



# Scaling AI with a Risk-Based Control Framework

From Experimentation to  
Enterprise Governance

Nemko Digital

4<sup>th</sup> June 2026

# Agenda

1. Introducing Nemko Digital
2. Two perspectives on risk
3. Case study: GenAI in Government
4. Q&A



# With you today

**Alicja Halbryt**  
*AI Trust Consultant*  
*Nemko Digital*



- **Human-Centred Technology Advocate:** Guiding human-centred innovation across policy and technology to deliver responsible and impactful outcomes.
- **Public Sector & Standardisation Expertise:** Formerly at the Dutch Ministry of Economic Affairs; expert contributor to CEN/CENELEC JTC 21 on European AI standardisation. ISO 42001 Lead Auditor.
- **Interdisciplinary Academic Background:** MA in Service Design (University of the Arts London) and MSc in Philosophy of Technology (University of Twente).
- **Focus on Ethical & Inclusive Innovation:** Committed to shaping emerging technologies that are responsible, inclusive, and grounded in real human experiences.

**Pep van der Laan, Ph.D.**  
*Digital Trust Expert*  
*Nemko Digital*



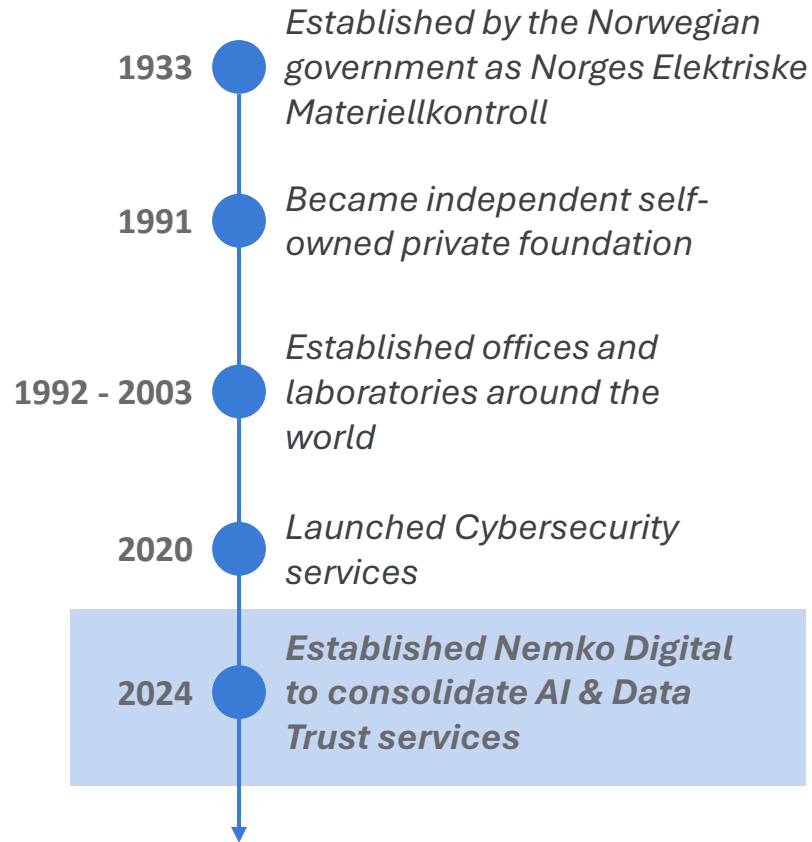
- **Scaling AI impact:** >10 years in realizing business value by scaling AI-powered digital products from initial proof-of-concept to enterprise-wide solutions.
- **Strategy advisory:** Extensive experience shaping the AI & Data transformation and architecture for global leaders and national champions across industries.
- **Capability building:** Led a team of 90 data engineers, AI developers, and data scientists through the transformation from the traditional consulting model and introducing modern delivery and development practices.
- **Growing Digital Trust:** Recognized for consistently bridging the gap between technology and the risk & legal stakeholders, building mutual understanding. Certified as ISO 27001 and ISO 42001 Lead Auditor.



# Introducing Nemko Digital

# Nemko: Compliance without Complexity

## Strong heritage



## Global reach & local presence

**28 locations on 3 continents**

Over **850** employees worldwide.

Offering services in more than **150** countries

Serving **7,000** customers across **80** countries.

In September 2025, Nemko and IBM jointly organized the **AI Trust in Electronics Summit** in Oslo



## Proven track record

Roster of clients and services (not exhaustive)

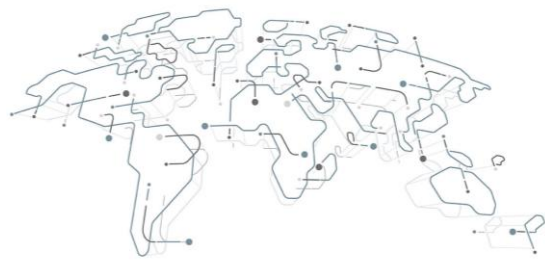


# Relevant experiences we bring in for you

These credentials show our proven ability to design and implement trusted AI and data governance frameworks **across industries**, from global corporations to government bodies.

We help organizations translate complex digital opportunities and regulatory requirements into **actionable** strategies, frameworks, and compliance measures that enable safe, ethical, and scalable adoption.

We approach AI Trust and compliance with a **makers' mindset**.



## Client Impact

AI Trust mark to show compliance with EU AI Act (multiple companies)

EU digital compliance for an IoT company

AI-powered conversational selling strategy for global retailer

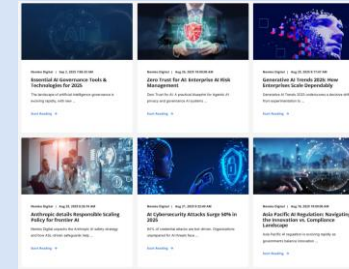
AI trust and compliance services for an international university

AI Risk categorization wrt AI Act (multiple companies)

GDPR-compliant loyalty scheme for a grocery retailer

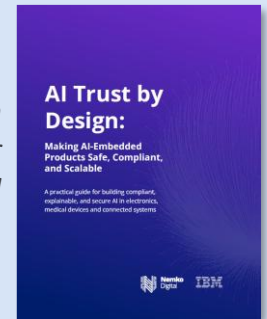
*Illustrative examples*

## Thought Leadership



Regular webinars on topics related to AI & Digital Trust

Whitepaper AI Trust in Electronics together with IBM



Contributed to whitepaper on AI governance with Deeploy



*Illustrative examples*



# Our popular services

We deliver Digital Trust through end-to-end compliance and advisory support, combining technical, regulatory, and process expertise.



**Regulatory Compliance**

AI, data,  
cyber



**Technical Assurance / AI Testing**



**ISO Readiness**  
ISO 42001, ISO 27001...

AI, data,  
cyber



**AI Assurance Tools**



**Global Market Access**

AI, data,  
cyber



**Governance Maturity**

AI, data,  
cyber



**Nemko AI Trust Mark**



**Strategy and roadmaps**

AI, data,  
cyber



# Two perspectives on risk

# Regulations overview

## US' AI Strategy



No single, comprehensive federal data privacy law

Allow innovators to experiment and deploy AI technologies freely

Semiconductor independence and workforce development

## UK's AI Strategy



Pro-innovation

No standalone AI legislation

Assesses risk dynamically according to the context in which it is used

## China's AI Strategy



Rules for algorithms, deep synthesis, AIGC labeling, and facial recognition

Strong state oversight and enforcement

Data governance (PIPL, Data Security Law, Cybersecurity Law)

National security and social stability priorities

## South Korea's AI Act



Risk-based regulation

Safety and transparency for high-impact AI

Human-centric protections

## Singapore's AI Framework



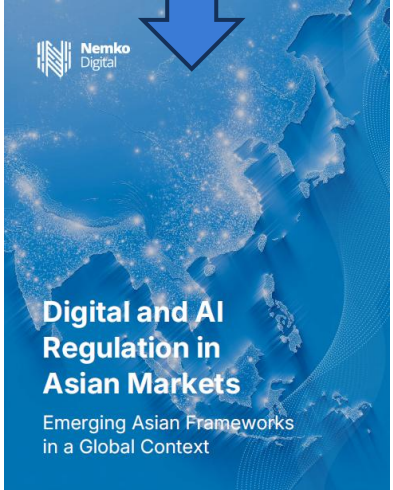
Risk Assessment

Human Accountability

Technical Controls

End-User Responsibility

Read our Asian regulation deepdive publication 27 Apr '26



Explore AI Trust Insights with expert articles on governance, ethics, and regulations to master AI compliance and build trusted solutions.

