WHITEPAPER

7 Indicators Your Regulatory Compliance Framework Needs an Upgrade

Regulatory compliance is a moving target, a mandate that continually shifts in both scope and complexity. Amidst regulatory change and a rapidly evolving business environment, compliance officers are tasked with sustaining a sound and relevant compliance program while mitigating costs. This is no easy task, as the current rate of change means the capacity of inefficient compliance frameworks and systems can become overwhelmed seemingly overnight—and at great cost, if a regulator discovers gaps.

The sheer volume of regulations companies must comply with is ever growing; even as legislators attempt to lessen the regulatory burdens on companies, new complex vulnerabilities emerge (cyber security, terrorist financing and data privacy, for example). Compliance programs must have the capacity and agility to manage change effectively.

Costly compliance "gaps and overlaps" lurk in the white spaces of a company's organizational chart, where work flows between business units, lines of defense, and personnel. New regulations trigger new layers in control, and often companies add additional staff rather than invest in tech-enabled compliance tools to manage new requirements. As compliance teams grow and splinter into specific areas of expertise, and overall compliance requirements become more complex, existing management tools and processes may not scale to the task of managing all that white space efficiently or effectively.

SAI GLOBAL | BWise®

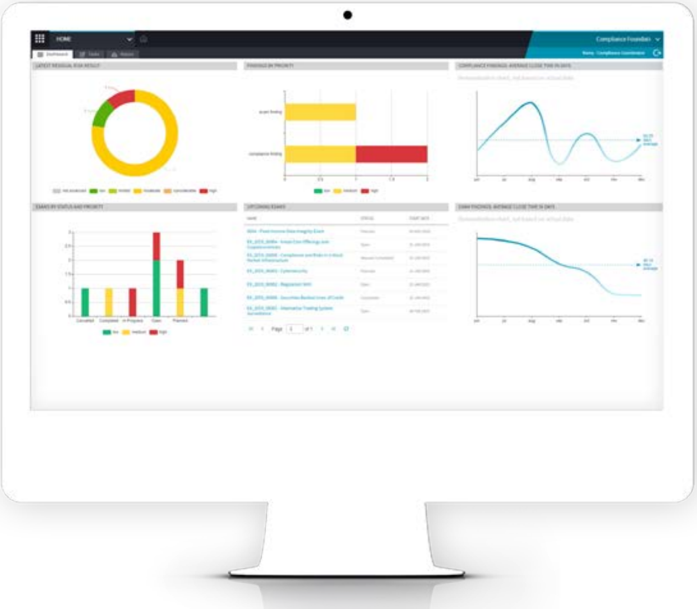
Noncompliance can cost nearly three times as much as meeting compliance requirements effectively, so it pays to stay compliant. Companies that fail to maintain a sound compliance framework are vulnerable to fines as well as reputational damage that can undermine share price and investor confidence. A surprising number of our largest clients came to market for compliance software because they were sanctioned for a regulatory failure and found themselves facing a tight deadline to implement dramatic changes in their compliance framework.

When is the right time to invest in upgrades to your regulatory compliance program? Ideally, while you are still in the driver's seat. A proactive investment mindset gives your company control over the timeline for designing and implementing a more mature, change-ready compliance framework. If you wait for regulators to find gaps in compliance, you will be making changes on their terms.

The signs of impending system failure are easy to spot, if you know where to look. Following are seven key indicators that it's time to take regulatory compliance to the next level.

1. Regulatory compliance analysts spend more time on administrative coordination than compliance tasks.

It's time to tech-enable your company's compliance program when compliance staff routinely spend more work hours on administrative tasks than high-value compliance work. Failing to automate administrative aspects of compliance workflows, such as sending emails, managing document versions, and manually tracking compliance controls and remediation issues in Access or Excel results in hours of wasted time for compliance personnel (who are becoming increasingly expensive in tight labor markets).



