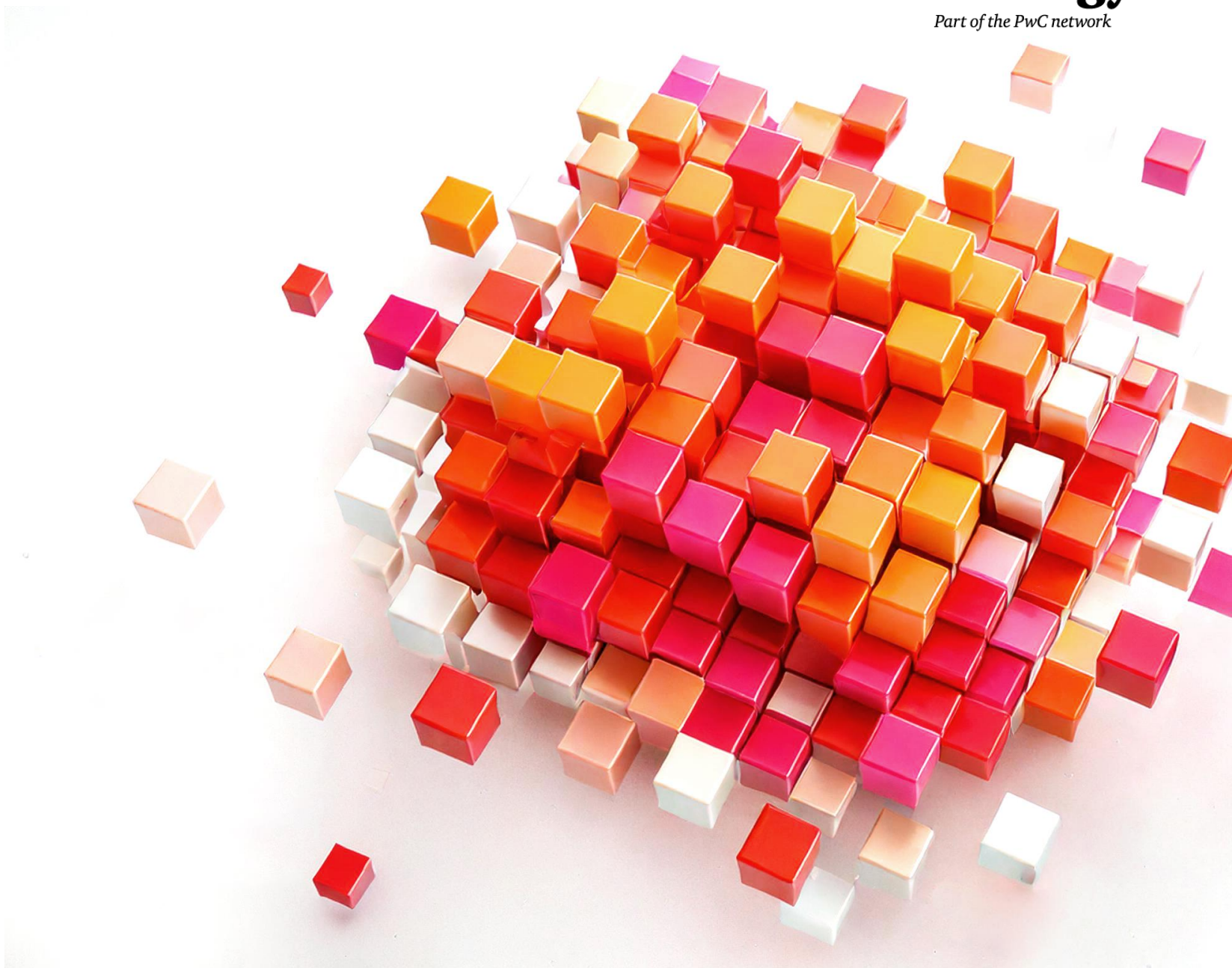
Data Day 2025

strategy&
Part of the PwC network

Harnessing the EU AI Act

How to boost innovation through effective AI Governance?