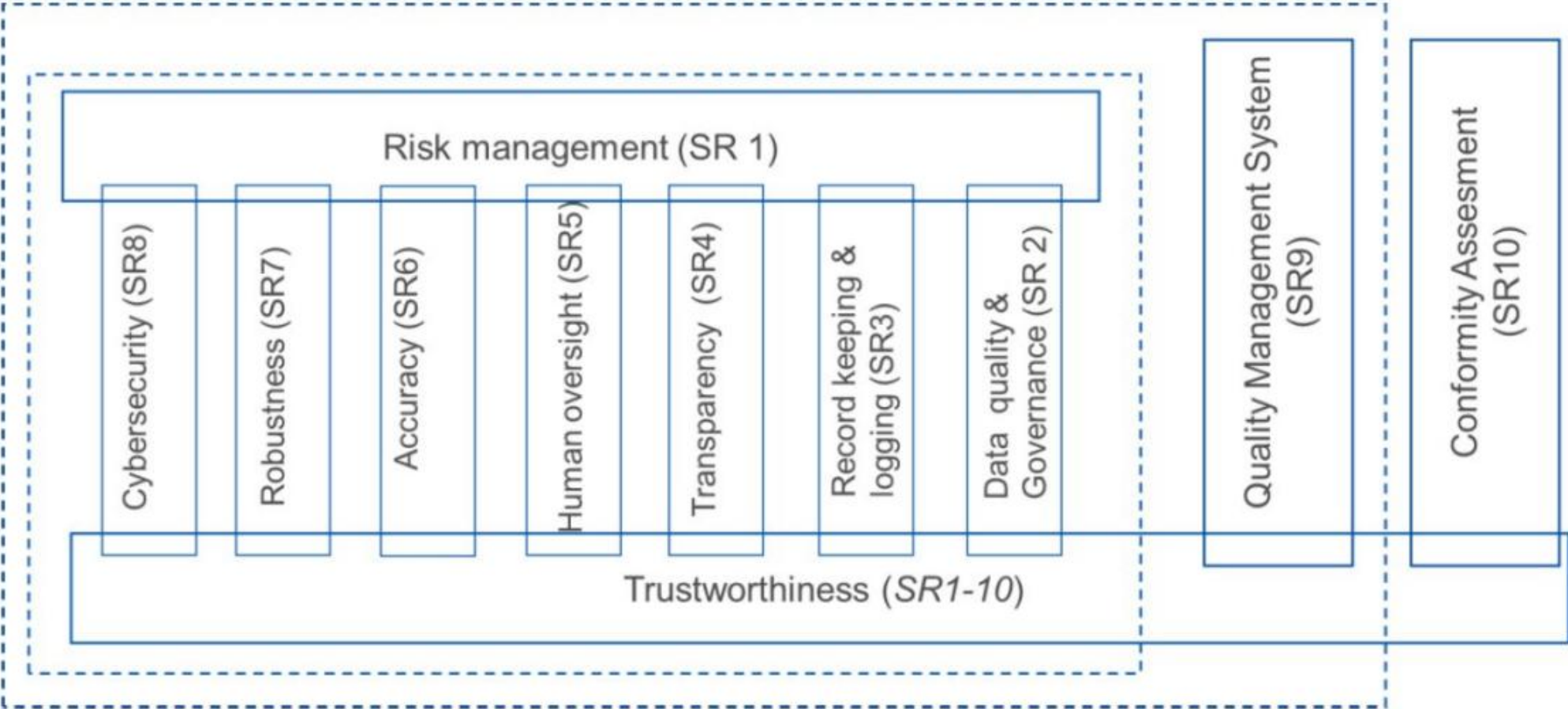


# AI regulations are focused on societal risks

|                 | Examples                                                                                    | Obligations                                         |
|-----------------|---------------------------------------------------------------------------------------------|-----------------------------------------------------|
| Prohibited AI   | <i>social scoring, predictive policing, emotion recognition in workplaces and education</i> | <i>Prohibited</i>                                   |
| High Risk AI    | <i>biometric identification, AI tools tracking employee performance, credit scoring</i>     | <i>Must undergo a conformity assessment</i>         |
| Limited Risk AI | <i>AI-written articles, chatbots &amp; virtual assistants, generative AI media</i>          | <i>Must adhere to transparency requirements</i>     |
| Low Risk AI     | <i>spam filters, grammar and spell checkers, video game AI</i>                              | <i>No obligations – Subject to codes of conduct</i> |
| GPAI            | <i>OpenAI's GPT-4 and DALL-E, Google's BERT, Meta's LLaMA</i>                               | <i>Subject to GPAI-specific requirements</i>        |



# Standards supporting the AI Act implementation



# Overview of EU AI Act standards

| Standard to-be-harmonised*                                                             | Status         |
|----------------------------------------------------------------------------------------|----------------|
| prEN 18229-1 "AI Trustworthiness Framework - Part 1: Logging"                          | Drafting       |
| prEN 18229-2 "AI Trustworthiness Framework - Part 2: Accuracy and robustness"          | Drafting       |
| prEN 18229-3 "AI Trustworthiness Framework - Part 3: Transparency and human oversight" | Drafting       |
| prEN 18228 "AI Risk Management System"                                                 | Public Enquiry |
| prEN 18286 "Quality Management System"                                                 | Formal Vote    |
| prEN XXX "AI Conformity assessment framework"                                          | Drafting       |
| prEN 18284 "Quality and governance of data"                                            | Drafting       |
| prEN 18282 "Cybersecurity of AI system"                                                | Public Enquiry |

At this stage, full coverage of the standardisation requirements is not expected before 2027.

\*standards which respond to the European Commission standardisation request

© 2026 All rights reserved by Nemko Digital: content and materials are not to be distributed or shared without prior permission.



# Standards at the most advanced stage

| Standard                                | Description                                                                                                                                                                                                                                                                                           | Status         |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| prEN 18228 “AI Risk Management System”  | Describes how risks of AI systems can be managed during the entire life cycle of an AI system. It applies to risks to health, safety and fundamental rights associated with an AI system. The standard describes terminology, principles and a process for identifying, assessing and managing risks. | Public Enquiry |
| prEN 18286 “Quality Management System”  | Primarily intended for organizations placing on the market or putting into service high-risk AI systems. Specifies the requirements and provides guidance for the definition, implementation and maintenance of a quality management system for organizations that provide AI systems.                | Formal Vote    |
| prEN 18282 “Cybersecurity of AI system” | Addresses organizational and technical solutions aimed at ensuring the cybersecurity of high-risk AI systems over the life cycle, appropriate to the relevant circumstances and the risks.                                                                                                            | Public Enquiry |

**\*standards which respond to the European Commission standardisation request**

© 2026 All rights reserved by Nemko Digital: content and materials are not to be distributed or shared without prior permission.