Regulatory Compliance dashboard

Manual compliance processes are not just inefficient, they are often ineffective. Manual AML monitoring processes, for example, are estimated to miss about 50% of the transactions that should be flagged as suspicious. Third-party risk management is another AML liability, one that is onerous and error-prone when processes are manual. Baseline risk ranking, information documentation, and screening processes can all be automated, integrated into the compliance framework, and monitored via a dashboard. Financial institutions have racked up $26 billion in fines for failure to comply with AML and KYC regulations since 2008. The insurance and real estate industries are prone to AML abuses as well.

Miring regulatory compliance staff in manual processes can also slow change management efforts or even worse, cause the company to act on incomplete information. Regulatory compliance analysts can spend hours exhaustively scouring the internet for new or changing rules and regulations, maintaining regulatory libraries, and mapping regulatory changes to relevant business process and compliance policies. That time can be more effectively applied to high-value analytical change management work such as risk assessing new regulations and effectively incorporating regulations of high materiality within compliance policies and procedures.

In a recent KPMG compliance survey, only 27% of CCOs felt strongly that their compliance program is keeping pace with regulatory changes—which leaves a lot of room for improvement in change management. Cutting the administrative burden of compliance can increase capacity to execute a more proactive, sustainable and agile compliance program.

2. Legacy compliance technologies have not been updated for years.

Most of the enterprise organizations we work with have matured beyond managing compliance through Excel spreadsheets and SharePoint to develop in-house compliance systems or build a user interface over a third-party database application like an Access. When your company's home-grown compliance system is so outdated it's driving staff to develop inefficient workarounds, it's time to look at a purpose-built compliance IT solution.

Companies that develop their own compliance IT framework in house are locked into an ongoing expense of maintaining the solution themselves. Often, the system is built in such a manner that future changes and system enhancements require the original developer to remain involved. Clients have come to us with legacy solutions that haven't been updated for years, because the programmer who originally developed the solution left the organization and nobody understood the back-end code well enough to maintain it. The cost of having a new programmer rework and update an aging home-grown system can be cost prohibitive, so companies tend to apply a band aid approach until a regulatory misstep forces them to evaluate a better solution.

We have observed another serious problem with home-grown compliance applications: They can enable a compliance culture that avoids adoption of best practices and rules changes. This enablement occurs in two ways. First, staff can go directly to the in-house developer and request workarounds to any changes in compliance processes or policies they are uncomfortable conforming with. Second, homegrown solutions are often built with requirements that reflect the compliance perspective the company is already following. The platforms are designed without benchmarking compliance practices of their industry peers or the compliance discipline as a whole. A home-grown system is rendered obsolete before day one of implementation when developer requirements don't take into account best practices or try to anticipate where compliance practices are heading.

The adoption of an out-of-the box solution is an opportunity for a company to upgrade the compliance program as a whole without being undermined by change resistance among employee ranks. A purpose-built compliance solution has best practices already built into the design, along with limits on who can control updates or exceptions to rules. Updates to compliance best practices and relevant regulations are automated, and while end users can customize certain aspects of their interface with the system, best practice standards and rules changes are rigid and must be adhered to.

3. Compliance teams operate in silos utilizing disparate compliance management tools —and one or more of them is in need of an upgrade.

Third-party risk assessment, regulatory inventory, AML and corruption, KYC assessment, regulatory exams, HIPAA privacy and BSA regulations—compliance encompasses so many distinct areas of subject matter expertise that our average client has 8 compliance teams, and we've worked with companies that have as many as 12. Compliance teams within large enterprises can evolve into separate silos supported by technologies that are fragmented around specific compliance functions. Global companies with business units that operate in different regulatory jurisdictions have additional layers of complexity in their compliance structure.

Fragmented operating systems make it difficult to align compliance activities across an organization; they cause inefficiencies on a mass scale and they obstruct enterprise-wide views of compliance. Siloed compliance teams lack a common set of controls, regulatory taxonomies, and regulatory libraries. They don't utilize the same data sources and they often interpret and apply regulations inconsistently, which leads to gaps and overlaps in compliance. Regulators won't cut you any slack because your organization's data is scattered across multiple platforms and hard to access.

It's also very inefficient and expensive to maintain independent technology systems for each compliance team: The reality is, some teams will have poor technology support while others will operate at a higher level. At some point, one of these compliance tech silos is going to fail—which presents an opportunity to investigate integrating all of them.

