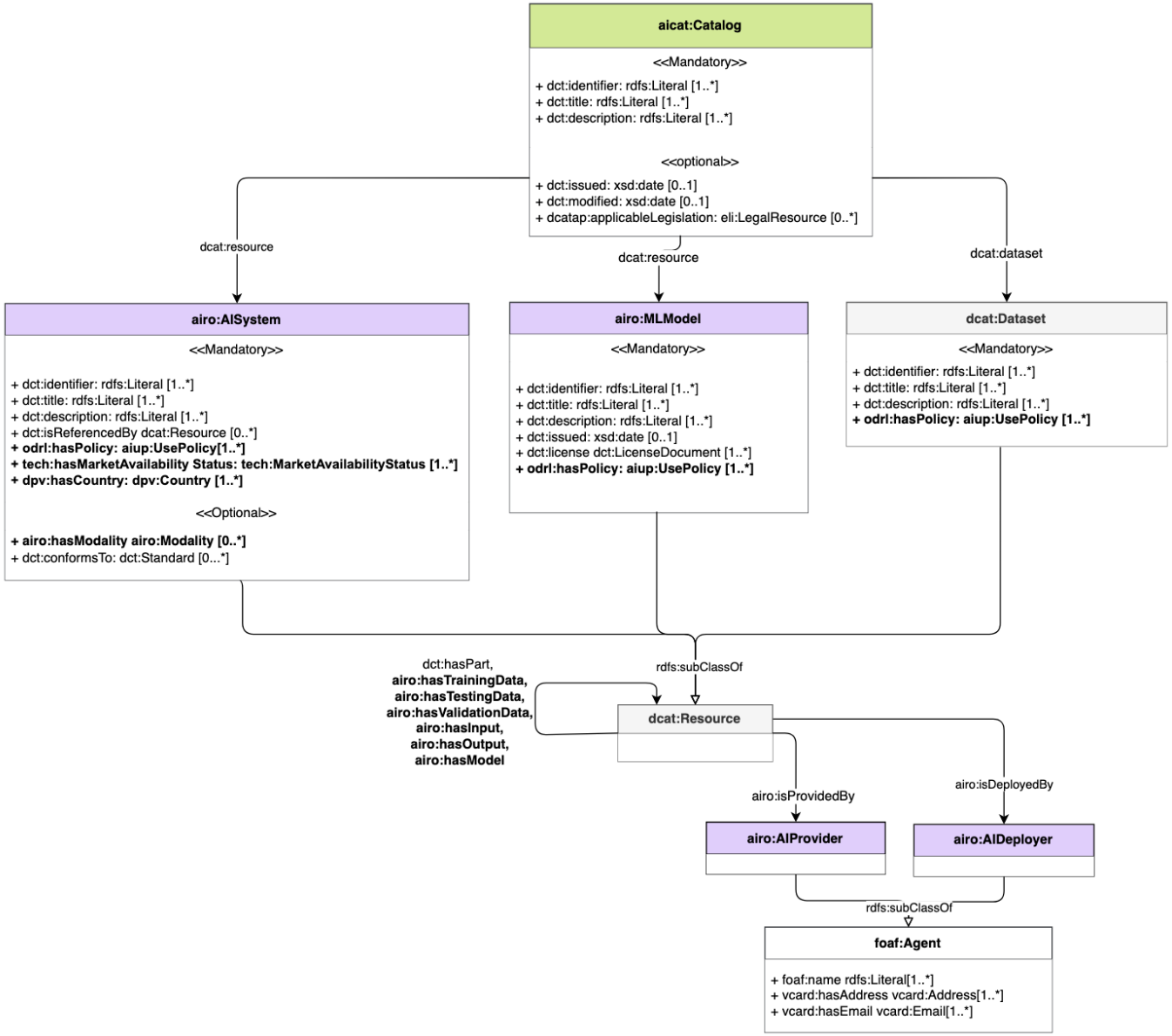
8. Pre-determined Changes

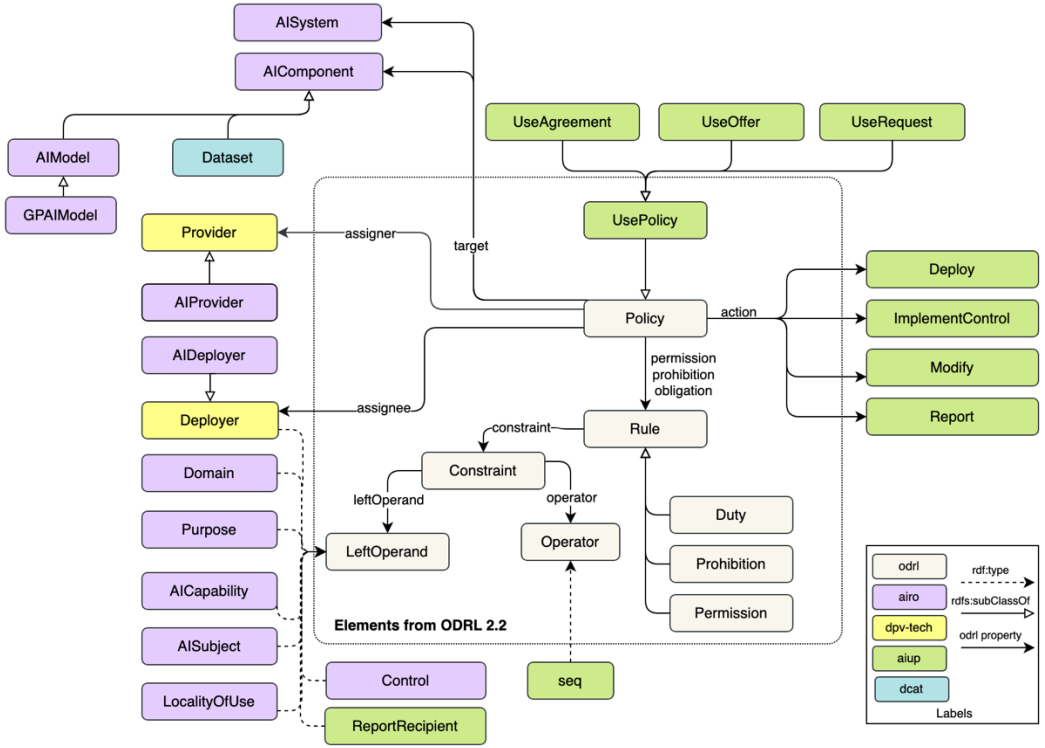
	frequency	Impact on ↓ Performance	Risks
Susbehaved model	2 Month	✓	✗
Mitigation measures	2 Week	✗	✓

9. Regulations & Certification

Regulations	[EU, GDPR & AI Act, self-assess] [IE, DPA, self-assess]
Standards	[ISO/IEC 27001:2022]
Codes of conduct	[EU, use of AI and data in teaching and learning for educators]