# Approaching risk from the business perspective

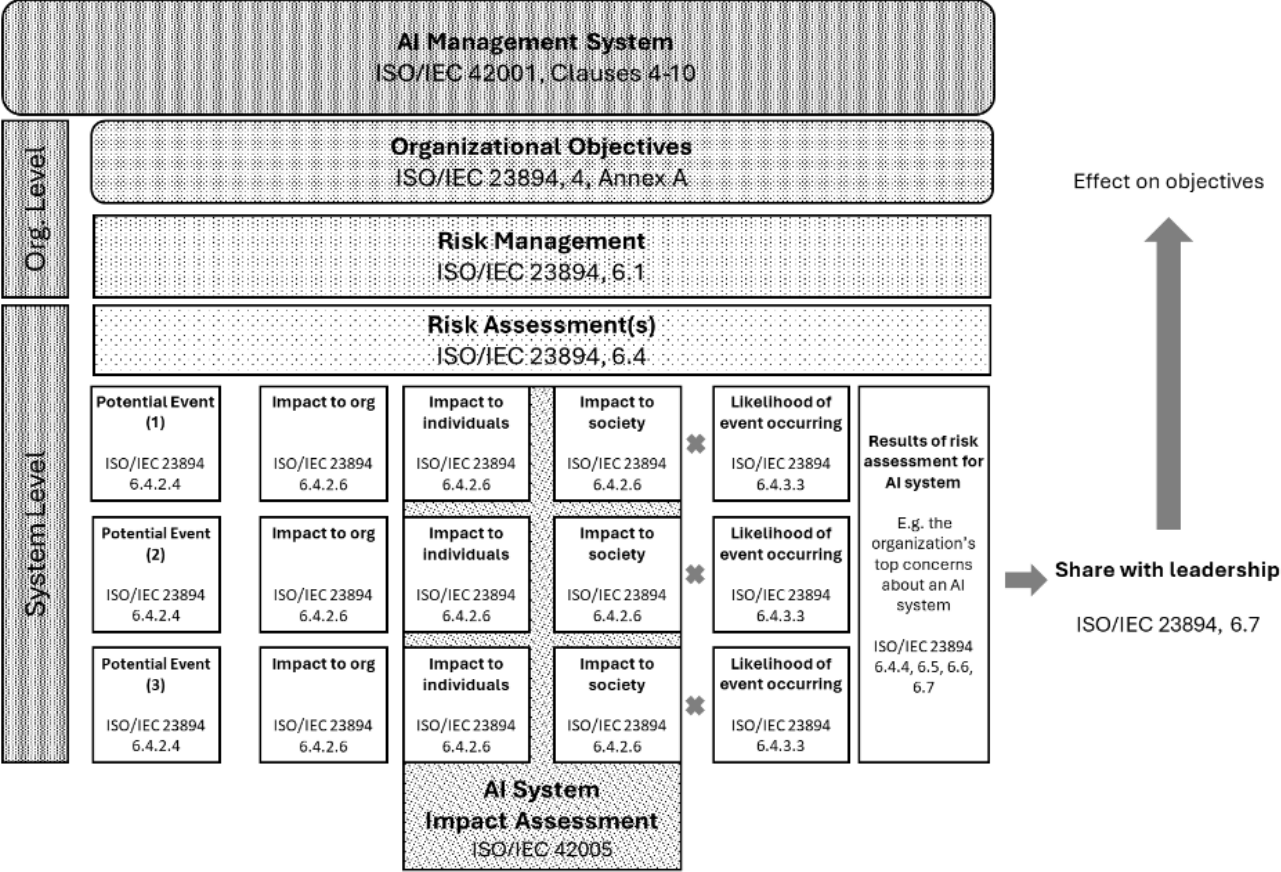
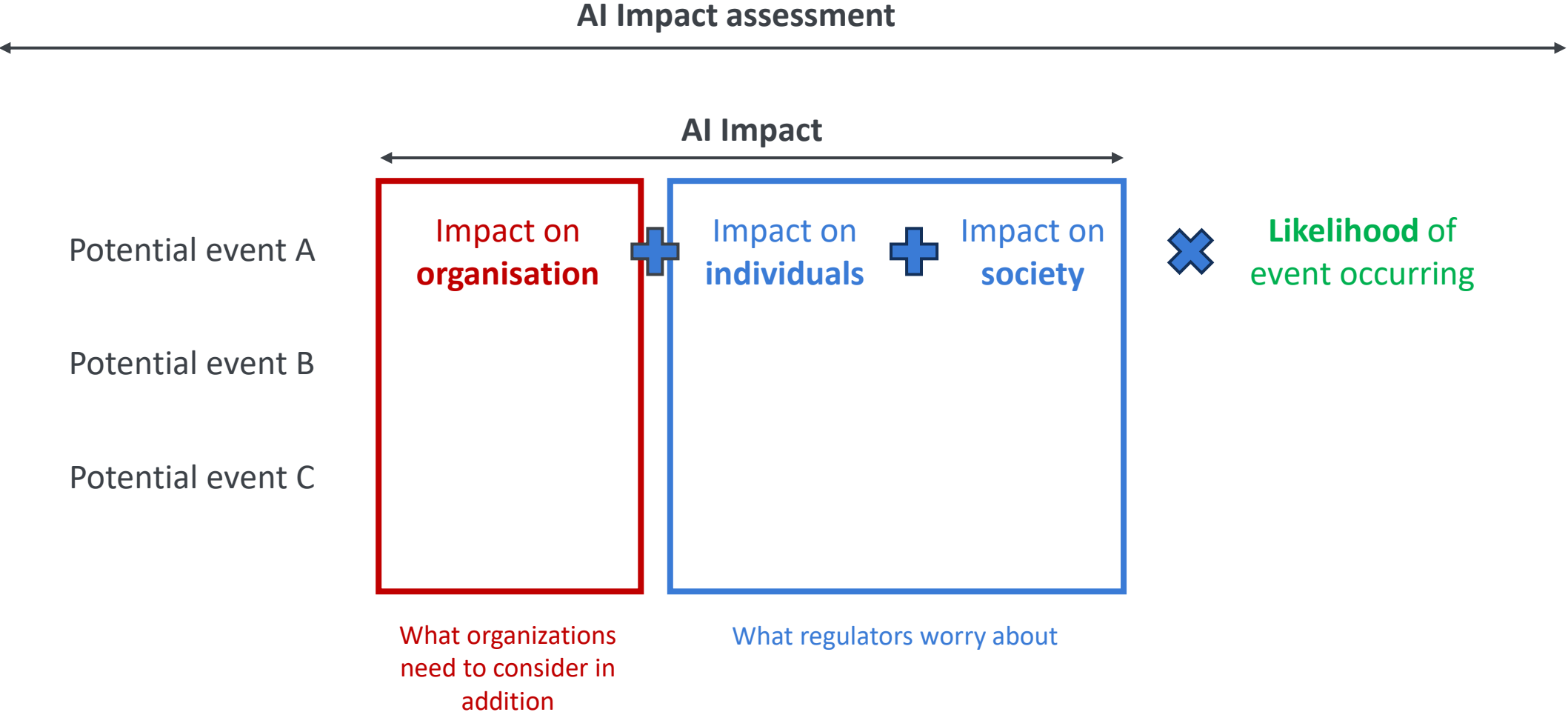


Figure B.1 — Relationship of ISO/IEC 23894:2023 to this document

ISO/IEC 42005:2024 Information technology — Artificial intelligence — AI system impact assessment

