How Continuous Monitoring Can Drive Better, Higher-Integrity Business Processes

With so much emphasis on compliance and governance, organizations are putting more attention than ever on ensuring that they are closely aligned with regulatory and internal process governance guidelines. With the right tools, and the right experience and expertise, continuous monitoring can be key to ensuring high-integrity business processes, enabling transparency with both internal and external stakeholders, and avoiding potential sources of waste and abuse.

Business processes and workflows have become more interconnected and, thus, more complex than ever. The proliferation of data, driven by a startling expansion of data sources, devices, services, tools and ERP systems, has made it more difficult to ensure that organizations are doing everything they can to reduce risk and avoid running into potential compliance and governance slip-ups—not to mention bottom-line losses.

Smart, well-intentioned organizations take great pains to put the right controls, policies and procedures in place to cover the key elements of any business process, including people, third parties and technology. But detecting data anomalies and unexpected, irregular behavior by users throughout the full span of business processes is challenging. Failure to properly detect unusual, high-volume data movement carries potentially high financial, legal, operational and reputational costs.

Whether we're talking about processes for external activities such as procurement and supplier onboarding and monitoring, or internal activities such as travel/expense monitoring, organizations are running into risks that are more complex, harder to detect and more burdensome. Until fairly recently, many organizations attempted to monitor and remediate issues manually with dedicated staff and fairly rudimentary tools such as spreadsheets or reporting software on a quarterly basis using sample data. But the spiraling complexity of these and other business processes has rendered those early remedies ineffective.

Fortunately, new tools have been introduced to provide continuous monitoring (CM) of these processes to detect and root out potential fraud and other risks. These solutions are automated, intelligent, context-aware, cost-effective and tightly tied into even the most interconnected sets of business processes.

sas | KPMG

TechTarget Custom Media

Why use CM to address business process-related risks

The question of whether to continuously monitor processes, controls and activities to ensure compliance and governance has been rendered moot by the sheer size and complexity of the procurement and supply chain environment. Organizations no longer have the option of deploying CM practices when they consider the increasing number of local, national and global mandates, as well as the growing number of industry requirements for risk management and sustainability.

Instead, the key issue organizations are wrestling with is the role that CM plays in the modern—and future—business environment. While compliance and good corporate governance certainly are key drivers for CM, at least as important is the need for smarter, more efficient and more comprehensive risk mitigation and management. With the pace of global business operations accelerating at a harrowing rate, organizations no longer have the luxury of reviewing data movement and user behavior in anything other than real time.

Additionally, organizations need their CM efforts to tightly integrate into all key business operations in order to spot and clamp down on risks and identify their sources. One factor making CM more essential is the harsh reality that much fraud and other inappropriate behavior takes place with the help of internal bad actors, not just outsiders hacking into systems. Identifying the source of collusion is a major requirement for any system, technology or process. This could mean overcoming the taboo that a manager you hired 10 years ago could be part of a fraud.

There also is the challenge associated with tightly interconnected and interdependent processes that, without CM-enabled controls, can be exploited faster than ever. Internal audits or other periodic assessments of processes and controls can miss an unacceptably large number of potential breaches, and can make it difficult to determine if anomalous behavior is inadvertent or intentional.

This requires CM approaches to be built upon, and driven by, sophisticated analytics that help spot what other controls may miss, or whether additional controls may be required.

Finally, it's important to understand that there are more real-world use cases for CM than ever. For instance, CM has long been an important defense mechanism for card and payment fraud (for cybersecurity), simply because the attack vectors were rapidly expanding and internal controls, tools, processes and people were often insufficient to keep up.

Process-to-pay systems is another area where CM has become more important. These include supplier onboarding, supplier invoice payments, contract compliance, employee expense processing (i.e., Purchase Cards, or P-CARDS), and more. Sustainability also has become a critical area where CM can pay major dividends, such as monitoring suppliers' and third parties' own efforts to conform with an organization's environmental, social and governance (ESG) mandates.

Supply chain management is another, highly complex use case where CM can pay big dividends. From the original manufacturer to the warehouse, and from the logistics supplier to the retailer to the consumer, there are many points along the way where the potential for either intentional fraud or simple human error pops up. When that does happen, organizations need to know about it and be prepared to act immediately.

Planning and deploying the right solution

The good news is that CM is fast becoming more widely understood, accepted, adopted and deployed as a way to ensure proper controls for organizational processes and systems are in place to help organizations reduce risks. The challenge, however, is that comparing systems from different technology partners is difficult because of the different philosophies and technologies of those partners.