pwc

AI Governance

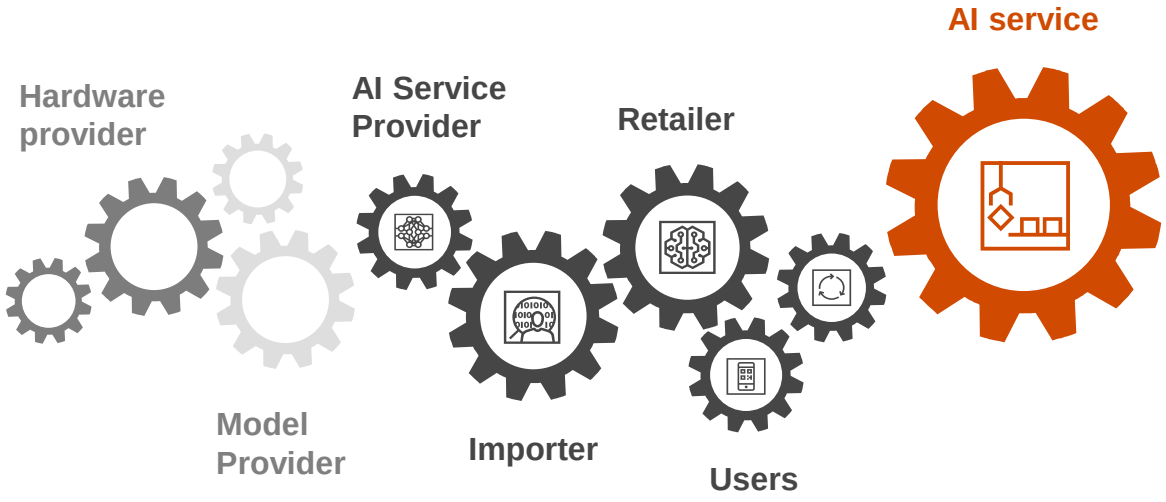
- Regulatory
- Transparency
- Risk
- Accountability
- Guiding Principles

The EU AI Act will have to be implemented from 2025 and imposes drastic penalties for non-compliance

Timeline

Aug 2024	**Entry into force**
Feb 2025	**Prohibited AI systems** **6 months** after entry into force
May 2025	**Codes of Practice** **9 months** after entry into force
Aug 2025	**Sanctions come into force** **12 months** after entry into force
Aug 2025	**GPAI Regulation** **12 months** (24 months if already on the market)
Aug 2026	**All other aspects of the EU AI Act (e.g. high risk)** **24 months** after entry into force
Aug 2027	**Product-based AI systems with high risk** **36 months** after entry into force

It's time to optimize your AI governance!



Conformity assessment along the entire AI value chain

The fines for non-compliance with the regulations amount to up to EUR 40 million or 7% of annual turnover.

The EU AI Act sets specific requirements based on an AI System's risk potential and the organization's role

EU AI Act

1 Scope

AI-Systems	Territory	Application state
Regulation applies to AI systems, defined according to article 3(1).	It addresses AI-systems in the Union, also if those providers are established or located in a third country.	The AI-system shall be placed on the market or put into service (for own use) (not AI focused R&D, testing or development)

2 Risk classification of AI

Prohibited systems	High risk	General Purpose AI	Transparency obligations

3 Roles within the AI value chain

Provider	GPAI Provider	Authorized representative	Deployer	Distributor	Importer

4 Range

Organization	Lifecycle	Conformity

5 Requirements

6 Guidelines

The EU AI Act addresses four risk classes which are associated with specific requirements

EU AI Act

Prohibited

Definition: AI systems with unacceptable risks are generally prohibited. These include systems for the subliminal manipulation of people, certain real-time biometric recognition systems in public spaces and systems that make assessments of natural persons based on their social behavior.

Requirements: No specific requirements needed

High risk

Definition: AI systems that are associated with a particularly high-risk potential due to their use in critical infrastructures, law enforcement or healthcare. High-risk AI systems can significantly affect people's rights, safety and well-being.