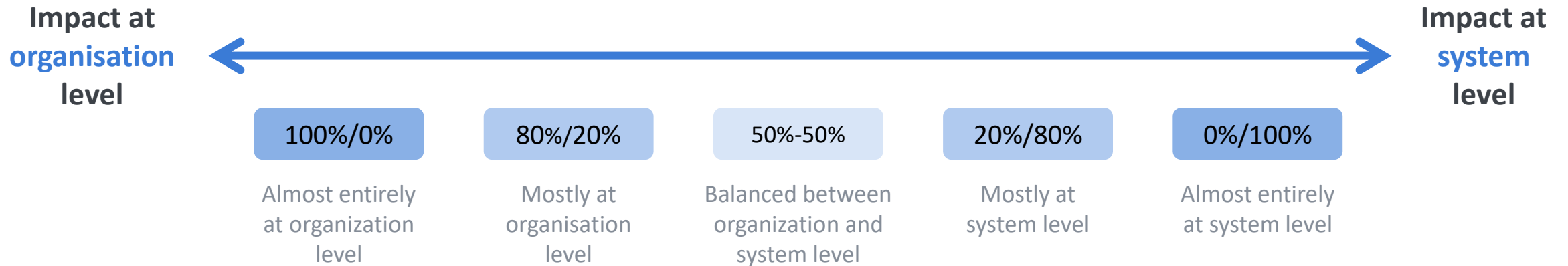


# Approaching risk from the business perspective



# Quiz

# When it comes to AI risk, where are you spending your time?



# Case study: GenAI in Government

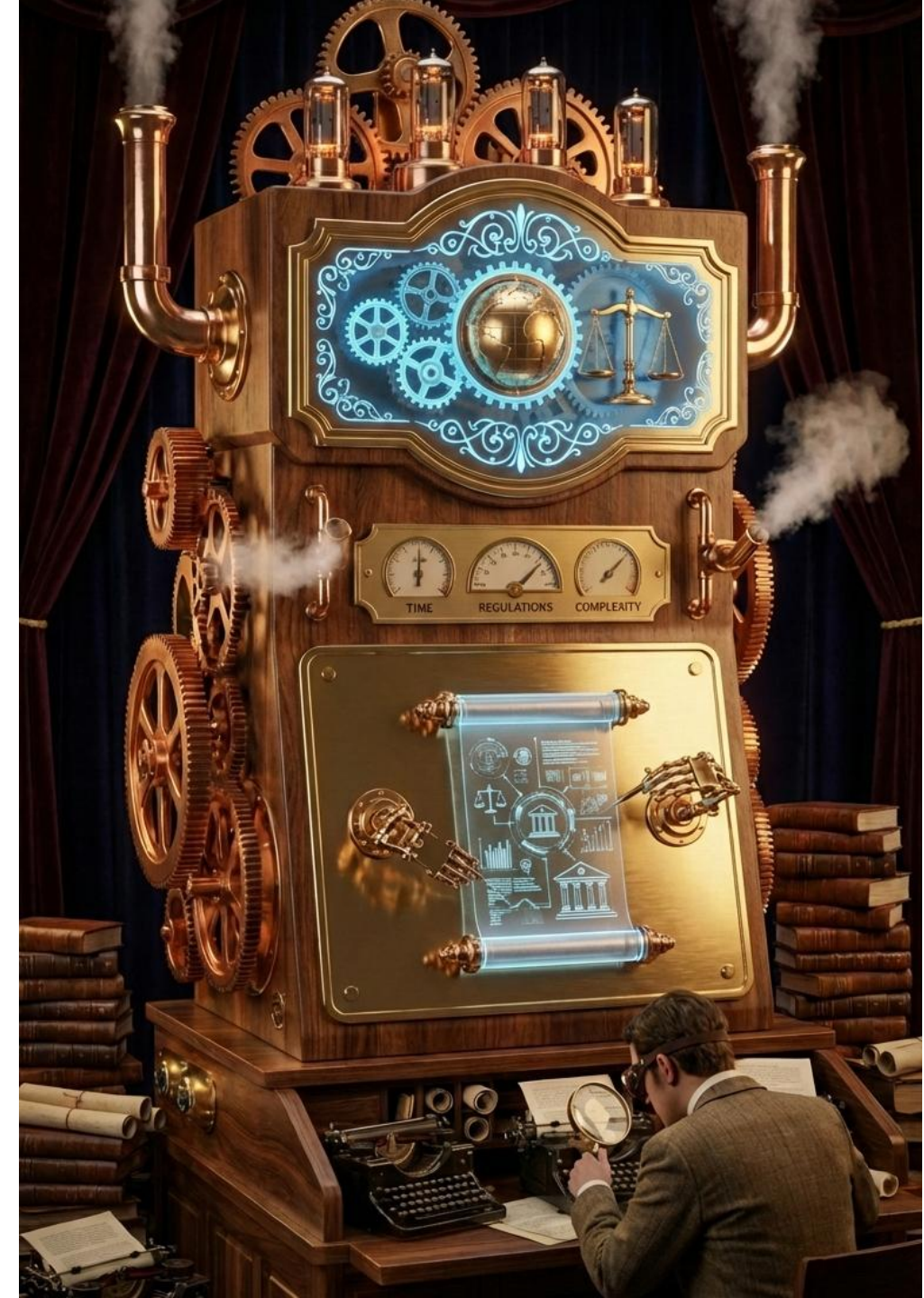
# The GenAI Use case(s)

Large corporations can ask a government body for a pre-assessment that provides up-front clarity on **how laws and regulations would be applied in specific scenarios** – to aid their internal decision making, assure compliance and avoid surprises.

For the government body, this process is **slow and time-consuming**: it depends on many rules and regulations and that require meticulous verification of formal requirements.

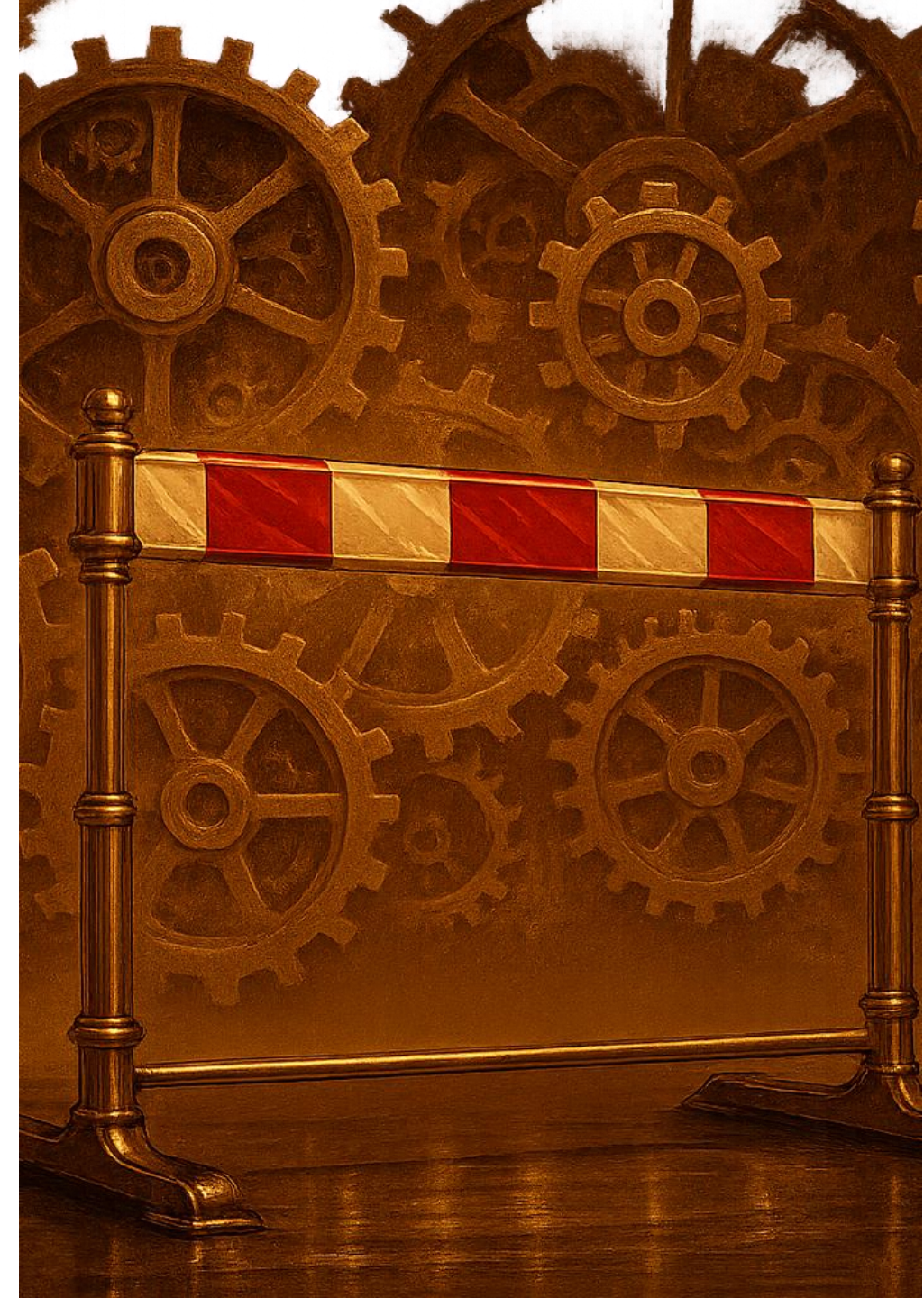
Initial application of AI in this process:

- **Write a report** assessing if the **formal requirements** are met and the request can legally be considered.
- **Find relevant clauses** in regulations and jurisprudence, supporting human assessors.



