Deloitte.

Revolutionize controls testing

Break the compliance-cycle mold and take a fresh look at organizational risks

More than a dozen years after Sarbanes-Oxley (SOX) was enacted, the cost of maintaining compliance has become onerous. Many companies find themselves investing significant effort, resources, and dollars into programs that don't produce customer-facing returns or align with strategic objectives. Additionally, companies are still facing operational failures due to poor control design and inherent limitations with traditional testing approaches. These failures can ultimately demoralize workers across the business and internal audit and allow instances of fraud, theft, and even suboptimized business processes to continue.

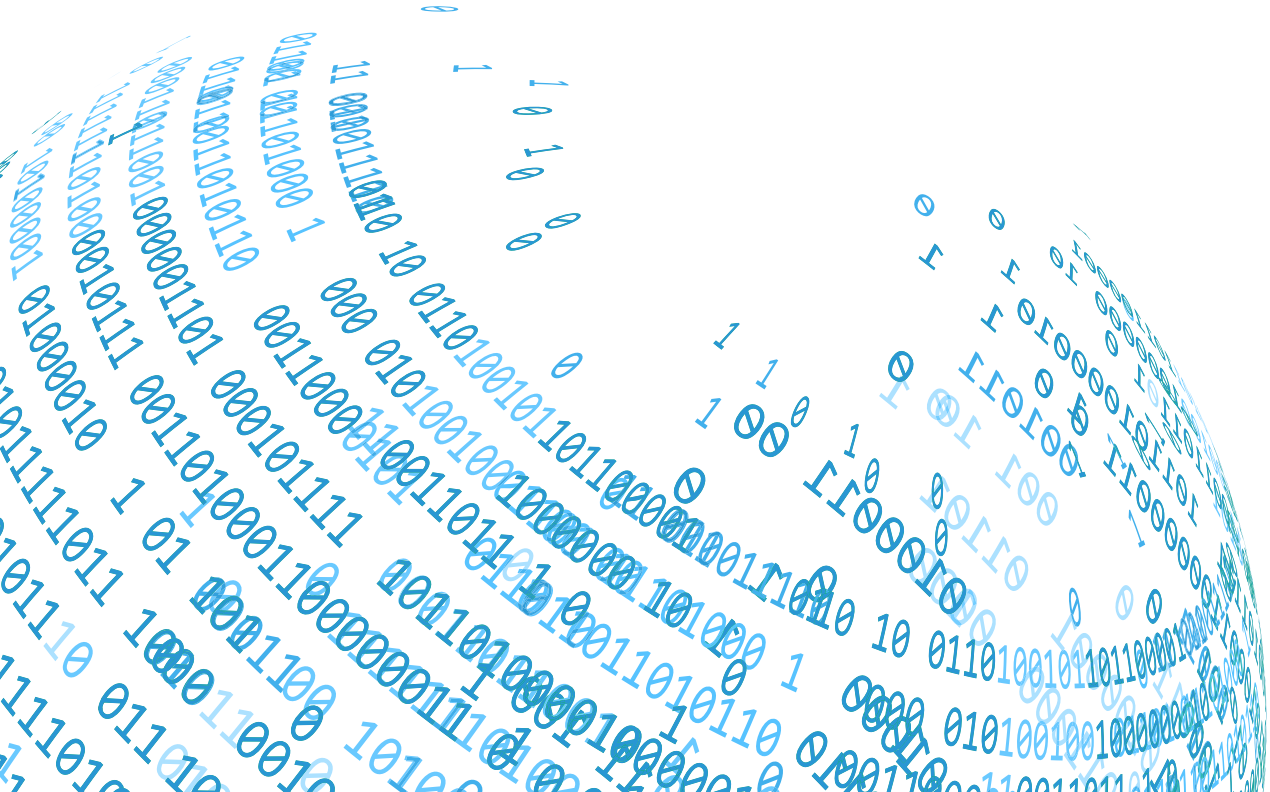
The common practice of investing in inefficient controls and ineffective compliance programs is counterproductive, but the way out is not always clear. Barriers to change can be daunting, so organizations often prefer to tweak their programs around the edges rather than transform them. Making incremental changes to common controls is not a bad thing, but often it creates a cycle of "maintenance" that is suboptimal at best. It is time to take a smarter approach by harnessing the power of digitization to help break the compliance-cycle mold.

Breaking the status quo

As multiple stakeholders across the enterprise compete for dollars and the interests of their specific functions, a decentralized environment can make it difficult to gain a comprehensive view of compliance efforts. Without a comprehensive view, it can be challenging to identify what works and what doesn't, spot opportunities for savings, and determine where collaboration among functions would benefit the organization. Though common, this decentralized, siloed approach not only leaves stakeholders fatigued and unmotivated to disrupt the cycle, but also stalls the overall productivity of the organization and can destroy synergistic value.

