

# AI in Control

Shedding light on the dark side of the moon

June 2023

Artificial intelligence (AI) systems have been steadily increasing their presence across all industry sectors. Our research shows that four out of five organizations have set AI as a top strategic priority, while almost all believe that AI is key to gaining competitive advantage in the market.

## AI adoption: the benefits and the risks

The media sector is using AI to detect fake news; organizations in the healthcare sector to run diagnoses; in the energy sector, companies employ smart grid algorithms to optimally distribute energy supply; the public sector uses AI systems to allocate children to schools. The benefits from AI systems seem overwhelming - except when something goes wrong!



We have already seen it with AI software used in self-driving cars that led to fatal accidents, with HR recruiting tools that were reported to be gender-biased, with chatbots that became racist within a day, with AI systems used in hospitals that were giving erroneous cancer treatment advice, or with face ID software that was easily fooled by 3D-printed masks. When AI systems do not perform as expected, a company or organization is very likely to be open to considerable damage - financial, reputational or legal.

# Why traditional IT controls are not enough

Controlling and safeguarding AI systems requires going beyond traditional IT controls. This is primarily due to two main reasons:

## Training Data

AI systems build themselves using data. Raw data, pre-processed data, transformed data or combinations of datasets are fed into the AI systems and train them in order to perform a task. In other words, the decision-making mechanism of an AI system relies often on statistical properties of the training data. If, for instance, training data encode racial bias, then the AI system will also show racial bias in its decisions. This is why new controls need to account for the statistical profiling of data, e.g. for outliers or heavily imbalanced classes; they must ensure that unfair treatment of certain protected groups is avoided and that results are free of bias and compliant with the company's policies and principles.

## Machine Learning Algorithms

The inner structure of AI systems is often based on complex algorithms and mathematical models, which offer no visibility on how decisions or predictions are made. For instance, an AI system that helps predict heart disease from patient records might be incapable of pointing to the exact patient data that led it to its prediction. This is why we need to put in place tools, methods and controls so that the underlying machine learning algorithms of AI systems are explainable, fair, agile and secure from harm or adversarial attacks.

## Are you in control?



Are you aware of the risks which the use of artificial intelligence algorithms entails?

Can you explain the algorithm-based decision to a customer or regulator so that they understand?



Are responsibilities around AI systems clearly defined and assigned?

Is there a consistent and scalable set of tools that would safeguard the uninterrupted use of AI algorithms against high demand?



Are the algorithm-based decisions in line with your ethics, value and brand?

Do you have data-driven control processes in place that monitor AI algorithms and detect when they begin to perform below an acceptable threshold?



# Our experience at your service

## Our framework

KPMG's **AI In Control Management framework** covering **17 categories** for managing risks and controls for AI solutions.

- We have identified **75 potential risks** across 17 different areas, and have defined **106 typical controls** that would help manage these risks.
- We have mapped these against the **37 COBIT processes** as well to ensure alignment to this widely accepted good practice governance and control framework.