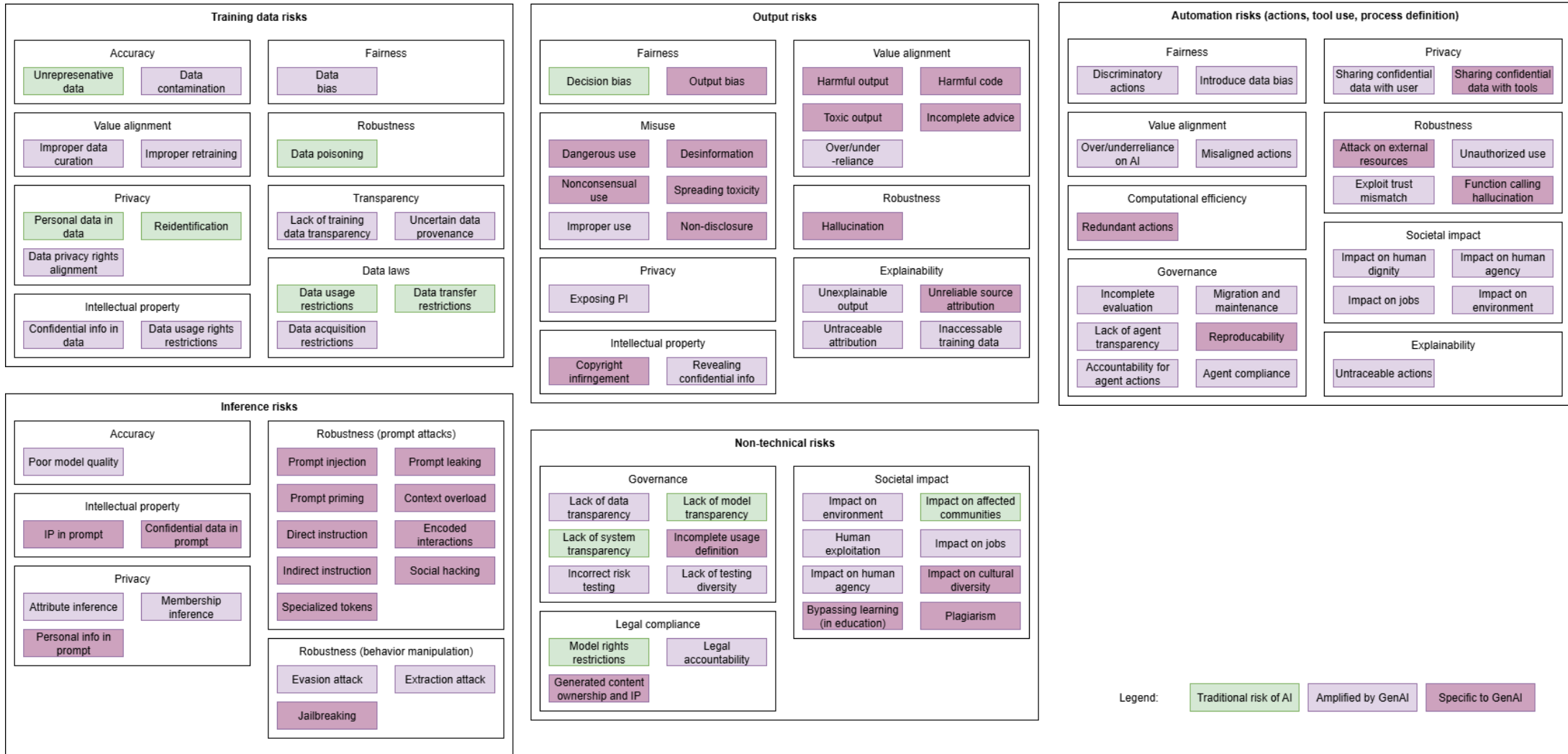
# Hurdles to scaling

- Promising pilot results and enthusiastic front-line workers, but existing processes do not support a clear **path to production**
- **Insufficient AI expertise** across the organization to properly identify and delimit AI-related risks and their potential impact
- **Risk-averse organization** with decision makers who are hesitant to 'green-light' any novel GenAI applications
- A missing **shared perspective** on how to assess and judge AI risks, nor which controls would be sufficient
- Lack of **formal ownership** for AI-related decisions, sending the product team on a wild goose chase for approvals
- **Stalled go-live decisions**, depriving the organizations and its clients from clear benefits (turn-around speed, efficiency)





