AI Trust in Electronics

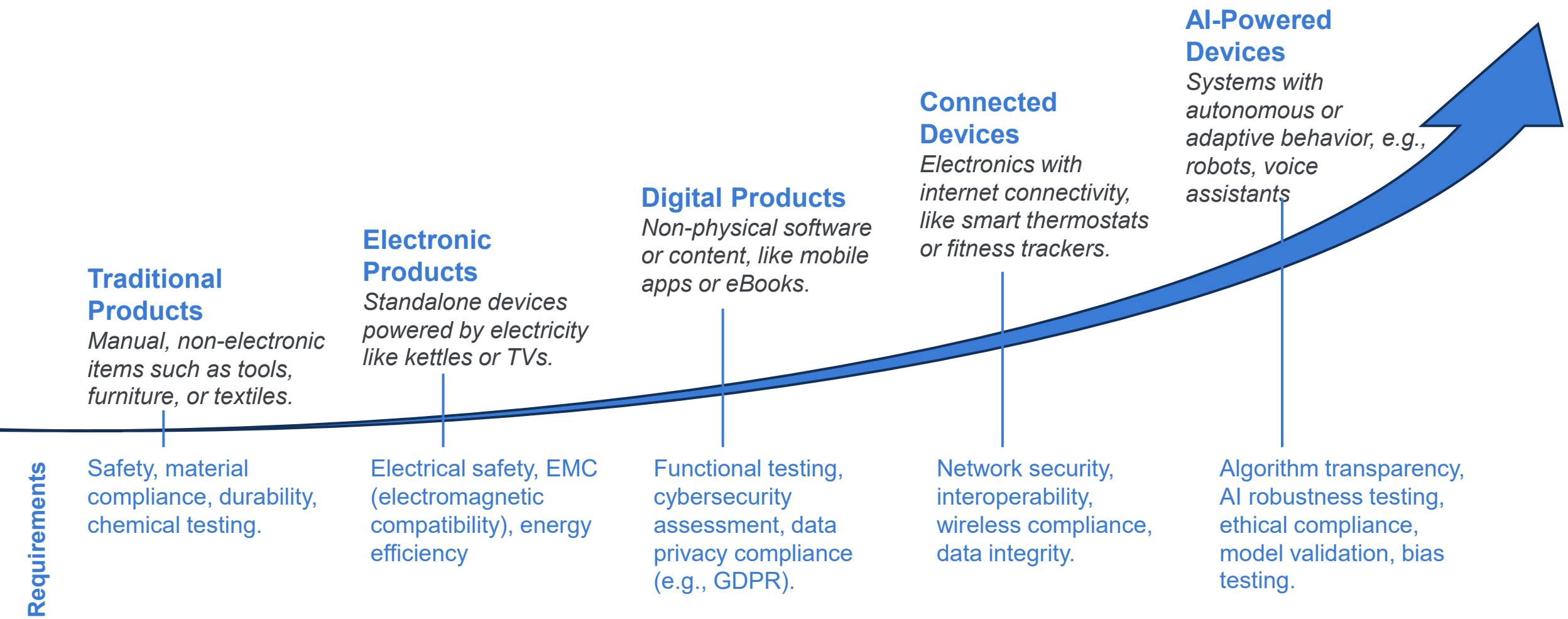
Nemko /IBM summit on AI in Electronics

Pep

September 4, 2025

Nemko Digital

The rising complexity of products bring continuous trust challenges



What does AI Trust mean?

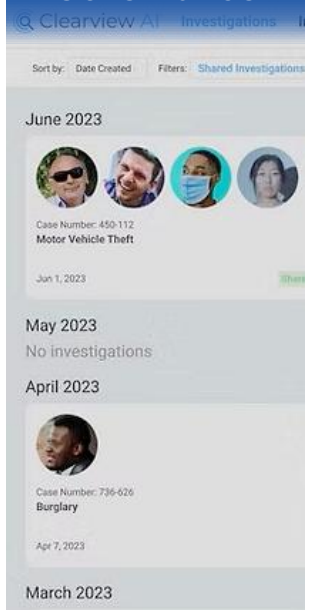
Technical robustness and safety

Google apologizes for Gemini depicting USA founding fathers as racially diverse

Transparency

New York Times sues Open AI over copyright infringement

Privacy and Data Governance



Clearview AI fined € 30.5 m over illegal database of faces

Diversity, Non-discrimination, and Fairness

NL Tax authority implements discriminatory fraud detection algorithm

Societal and Environmental Well-being

Open AI spends $10s of millions in compute on saying ‘please’ and ‘thank you’

