Deloitte.

Testing and monitoring: The fifth ingredient in a world-class ethics and compliance program

Testing and monitoring takes the pulse of the compliance program, ensuring its ongoing health

Testing and monitoring is one of the most critical elements of an effective ethics and compliance program, and is a required program component in certain industries. Why? Because without testing, it is difficult or impossible to understand what is working and what needs enhancement. Similarly, robust monitoring programs serve as an early warning system that allows compliance professionals to identify—sooner rather than later—potential compliance issues.

As important as testing and monitoring are, they are often misunderstood and undervalued. Implementing and sustaining efficient and effective testing and monitoring programs continues to challenge organizations for many reasons, including the lack of skilled resources, the difficulty of design and of driving consistency across the enterprise, and the reliance on others in the organization for both the data and, in many cases, the execution of the programs.

The emphasis on other compliance program elements—such as risk assessments, training, or policies and procedures—has sometimes led to the undervaluing and under-resourcing of the testing and monitoring functions. As compliance programs mature, these elements serve as an invaluable source of information about deviations in expected behavior that might open the window to potential material or systemic compliance risks. What's more, companies often say that the implementation of new laws and regulations presents risk, yet this is an area that is often not tested, or not tested sufficiently, to determine whether the organization is complying with the requirements.

The lack of effective testing and monitoring can have a ripple effect on other areas of the compliance program. In a number of recent studies and surveys,[1] compliance professionals consistently indicate frustration with the quality of metrics used to measure the effectiveness of their compliance programs. The outcome of ongoing testing and monitoring programs—especially when considered over time—drives metrics that can point not only to the effectiveness of the program design, but also to the effectiveness of the program's operations. Although for some industries, particularly financial services, compliance metrics are already well established or even mandated, for many companies these activities create new, more insightful metrics related to program performance than those compliance professionals have relied upon in the past.

Similarly, robust testing and monitoring—and the data associated with it—provides relevant and reliable information to stakeholders of the ethics and compliance program:

- **Regulators** view testing and monitoring activities as a demonstration of the company's commitment to ethics and compliance. Moreover, for some industries such as financial services, testing and monitoring programs are a regulatory requirement, and companies may face fines or penalties for failing to implement them.
- **Boards** require substantiated information on the effectiveness of the ethics and compliance programs in order to execute fiduciary duties.
- **Internal and external counsel** point to these activities as indicators of the company's diligence around ethics and compliance as part of their legal strategies.
- **Employees, customers, and investors** desire a deeper understanding of ethics and compliance programs and may even use this information to make employment, purchase, or investment decisions.

For all these reasons, and many others, we have identified a robust testing and monitoring program as the fifth distinguishing factor for a world-class ethics and compliance program.

[1] In Focus: 2015 Compliance Trends Survey Report and In Focus: 2014 Compliance Trends Survey Report.

Testing and monitoring: defined and contrasted

Many ethics and compliance professionals use the terms "testing" and "monitoring" interchangeably. While testing and monitoring may be two sides of the same coin, and one cannot be fully optimized without the other, they are not interchangeable. In fact, both their design and desired outcomes are quite different. Commonly recognized definitions of each are as follows:

- **Testing program:** A dynamic, risk-based, independent compliance oversight process designed to periodically select and review a sample of business products, services, communications, and other areas to gauge and report on the operating effectiveness of compliance controls and/or adherence to stated policies and procedures.
- **Monitoring program:** The ongoing surveillance, review, and analysis of key business performance and risk indicators that allows the organization to identify potential compliance violations. While many seek to implement "automated" monitoring programs, monitoring activities can be either automated or manual.

These definitions make the goals and objectives of testing and monitoring clearer; however, the specific steps for reaching these goals and objectives are not always easily defined. Even if regulatory expectations related to these critical elements are clear—as they may be in certain areas of the banking and pharmaceutical industries—detailed information about the specific testing and monitoring activities that will meet those expectations may not be. In other sectors, regulatory guidance related to the specific expectations of testing and monitoring activities may not be available at all. Even in cases where there is clarity around regulatory expectations, the design, implementation, and sustainment of an effective testing and monitoring program is one of the most challenging tasks facing those responsible for the risk and compliance functions.

In the next section, we will explore the distinguishing characteristics of "great" testing and monitoring programs.

Great testing programs

Great testing programs have a number of common attributes:

Compliance is tested at the level of accountability. In a great testing program, compliance testing is executed at each level of the organization. In this model, weak controls are quickly identified in the business where they are most likely to be remediated quickly.