Compliance IT integration facilitates—and sometimes catalyzes—alignment of compliance activities across the entire enterprise. An integrated, configurable enterprise-wide compliance solution reduces risk, improves collaboration and communication, enables comprehensive reporting, standardizes data sources and regulatory libraries, and eliminates redundancy across the organization—all of which raise visibility of the impact of the compliance program on the organization as a whole. An integrated compliance platform reinforces a top-down message to the entire organization that compliance is a priority.

Integrating supporting compliance technologies into one platform also provides a critical foundation to achieving a high state of compliance maturity. Traditional compliance teams have a task driven, project-based mentality, viewing compliance as having a start and end date. The clients we observe with highly mature compliance cultures view compliance as an enterprise-wide process, where all company workflows feed into the compliance framework and all members of the organization are part of the compliance team. An integrated GRC solution is indispensable to achieving that level of maturity.

4. Compliance reporting is a manual process.

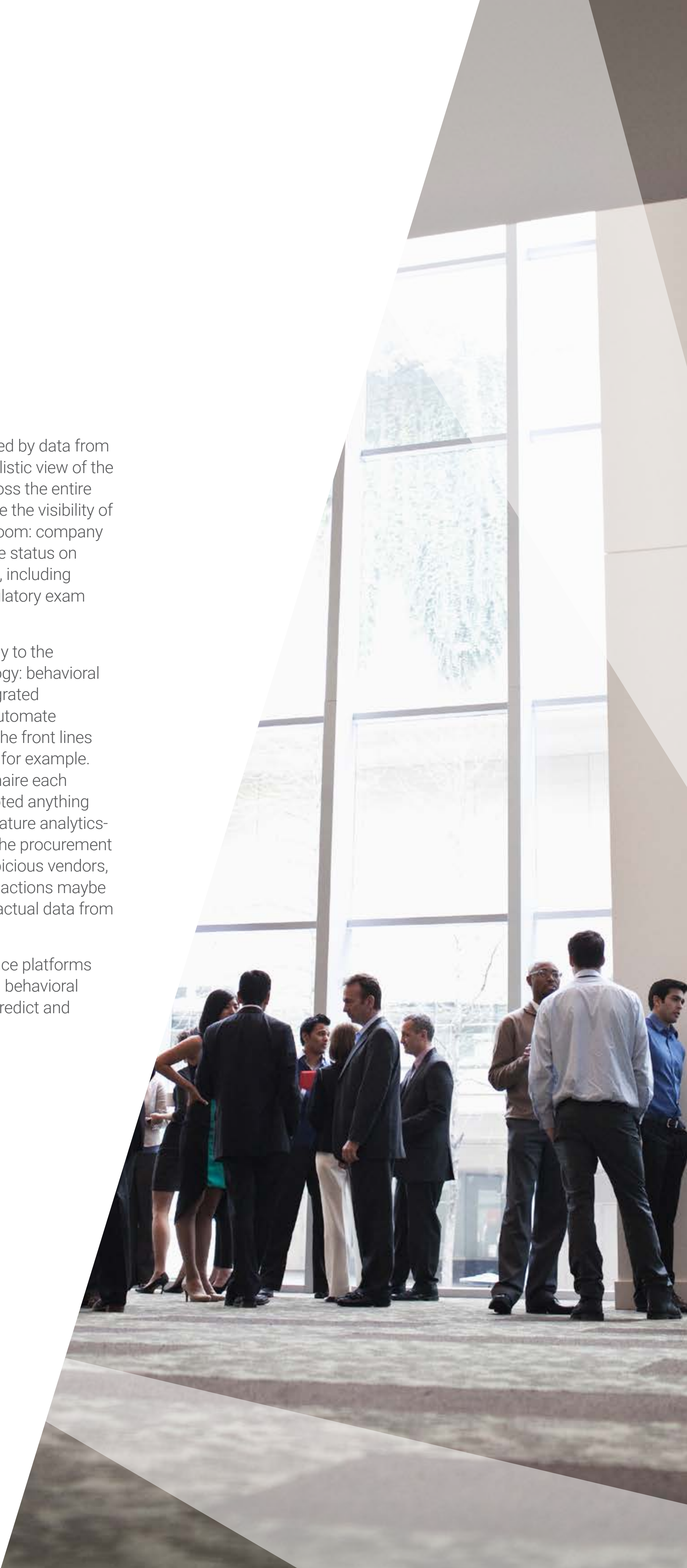
Your company has outgrown its compliance operating system if reporting is a cut and paste manual process. In this age of automated data visualization, manual processes for aggregating data and creating compliance reports is a waste of compliance manpower—and a lost opportunity to provide CCOs and the board with meaningful insights into compliance effectiveness.