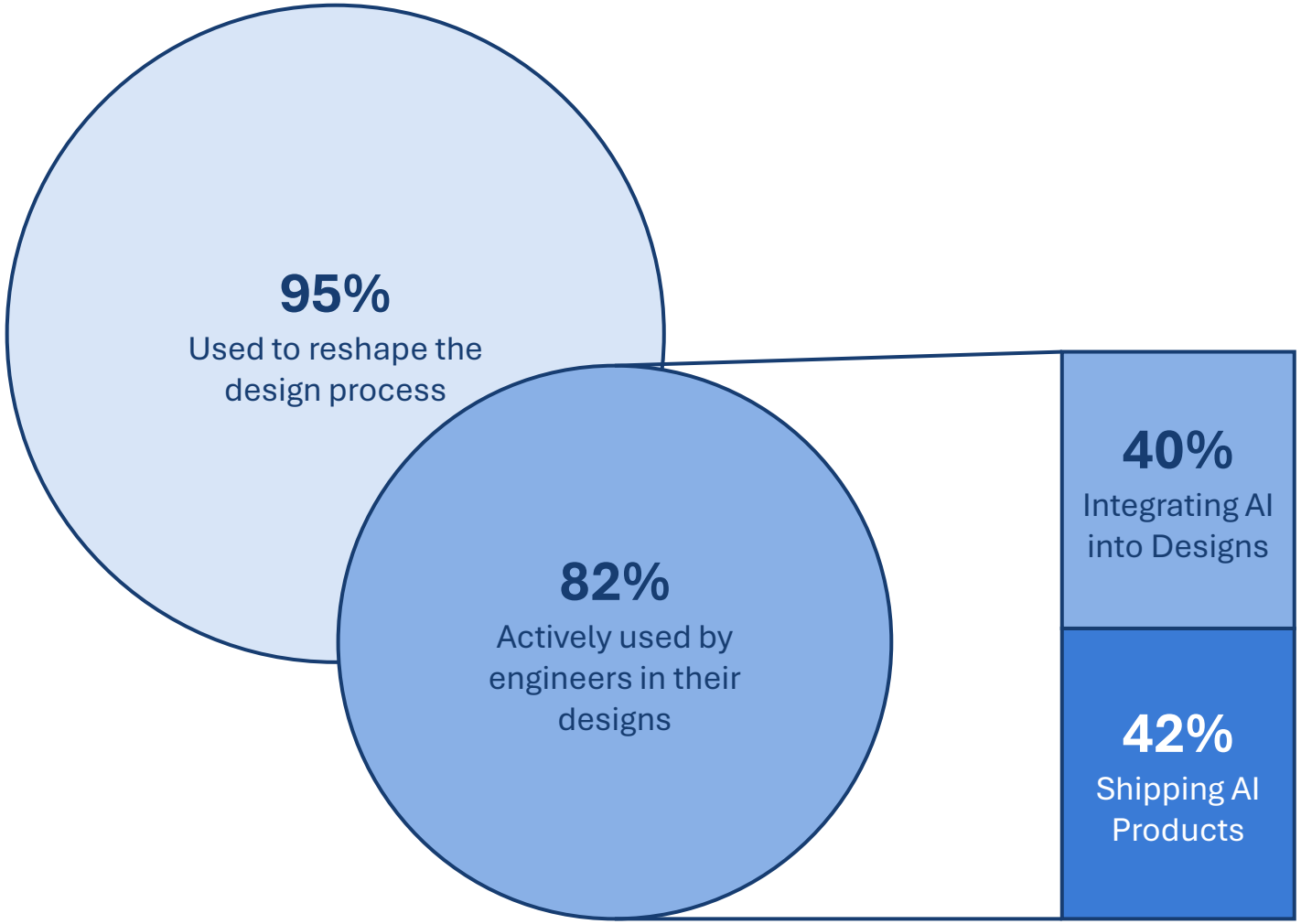
Accountability

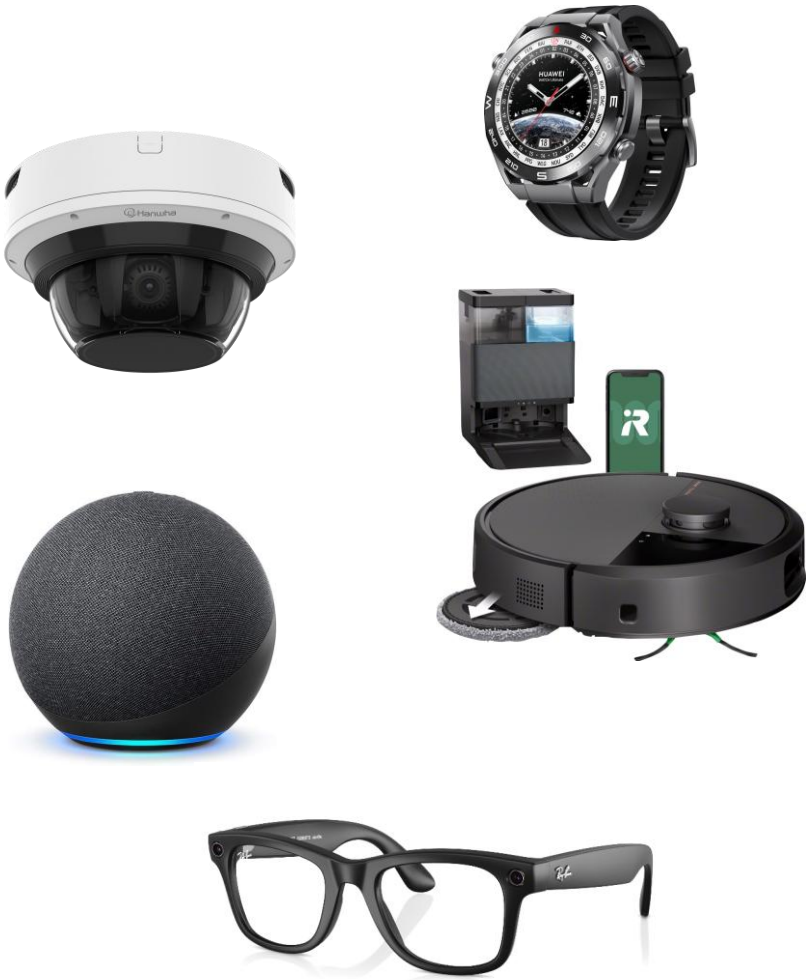
Tesla car in self-driving mode doesn’t detect pedestrian

Human agency and oversight

Lawyer cites fake cases in court – as suggested by ChatGPT

AI in Electronics are everywhere





Source: R&D Forum online; Avnet survey (1200 Electrical engineers, Jan. 2025)

AI Trends in Electronics

- **AI at the Edge**
- **AI Enabled Firmware**
- **AI orchestration**
- **Federated Learning**
- **Hybrid AI architectures**

Sources: Hanwha Vision; Nemko Digital analysis

Product example

Supplier's Platform

- Post-market monitoring
- Quality & Incident Management
- Algorithm updates
- New use-cases

Smart Camera

- Neural processing unit
- On-device blurring
- Smart capture
- Occupancy monitoring

Client's Security system

- Cloud-based configuration
- Room-to-room tracking
- Crowd surveillance
- Heat maps

EU regulation for AI in Electronics

Domain	EU Regulation	Applicability
Artificial Intelligence	**AI Act**	Adopted / 2026
Data protection and governance	**General Data Protection Regulation (GDPR)**	In force
	Data Act	In force
	Data Governance Act	In force
	ePrivacy regulation	In draft / TBC
Cyber security and digital resilience	**Cyber Resilience Act (CRA)**	In force
	Network Information Security Directive (NIS2)	Adopted / 2027
	Digital Operational Resilience Act (DORA)	In force
	Cybersecurity Act	In force
Product Safety and Conformity	**Product Liability Directive – revised**	Adopted / 2026
	Radio Equipment Directive (RED)	In force
	Machinery Regulation – revised	Adopted / 2027
	General Product Safety Regulation (GPSR)	In force
Market and Critical Infrastructure	**Digital Services Act (DSA)**	In force
	Digital Markets Act (DMA)	In force
Sector-specific	**European Health Data Space (EHDS)**	Adopted / 2026