- **The first line of defense**: At this level, the business unit leadership—which is primarily accountable for the development of controls and activities to prevent, detect, and respond to compliance failures—invests the time and resources to determine that such controls and activities are adequately designed and operating effectively.
- **The second line of defense**: Within the second-line testing program, the individuals who perform the testing must not be the same individuals who are responsible for the execution of the controls. Here, the compliance function—whether it be the "centralized" compliance function at headquarters, the compliance team within the business unit, or a combination of the two—should also invest time and resources to develop and execute independent compliance control testing. For purposes of executing the testing programs, these individuals are accountable to the independent compliance function, regardless of whether that function resides at "corporate" or within the business unit, under a federated compliance model.
- **The third line of defense**: Internal audit should be responsible for "testing the tests." In some industries, internal audit plays a broader role. For example, in the financial services industry, internal audit functions go a step beyond testing the tests. Rather than rely on the results of second-line testing, they perform additional transactional and process-related testing.

In all instances, and at all levels, independence related to testing is an essential aspect of effective testing.

Regardless of industry sector, our experience indicates that a disproportionate number of compliance problems are identified by the third line of defense—internal audit. This may indicate that compliance testing in the business unit (the first line of defense) and in the compliance function (the second line of defense) is ineffective at identifying compliance vulnerabilities.

Programs draw on a range of skillsets. Outstanding testing programs involve professionals with specialized knowledge or skillsets that may be different from those found in a traditional corporate compliance and internal audit department. In many instances, professionals with knowledge of the applicable rules and regulations, expectations of regulators, and drivers of compliance risk are required to design and execute testing programs. This is not to say that existing compliance or internal audit staff cannot be trained to meet those needs. However, in the post-Sarbanes-Oxley world, many internal audit departments have focused on professionals with more traditional financial accounting controls experience. These individuals often do not have the deep regulatory and compliance subject-matter expertise required to execute effective compliance testing. Incorporating continuous training and including cross-training of personnel in different functional areas can further enhance the knowledge and effectiveness of the team.

The program is designed using a risk-based approach. Another distinguishing characteristic of a leading testing program is the process used to design the testing itself. As is almost always the case in compliance programs, it all starts with a robust compliance risk assessment (which is the third topic in this series of publications). A great testing program takes the output of the risk assessment and goes an important step further: key compliance risks are mapped to the business units and business processes where those risks are most likely to present themselves. This is sometimes called an "applicability analysis." The process flows within those operating areas are documented clearly, where both vulnerabilities and key controls are identified. This process drives the compliance testing, which is designed to be repeatable and to generate actionable results.

Great testing programs are repeatable and statistically valid. While it is good to know if a control is functioning well right now, great testing programs recognize that sustainable quality is achieved when key risks and the related controls are tested periodically using statistically valid sampling methodologies.

Great monitoring programs

Highly effective monitoring programs also have a number of key attributes in common:

The key risk and performance indicators the program monitors are meaningful. In the past, monitoring programs have relied too much on key risk indicators (KRIs) and key performance indicators (KPIs) that are easy to monitor, such as hotline call volume or ethics training completion rates. While this data is important, other data exists within organizations that provides more meaningful insight from a testing and monitoring perspective. Admittedly, it is no small task to identify the transactions or other data (for example, gifts or entertainment expenditures) that will provide meaningful monitoring value. Nevertheless, organizations that take the time to do so will likely find the value generally makes up for the effort. Moreover, well-conceived KRIs and KPIs often provide meaningful operating insights, offering business unit leaders a powerful incentive to allocate resources to gather the information.

Program owners understand how to harness the power of data. Monitoring programs sometimes rely on the availability of large amounts of data, and often that data exists in another function within the organization. The decentralized nature of data presents several challenges to ethics and compliance professionals. First, companies may need to invest in technology applications to efficiently manage the testing and monitoring processes, or in analytical tools that can process large datasets, ideally on an ongoing basis. Second, quality data is critical to this endeavor. Poor data quality and data governance must be addressed in order to implement a data-analytical approach to monitoring. Finally, the compliance function must collaborate with other internal teams—the ones that have the data—to obtain the needed information. If the company is operating with limited resources, this may require some diplomacy and a clear business case—answering the question, "What's in it for me?"—to encourage participation. In making the "case for compliance" to the business, an important message is that compliance monitoring can improve business processes, reduce redundant and manually intensive controls, and enhance decision-making.

As with testing, repeatability is key. Monitoring activities—whether or not they are automated—are most valuable when they are performed on an ongoing basis. Trend data is critical for analyzing changes in underlying business processes, as well as emerging risks. When it comes to effective monitoring programs, a "once and done" approach simply does not work.

