How digitization is strengthening compliance and anti-fraud programs

Detect anomalies early and accurately. Predict and prevent recurrence

Carolina Macri
Associate Partner | EY Forensic & Integrity Services | Global Center of Excellence for HANA Solutions

Tomás Kong
Finance and GRC Solution Management | SAP

White paper

Table of contents

Digitization is working everywhere

There is little doubt that digitalization is changing almost every business process in every industry. It is already making a huge difference to established leaders in the hospitality, banking, and transportation sectors. It is also helping market entrants with new business models rapidly gain market share. Even traditional sectors such as automotive and utilities, historically protected by heavy asset investments, are beginning to see major disruptions to their business models and their positions in the market.

Digitalization enables new products and services to be created in flexible ways, ensuring that offerings are designed around consumer needs — think transportation services instead of car sales — and industry boundaries are blurred. The enterprise of the future will be defined more by how well it serves its customers than by the goods or services it offers.

Digitalization creates both opportunities and threats; it remains to be seen who will be the winners or even the survivors. But one thing is certain: change is inevitable. Organizations know this and there's a clear sense of urgency. Almost every major company we have worked with in the past two years is undertaking some kind of digital transformation initiative and this is receiving management attention at the highest level. Business processes are being rethought and new business models tested. The world of business IT is shifting from being a cost center, ready for outsourcing, to a potentially critical competitive weapon. We have seen internal start-ups, strategic acquisitions, and even companies where procurement processes have been simplified just to allow digital transformation to progress more swiftly.

A chief compliance officer's nightmare

Business processes are being redefined at an incredible speed: B2B transactions are now being performed electronically, with little to no human intervention. For example, SAP's Ariba solution now has three million companies connected to automate their B2B transactions. Mobile devices and sensors are being integrated with enterprise systems, making them sensitive to even small events in the real world. Computing power and algorithms are making sense of all this newly accessible data, delivering a higher degree of automation and enabling better decision-making. At the same time, an increasing proportion of value chain functions are being performed in fluid business networks formed by multiple organizations and even freelancers.

Transaction sizes are becoming smaller, as the overhead costs per transaction (increasingly electronic) decrease, further reducing human intervention and control. We are also seeing regulators and, increasingly, the public through social media, holding companies accountable for compliance violations within these value chains. This can easily become a chief compliance officer's (CCO's) nightmare.

What to do about it

Traditional compliance and fraud prevention programs are built on four-eyes principles, management oversight, and sign-offs. Add that to occasional, often inconsistent audits and the resulting systems fall short of meeting these new challenges. They are simply too slow, too ineffective, and too expensive.

How do other sectors deal with this new category of challenges? Social networks for example, are facing increasing tough regulatory issues. Operating in a fluid, fast-moving and often anonymous environment from the beginning, these businesses have never relied on traditional methods of ensuring compliance. Despite being far from perfect, there is much to learn from them. The compliance programs of social networks, as well as large e-commerce players, rely on two pillars: community integrity and the significant use of sophisticated algorithms.

Community integrity builds on most people's natural desire to keep a community "clean", as long as they feel that the community is worth being kept that way. Every member is encouraged to raise or even correct violations, supported by a high degree of transparency. With Wikipedia for example, the community effect works remarkably well, especially considering it does not even require contributors to register with their real names. The corporate equivalent is employees embracing integrity in everything they do, ensuring transparency and fostering a culture of speaking up. Employees will actively work to keep the company on the right path out of the desire to "do the right thing". However, this commitment to integrity needs to go beyond words. Leadership needs to set an example, a culture of transparency and fairness must be established, and promotions – as well as incentives – need to reflect how results have been achieved, not just the results alone.

The second pillar is the use of modern technology. Companies can use the same technologies that revolutionize their business processes to protect and strengthen their compliance, integrity, and anti-fraud programs and to take them to the next level. Digitalization provides extended analytical capabilities and intelligent algorithms to help screen huge volumes of data automatically. It also enables the identification of problematic transactions with greater accuracy than any manual effort. These algorithms can be used to eventually analyze every transaction as it happens – making split-second decisions on which to pass – and which to interrogate for further analysis. There is little room for error: too many missed exceptions and the system fails, whereas too many false positives could seriously harm a company's business.

Many CCOs and heads of internal audit understand this very well. Their challenge is to turn this vision into reality, but most have neither the requisite budgets nor the required technical skills within their teams. The exception is where catastrophic events have forced a company into swift and decisive action.

Making it work

Making the transition to the next level of business integrity management cannot be achieved by compliance/audit departments alone. Instead, capabilities that enforce compliance, prevent fraud and detect errors need to be deeply embedded into every aspect of a company's operations. If a software system could prevent somebody — or a malicious or defective algorithm — from doing the wrong thing, it eventually has to actually do it. For that to happen, large amounts of data need to be constantly analyzed to identify errors, initial signs of major risks and suspicious patterns. Whenever possible, the reaction needs to be swift, so that intervention can occur before damage is done.

These are not just design criteria for a fraud detection system, they should be criteria for any comprehensive enterprise solution. Capabilities that meet compliance and fraud prevention requirements need to become integrated elements of every IT system and every business process. Therefore, CCOs and internal audit must forge close partnerships with the lines of business as well as IT. They also need to have a seat at the table when design decisions are being made and when the budgets for digitalization initiatives are allocated. In turn, this requires them to be a true partner in these, often technical, discussions.

For the technology side, the key to making this a reality lies with enterprise IT vendors.