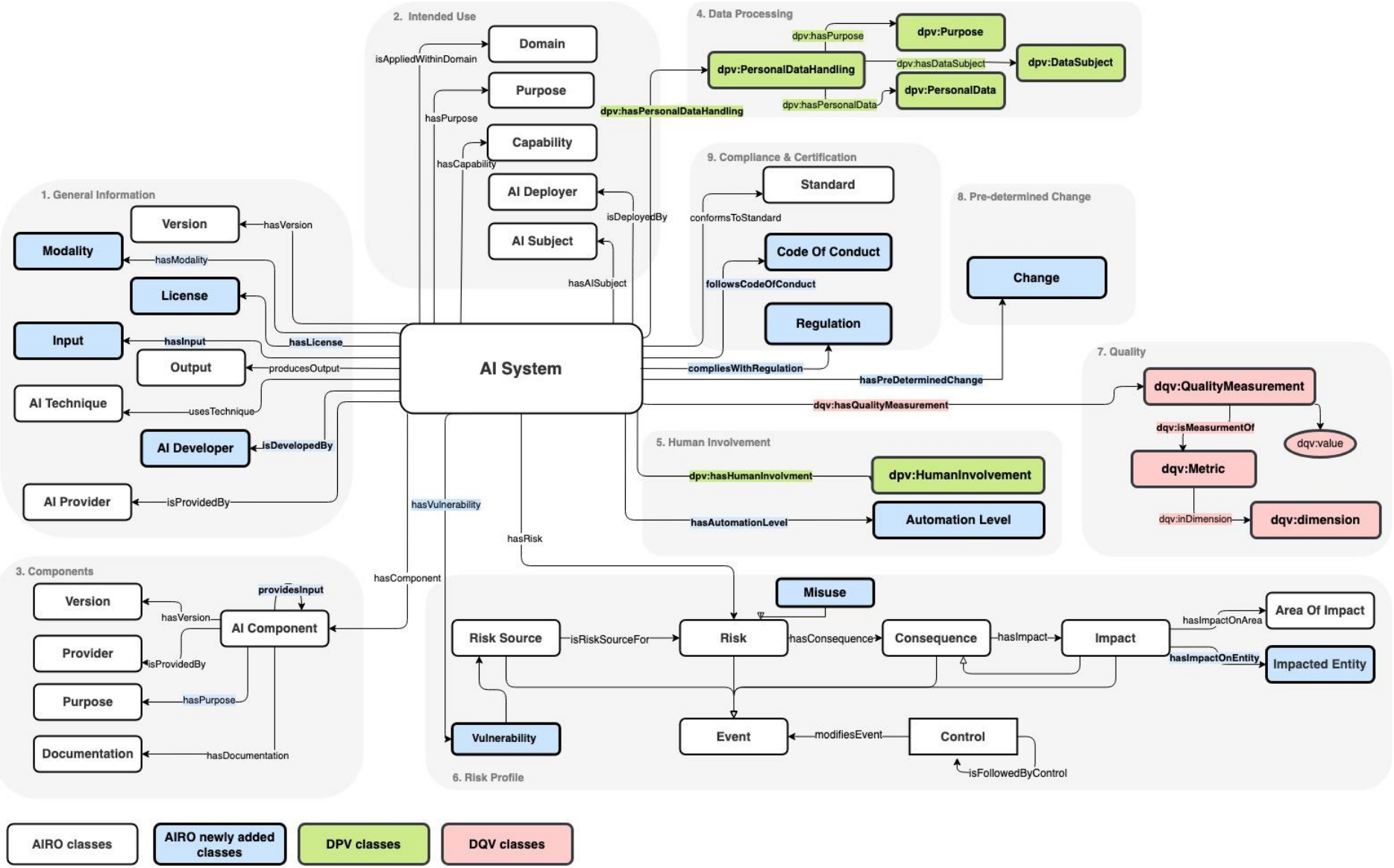
AI System Catalogues and Usage Policies: DCAT and ODRL





AIUP: an ODRL Profile for Expressing AI Use Policies to Support the EU AI Act", Delaram Golpayegani, Beatriz Esteves, Harshvardhan J. Pandit, and Dave Lewis, SEMANTiCS 2024

AI Semantic Model Extensibility



Conclusions

- AI systems are now *regulated* in the EU
- New risks management and documentation *obligations on AI Providers*
- Requires lots of complex, multi-party *information exchange*
- Many legal uncertainties, lots of *regulatory learning* needed – a *'regulatory turn'* in AI Ethics
- *Multistakeholder engagement* must represent citizen views on fundamental rights impact: reporting and redress, public observatories, incidents logs, legitimized regulatory learning
- Semantic Web Technologies offer *FAIR, open, extensible, decentralized* models for AI Risk and Documentation
- *Standardized tools* for regulatory info automation support for scaleable compliance