# Building on IBM Risk Atlas, we built a client-specific version

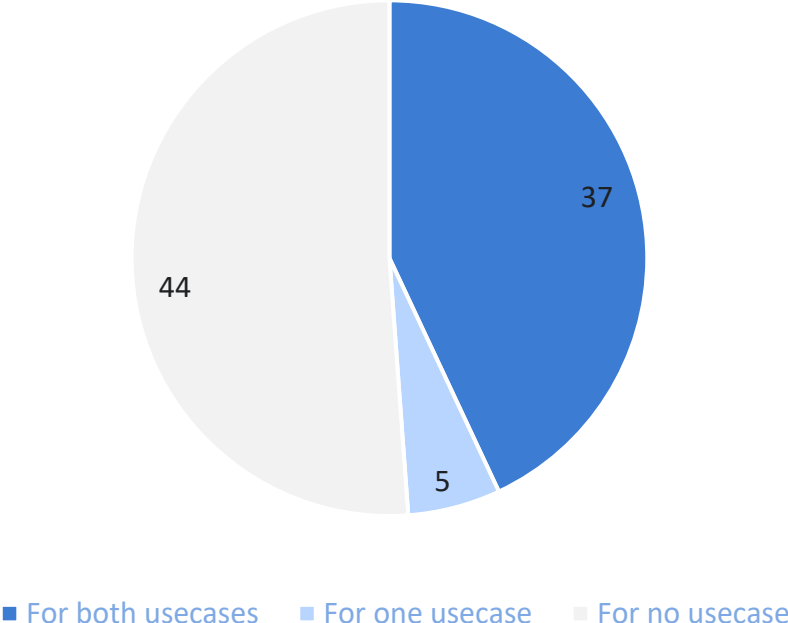


Bron: IBM AI Risk Atlas

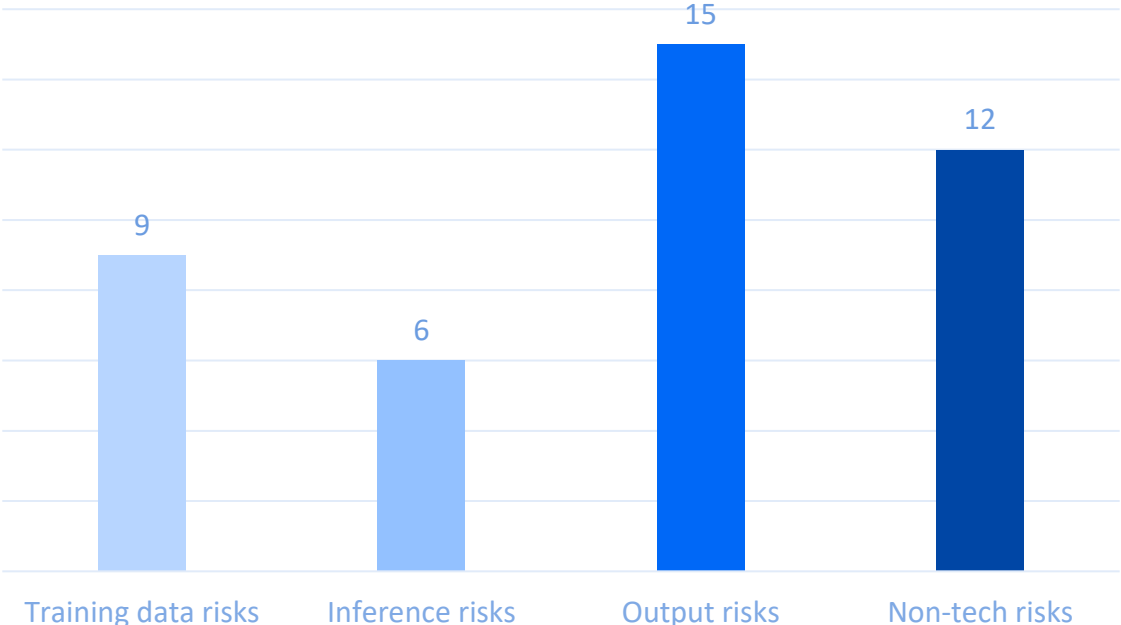


# Based on the use case characteristics, we selected the relevant risks

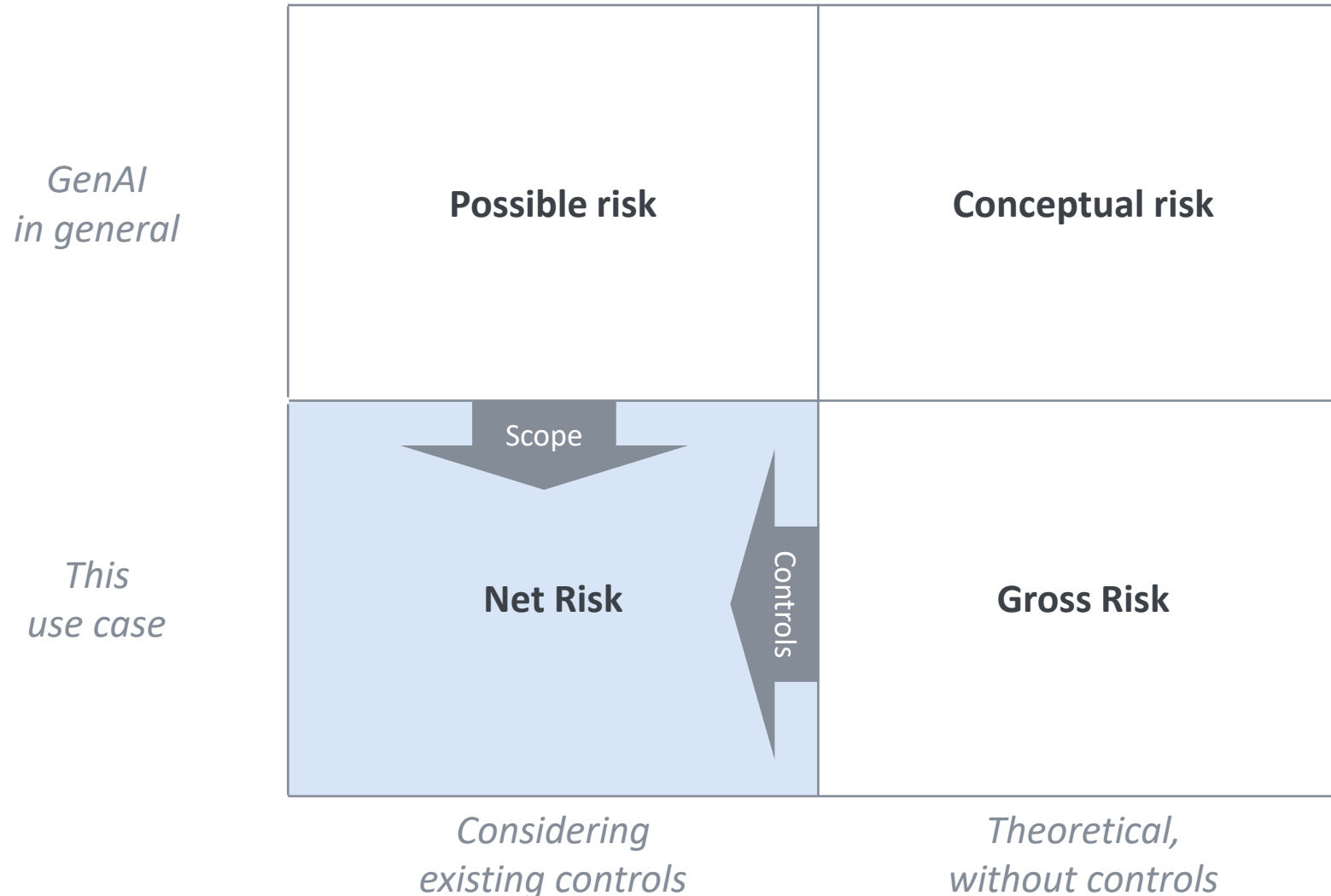
### Risks classified by relevance



### Relevant risks by life stage



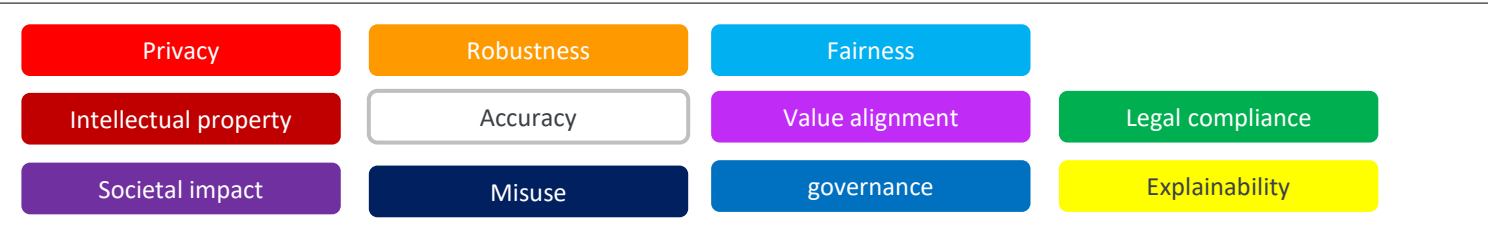
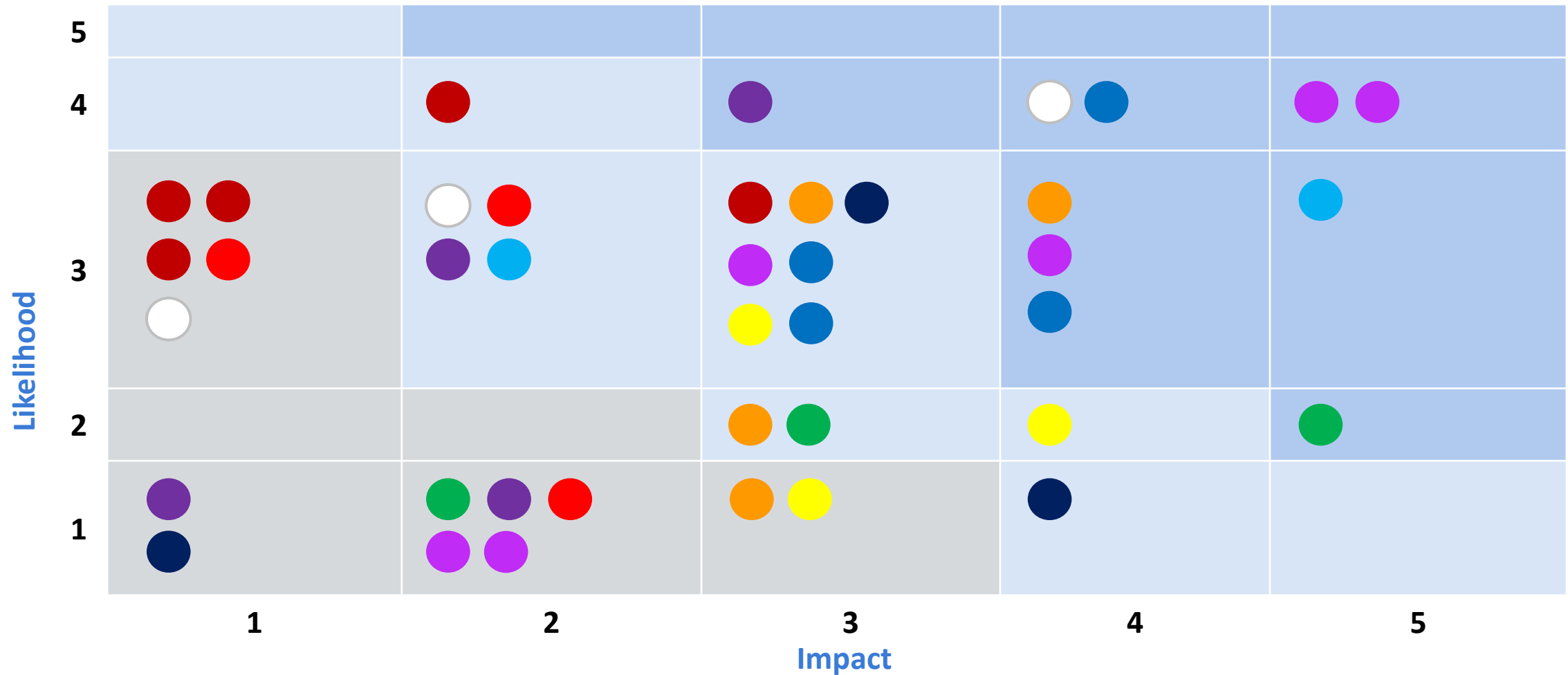
# Risk estimation based on use case-specific Net Risk