Other leading standards

ISO IEC

IEEE SA

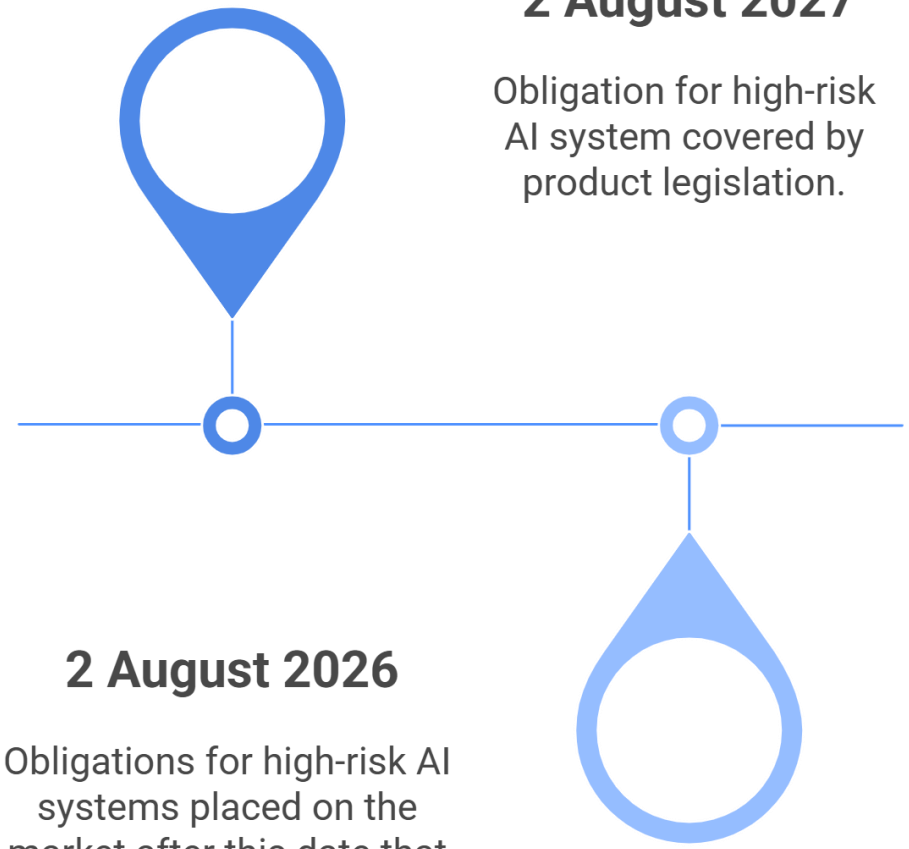
NIST

Gartner

ETSI

Sources: EU regulations; Nemko Digital analysis

Timeline for High-Risk AI systems



2 August 2027

Obligation for high-risk AI system covered by product legislation.

2 August 2026

Obligations for high-risk AI systems placed on the market after this date that do not fall under product legislation (art 6(1)).

Additional remarks

- High risk systems placed on the market before August 2nd 2026 **are only required to comply** they undergo **significant design changes**.
- However, if they are intended for use by **public authorities**, the provider or deployer must comply by **August 2nd, 2030** regardless of design changes

Additional guidelines

The European Commision will provide additional guidelines specifying the practical implementation of **Article 6** (the classification of high-risk AI systems), including post-market monitoring plan before August 2nd, 2026.