Requirements:

- Risk management system
- Data governance
- Technical documentation
- Record keeping
- Transparency obligations
- Human oversight
- Accuracy, robustness and cybersecurity

GPAI

Definition: Designed to optimize generality and versatility of outputs and often trained on a wide range of data sources and large amounts of data to perform a variety of tasks. GPAI is specifically designed for the generation of content such as text, images or audio.

Requirements GPAI:

- Technical documentation
- Instructions for use
- Compliance with the Copyright Directive
- Publication of a summary of the training content

Requirements GPAI with systemic risk:

- Model evaluations
- Cybersecurity
- Evaluation of potential systemic risk
- Tracking and reporting incidents

AI with transparency obligation

Definition: Operators and providers of specific AI systems that interact directly or indirectly with human end users or affect them are required to adhere to heightened transparency obligations. This encompasses AI systems intended for human interaction or those that categorize individuals biometrically.

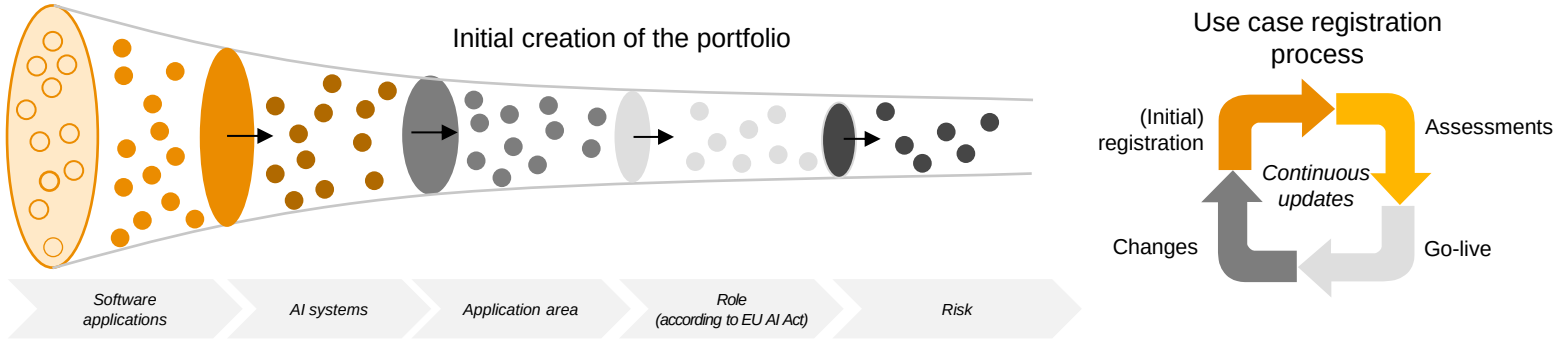
Requirements: Transparency and disclosure requirements

Lifecycle Management is rooted in the requirements of high-risk AI systems according to the EU AI Act

Risk	Organization	Lifecycle		Conformity
Risk Classification Art. 5, 6, 52	Roles, Rights, and Responsibilities Art. 17	Data Management & Governance Art. 10	Transparency & Explainability Art. 13, 52	Technical Documentation Art. 11
Impact Assessment Art. 29a	Resource Management Art. 17	Design, development and Testing Procedures Art. 17	Logging, Recording & Traceability Art. 11, 12, 20	Conformity Assessment & (CE)-Marking Art. 43, 49
Risk Management Art. 9	Accountability & Reporting Art. 17	Accuracy, Robustness & Cybersecurity Art. 15	(Human) Oversight & Monitoring Art. 14, 61	Registration & Reporting Art. 60, 62

The implementation of AI Governance and Security along the entire Lifecycle helps companies to ensure compliance

AI Portfolio Management



Documentation, governance, templates and audit artefacts

- Ethics standard
- Guiding Principles for AI
- Requirements docs
- Training & Awareness Plan
- AI value case templates
- AI use case inventory
- Risk Catalog
- Third party contracts
- Technical documentation
- Risk assessments
- Test reports
- Statement of Applicability

AI Portfolio

Inventory System: Centralized location showcasing all AI Systems – including Responsible AI metrics, controls & lifecycle status dashboards

