Monitoring and testing

Enhancing your compliance effectiveness and agility

Compliance briefing series

kpmg.com

Julie Gerlach

Julie Gerlach is a Managing Director in KPMG's Advisory practice based in Atlanta. With over 17 years of risk consulting experience, she is a national lead for KPMG's compliance integration and compliance transformation initiatives. During her career, Julie has provided internal audit co-source and SOX 404 assistance services to clients in various industries including financial services, manufacturing, and distribution. She has led internal audit assessments where she has advised clients on leading internal audit practices. Additionally, she has managed co-sourced internal audit functions and has lead team in controls documentation and testing engagements. Julie serves as a national knowledge leader for internal audit leading practices.

Julie received her BS in Accounting from St. Vincent College in Latrobe, PA and is a licensed CPA in the District of Columbia.

Amy Matsuo

Amy Matsuo is the national leader of KPMG LLP's (KPMG) Regulatory Risk practice, which advises companies on enterprise-wide compliance and other regulatory risk management issues. She leads the firm's multi-industry compliance transformation solution, serves as the program leader for the KPMG-sponsored Chief Compliance Officer Exchange, and is the service line lead for the U.S. Regulatory Center of Excellence.

Amy received the 2014 Women Leaders in Consulting Award for client service. A frequent national and board presenter, she is both published and quoted on regulatory topics, enterprise-wide compliance programs, and fair banking and conduct risk practices. Additionally, she serves on the Women's Advisory Board of KPMG and is a member of its thought leadership committee. She also is on the national nonprofit board of One Simple Wish. She holds a Master of Public Policy degree from Georgetown University and a Bachelor of Arts degree from the University of Pittsburgh.

Richard H. Girgenti

Richard Girgenti is the U.S. and Americas leader for KPMG's Forensic Advisory Services and a member of the firm's Global Forensic Steering Group. He serves as the executive sponsor for the KPMG compliance transformation initiative and the KPMG-sponsored Chief Compliance Officer Exchange.

Richard has more than 40 years of experience conducting investigations, both nationally and globally; helping clients assess, design, and implement compliance programs; and providing fraud risk management advisory services to public and private corporations as well as to federal and state government entities and not-for-profit organizations. He was also a state prosecutor in the Office of the Manhattan District Attorney.

Richard is the coauthor of two books: *The New Era of Regulatory Enforcement: A Comprehensive Guide for Raising the Bar to Manage Risk* (McGraw-Hill, April 2016), and *Managing the Risk of Fraud and Misconduct: Meeting the Challenges of a Global, Regulated and Digital Environment* (McGraw-Hill, March 2011). He holds a Juris Doctor degree from Georgetown University Law Center and a Bachelor's degree from Seton Hall University. He is a Certified Fraud Examiner.

Monitoring and testing: Enhancing your compliance effectiveness and agility

Improving compliance monitoring and testing

U.S. organizations have long been expected to monitor and audit their compliance programs[1] and generally have implemented a three lines of defense model that forms a foundation for their compliance efforts and specifically for their test activities. By allocating monitoring, auditing, and more generally test, activities across their three lines of defense[2], organizations build a more sound compliance program that better manages compliance risks and more quickly identifies any gaps in process controls that could present compliance exposure.

In today's economic climate, compliance leaders are increasingly challenged to "do more with less." This is prompting many to take a second look at their risk-based approach to monitoring, auditing and testing,[3] in an effort to more efficiently execute their obligations. This can include, seeking greater coordination and communication across the three lines of defense; specifically defining who owns responsibility for **testing** specific controls in place to mitigate each risk in order to eliminate unintentional duplication; and assessing whether they can further leverage resources and data for consistent test populations across all three lines. Others are going further- embarking on a journey to realize a more systematic, disciplined, and sustainable approach to their monitoring and testing activities that is also more agile and cost-effective.

This article focuses on how compliance leaders are executing their monitoring and testing responsibilities; how they are seeking to further enhance their monitoring and testing activities to realize greater value in their compliance efforts,[4] the role of data and technology in compliance monitoring, and also current challenges. This article includes insights from KPMG professionals' firsthand discussions with executives and their stakeholders and provides key takeaways to help organizations bolster their compliance monitoring and testing efforts.

[1] The U.S. Sentencing Guidelines set forth in Section 8 that an "organization shall take reasonable steps—(a) to ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct; (b) to evaluate periodically the effectiveness of the organization's compliance and ethics program.

[2] Generally organizations **consider monitoring** to be the responsibility of the compliance department (second line of defense) and within more mature organizations, also a first line of defense responsibility. In contact **auditing** is the sole responsibility of the Internal Audit department.

[3] The term "Testing" is used extensively in the Financial Service industry. In the Federal Reserve's bulletin **"Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles,"** SR-08-8, dated October 16, 2008, the regulator refers to "monitoring and testing," attributing testing responsibilities to the second line of defense. Per this source, Compliance testing is necessary to validate that key assumptions, data sources, and procedures utilized in measuring and monitoring compliance risk can be relied upon on an ongoing basis and, in the case of transaction testing, that controls are working as intended."

