Unlocking an optimized compliance monitoring program

The future of monitoring and testing

Consensus across all industries on key ethics and compliance areas to enhance include technology and data analytics, risk assessments, regulatory change management, and monitoring and testing:

53%
technology and data analytics

35%
risk assessments

29%
regulatory change management

27%
monitoring and testing

Source: KPMG 2023 Chief Compliance Officer Survey (March 2023)

Evolving monitoring and testing programs

Emerging technologies, regulatory pressures, and the desire to keep costs flat or decrease costs without negatively impacting the volume and quality of compliance activities are all factors driving organizations to utilize compliance analytics for more strategic and predictive analyses. Data analysis is critical for monitoring but also to drive efficient risk and operational management. Additionally, understanding advancements in emerging technologies, such as generative artificial intelligence (GenAI), plays a role in facilitating more strategic and predictive analyses in the field of compliance analytics.

This article provides key takeaways supplemented with industry insights from chief compliance officer and chief risk officer surveys to help organizations take steps in bolstering their compliance monitoring, testing, and data analysis efforts via creating balanced testing frameworks and data analytics and unlocking automation and emerging technologies.

A business case for change

Drivers

- Expectations for "real time" compliance and risk management.
- Increased market competition and pressure to cut operating costs.
- Converging risk management and controls across operating and business units.
- Regulatory expectation for efficient and effective front line and compliance functions.

Actions

- Implement an efficient and balanced testing framework.
- Develop a better understanding of data and IT infrastructure.
- Automate compliance monitoring, testing, and data analysis.

Step 1: Balanced testing and monitoring framework

Inefficiencies across an organization usually increase based on the number of disparate testing and monitoring programs. This discrepancy may lead to an inability to detect root cause and/or systemic issues at an enterprise level. Increasingly, organizations are looking to both automate and consolidate testing, monitoring, data analysis, and surveillance activities through consistent standards, policies, framework, plans, scripts, and reporting.
In modern organizations, optimizing the testing framework is critical to mitigating risk, safeguarding assets, and ensuring financial stability.

It is important that organizations balance testing and monitoring programs to demonstrate they have a comprehensive understanding of compliance risk areas. Organizations should recognize how different areas of focus will shape testing, monitoring, and surveillance. For example, e-communications may require heightened surveillance and monitoring, employee ethics hotline may only require surveillance or monitoring, and third-party risk management monitoring for anti-bribery and corruption may require periodic compliance testing. The specific strategies an organization deploys should be strategically tied and driven by a thorough risk assessment process. Below are steps compliance leaders can take to balance their testing and monitoring frameworks.

Understand skills across the Front-line units and compliance.
To optimize testing and monitoring activities, it's important to understand the responsibilities across both front-line units and compliance, and for leadership to provide the tools and talent required to perform these activities. However, most organizations have yet to achieve optimal risk ownership within front line units. This leads to compliance teams assisting in risk mitigation rather than supporting, monitoring, and overseeing the front-line unit's risk management activities. These blurred responsibilities create inefficiencies that can result in duplicative efforts and inefficient testing.

73%
of CCOs expect regulatory expectations to rise going forward.

46%
of respondents believe that data analytics modeling for compliance monitoring will be the biggest challenge in the next two years.

53%
of respondents identified technology and data analytics as the top ethics and compliance activity to enhance.

96% of technology-driven risk management

96% of IT infrastructure and security, advanced data

91% of advanced data and analytics

are the top **three** priority areas for greater resource allocation

Compliance leaders should perform skills assessments within their functions to not only understand skill deficiencies but also identify where reliance on front line unit resources exists so that resources can be allocated accordingly. In that regard, compliance leaders should challenge front line units when they do not have the tools, skills, or capacity to properly own and manage their risk. Front line units require strong knowledge of their businesses' products and services along with the ability to test, monitor, and mitigate their compliance risks. Compliance units require complementary skills but also a deep understanding of relevant regulations and internal policies and standards in addition to strong knowledge for assessing risks across products and processes. Compliance leaders can use the skills assessment results to identify upskilling opportunities and develop talent management plans to move the compliance function closer to its targeted operating model.

Balance control and substantive testing. Control testing and substantive testing both have advantages and limitations, but it's important that organizations find the right balance between the two to evaluate critical risks and control weaknesses. Control testing helps to identify inefficiencies and opportunities for process improvements within your organization while identifying potential control weaknesses or failures.