Conclusion

As organizations look to establish best-in-class ethics and compliance programs, testing and monitoring is one of the essential components they need to build and leverage. With robust testing and monitoring programs, a company can not only gather critical information on weaknesses in their compliance program, they may also have advanced warning of any looming problems before they become significant and potentially damaging. That alone makes testing and monitoring one of the key ingredients of a world-class ethics and compliance program.

Testing and monitoring: How it works in practice

Testing and monitoring are often confused because they each can be performed on the same business processes and activities. The table below illustrates how the two differ.

Business process/ Compliance risks	Testing example	Monitoring example
Gifts and entertainment: Violations of Foreign Corrupt Practices Act and/or industry-specific regulations related to customer entertainment	Risk-based, periodic testing of gift and entertainment logs and individual employee expense reports	Data analysis of a large number of gifts and entertainment logs and aggregated employee expense reports to identify anomalies, outliers, and "red flags"
Lending Practices: Discriminatory or predatory lending practices prohibited by banking or consumer regulations	Perform "matched-pair" file reviews by comparing similarly situated protected class and non-protected class applicants who received different credit decisions or terms	Monitor distribution of applicants and customers from specific products and loan types to identify sales practices that may result in borrowers of protected classes receiving unfavorable terms

Contacts

Please contact one of our Enterprise Compliance Services leaders for more information.

Nicole Sandford
Partner | Deloitte Advisory
National Practice Leader,
Enterprise Compliance Services
Deloitte & Touche LLP
+1 203 708 4845
nsandford@deloitte.com
Stamford, CT

Keith Darcy
Independent Senior Advisor to
Deloitte & Touche LLP
+1 203 905 2856
kdarcy@deloitte.com
Stamford, CT

Maureen Mohlenkamp
Principal | Deloitte Advisory
Deloitte & Touche LLP
+1 212 436 2199
mmohlenkamp@deloitte.com
Stamford, CT

Brian Clark
Partner | Deloitte Advisory
Deloitte & Touche LLP
+1 816 802 7751
bclark@deloitte.com
Kansas City, MO

Laurie Eissler
Director | Deloitte Advisory
Deloitte & Touche LLP
+1 313 396 3321
leissler@deloitte.com
Detroit, MI

Nolan Haskovec
Senior Manager | Deloitte Advisory
Deloitte & Touche LLP
+1 212 436 2973
nhaskovec@deloitte.com
New York, NY

Kevin Lane
Principal | Deloitte Advisory
Deloitte & Touche LLP
+1 214 840 1577
kelane@deloitte.com
Dallas, TX

Thomas Nicolosi
Principal | Deloitte Advisory
Deloitte & Touche LLP
+1 215 405 5564
tnicolosi@deloitte.com
Philadelphia, PA

Holly Tucker
Partner | Deloitte Advisory
Deloitte Financial Advisory Services LLP
+1 214 840 7432
htucker@deloitte.com
Dallas, TX

Additionally, feel free to reach out to our team of former compliance officers who are located across the country and experienced in a wide variety of industries.

Martin Biegelman
Director | Deloitte Advisory
Deloitte Financial Advisory Services LLP
+1 602 631 4621
mbiegelman@deloitte.com
Phoenix, AZ
Industry: Technology

Rob Biskup
Director | Deloitte Advisory
Deloitte Financial Advisory Services LLP
+1 313 396 3310
rbiskup@deloitte.com
Detroit, MI
Industry: Consumer & Industrial Products

Timothy Cercelle
Director | Deloitte Advisory
Deloitte & Touche LLP
+1 216 589 5415
tcercelle@deloitte.com
Cleveland, OH
Industry: Insurance

Michael Fay
Principal | Deloitte Advisory
Deloitte & Touche LLP
+1 617 437 3697
mifay@deloitte.com
Boston, MA
Industry: Investment Management

Howard Friedman
Director | Deloitte Advisory
Deloitte & Touche LLP
+1 713 982 3065
hfriedman@deloitte.com
Houston, TX
Industry: Energy & Resources

George Hanley
Director | Deloitte Advisory
Deloitte & Touche LLP
+1 973 602 4928
ghanley@deloitte.com
Parsippany, NJ
Industry: Insurance

Peter Reynolds
Director | Deloitte Advisory
Deloitte & Touche LLP
+1 973 602 4111
pereynolds@deloitte.com
Parsippany, NJ
Industry: Investment Management

Thomas Rollauer
Director | Deloitte Advisory
Executive Director, Deloitte Center for
Regulatory Strategies
Deloitte & Touche LLP
+1 212 436 4802
trollauer@deloitte.com
New York, NY
Industry: Financial Services/Banking
& Securities