[4] For additional steps that organizations can undertake to move towards greater agility and proactive compliance management to realize the value of compliance (complementary to a compliance monitoring and testing program) see KPMG's "The Compliance Investment" at https://advisory.kpmg.us/content/kpmg-advisory/risk-consulting/compliance-transformation/compliance-investment.html.

The journey forward: How a retailer improved its monitoring capabilities

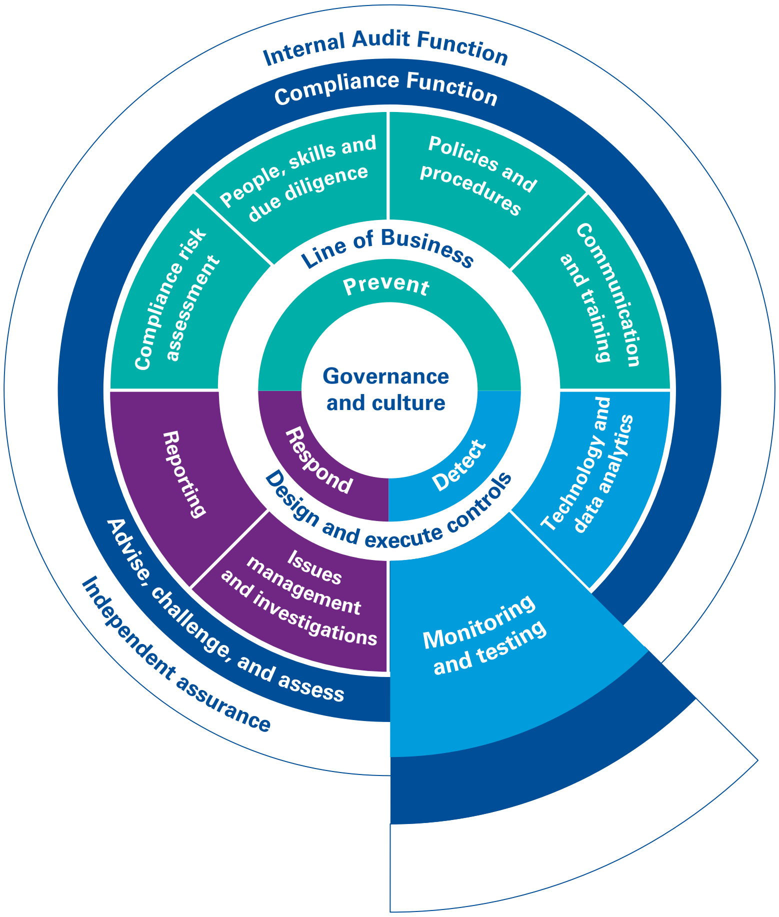
A Fortune 100 retailer faced regulatory pressure to enhance components of its compliance program in order to comply with Anti-Bribery and Corruption (ABC) regulations. Regulators questioned the organization's control environment and its ability to detect and report potential violations. The organization's compliance leaders recognized the need to improve their compliance activities with a goal of achieving a sustainable and risk-based program. They enlisted external subject matter experts to assist with several tasks: inventory the organization's global internal control structure across all three lines of defense; assess the current control environment; design an enhanced control structure, inclusive of its technology infrastructure; and test the new controls to ensure they are functioning as designed and in a risk-based and sustainable way.

During this large-scale multi-year project, compliance leaders worked with these subject matter experts to: design a global process with the ability to be customized for specific market conditions; embed more accountability in the business as the first line of defense, including by assigning more monitoring responsibilities to supervisors; create a centralized governance structure with responsibility for elements of program effectiveness assigned to senior leaders in finance and compliance; and establish greater visibility for compliance leaders into their Anti-Bribery and Corruption (ABC) compliance risks globally, enabling them to better spot risk indicators and identify root causes. Fundamental to this project was enhancing the organization's technology infrastructure to enable better dash-boarding and Key Risk Indicators (KRIs) and to address changes to its human resources models.

Stakeholders in the organization have realized greater compliance agility and effectiveness in their new targeted control environment. They also recognized the benefit of having all stakeholders at the table at the beginning of such an initiative to agree on the design of the control environment and the goal to enhance monitoring capabilities. In addition, they learned how a cross-functional team can enhance sustainability of the changes while also helping to reduce over-engineering of the process and prevent a control environment that is viewed as more restrictive than needed for compliance.

The compliance framework

Monitoring and testing are key elements in a compliance program framework, as shown below. Testing and monitoring exercises are intended to provide information to compliance leaders and senior executives about the operation of compliance controls across the organization, provide evidence to support an assessment of the operating effectiveness of a control system, identify abnormalities indicative of internal control failures, potential misconduct, potential compliance violations, and consumer or customer harms.