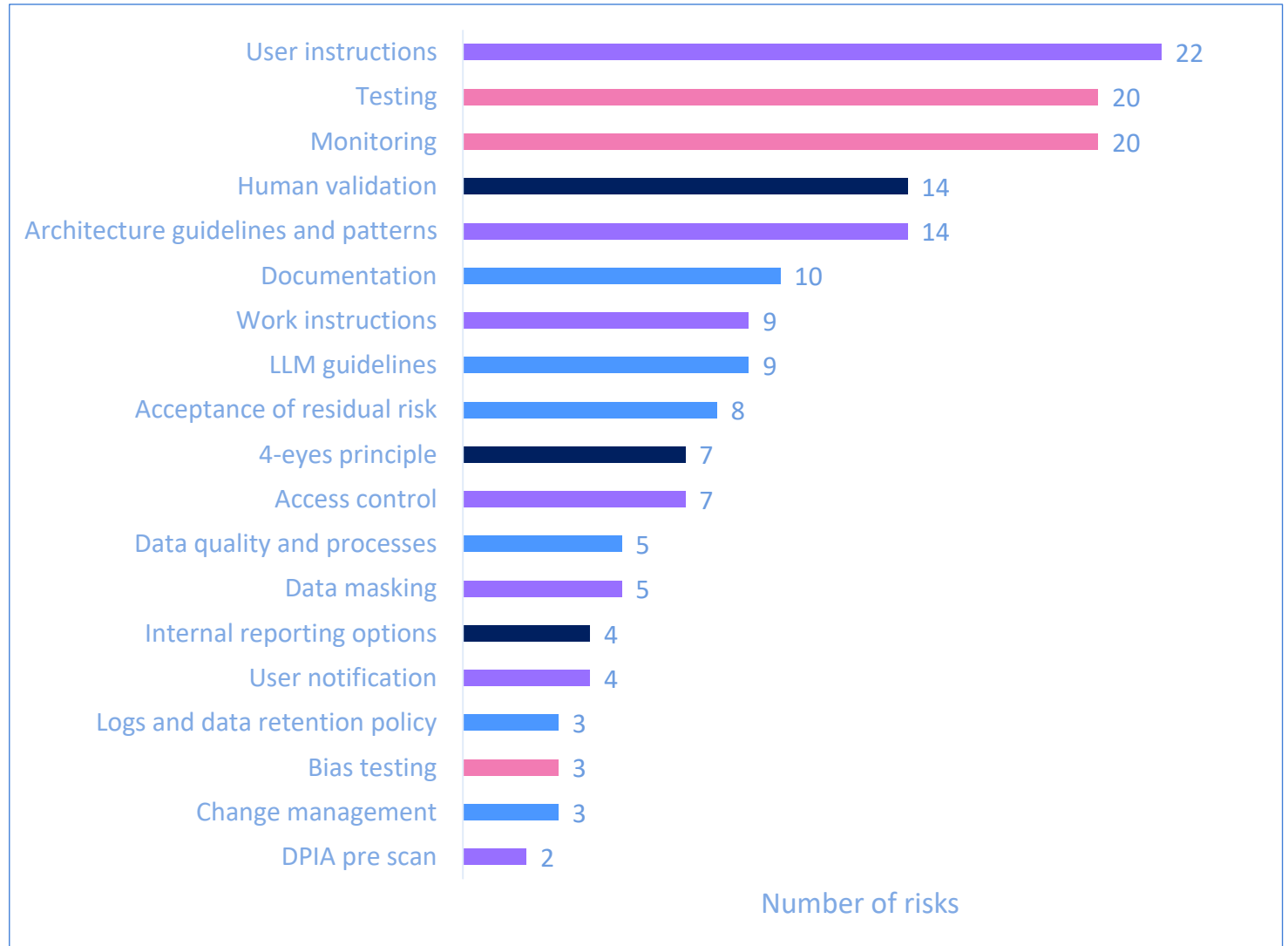
- Where **Net Risk** is not acceptable, additional controls are necessary
- Implementation of additional **Controls** will bring down the Net Risk
- In the end, the remaining **Rest Risk** has to be accepted



# For the relevant risks, we determined the likelihood and impact



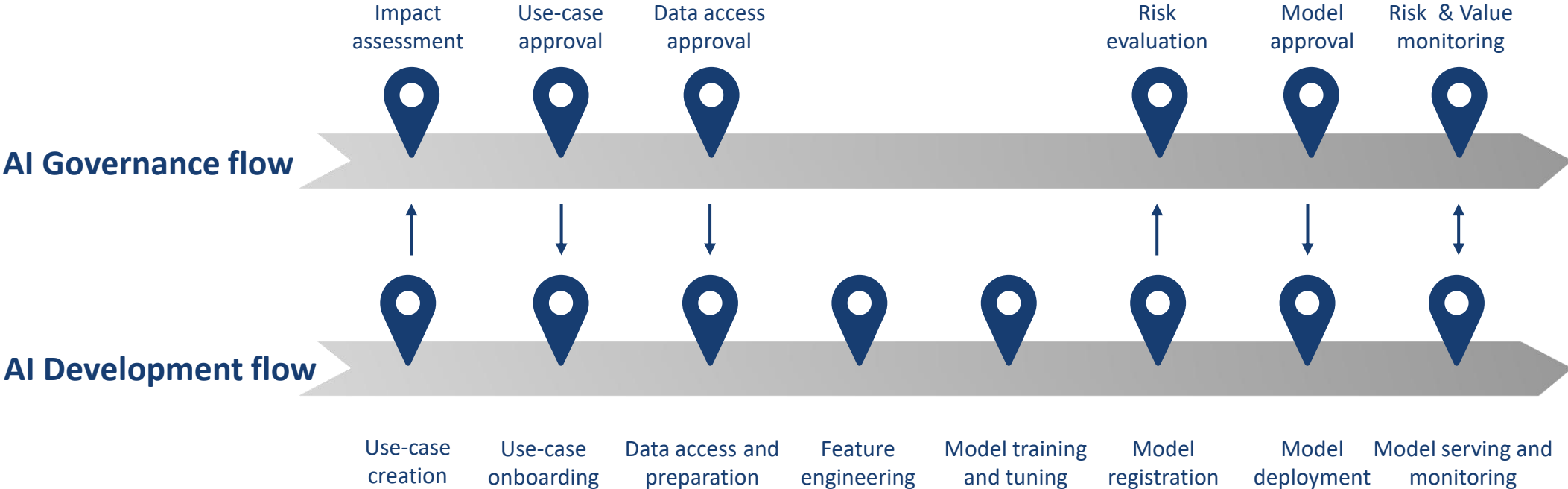
# To make the framework operational, we added a taxonomy of controls



