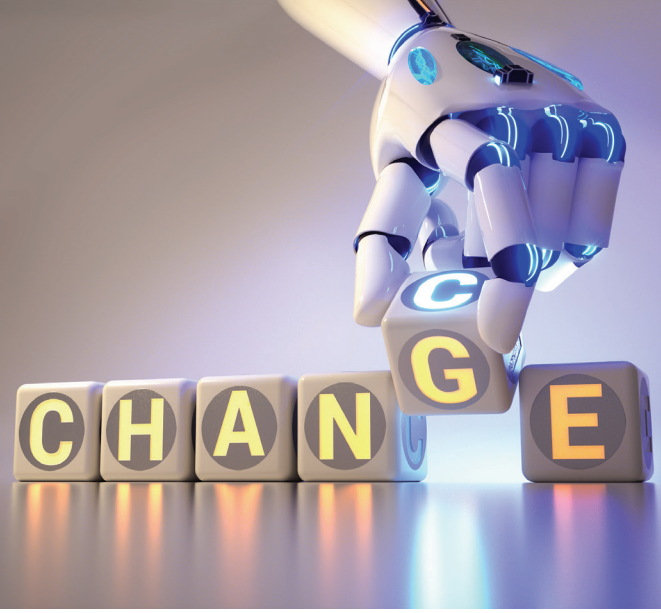
KPMG

Artificial Intelligence: Challenges for non-executive directors



Audit Committee Institute
Part of the KPMG Board Leadership Centre

Until recently Artificial Intelligence (AI) was considered something that would be available on a 3-5 year time horizon. However, the horizon has shifted: companies are exploiting AI today. We are seeing organisations adopting AI for specific use cases, with some at an advanced stage in some parts of their business. KPMG research suggests that within the next three years the 100 largest companies in the US expect to increase their annual spending to $15 billion on AI capabilities, double that of today.

According to KPMG's Guardians of Trust report, 2018, gaining trust around AI is a top goal of leaders: 45% of surveyed executives say that trusting AI systems was either challenging or very challenging in their organisation. However the same report found that most leaders were unclear on what an AI governance approach should be. Some 70% say they don't know how to govern algorithms. Executives worry about the impact that bad or unethical machine-driven decisions would have on their brand reputation. They want to understand the 'how' and 'why' behind complex decisions made in so-called black boxes.

Control Framework

In addition, we expect to see new policy initiatives and regulations around data and AI: the end of self-regulation and the rise of a new oversight model. In the US, the 'Algorithmic Accountability Act' bill has been published as a potential approach. And the European Parliament has asked the European Commission to consider an international approach to regulation of algorithms.

Investing in a control framework, including methodologies and a toolset that can help business users gain control over their AI programmes will be key to building trust.

The control framework will need to address:

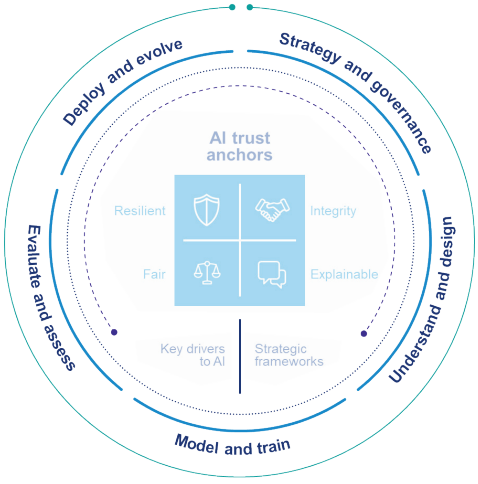
— Gaps in corporate governance: "Is this in line with the organisation's ethics & values?"

— Lack of explainability: "How do I to explain this to the customer (or regulator)?"

— AI getting decisions wrong: "Am I at risk of approving/rejecting the wrong things?"

— AI getting out of control: "Can we stay in control of the decisions it makes?"