SAP's strategy is to support business integrity

At the center of SAP's strategy is an integrated software solution called SAP Business Integrity Screening (formerly SAP Fraud Management). This application leverages the capabilities of the SAP HANA ® platform, especially its speed, built-in predictive analytics, text mining, and geo-spatial capabilities to enable a largely automated continuous compliance exception, error, and fraud monitoring process.

SAP Business Integrity Screening

SAP Business Integrity Screening enables the set-up of comprehensive continuous monitoring of large amounts of data using sophisticated algorithms. It will also supports the integrated, guided management of follow-up processes, including fraud investigations, risk mitigation efforts and corrective actions.

Relevant data from SAP and non-SAP systems can be selectively replicated into the underlying SAP HANA database in near real-time, where flexible views can be created, for example to merge data from different sources or to create the relevant KPIs (such as benchmark figures on the fly). In addition, rules and algorithms allow the identification of anomalies, compliance violations, and suspicious patterns based on a multitude of data points using the rules engine and predictive algorithms. The detection algorithms can be performed as mass detection of, for example last week's purchase orders, or in real-time for individual transactions with the possibility to stop – and later release – high risk transactions. When exceptions are found, the system sends an alert and triggers a workflow to ensure the right person is alerted and the exception is treated through an organized, auditable, and effective process.

Where companies already use SAP S/4HANA as their ERP, SAP Business Integrity Screening can run completely integrated on the original line-level data and no replication is needed. Since early 2017, SAP Business Integrity Screening incorporates the capabilities of SAP Business Partner Screening, an application that supports the screening of third parties based on compliance databases such as World-Check and Dow Jones. This is particularly important since the trend towards operating in fluid business networks has increased the need for an integrated third-party due diligence processes.

Use case one: Continuous monitoring of internal processes

Business challenge

Reduce error rates, prevent compliance violations, and detect fraud in back-office processes while reducing cost caused by manual controls and increasing agility.

Approach

Two large high-tech organizations use SAP Business Integrity Screening to establish a broad and deep continuous monitoring system. Both projects are very similar in scope, aiming to establish an integrated monitoring system using sophisticated algorithms to eventually span the entire company. While driven by a desire to prepare their compliance and anti-fraud systems for the digital evolution of their business processes, both companies appreciate the potential to improve business performance through increased transparency and reduced error rates. In each case, the projects have been started before the transition to SAP S/4HANA occured, while taking into account the S/4HANA roadmap in order to support a smooth transition, partially in a mixed environment. Each company now has a clear vision as to how to drive integrity in times of dynamic and rapid change in their core business.

Results

More effective controls, reduced manual control efforts, much greater transparency, and reduced error rates: for example a reduction in duplicate invoices.

Use case two: External fraud in utilities

Business challenge

Every year, utility companies lose very significant amounts of money to fraud. In some developing countries, revenue losses can be as high as 15% due to meter manipulations, meter bypassing, data manipulation or data quality issues. The loss prevention process is often largely manual and does not leverage the possibilities that modern data analytics provides. More effective field inspections through the identification of those customers most likely to manipulate or bypass meters, and the identification of non-billed readings, can lead to significant and speedy revenue recoveries.

Approach

We support several utility companies using SAP Business Integrity Screening to identify and reduce losses in their meter-to-cash process. SAP Business Integrity Screening helps them better organize their loss prevention activities and leverage predictive algorithms to identify those of their customers that are more likely to evade the system or experience meter failure.

Results

The utility companies' field inspections – the main purpose of which is to uncover fraud – became much more effective, leading to increased rates of revenue recovery. Targeted analyses identify revenue losses due to misconfigurations, data quality issues, as well as fraudulent data manipulation eliminating sources of revenue leakage.

Use case three: Integrated 3rd party due diligence

Business challenge

As companies increasingly rely on business partners within their value chain, gaining a tighter grip on third-party compliance risk becomes increasingly important. Failure to take appropriate measures to detect and prevent compliance violations – for example regarding corruption or sanctions – can cause significant reputational and also financial damage.

Approach

We advised a high-tech company in setting up an integrated third-party screening approach. This uses SAP Business Partner Screening (now part of SAP Business Integrity Screening) in conjunction with the SAP Global Trade Services sanction list screening capability across multiple business units. The aim was to establish an integrated, reliable, and efficient way of defining and providing a consistent, highly IT-supported third-party management process, spanning heterogeneous business processes and ecosystems to reduce third-party compliance risks, as well as potential fraud.

Results

Reduced risks through a consistent approach to business partner due diligence across multiple business systems.

Becoming a better business

Failure to achieve compliance and ensure business integrity in a changing environment can become the biggest roadblock for companies' digital transformations. Traditional programs are already falling short regarding speed, effectiveness, cost efficiency, and the burden they impose, especially on to line management.

Managing the transition towards integrated business integrity management is therefore one of the most important tasks for every CCO. This requires close partnerships with the different lines of business. It is important to establish a joint understanding that an integrated and automated integrity and fraud prevention approach is not only the right path for compliance management, it also offers multiple opportunities to become a better, leaner and more agile business. This requires compliance, risk and internal audit teams to play different roles and to acquire quite a few new skills. EY and SAP can help at every step of the way.

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities. EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

About EY Forensic & Integrity Services

Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority — no matter the size or industry sector. With approximately 4,500 forensic professionals around the world, we will assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide.

EYG no. 011187 – 18 Gbl.
ED None.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.