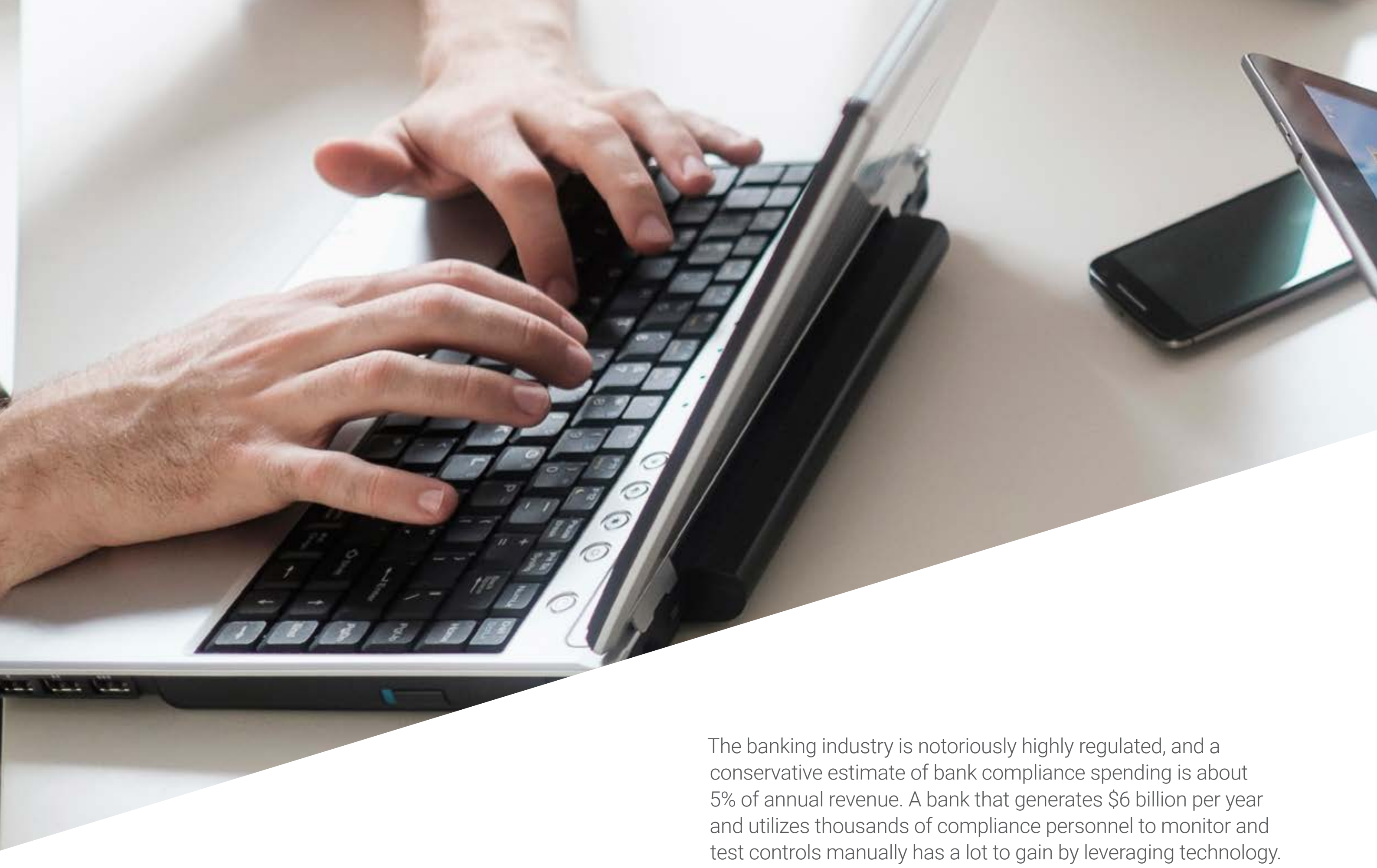
Automation of reporting from a centralized data source is the hallmark of a mature compliance model, and regulatory change management is dependent upon it. Yet KPMG recently reported that only 47% of CCOs report having an integrated reporting system across their organizations that includes compliance monitoring.

