Risky business

Managing risks in the dynamic digital era

Introducing automation into risk management processes is a complex task; and many challenges exist, which inhibit effective and long-lasting results.

Today's organizations are racing to cope with rapid change, increasing data volumes, and a desire to leverage data, to deliver business goals. In order to remain competitive and accommodate change, organizations are embarking on digital transformation journeys which are revolutionizing systems, processes, and teams through the implementation of analytics, robotics, and automation. The rush to automate starts by embracing digital tools that aim to improve processes and contribute to the collection and storage of data, which enable strategic and informed business decision-making. Digitization plays another essential role and enhances the customer experience by creating more dynamic touchpoints between the service provider and the user.

Introducing automation into risk management processes is a complex task; and many challenges exist, which inhibit effective and long-lasting results. Challenges span across people, processes, and technology, which range from underestimation of budgets required to enable automation, poor development and training of employees, and the desire from senior management to rapidly realize results. A final key risk that is often overlooked is data quality. Dealing with poor data quality residing in systems is key to success; clean and well managed data is a priority to ensure delivery of objectives. These high barriers to entry often cause reluctance to adopt technology amongst risk management specialists and internal audit (IA) professionals.

Challenges of introducing automation into risk management include:

- Significant budget required;
- Extensive collaboration with IT and data teams;
- Poorly defined vision and target state;
- Sufficient change management which ensures IA data requests accommodate business and technology changes;
- IA Op Model change;
- Training and repositioning of IA employees; and
- Poor data quality in source systems.

How would technology help IA functions deliver improved services?
A technology-driven IA approach and team leveraging the emerging trends enables the function to adapt a more integrated approach across lines of defense, deliver more value, and significantly increase efficiency.

Data/risk analytics
Internal audit functions are transitioning to data-driven operations; however, the adoption is slow and most are only embedding descriptive analytics and visualization into existing audits and processes to automate testing. Whilst embedding analytics in this fashion allows for full population testing across databases, it only enhances findings at the time of audit and does not offer immediate value to first and second lines of defense.

Technology solutions including continuous monitoring and process mining combined with an effective operating model offer value to both IA and first and second lines of defense, as issues are identified in real-time and are remediated as they occur. Moreover, IA can focus on what matters and reduce the costs of their standard operations.

Continuous control monitoring (CCM) is a technology-based solution which leverages data to continuously monitor processes and control failures. CCM empowers and enables the first line to own and operate their operational processes, while retaining transparency and audit trail. This trail, in turn, allows the second and third lines of defense to monitor first-line activities, thus eliminating redundancies in testing and associated costs.

Process mining monitors data within systems to reveal an end-to-end view of what is actually happening during processes and whether policies are being broken. However, the real value arises as monitoring identifies process inefficiencies and opportunities to streamline processes to drive business value.

Utilizing advanced analytics in specific scenarios, such as process mining and controls monitoring, deliver a proactive approach to IA which allows IA teams to predict and prepare for future risks before materializing, whilst adding business value.

Artificial intelligence (AI)

Artificial intelligence, which uses machine learning techniques, can be defined as the simulation of human intelligence by computers and machines which handle complex tasks by following a set of rules known as an algorithm.

Given that technology trends are a main driver in today's risk management functions, what would be more beneficial than adopting the AI trend in analyzing the huge amounts of data and identifying patterns and key points that may take hours by an internal auditor to perform? AI and risk management professionals would work in parallel. The first would provide, in an efficient manner, the key insights around the area to be analyzed, while the second would still make the judgment and derive the final result.

Embarking the transformation

Looking ahead, on the breadth of demands on internal audit, and pace and scale of innovation in the profession, point to the need for an update, but not an overhaul. To assist organizations in this journey, Deloitte's Internal Audit 4.0 framework:

- Starts with purpose and the notion of aligning internal audit activities to the organization's purpose, vision, and strategy.
- Challenges internal audit functions to add the "Accelerate" component on top of the "Assure," "Advise," and "Anticipate" components of the framework (as shown in the illustration) to the remit to support organizational learning and management action in ways that match today's pace of change.
- Fully embraces the use of digital technologies across all aspects of the function to help drive insights, collaboration, quality, and productivity.
- Promotes a continuous improvement mindset that enables agility and digitalization through encouraging purposeful and structured focus on incremental improvement.
- Outlines the key principles and building blocks that functions need to consider as they design, build, and evolve their operating models.

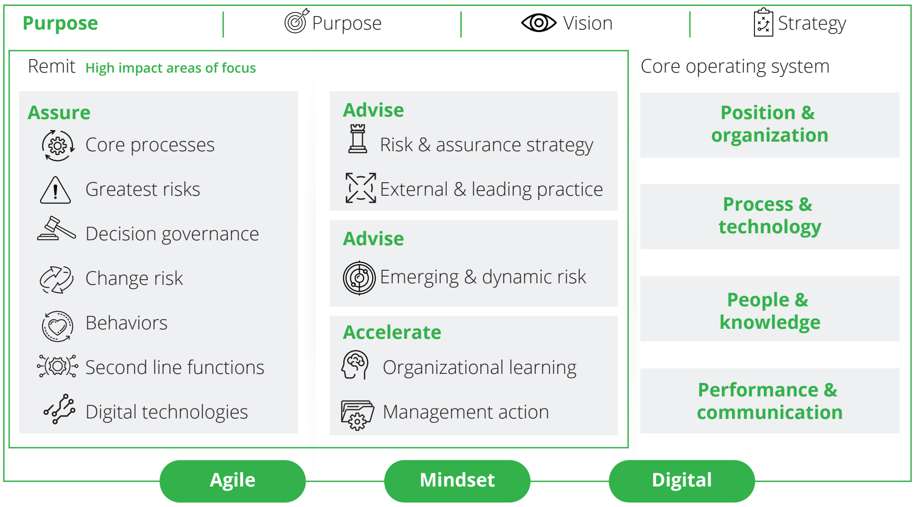

Figure 1: Internal Audit 4.0

While internal auditors might perceive the digitization of the internal audit function and capabilities as a risk for their professions, it is in fact an opportunity to transition from the traditional tasks into more value adding activities. As automation is applied on IA methodologies and techniques, results including efficient risk management, cost reduction, and increased productivity are realized. We no longer see it as a set of activities leading to reporting identified issues, but more as working hand-in-hand with different business units to help them improve, and with top management to support in making strategic decisions.

With that having been said, isn't it the right time for auditors and risk management professional to shift their mindset, embrace innovation, and surf the transformation wave? ●

By **Ziad El Haddad**, Partner, **Daniel Brierley**, Director and **Rabih El Sabaa**, Senior Manager, Risk Advisory, Deloitte Middle East