This requires securing four trust anchors: integrity, explainability, fairness, and resilience.



The goal is to seamlessly maintain these anchors throughout the entire AI lifecycle, from strategy and use case ideation, through model build and training, through continuous monitoring and operations to further development of the model. However based on KPMG's AI 100 survey, many companies are just beginning to focus on this compared to other deployment priorities; only a handful of the more mature organizations already have these frameworks in place.

This is compounded because AI development typically relies on Agile development techniques. In addition 'Devops' (combining software development with IT operations where traditional change controls are often not present) is a common approach to AI development.

Executives need full visibility of the various performance & operational metrics related to the trust imperatives of the AI models. They need to understand the key controls that failed when assessing a model, details of an assessment and also be able to request new assessments of models.

Risk professionals need access to a consistent set of methods and associated tools to be able to evaluate and assess AI models on all of the trust imperatives as well as all phases of a development. They should be able to analyse and record the findings in order to produce an exception report along with recommendations.

According to a report by Forrester Consulting on behalf of KPMG, 94% of businesses believe that adopting AI is the key to competitive advantage. However close to the same percentage (92%) question the trustworthiness of the data and analytics they receive.

Organisations need to recognise AI is happening now and will move very quickly. They need to seek to manage the risks and build in control from the start. Executives and AI leaders should be seeking guidance on setting the control environment and had AI systems audited prior to go-live.

Further reading

Guardians of Trust, KPMG, 2018

Trust in Artificial Intelligence, KPMG, 2018

Emerging technologies: An oversight tool, CAQ, 2018

Key challenges for non-executive directors to ask:

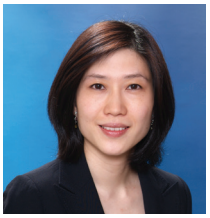
1. Who owns AI in the organisation? An AI Council? CTO? CFO? This will impact the direction of AI and also the level of focus on control as a concern.
2. Do you trust AI? What mechanisms have been put in place to provide you with assurance that you can trust AI? Have you considered the impact of negative press coverage if, for example, bias was found in your AI system?
3. Can you explain your models to Audit or to a regulator? If not, what basis do you have for confidence that the four trust anchors of integrity, explainability, fairness, and resilience are covered?
4. Is there governance, control and oversight of the development and delivery of AI solutions including agile development approaches, solution testing and release strategies and DevOps development?
5. How extensive is the use of AI in the organization? Do you know what AI is planned/has been implemented?
6. Are you including AI in the operation of business, financial, operational and IT controls? Are you satisfied this has been tested and have you considered integrity, explainability, fairness, and resilience?
7. How have you approached AI governance, considering the algorithm/model and the data that was used to train the model and on which it operates?
8. Do you have a control framework, methodologies and tools to assess and monitor AI?
9. Are Audit, Risk and Compliance functions engaged with AI projects to ensure control requirements are appropriately considered and embedded from the start?
10. Does the organisation have a strategy for the three lines of defense? What are the respective responsibilities of each line and is that well understood?
11. Is there an audit strategy for AI? How are you aligning sources of assurance to make best use of resources?
12. Have you considered what you need in terms of people, process and technology to articulate clear control requirements to AI programmes and to audit AI solutions?

Contact us

Henry Shek
Head of ITA Risk Consulting
KPMG China
+852 2143 8799
henry.shek@kpmg.com

Richard Zhang
Partner, ITA, Cybersecurity
KPMG China
+86 (21) 2212 3637
richard.zhang@kpmg.com

Li Fern Woo
Head of IARCS CN
KPMG China
+86 (21) 2212 2603
lifern.woo@kpmg.com



Alva Lee
Head of IARCS HK
KPMG China
+852 2143 8764
alva.lee@kpmg.com

kpmg.com/cn/socialmedia

For a list of KPMG China offices, please scan the
QR code or visit our website: https://home.kpmg.com/cn/en/home/about/offices.html

You can learn more about
KPMG Board Leadership Centre via the QR code