Substantive testing, on the other hand, enables a comprehensive assessment that uncovers the minute details that may have otherwise gone unnoticed. By validating detailed records against the organization's risks, the organization can detect areas of non- compliance and effectively guide corrective action.

If an organization relies too heavily on substantive testing, it may miss control weaknesses that could lead to errors or fraudulent activities. Conversely, if an organization relies too much on control testing, it may overlook executional errors that fall outside of outlined processes and controls. Too much reliance on only one method without the other will inevitably result in gaps in the overall compliance testing program. Finding the correct balance between substantive and control testing is essential for organizations to ensure that they are accurately assessing their risks and implementing effective controls to mitigate those risks.

Leverage technology. Integrating automation into the testing and monitoring process can offer significant benefits such as cost savings, improved efficiency, and increased accuracy. Automation and data analytics allow organizations to test in real-time without the need for manual processing. Technology can be integrated into substantive testing activities, allowing organizations to substantively test across full populations rather than samples, which increases testing effectiveness while saving

38%

of Financial Services organizations are currently implementing technology and automation solutions, which includes data and analytics solutions that support artificial intelligence implementation.

Source: KPMG 2023 Chief Compliance Officer Survey (March 2023)

both time and money. The ability to conduct thorough substantive testing on a sample or entire population provides banks with increased flexibility and the ability to adjust testing plans as needed. In turn, this allows compliance teams to prioritize areas of concern and allocate resources accordingly, which in return increases the efficiency of the entire testing program.

While leveraging automation and technology streamlines the testing process, compliance technology is not at a point where manual testing can be eliminated in its entirety. Reasons include:

- **Obstacles in adoption and implementation.** Implementing technology is often restricted by upfront cost, lack of in-house expertise, and compatibility issues with legacy systems. Once implemented, automation requires technology, technical skills, and the ability to accurately identify complex situations or unique outputs into
algorithms. This is still a mindset and paradigm shift for many.

- **Data quality and availability.** The effectiveness of automated testing and monitoring is dependent on the quality and completeness of the underlying data. If the data is incomplete, inconsistent, or inaccurate, testing and monitoring results may not provide accurate results.

- **Risks with emerging technology.** Emerging technologies including GenAI enhance testing and monitoring but pose significant risks such as yielding inaccurate and/or biased results. As the
sophistication of technology used in monitoring and testing increases, so too should the technology used to manage the inherent risks introduced by these technologies.

Although the obstacles posed by technological integration may seem daunting, the increased efficiency and effectiveness gained through automation far outweigh the challenges. Compliance leaders should be encouraged by the number of enablers and frameworks developed in recent years, allowing for increased adoption and reliability.

Step 2: Mastering the data—A practical approach

52%
of survey respondents expect to enhance the promotion of compliance culture, while

51%
plan to increase the usage of technology and/or AI over the next two years to demonstrate the business value of Compliance.

98%
of respondents expect to have almost the same or slightly increased budgets for ethics and compliance functions.

97%
of respondents anticipate maintaining or increasing the number of full-time employees for these functions. These survey results indicate that organizations are prioritizing the maintenance and improvement of their ethics and compliance programs.

As organizations seek to measure their compliance program's effectiveness through monitoring, testing, and data analysis, they look to their available data to inform their testing strategy. However, for many compliance leaders, the available data is unreliable and/or unavailable, and they often have to use data resources from various testing groups within the organization,
across different functions, with competing priorities and interests. In the KPMG 2023 Chief Compliance Officer Survey, compliance leaders identified technology and data analytics as the top area
to enhance in the next two years and forecasted future budget increases within their organizations to focus on data analytics, process automation, and artificial intelligence (AI).

Compliance leaders point to several common challenges surrounding the availability of data:

- The data may have **questionable integrity or accuracy**.

- The process of **gathering data across the enterprise is often challenging,** especially in decentralized organizations where information silos exist.

- Often **compliance functions do not have the right or sufficient talent to support data intensive needs**.

- **Monitoring, testing, and data analysis activities are often driven by manual input and data interpretations**, which increases the risk of errors to propagate and limits enterprise-wide insights.

- **Regulators have adopted heightened risk and compliance standards, particularly around quality data governance, data risk and controls, and data lifecycle management** to support functions across the organization with capturing, managing, and analyzing reliable data.