For example, many organizations have not conducted a significant overhaul of their SOX control programs since 2004. As their businesses changed, they added bolt-on programs, but there seemed to be no commensurate reductions in effort and expense. Why? This piecemeal approach often increases costs and potentially misaligns effort with risk. The actions stemming from risk assessments frequently do not keep pace with the rate of change, which leads controls and compliance departments, as well as internal audit, to test the same controls year over year.

Given the large number of resources that traditional SOX compliance programs require, material changes in them often correlate to significant shifts in the business, such as M&A activity; a new revenue stream; a new shared services environment; implementation of a new system; or adjustments forced by external regulators, auditors, or standard-setting bodies. But without those shifts, the status quo often remains: As soon as external auditors sign off, the cycle resets without invoking change, producing another year of limited returns and further increasing the total cost of compliance.



Reevaluate your control environment

Traditional testing approaches, derived from statistical methods and used for decades, identify the symptoms of failures; however, they are limited in their ability to uncover and address root causes. Thus, additional analysis is often required, commonly based on manual techniques that attempt to extract meaningful inferences from a small sample of data. These traditional sample-based approaches mirror the siloed structure of the compliance programs themselves. Not encompassing the full population, they lack a comprehensive perspective, which can lead to unrecognized fraud, corner-cutting, longer closing cycles, inconsistent reports, user confusion, and unnecessary expense.

However, new advances in technology and computing power can exponentially improve risk assessment and enable a new breed of controls that utilize automated, advanced analytics. This enhanced risk assessment is designed to reduce the overall scope and creates value by directing effort toward the risks that actually matter. Meanwhile, the new analytics-fueled controls empower organizations to quickly and continuously monitor control performance. By screening entire data sets, they provide comprehensive, conclusive information around issues in the control environment, allowing organizations to identify and address the root causes before costly, systemic control failures might occur.

Overall, these new capabilities enable organizations to take a fresh look at their control environments, empowering them to address the overall IT and business risks while harmonizing efforts across multiple regulations and compliance activities.

They also bring a holistic focus and a unified view by introducing detailed analytical dashboards. These enhancements collectively enable the organization to pivot from doing compliance for the sake of compliance to providing greater value. As controls are streamlined, people can shift their focus towards more strategic activities, such as performing analysis and providing insights in support of key business priorities.

A US-based bank, which operates in multiple jurisdictions across the globe, wanted to more efficiently address third-party reporting requirements for IT and security compliance. The bank engaged Deloitte to help it achieve this goal. Prior to the engagement, the bank assessed and tested each regulatory requirement separately by line of business. Understanding that compliance questionnaires contain significant overlap and duplication, Deloitte developed an integrated risk and control framework that could be applied against more than 20 standards and regulations, mapping requirements to the bank's controls so they could be rationalized and harmonized. By applying this framework, the bank put a cohesive testing and monitoring program in place. Now, it can test once and apply the results broadly across compliance requirements. A central dashboard delivers a single view of compliance enterprise-wide, providing clarity throughout the compliance landscape. **The framework enabled the bank to lower its total cost of compliance by 40 to 50 percent and reduce the number of controls by 60 percent.** Deloitte reassesses the framework quarterly to help the organization to optimize its compliance spend on an ongoing basis.

Change the scope of controls across compliance, operations, and finance

Leveraging automation enables organizations to break the compliance-cycle mold by fundamentally changing how controls work across compliance, operations, and finance. By aggregating data from disparate sources, organizations can deliver quick wins within data-driven processes such as accounts payable, IT security, and change management. With the data centrally aggregated, analytics can detect anomalous patterns, inappropriate behaviors and activities, and even identify individuals who warrant increased monitoring—without the typical lag or the significant overhead associated with traditional monitoring.

For example, by applying analytics to the system-change control process at a large bank, the CIO identified numerous concerns regarding routine IT governance activities in the department. After further analysis, he discovered that several components were suboptimized, leading to misalignment with strategic direction, system downtime, extended processing time during financial close, and numerous common practices that did not align with established department protocols.

Once organizations implement automation, accessible data, and visualization capabilities, they can start using them—extending them where necessary—to modernize controls across the enterprise. Executives can observe the status of various controls through centralized dashboards and apply this intelligence to make key operational decisions continually, rather than annually or specifically, based on an event. Compliance can use the same dashboards to drill down further into the data to reassess risk factors, examine day-to-day procedures, and realign the control framework to upgrade or replace existing controls. Internal and external audit teams can also leverage this ongoing flow of analytical data to create additional views for testing, perform control activities, and continuously monitor efforts. Using technology enablement to move past routine activities creates a big opportunity for audit and compliance teams to add value as they reallocate their time to process improvement, modernization, and projects that impact the customer experience.