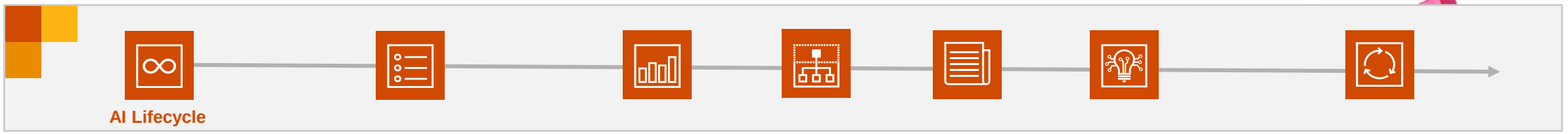
Risks: Identify & classify risks associated with each AI System and streamlining against existing regulations (EU AI Act). Follow-up with control creation according to SOX AI and ISO 42001 to mitigate identified risks.

Documentation: Continuous recording of metadata, technical details, system changes & Audit trails

Compliance: Ensure the AI Systems comply with the relevant regulations (ISO 42001, EU AI Act, SOX AI)

Incident management: Recording of user feedback and reporting malfunctions

Along the Lifecycle, the definition, application and review of controls ensures a standardized approach



- **Regulatory Conformity**
- **Risk Governance**
- **Creation of Trust**
- **Standardization**

Ensure that the legal requirements are met

Identification, assessment and mitigation of phase-specific risks

Addressing trustworthy AI dimensions through targeted measures

AI System Monitoring (for Deployer)

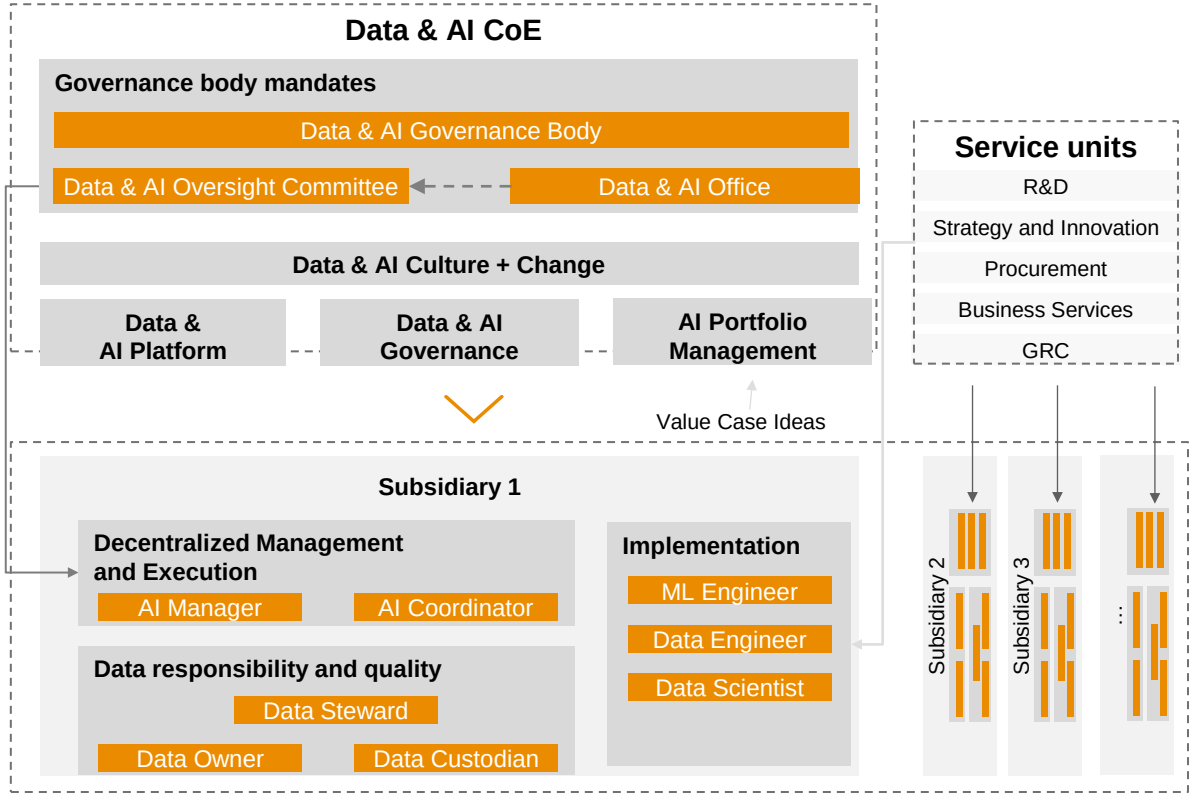
Post Market Surveillance (for Provider)