Instead, organizations should look for open and interoperable analytics-based CM solutions that map to a set of capabilities proven to help identify, block and mitigate the impact of those risks. Those capabilities include:

- Efficient and comprehensive triage and prioritization of true positives based on integrated machine learning tools that build upon knowledge gained from past experiences.
- An emphasis upon data cleansing and data quality—in particular, supplier and item duplication.
- Designs built upon usability, with "soft IT" skills built into the CM solution based on input from subject-matter experts. These include detection scenarios and models, as well as pre-canned workflows and reports.
- Easy customization so users can create and change rules based on rapidly changing experiences. Interfaces, workflows and other issues must be quickly and easily adaptable with a business-friendly user interface for users that are not IT experts.
- Improved and heightened alert detection rules instead of static dashboards, since bad actors are constantly upping their games when it comes to finding ways to beat the systems.
- Tight integration of technologies with innovative services and proven expertise in workflows, compliance, governance practices and more.
- Delivery of an end-to-end solution that integrates into existing infrastructures and augments current capabilities, from solutions conceptualization and planning through development, deployment and fine-tuning.

Merging tools, process knowledge and business acumen: The SAS and KPMG alliance

In order to properly plan, build and deploy a flexible, analytics-driven and automated CM solution for a wide range of use cases, organizations need to ensure they are working with partners with the full range of capabilities. Those should include technologies, process expertise, in-depth knowledge of compliance and governance, deployment expertise and the ability to work closely with both IT and business leaders.

SAS and KPMG have collaborated to design and implement a number of CM solutions built upon SAS's data analytics platform and KPMG professionals' experience in compliance, risk management, consulting, and investigation and forensics services. The two companies have a well-established track record in deploying CM solutions for numerous use cases, such as procurement integrity, supplier integrity, sustainability and employee expense transactions, to name just a few. Their collaborative efforts help provide a synergistic solution that far exceeds what an in-house-deployed and -managed solution typically can achieve.

SAS and KPMG provide continuous monitoring based on SAS Viya, a powerful data analytics platform that drives CM by:

- Automating explainability and interpretability.
- Facilitating access to authorized data sources such as EDP systems.
- Efficiently storing and archiving large volumes of unstructured and structured data.
- Surfacing actionable analytics.
- Preparing a comprehensive and accurate model inventory.
- Documenting analytics consumption controls.
- Providing a complete view of environmental governance and monitoring.
- Automating documentation processes.
- Delivering both active and passive analytical process management.

SAS Viya is the open analytics platform for all phases of a typical model development lifecycle, leveraging automation and cloud efficiencies to relieve the long-standing and growing pressures on in-house staff and infrastructure.

KPMG, a SAS Platinum partner, leverages its 3,000-plus network of forensics professionals to customize a CM solution based on a number of factors, including the industry served, geographies covered and client-specific goals and challenges.

KPMG firms have a well-established history of working with both business executives and IT leaders to efficiently marry CM solutions with operational, regulatory and governance goals, with a special emphasis on risk management and mitigation. KPMG professionals support clients in executive-level conversations and risk detection investigations, including assessments and analysis, using well-documented methodologies that are applied according to a number of local compliance requirements.

The combination of SAS Viya's analytics strengths and KPMG professionals' consulting, forensics and deployment experience gives customers confidence that their CM solutions can help reduce risk and improve business outcomes across a range of use cases.

Conclusion

Without CM tools, systems and end-to-end solutions based upon sophisticated data analytics and real-world experience, organizations will continue to face higher degrees of fraud risks and will struggle to identify and prevent these risks before they make an impact.

CM solutions should be based on the principles of automation, interoperability, contextual awareness, real-time detection and response, alert triage and alignment with an organization's key business objectives. Doing so requires a proven mix of technology, process awareness and business consulting that creates confidence among business executives, technology leaders and board members.

SAS and KPMG have forged a strong alliance that delivers CM for a wide range of use cases. SAS' leadership in data analytics and KPMG firms' history of compliance, risk management and SAS solution deployment offers organizations a tightly integrated solution that closely aligns with key business goals and with other corporate systems.

The result is proactive detection, investigation and mitigation of potential fraud and other risks at any point in an organization's business processes, controls and workflows.

For more information on how SAS and KPMG can help your organization with modernized CM solutions, please visit www.sas.com/cm4pi.