One organization was spending more than 600 hours two to three times a year to test a sample of 75 change management events. **With Deloitte's digital testing and controls automation (DTCA) methodology, the organization was able to test nearly 15x more events (1,100+) in less than half the time.** In addition to improving efficiency, the company can now view data holistically, which enables it to get beyond superficial issues like missing signoffs and address real issues around governance within the IT organization.

The power of DTCA across all three lines of defense

The DTCA methodology can be leveraged across all three lines of defense to enhance an organization's control execution, control and compliance monitoring, and control testing functions. See the following illustrative example of how DTCA can be used for access terminations within an organization:

First line
Business unit

On a daily basis, automatically compare HR termination feeds and notices to network and application user listings to identify any terminated employees with active access requiring action.

Second line
Compliance and risk

On a weekly basis, monitor exception reports detailing terminated employees with an "active" status on network and applications requiring action.

Third line
Internal audit

On a quarterly basis, test 100 percent of terminations by comparing HR terminated employee listing against network and application active user listings. Further, provide results of testing to external auditor for reliance purposes.

Leveraging the same data for all three lines of defense helps organizations consolidate and harmonize efforts in a collaborative environment that maximizes resources and dollars, producing more meaningful results.

Achieve meaningful business outcomes

Scalable and repeatable tech-enabled controls reduce the time, effort, and dollars spent on the total cost of compliance and enables organizations to reallocate higher-level resources to more strategic and valuable tasks. Automating routine activities and better leveraging scarce resources keeps people focused on business priorities so management can achieve its long-term vision.

Overlaying data analytics onto a tech-enabled control environment creates easy-to-digest visualizations that provide fresh insights and meaningful business outcomes, as demonstrated in the following examples:

After years of performing the same evaluation of its change management process across several IT platforms, a global asset management firm discovered that its routine checks were not picking up on issues beneath the surface that were impeding its change management process. The firm engaged Deloitte to identify the root cause of the slowdown. Leveraging DTCA, the engagement team performed a trend analysis on 100 percent of the company's system changes in half the time that the company traditionally spent conducting its former sample-based approach. The analysis uncovered a series of governance-related issues that were causing system downtime and delays that ultimately slowed down their financial close process. Once corrected, the company was able to close faster and better govern its system changes.

An organization wanted to revisit its SOX program and identify opportunities for process efficiencies and control rationalization. The Deloitte team helped management improve the control environment by taking a modernized approach to their risk assessment, resulting in the opportunity for consolidating duplicate controls and shrinking the number of controls tested by each audit group. Through the engagement, the company reduced its overall number of controls by 71 percent and decreased its testing hours by 38 percent.

Deloitte used DTCA to assist a leading global bank in analyzing numerous security profiles and transactions related to its wire disbursements process, uncovering critical segregation-of-duties violations that would likely have previously gone undetected due to the complex nature of the bank's IT environment. DTCA enabled the engagement team to visualize the entire population of disbursements and identify those with the greatest risk profile. In one situation, an individual was identified with both the ability to update payee information and process disbursements and the ability to circumvent their $50,000 authority limit by splitting larger amounts into separate transactions. By adding new dimensions to the bank's monitoring process, they were able to identify a series of inappropriate transactions that would have likely gone undetected. With DTCA, analyzing security profiles and transactions has become a continuous process, alerting the company to violations and risks in real time.

A large industrial company engaged Deloitte to help it transform its controls environment by assessing the internal implementation of an SAP Revenue Accounting and Reporting application. To better understand how the IT department was managing the implementation, the engagement team initially performed impact and gap assessments, identified potential pitfalls related to the system implementation, and provided the company with recommended actions, including opportunities to gain efficiencies in its control and compliance programs, so that the company could get ahead of potential challenges and avoid surprises after going live. The team used automated tools to test the controls prior to go-live and review how management remediated the issues. Serving as an objective voice to the project governance team helped the company to achieve its value targets for the project.

A global manufacturing company wanted to define its current state of cyber in terms of capability, coverage, and effectiveness and to identify and prioritize potential areas for future investment. The Deloitte team designed a program based on NIST 800-53 to assess common shared controls and business unit implementations. The program enables broad coverage across controls and sites over a three-year period, continuously identifying ongoing issues and changes to strategy. Through these assessments, management obtained greater insight into the company's current state, including the maturity of recently deployed solutions, as well as a better understanding of which areas warranted strategic investment, such as privileged access management.