The pace of technology in product delivery and operations has grown exponentially. A best practice for enhancing monitoring, testing, and data analysis activities is to include compliance professionals in the decision-making processes related to an entity's data management and IT infrastructure. By prioritizing collaboration between IT and compliance leaders, organizations stand to benefit from enhanced data analytics capabilities that

effectively consider risk management and oversight needs. For these organizations, it is common to see compliance leaders focused on:

Developing a better understanding of data and IT infrastructure: Since compliance monitoring, testing, and data analysis are only as good as the data they use, compliance leaders are increasingly teaming with IT and other cross-functional stakeholders to a) understand the relevancy of the data sources across various systems and silos, b) better understand quality of data, c) identify where pockets of data need to be further remediated based on the value of the data and the potential risks, d) assess whether there are gaps or inconsistencies in data feeds or inputs, and e) analyze the root causes of any issues.

Leaning in on building data skills and resources within compliance: The technology-supporting compliance automation for monitoring, testing, and data analysis has made significant advances, and compliance leaders should be encouraged to take advantage of the advances. Compliance leaders should use this opportunity to "lean in" and take the lead in developing
compliance automation as well as data and analytics capabilities. With a more active role, compliance leaders can equip their teams to focus on their oversight role and conduct monitoring and testing from a risk-based perspective.

Focus on enhancing monitoring and testing framework:
As compliance leaders lean in to develop data capabilities within their organizations, there are key steps they should consider prior, during, and once these capabilities are established. To start, obtaining an overview and inventory of the data and technology architecture and solutions that support the organization's efforts across the enterprise (i.e., the scope of the current data analytics capabilities and related business requirements) can be used to inform the development and enhancement of their monitoring and testing framework. These enhancements may include innovative and advanced solutions in machine learning, predictive analytics, and disruptive ways of approaching challenges that exist in large enterprises. Additionally, the enhancements could include exploring other emerging technologies, such as GenAI, which holds promising potential to enhance the development of a robust, efficient, and comprehensive technology infrastructure.

50%+
of respondents use data analytics and compliance KPI/KRI metrics to measure ethics and accountability company-wide.

Source: KPMG 2023 Chief Compliance Officer Survey (March 2023)

Step 3: Unlocking the potential for monitoring, testing and data analysis

The purpose of compliance automation is to bring together disparate data for a more effective compliance risk management program, this includes, but is not limited to, enhancing the assessment of risks, streamlining monitoring, and refining issue management. For example, an organization may aggregate data from its internal investigation system, operational systems (including transactions and product data), and employee HR and training data in order to apply queries that will enable it to better understand employee risk or specific misconduct risks within certain lines of business across

jurisdictions. By aggregating the disparate data, the analysis becomes "richer", and the metrics point out "higher-risk" areas visually for targeted monitoring, testing, and data analysis. A similar approach can be applied for managing third-party risks and unfair, deceptive, or abusive acts and practices (UDAAP) risks, among others. Without such aggregation, compliance leaders may view their data in isolation where risk factors can be unintentionally buried or may appear insignificant.

Steps to unlocking the potential

1. **Strategy** — Develop data and automation strategy for risk and compliance.

2. **Encourage** — Encourage the adoption, understanding, and involvement by compliance.

3. **Develop** — Define and prioritize key risks for which activities can be automated or digitized.

4. **Identify sources** — Data and systems available to support strategy

5. **Identify gaps** — In source data and systems to develop plan to feed into data strategy.

6. **Build** — Build capabilities within the compliance unit to systemically test and monitor risks.

Compliance leaders across industries also recognize that automated compliance monitoring, testing, and data analysis is a useful and valuable means to better allocate resources using a risk-based approach and as a tool to target higher risk areas for mitigation. As the front-line unit's testing matures with data analytics, compliance departments can focus on supporting, monitoring, and overseeing the front line's risk management activities.

Since automation can be costly to design, implement, and evaluate, compliance leaders tend to be strategic in incorporating technology into their monitoring efforts. This is made possible through the strategic imperative that monitors key performance Indicators (KPIs) and

key risk indicators (KRIs). Additionally, a powerful use of data in testing and monitoring is for addressing risks where there is a desire, and capabilities, to perform full population substantive testing. In these instances, the cost of the analytics will remain the same agnostic of the population size and can be run on a periodic basis.