Bridging the gap between Compliance for Process and Product

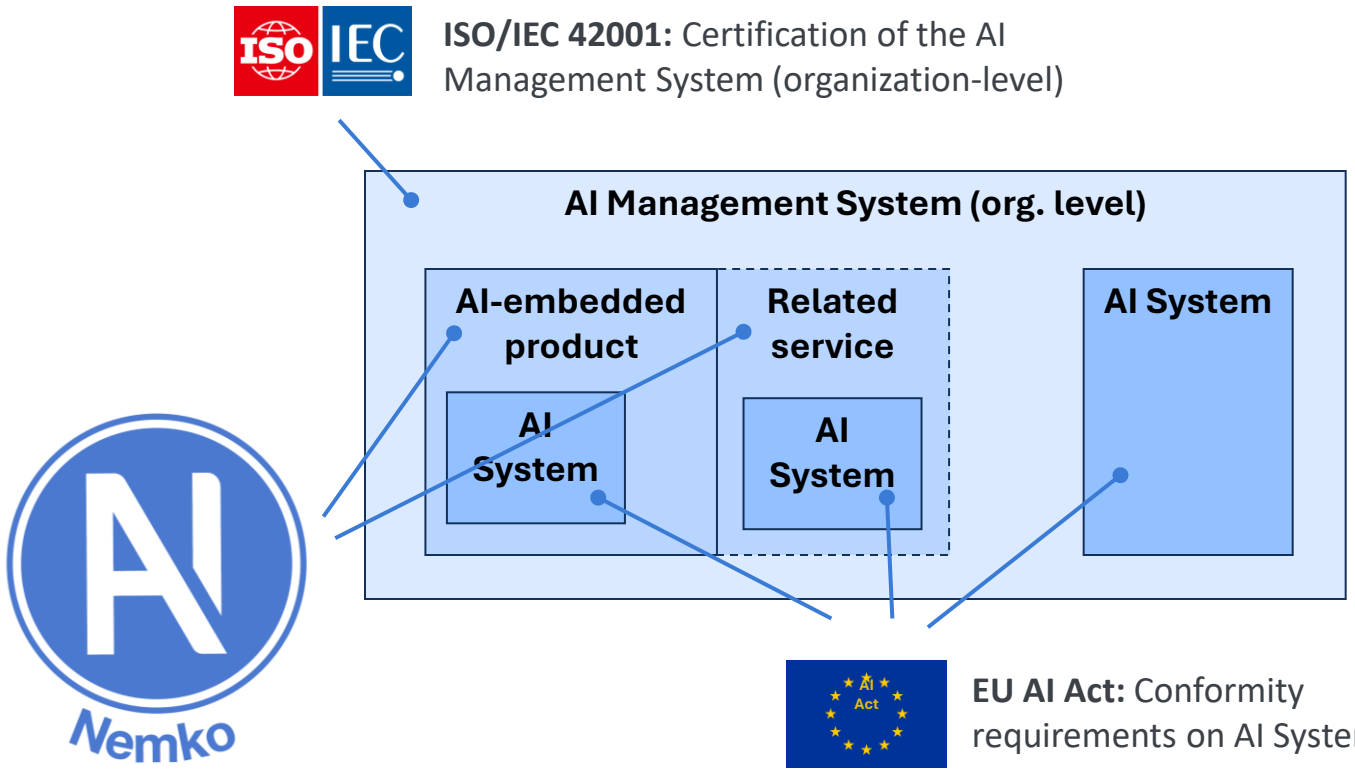
Benefits of Nemko's AI Trust Mark for market-ready AI

Effective

- **Product-focused** and market-entry aligned
- **Harmonized** with leading international standards and regulations
- **Clear, measurable end state** for compliance readiness.

Efficient

- Validation of relevant **ISO 42k** processes for the product going to market.
- Integrates existing guidance to smoothen **EU AI Act** conformity checks



Value drivers for AI governance, compliance & quality management

- *Compliance with upcoming regulation*
- *Reputation as leading global company*
- *Control to prevent incidents / harm*
- *Stakeholder demands around use of AI*
- ***Competitive advantage on the market***

What keeps executives up at night

Common pain points in AI Trust

How can we demonstrate to our **customers** that our AI can be trusted?