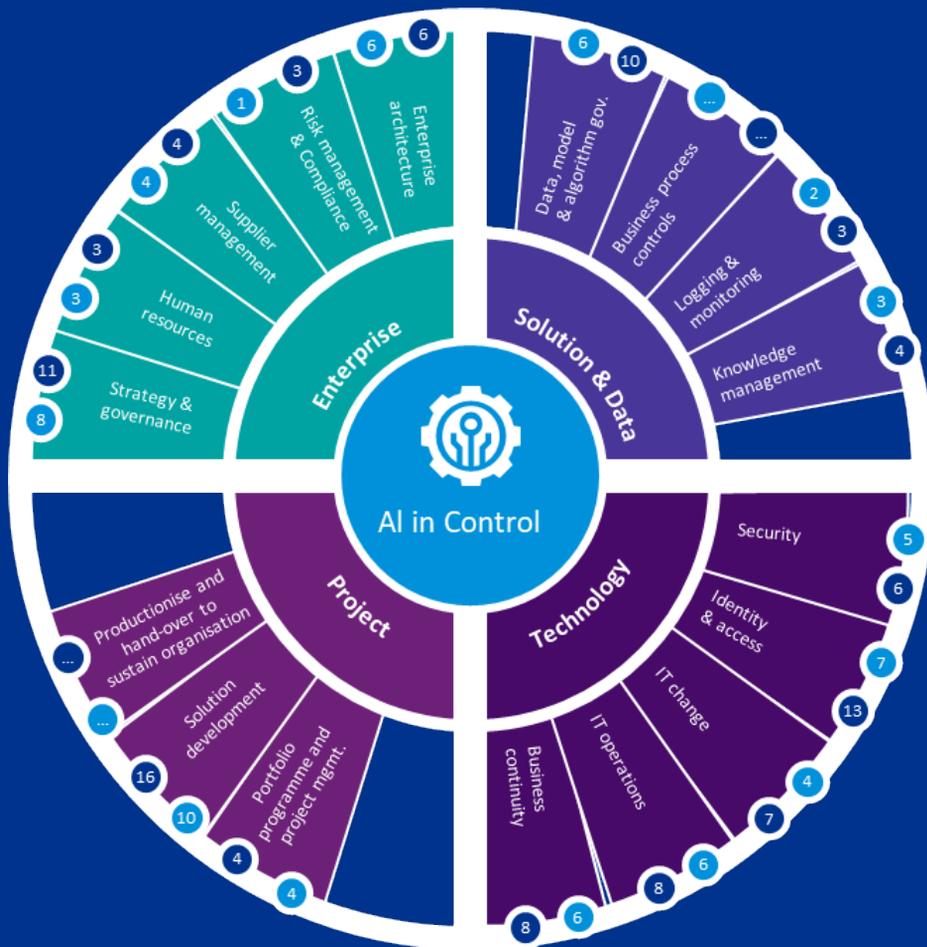
## Our services

### AI Governance Assessment

Evaluation and assessment of current AI solution using a bottom-up approach in evaluating the AI roadmap, policies, processes, and controls associated with (a) given model(s).

### AI Governance Implementation

Design and implementation of AI governance and operating model including the AI strategy, policies, processes and controls to support trusted AI objectives.



# Why KPMG?

## Subject Matter Expertise

Our dedicated team offers a unique combination of experienced professionals with expertise in artificial intelligence (AI) and audit technology. Together with their extensive experience across multiple industries, they know how to deliver assessments of AI solutions so that they produce high-quality results and are safe.

## Market Understanding

Due to increased awareness of the risks related to the use of AI, numerous companies are assessing the quality of their AI solutions. We help them to ensure that business decisions and outcomes from AI systems are safe and of high quality. This results in a specialized, highly experienced team with extensive market expertise.

## Latest Best Practices

With our global network of qualified professionals, we are always up-to-date when it comes to new trends in relevant standards, tools or methodology. This information is continuously monitored and incorporated in all of our engagements.

## State-of-the-art Assessments

With AI Assessment, we conduct diagnostic reviews of AI solutions. We put in place tools, methods and controls to evaluate business-critical algorithms. We oversee design, implementation and operation of AI programs to help address AI's inherent challenges: integrity, explainability, fairness and agility.

## Leading Practise Frameworks

Using our experience and understanding of relevant processes, we have developed a Risk and Controls framework for AI solutions that includes 108 typical controls to manage 78 potential risks. This will enable professionals and AI practitioners to implement a holistic approach to managing the risks around the use of AI.

---

## Contacts

**KPMG AG**  
Badenerstrasse 172  
PO Box  
8036 Zurich

[kpmg.ch/data-quality](https://kpmg.ch/data-quality)



**Mark Meuldijk**  
Partner  
Data & Analytics and  
Intelligent GRC

+41 58 249 48 84  
[markmeuldijk@kpmg.com](mailto:markmeuldijk@kpmg.com)



**Manousos Theodosiou**  
Consultant  
Data & Analytics

+41 58 249 75 33  
[mtheodosiou@kpmg.com](mailto:mtheodosiou@kpmg.com)

---

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence. If you would like to know more about how KPMG AG processes personal data, please read our [Privacy Policy](#), which you can find on our homepage at [www.kpmg.ch](https://www.kpmg.ch).