Closing thoughts

Over the past five years, the way organizations operate has changed dramatically, but controls and compliance programs have not kept pace. Addressing risks across compliance, operations, and finance using an enhanced controls platform that incorporates automation and advanced analytics increases insight into risk exposures; improves the quality, effectiveness, and cost of controls testing; and reduces the burden on the business.

For companies that want to accelerate transformation of their controls environment, outsourcing controls compliance may be a good option, since it provides access to resources who understand the current regulatory environment, have extensive industry knowledge, and are trained in the latest technologies, techniques, and methods. As a result, compliance-spend reduction, as well as ROI improvement, can be significant, as internal resources are reallocated to more important work and produce higher-quality output. Plus, a progressive, independent advisory firm can create additional value by helping to tighten the overall scope of a controls audit in an effort to reduce "program bloat."

With or without outsourcing, an enhanced controls platform is beneficial to interrupting the cycle and fundamentally changing the controls environment. This platform should incorporate automation to achieve quick wins and rework existing controls and analytics to analyze control effectiveness and business outcomes. The time to act is now, as companies are digitizing, automating, and improving data access. There is a significant opportunity to break the compliance-cycle mold and take a fresh approach to organizational risk—and to do so in a way that creates meaningful change for employees as they pivot from being checkers of facts for the lines of defense to generators of ROI for the business.

Deloitte's controls advisory approach

Deloitte's integrated controls advisory platform changes an organization's approach to compliance, moving it from a check-the-box mentality to one where executives can truly understand the state of their controls, drive insights, spot trends, change behavior, and identify weaknesses. Executive dashboards and continuous monitoring provide a holistic view of the control environment that can be quickly and easily analyzed. Transforming the control environment through digital testing and automation drives efficiency, reduces risk, and enables strategic alignment that provides valuable insights into the heart of the business and its core operations.

Our suite of tech-enabled solutions takes full advantage of emerging technologies like robotics, cognitive, and data analytics. These digital enablers enable companies to deliver meaningful business outcomes faster and more cost-effectively while realizing optimal benefits and an improved return on investment. The suite is flexible and scalable to work across the spectrum, ranging from organizations seeking wholesale change to those that are looking to address a specific pain point.

Controls transformation – Applies tech-enabled solutions to traditional control methods for a smarter, faster approach.

Cyber controls assessments – Helps organizations develop, manage, and report on cybersecurity controls and identify gaps. This assessment prepares them for a cyber attestation that can provide greater assurance to stakeholders.

Digital risk management – Helps organizational stakeholders understand, govern, address, and manage the associated risks from digital tools, algorithmic risk, artificial intelligence, and cognitive bias.

Digital Testing and Controls Automation (DTCA) – Uses a combination of proprietary tools and leading commercial automation software to leverage existing underutilized licenses and resources. DTCA drives efficiencies, reduces the risk profile, and provides valuable insights at a pace that aligns with an organization's risk appetite.

Transformation Assessment Services (TAS) – Gives executives an insider's perspective during large business transformations by amplifying their ability to probe deeply to identify potential issues and pitfalls before they lead to costly delays or defects.

Contacts

Stuart Rubin
Managing Director | Risk & Financial Advisory
Deloitte & Touche LLP
+1 561 962 7826
stuartrubin@deloitte.com

Joseph Gaglio
Principal | Risk & Financial Advisory
Deloitte & Touche LLP
+1 313 394 5109
jgaglio@deloitte.com

Adam Berman
Partner | Risk & Financial Advisory
Deloitte & Touche LLP
+1 212 436 7267
aberman@deloitte.com

Patricia Salkin
Managing Director | Risk & Financial Advisory
Deloitte & Touche LLP
+1 609 806 7279
psalkin@deloitte.com

Neil White
Principal | Risk & Financial Advisory
Deloitte & Touche LLP
+1 212 436 5822
nwhite@deloitte.com

Geoff Kovesdy
Principal | Risk & Financial Advisory
Deloitte & Touche LLP
+1 212 436 5149
gkovesdy@deloitte.com

Special thanks to the following for their contributions to this publication:

Micah Apolzon, Brandon Bogard, Rick Borelli, Alyssa Culp, Akshay Dhawan, Lea Grandbois Dulin, Jennifer Gerasimov, Tom Holland, Shilpa Pai Ivanick, Pankaj Jalan, Katherine Fortune Kaewert, Gloria Kwok, Brian Liebman, Adam Mark, Irshad Niamathullah, Biljana Petrovski, Jon Raphael, Tushar Sainani, Steve Schlegel, Rajeev Singhal, Kelly Snow, and Matt Tilner.

Deloitte.