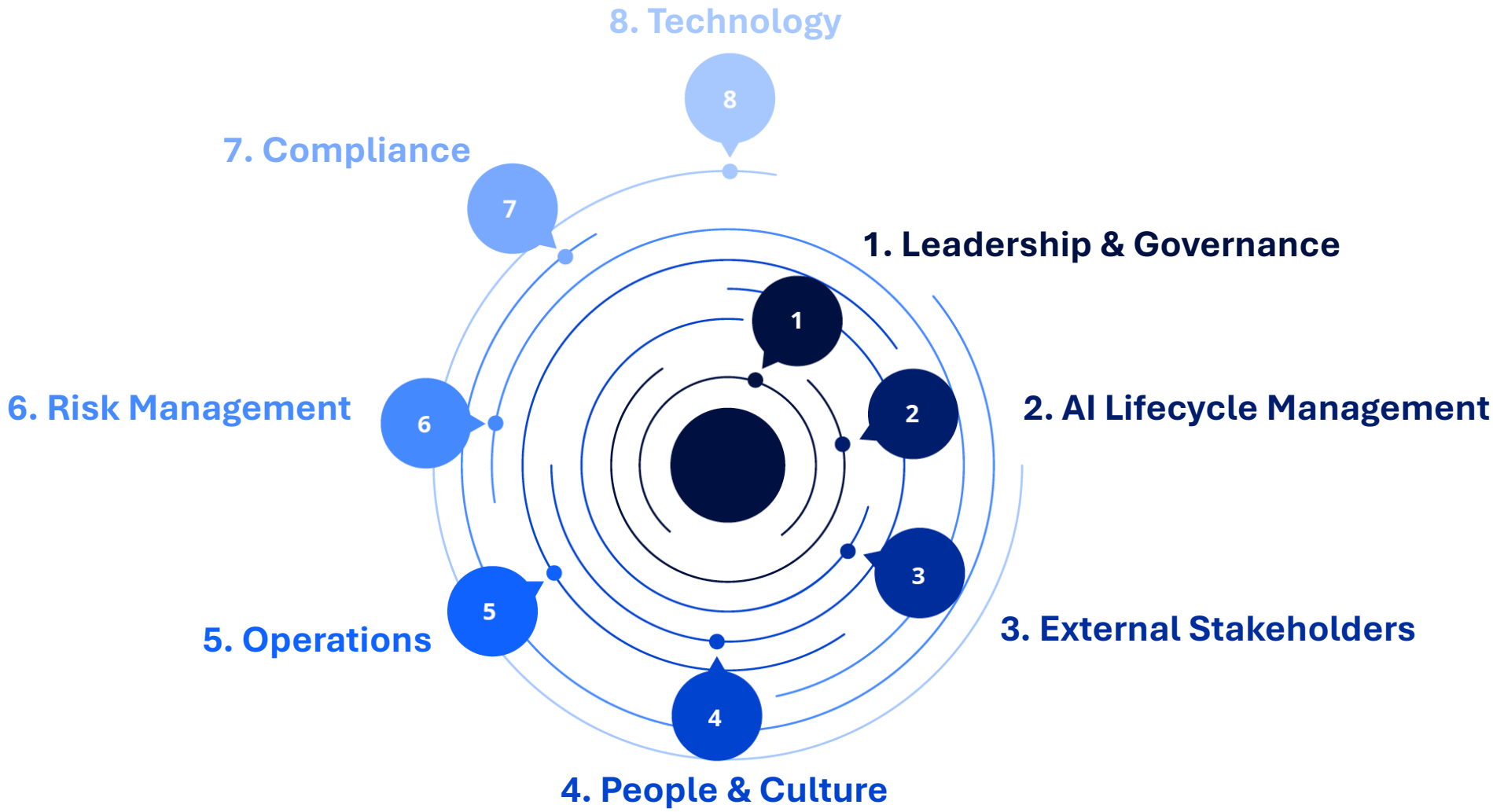
How do I manage compliance when I have **100s of AI-products**?

How do we ensure that our AI-products don't **fail silently**?

How can we stay in control over products with **Agentic AI**?

How do I ensure that our AI-products **remain reliable** in a changing environment?

Eight essentials organization building blocks for your AI success



Nemko's AI Maturity Model helps you drive structural improvement

1	Leadership & Governance	AI Strategy & Business impact	Value/business case & ROI	Governance & org design	Ethics & principles	Finance & resources	Human rights & Sustainability
2	AI Lifecycle Management	Use case scoping design	Data collection & quality	Development & testing	Deployment & monitoring	Decommission & retirement	Human in the loop
3	External Stakeholders	Partnership & co-development	Customers & end-users	Supply chain & procurement			
4	People & Culture	AI trainings & literacy program	Change & adoption	Culture: AI mindset	Incentives & policy alignment		
5	Operations	Processes & procedures	Internal controls	Continuous improvement	AI Performance management	Data management	AI inventory
6	Risk Management	Risk assessments & mitigation	Risk tracking & escalation	Incident & crisis management			
7	Compliance	Documentation & record keeping	Regulatory monitoring	Audit readiness& assurance	Data privacy requirements	Transparency & explainability	Fairness
8	Tech (Infra, Data & Cyber)	Technical infrastructure	Architecture & solution design	Cybersecurity	Data pipelines & platforms		