# Key metrics: from confusion to clarity

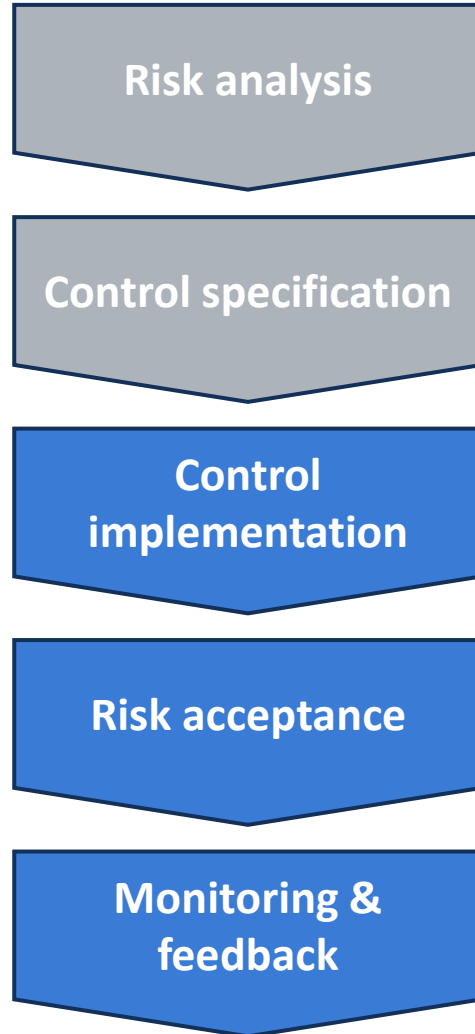


# The framework enhances existing development and governance flows



# We defined ownership principles and a risk management playbook

## Implementation steps



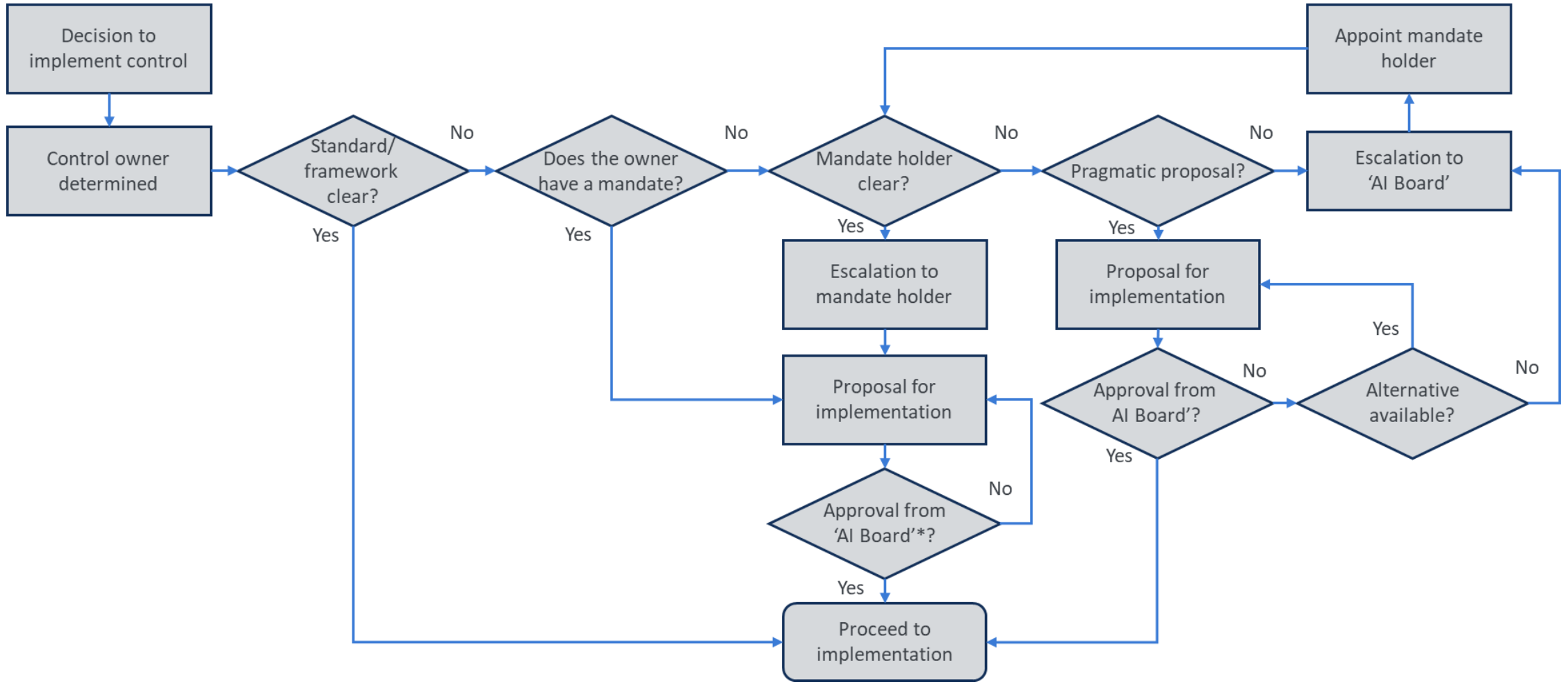
## Ownership principles

- Accountability for **individual controls** (implementation, operation, effectiveness) dependent on the nature of the measure. For example:
  - Model monitoring: Product Tech Lead
  - AI literacy: Business Team Lead
- Accountability for **risk acceptance** lies with the Business Owner (with exception of cross-functional risks)
- Accountability for **oversight and coordination** lies with the Product Owner

## Risk Mitigation Action Plan



# Example: clarifying approval decision flows where norms are missing



\*Typically represented in the AI Board: Tech, Security, Data, Legal, Ethics, Risk, Business.



# Value delivered

**01.**



The new framework created a clear path for the GenAI use case moving into production in a safe, controlled, and responsible way.

**02.**



The organization now has a clear and repeatable approach for assessing and operationalizing GenAI use cases. Risks are transparent, responsibilities are clearly defined, and control requirements are concrete and actionable.

**03.**



Internal discussions shifted from abstract concerns to joint execution, enabling teams to work together to bring GenAI into practice.

**04.**



The framework now serves as a foundation to scale GenAI across the organization, supporting a growing portfolio of use cases while maintaining trust, quality, and regulatory readiness.



# Don't focus on regulation alone!

**Any questions?**




# Call with our AI Act experts now!

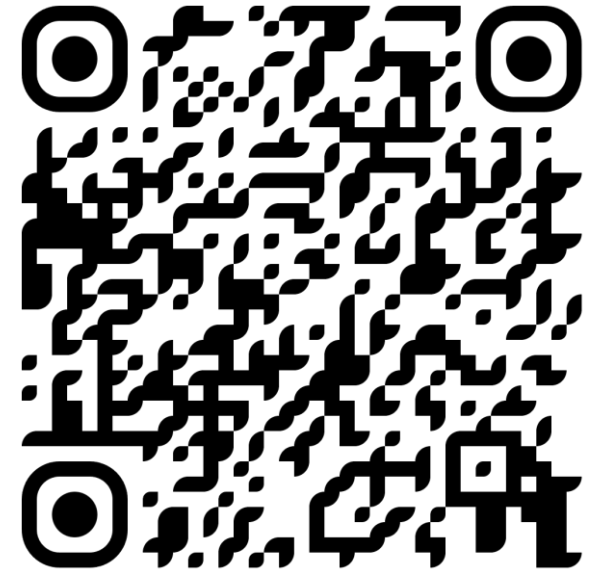
Don't wait for the next step

 Open to Webinar Participants

 Complete Application Form

 Share topic you want to talk about

<https://links.nemko.com/scaling-ai-offer>




Scan to apply

# Stay updated!

 **Nemko Digital**  
1,338 followers  
[Visit website](#)  
1w • 🌐

Germany's real estate sector, renowned for its inspection excellence, is navigating a new frontier: #DigitalTrust. As buildings transform, understanding the interplay between traditional safety and modern digital solutions is key.

 **Nemko Digital**  
1,338 followers  
[Visit website](#)  
23h • 🌐

As AI enters physical products, compliance is changing. Learn how product regulation, the EU AI Act & safety rules intersect for embedded AI systems. ...more

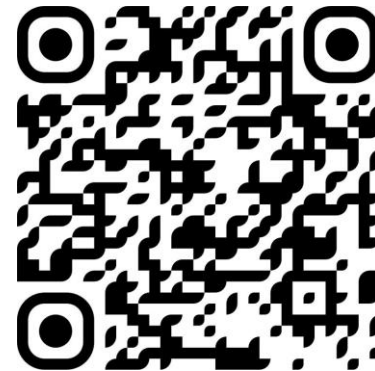


**Dissecting What's  
Needed to Scale  
Agentic AI with  
Confidence**



**The AI Trust  
Standard** *Newsletter*

Your Monthly Update on **Responsible AI**



Follow us

Nemko Digital Newsletter

**Product Regulation in the Age of Embedded AI**

Nemko Digital





**Nemko**  
Digital