Control Definition | **Controls Implementation** | **Controls Evaluation** | **Controls Monitoring**

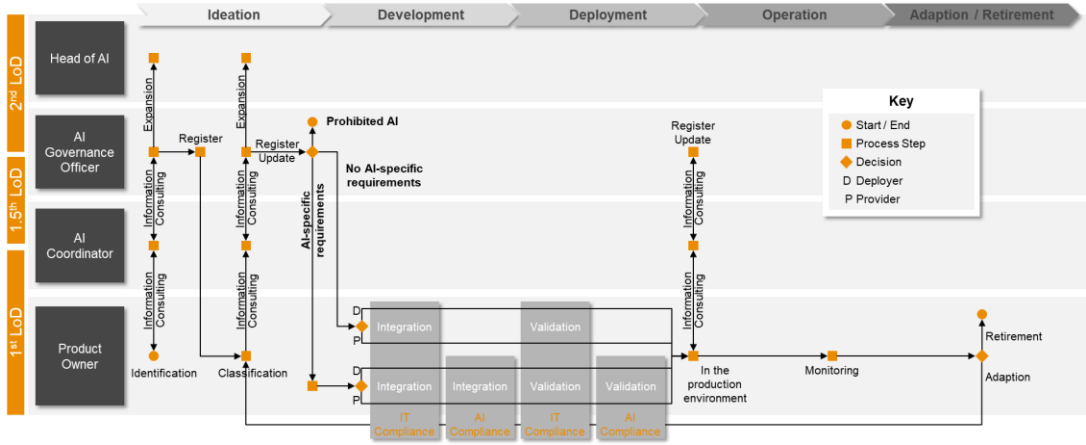
Established process with roles, responsibilities and work products (supported by appropriate tooling)

Transfer of the responsibility concept into an operating model and consensual agreement with all parties involved

Accountability within the organization



Accountability along the lifecycle

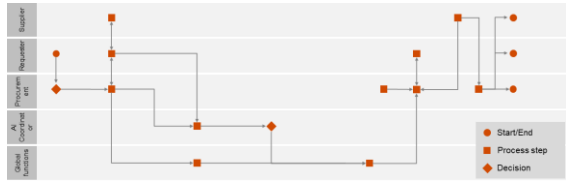


Provider

Software development process

Deployer

Procurement process



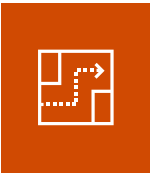
Key Takeaways

Create **standards** for AI within your organization that covers the overall requirements from the AI Act and operationalize them in **AI system specific controls** over the AI lifecycle and ensure **traceability**

Deploy an **AI inventory** with a holistic **underlaying meta model** and a corresponding **registration process** to create transparency over existing AI systems and associated risks

Following within the AI lifecycle a **risk-based approach** by ensuring that risks are continuously **identified**, **assessed** and **mitigated** and that there a **clearly defined entry gates** for new AI use cases

Define the **accountabilities** for AI over the entire lifecycle (checkpoints and quality gates) and within your organization and if necessary create **new roles** to fulfill the specific **responsibilities**



Create a sufficient degree of **awareness** for AI and its characteristics within you organization so that all employees are capable to **use AI responsibly** and all roles (within the AI governance) can **fulfill their role**

Thank you

Vivien Bender
Manager
PwC Frankfurt | Risk & Reg TPR
vivien.bender@pwc.com

pwc.com