KPMG

Why AI must be included in audits

By Paul Holland, Shamus Rae and Paul Taylor

Artificial intelligence has been with us for much longer than most people think.

It's now over 20 years since the IBM supercomputer Deep Blue beat chess champion Garry Kasparov, a milestone moment when we began to wake up to the fact that a computer can match - and then outdo - what a human can.

Since then, the conversation has largely been confined to the halls of academia and the secret labs of technology companies. It's only very recently that we have begun to see what AI can do in the real world.

For instance, JP Morgan's COntract INtelligence AI system (COIN) is an AI-system that has saved thousands of hours of work reviewing financial deals. In 2016, Apple supplier Foxconn replaced 60,000 factory workers with robots, and in late 2015, the Bank of England was already predicting the loss of 15 million UK jobs to automation.

Indeed, nations are racing to be the first to conquer the possibilities of AI, with China currently pulling out in front.

The question for every business and every industry is: Are you ready for AI?

The pace of change

We are currently experiencing technological advances at a rate never seen before.

In the next five to 15 years, we will likely see the Internet of Things permeate our homes and robots and drones delivering our parcels. There will be smart robots, quantum computing, 4D printing and even a brain-computer interface.

The technology innovation curve is accelerating along with the adoption curve. In other words, just as we take delivery of our new iPhone X, we are already thinking about what comes next. The time it takes from researching a product to it appearing on the market is also dramatically reducing.

Deciding which of these technological breakthroughs is strategically important to a business depends entirely on the individual organisation and the industry it operates in.

But there are certain elements, such as mobile technology, data analytics, digital payments, cloud and cyber security, that switched-on businesses will have already adopted or begun to adopt.

KPMG's Outlook survey tells us that over half of CEOs believe that their organisations will face more disruption in the next three years than they have done in the last 50.

In previous CEO surveys, CEOs understood how fast things can change but they also underestimated the impact of technology. In this latest survey, two thirds saw disruption as an opportunity and believed they needed to disrupt their business, but only a quarter had a Chief Digital Officer.

AI as opportunity – and threat

While AI presents businesses with significant opportunities to enhance their operations, its capabilities are just as attractive to cyber criminals.

AI and machine learning will improve the ability and increase the speed with which hackers can find weaknesses within networks. They will be able to automate the mounting of probes for attacks and their ability to test and develop new malware will also be enhanced.

Machine learning could also be used to hone the language of phishing attacks – one of the biggest threats to businesses – into something that sounds so natural that it will be almost indistinguishable from the real thing.

Of course, those involved on the front line of defending businesses from such attacks can also employ the services of AI and machine learning to stay one step ahead, plugging any network and system gaps before the criminals find them.

Monitoring the AI

There are two questions that an internal audit function typically asks: Audit of AI - looking at all the uses of AI in the organisation, or Audit with AI - using AI to improve internal risk processes.

In Audit of AI, we see businesses do everything from nothing to a high level of governance and risk assessment. But we've seen only a handful of cases where businesses have an audit programme defined and piloted.

In Audit with AI there are four possible use cases. The audit process (quality review and reporting); risk assessment (identifying risks using data); audit delivery (identify previously unseen patterns) and first line (continuous monitoring and alert systems).

At our IT internal audit conferences, we perform a snap poll which aims to gauge our client's internal audit's involvement with managing risks around their organisation's AI solutions.

While over half said that AI was already being used, 80% said they were not confident of its governance, and 45% planned to perform an audit on their AI solutions.

90% agreed that the AI function should be involved and that AI projects should be subject to internal audits. But 70% admitted that they weren't clear on what their audit approach should be.

Clear alignment

KPMG has developed a risk and control framework which looks at 17 categories for managing risks and controls for AI solutions. We identified 78 risks in total, and 106 controls.

The important areas to look at include things like strategy, governance, human resource management, security management, and IT operations.

For instance, how are AI initiatives aligned to enterprise strategy and how is innovation driven? Who in the organisation will be responsible for the use of AI and any mistakes it makes? How will you protect against new AI threats, and how will you manage the AI inventory?

Businesses must approach AI with a focus on specific areas. Do we know what the risks are, the controls we need and how we would audit them? Is the audit function influencing the strategy of 3 lines of defence, and can it clearly articulate its own strategy?

AI is no longer a theoretical possibility; it's here. It will continue to evolve, presenting us with great opportunities, but also a whole new set of risks to consider.

Now is the time for internal auditors to play a leading role, get fully involved, and help their businesses get it right from the outset.

kpmg.com/socialmedia