An automated compliance reporting dashboard, fed by data from a robust compliance technology, can provide a holistic view of the overall state and effectiveness of compliance across the entire enterprise. Compliance reporting dashboards raise the visibility of the value of compliance in the C-suite and boardroom: company leadership and board members can get a real time status on compliance activities throughout the organization, including monitoring and testing, vendor due diligence, regulatory exam status, and regulatory change management.

Automated compliance reporting is also a gateway to the next-generation capability of compliance technology: behavioral analytics. In the compliance analytics phase, integrated compliance platforms will not only dramatically automate compliance work, but will pull external data from the front lines to defense to do it. Take AML and KYC processes for example. Most companies send a yes/no/maybe questionnaire each month to the front-line staff asking if they have noted anything suspicious in customer or vendor transactions. Mature analytics-based compliance systems will be connected to the procurement system and generate a printout detailing any suspicious vendors, purchases, or activities. Out of thousands of transactions maybe 10 would be flagged to the compliance based on actual data from the procurement system.

The integration of first-line systems with compliance platforms is the future of compliance technology, employing behavioral science to give compliance leaders the ability to predict and prevent compliance problems before they occur.





5. Compliance controls are monitored by volume, not exception.

Every compliance officer faces the same problem—the burden of monitoring a huge volume of internal controls. When a compliance team reaches the point that they are so overwhelmed administrating procedural adherence to controls that they never get adequate time to remediate material exceptions, the company is highly vulnerable to fines and regulatory pressure. A number of clients come to us because they've been managing compliance by volume and have been slapped with a multi-million dollar fine and an MRA to resolve on a deadline.

Remediation of issues by volume means staff may disproportionately spend time on issues of low or medium materiality, rather than focusing on high-risk material issues. Cumbersome issue tracking methodologies and fragmented efforts across compliance silos make it difficult to coordinate compliance activities between lines of defense, causing duplication of effort and increasing the risk of remediation efforts lagging past their due dates (or falling through the cracks altogether).

Managing change is everything in compliance—a cost-effective, sustainable program needs a common set of enterprise-wide controls and technology tools that can help identify and track the controls that have the highest material impact on a company. Adopting a risk-based approach to monitoring controls is an important step in maturity for any company's compliance program. According to a recent report by McKinsey & Company, shifting from a procedural-based to a risk-based approach can free up to 30% of compliance capacity.

The banking industry is notoriously highly regulated, and a conservative estimate of bank compliance spending is about 5% of annual revenue. A bank that generates $6 billion per year and utilizes thousands of compliance personnel to monitor and test controls manually has a lot to gain by leveraging technology. If the bank manages to reduce compliance overhead by 20% through automation of control monitoring and testing, that's a $3 million improvement on the bottom line. Automation represents a huge cost savings opportunity, both in terms of man hours and prevention of penalties from regulators.

Risk-based compliance monitoring requires an enterprise-wide view, which for many companies will require an investment in compliance technology. Purpose-built regulatory compliance tools centralize regulatory libraries, triage compliance risks by materiality and bring visibility to highest-impact issues and remediation status. The compliance team can eliminate duplication of effort, shine light into compliance gaps that require immediate attention, and increase capacity for high value work—like remediating exceptions in advance of regulatory exams.