Once a strategy is designed, the organization can start building the intelligence capabilities needed for proactive signaling of future risks. The continuous intelligence learning can lead to consistent and improved predictive algorithms and machine learning models to identify misconduct behaviors more proactively.
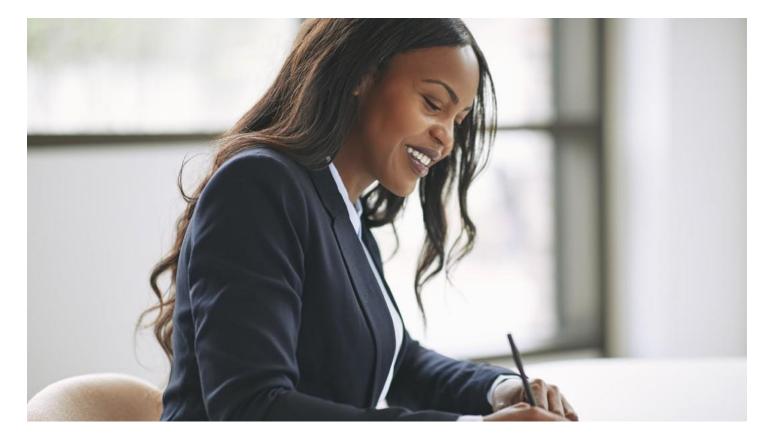
How KPMG can help

Organizations have implemented monitoring, testing, and data analysis programs that vary and are often influenced by their industry and existing regulatory obligations. Compliance continues to evolve, mature, and embrace greater predictive analytics in such areas as compliance monitoring, testing, and data analysis activities including consumer protection, payment/financial transaction monitoring, KYC, procurement/supplier diligence and contract management, sanctions screening, and transaction monitoring for suspicious activities.

Integrated platforms coupled with AI tools can help facilitate faster, more comprehensive, and more accurate monitoring, testing, and data analysis, freeing staff from repetitive- and "low-value" tasks and allowing them to focus on high-value activities that require subject matter and domain knowledge.

KPMG can assist with identification, assessment, prioritization, and development of your data analytic strategy, implementation, and associated automated tools. To help, KPMG offers the following services/tools:

- **Regulatory & compliance transformation:** To help organizations enhance compliance, integration, and automation for a stronger risk management approach.

- **Intelligent automation:** To enable organizations to achieve business-wide digital transformation, leveraging emerging technologies to transform operating models, innovate to remain competitive, and reimagine the customer experience.

- **Intelligent automation with KPMG Alliance partners:** KPMG has strategic technology alliances across the intelligent automation (IA) landscape, including IBM Watson and Microsoft, with open-source technology, deep technical resources, and KPMG accelerators to help create powerful value through advanced analytics and machine learning.

- **Data analytics:** To provide a 360-degree view of potential compliance and ethics exposures, allowing holistic evaluations of compliance program effectiveness.

Conclusion

Leveraging automation and technology to achieve greater monitoring, testing, and data analysis risk coverage is a priority for many organizations, but in order to automate, they must first take a balanced approach to developing their testing framework and focus on finding the right balance between substantive and control testing while incorporating automation into the process.

Subsequently, they must understand and master their existing data and evaluate risk to anticipate impacts and govern activities. From there, inefficiencies need to be corrected, such as reducing duplicative activities

and strengthening existing ones to meet regulatory requirements so that processes that would normally be handled manually can be automated.

Further enablement of technology and data analytics, while being strategic in its implementation to short- and long- term compliance requirements, could unlock the potential for balanced compliance monitoring, testing, and data analysis—a useful and valuable means to better allocate resources, as well as identify new talent and overall investment requirements for compliance.

Contact us

Todd Semanco
Partner, Financial Services Risk, Regulatory & Compliance
T: 412-232-1601
E: tsemanco@kpmg.com

Mike Lamberth
Partner, Financial Services Risk, Regulatory & Compliance
T: 804-241-2795
E: mlamberth@kpmg.com

Hernando Garcia **Director, Financial Services Risk, Regulatory & Compliance**
T: 212-954-3287
E: hernandogarcia@kpmg.com

Authored by Joshua Laguerre, Scott Page, and Pablo Pazos

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: in | **kpmg.com**