AI Governance Maturity in practice

5. Market Leading
- AI as differentiator and innovation driver
- Real-time monitoring with automated controls
- Compliance by design drives efficiency

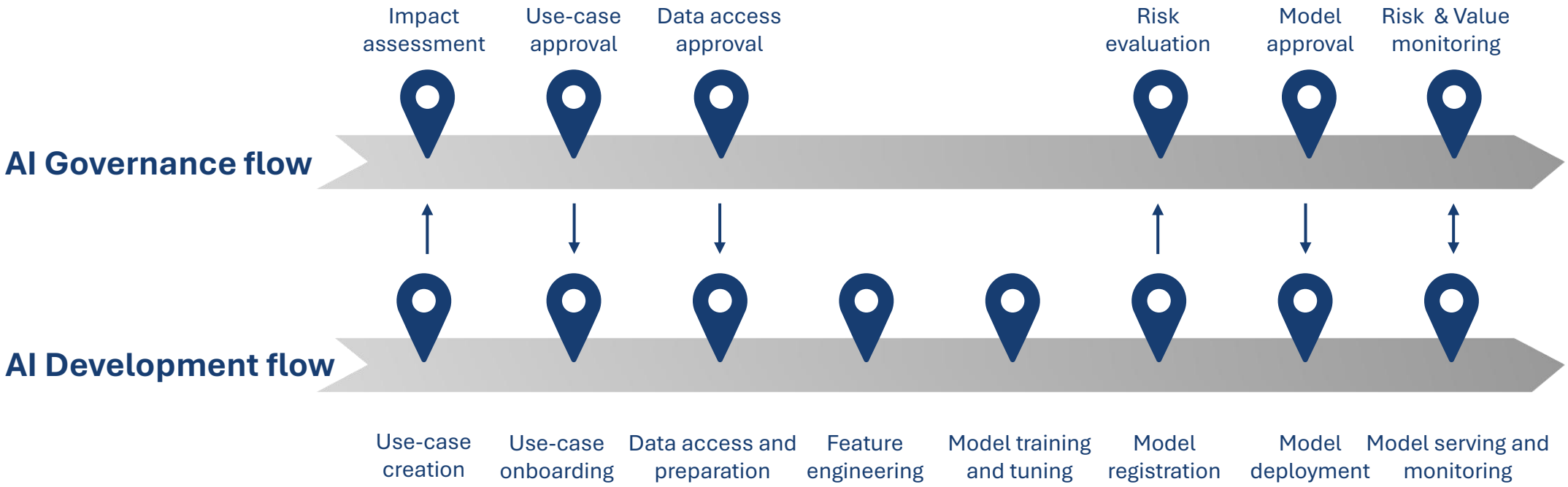
4. Advanced
- AI embedded at the core
- KPIs for accuracy, transparency, fairness
- Aligned to standards and best-practices

3. Evolving
- AI aligned to business priorities
- Developing AI lifecycle controls
- Initial org-wide principles and policies

2. Founding
- Scattered AI initiatives
- Emerging risk frameworks and literacy
- Reactive and inconsistent governance

1. Exploring
- AI experimentation and exploration
- Lack of use policies and governance
- Scattered and undirected

AI Maturity requires solid governance



watsonx.governance

Life Cycle Management

Risk Management

Compliance Management

The AI Agents are coming

Agentic Systems in brief

Interaction
- Personalization
- Intent recognition
- Conversation flow

Orchestration
- Planning
- Collaboration (MCP, A2A)
- Validation

Knowledge
- Vector databases
- Graph databases
- External sources (APIs)

Actions
- Function calling
- System and Tool access
- Resource availability

New and amplified risks (selection)

	Training data	Inference	Output	Non-technical
GenAI	Data bias	Jail breaking	Output bias	Unintended use
	Privacy	Hallucination	Harmful code	Content ownership
	Transparency	Prompt attacks	HAP	Over-reliance
	IP & Copyright		Explainability	
Agentic AI	Data quality	Error amplification	Harmful actions	Human dignity
		Value alignment		Accountability

Sources: IBM AI Risk Atlas; Nemko Digital analysis

Stop bolting on trust as a **feature**

Start building with it as the **foundation**

Download our whitepaper