6. Your company plans to acquire new businesses or expand into new markets.

Many companies are turning to acquisitions and new markets to augment organic growth, which makes them subject to a larger regulatory regime. Whether a company is expanding into domestic or foreign markets or acquiring an existing company, it is the job of the CCO and regulatory compliance team to ensure a smooth transition from a compliance standpoint.

The compliance challenge with M&A transactions in particular is a mandate from the DOJ and SEC to ensure the ethical cultures of the two entities are aligned. With regards to corruption, for instance, the acquiring company needs to ensure that the Code of Conduct, policies and procedures of the target company are consistent with its own; if not, the acquiring company needs to apply its own anti-corruption regime to the newly acquired company within 18 months or as quickly as possible.

Foreign Corrupt Practices Act (FCPA) violations are a perfect example of an area where M&A compliance failures become costly. The FCPA Resource Guide, published jointly by the DOJ and SEC, states that in a merger or acquisition the successor company assumes the predecessor company's liabilities—including FCPA violations. However, in cases where due diligence failed to turn up existing violations, guidance states that "implementation of an effective compliance program may also decrease the likelihood of an enforcement action" and that the DOJ "may consequently decline to bring enforcement actions." During 2018, 16 companies paid a record $2.89 billion to resolve FCPA cases. That includes amounts assessed in resolutions with the DOJ, SEC, or both. The top three enforcement actions levied fines in the following amounts: $1.78 billion, $585 million, and $280 million. That's a strong business case for shoring up compliance prior to engaging in M&A activities.

Even merely offering new services that are directly related to an organization's current industry can bring about new regulatory obligations. For example, there are differing regulations that hospitals must follow for specific surgical procedures such as heart surgery, brain surgery and orthopedics. To make matters more complicated, healthcare institutions must comply with regulations at federal and state levels, each of which can differ based on services provided.

CCOs are not always brought into acquisition or business expansion planning as soon as they would like, yet they are often called upon to ensure a smooth transition. A scalable, enterprise-wide GRC platform that populates best practices into the organization's compliance ecosystem can accelerate a compliance team's ability to accommodate new regulatory requirements, align corporate cultures across business units, and manage change effectively.

7. New regulations are having a seismic impact on your compliance program.

A sudden, unexpected increase in the volume of work related to regulatory change management can overwhelm the capacity of manual processes within your compliance framework. It's difficult to anticipate the next fiscal crisis or corporate scandal that will result in sweeping regulatory change. The financial crisis that triggered a recession and spawned Dodd-Frank happened over 10 years ago, and the banking industry is still grappling with high compliance costs and overhead as a result.

Manual compliance processes can also have difficulty absorbing less traumatic events than a recession and sweeping legislation. A spike in regulatory notifications that are deemed to have a material impact, an unusually high number of on-going regulatory exams, or a significant volume of new regulations that need to be risk assessed all have the potential to overburden a fragmented compliance framework. Any one of these situations presents a business case for integrating compliance processes and technologies across the enterprise.

The price of compliance failure can be high—for large financial institutions grappling with Dodd-Frank, it's been $243 billion. Fortunately, multi-point compliance IT solutions can be adopted in stages, so investing in capacity for regulatory change-readiness doesn't have to break the compliance budget. If it prevents fines, the system will more than pay for itself.

Regulatory compliance solutions offer a significant opportunity for organizations to fortify their compliance programs while at the same time utilizing fewer resources. SAI Global can help assess whether your company's regulatory compliance requirements have outgrown your existing compliance framework and systems. Visit www.bwise.com or www.saiglobal.com/risk for more information.

About SAI Global

SAI Global helps organizations proactively manage risk to create trust and achieve business excellence, growth, and sustainability. Our integrated risk management solutions are a combination of leading capabilities, services and advisory offerings that operate across the entire risk lifecycle allowing businesses to focus elsewhere. Together, these tools and knowledge enable clients to develop an integrated view of risk. To see our tools in action, request a free demo.

We have global reach with locations across Europe, the Middle East, Africa, the Americas, Asia and the Pacific.

For more information visit **www.saiglobal.com/risk**.

SAI GLOBAL | BWise®