Internal Audit Function
Compliance Function
People, skills and due diligence
Policies and procedures
Compliance risk assessment
Communication and training
Line of Business
Prevent
Governance and culture
Respond
Detect
Reporting
Technology and data analytics
Design and execute controls
Issues management and investigations
Monitoring and testing
Advise, challenge, and assess
Independent assurance

How to adapt an inherited structure

Today's compliance leaders often have inherited legacy governance, compliance, and internal audit structures that may predate organizational efforts to make compliance a stand-alone entity. These legacy structures continue to have an impact in a variety of ways. Most significantly, they can result in overlapping responsibilities between compliance and internal audit, confusion in reporting lines, diverse technology systems, and other obstacles to change. Legacy structures often hamper a chief compliance officer's (CCO) vision of targeted program enhancements and can obscure an understanding of where specific testing and monitoring responsibilities reside within the organization.

Roles and responsibilities in the three lines of defense

Compliance leaders sometimes differ in the nomenclature they use to describe the "testing" tasks assigned to each of their lines of defense; however, typically the term **"testing"** encompasses activities within each of the three lines of defense. Organizations generally allocate monitoring, testing, and auditing responsibilities among the three lines of defense as follows:

— **Internal audit (3rd line):** Internal audit constitutes the third line of defense and provides independent assurances.[4] Internal Audit tends to focus on the organization's internal controls and processes, and in recent years has expanded to perform operational and efficiency reviews.[5] The internal audit function typically also has responsibility for auditing compliance requirements with applicable laws and regulations across the organization, and it may also audit the compliance function such as the CCO and the ethics hotline. In practice, some organizations may divide responsibilities between internal audit and the compliance function based on the materiality of risks.

— **Compliance function (2nd line):** The various risk control and compliance oversight functions established by management constitute the second line of defense. This line thus has responsibility for "overseeing" compliance with laws and regulations.[6] The compliance function typically conducts "monitoring," "surveillance," and "testing" specific to the compliance risks or regulations affecting their organization. They therefore have responsibility for conducting regulatory reviews and assessments of whether the lines of business meet their regulatory and compliance requirements.

— **Business and operations units (1st line):** Management control is the first line of defense in risk management. This is the function that is expected to **own and manage compliance risks and** is also responsible for implementing corrective actions to address process and control deficiencies.[7] First-line functions typically have responsibility for supervision of compliance within their unit and have an established supervisory program that helps assess and evaluate compliance risks. This includes "quality assurance reviews" that are a component of monitoring.

[4] See Also the Institute of Internal Auditors (IIA) Position Paper "The Three Lines of Defense in Effective Risk Management and Control," January 2013 at https://na.theiia.org/standards-guidance/Public Documents/PP The Three Lines of Defense in Effective Risk Management and Control.pdf

[5] See "The New Era of Regulatory Enforcement: A comprehensive guide for Raising the Bar to Manage Risk" by Richard H. Girgenti and Timothy P. Hedley at page 39.

[6] Id. Note: the second line of defense is generally considered to include compliance, risk and legal.

[7] Id.

Irrespective of the terminology an organization uses, compliance leaders need to ensure the terminology is consistent across the enterprise and well understood by employees. In addition, having clearly defined roles and responsibilities for each line of defense in the monitoring and testing structure helps a compliance leader to realize greater efficiencies (potentially through elimination of duplicate test work and/or centralization of monitoring and testing activities) and importantly to instill greater accountability.

To this point, compliance leaders should also be actively engaged in determining how their organizations can more efficiently and effectively enhance their monitoring and testing approaches. In their journeys to realize more refined monitoring and testing, compliance leaders are frequently focused on the following areas:

— **Is there duplication in our test work, and if so how can it be reduced?** Through closer coordination and communication across the three lines of defense, an organization can reduce testing duplication. This can be achieved, in part, by organizing meetings between the compliance and internal audit teams at the beginning of the year to discuss the anticipated scope of test work for each line; coordinate timing and scopes, if possible; and streamline approaches. For example, if internal audit is auditing a particular risk for the year, the compliance team may deprioritize their testing of that same risk until the following year.[8] Alternatively, some organizations have empowered internal audit to rely on the compliance test work or monitoring of a particular risk, when the risk assurance function has satisfied requisite standards, and issue a "reliance audit."

— **Should we establish a centralized compliance testing and monitoring team?** Establishment of, or migration to, a centralized compliance testing team can enable an organization to achieve more robust governance and oversight of compliance through better aggregation of test results and, consequently, more comprehensive data analytics. It also can enable a more standardized and consistent testing approach across the organization. Due to the nature of a centralized structure, such a team tends to be better situated to identify emerging risk areas around the organization, identify and incorporate regulatory changes, and integrate risk trends into their annual business (and compliance) plans.

[8] Note: for more heavily regulated industries such as financial services, this approach may not be an option.

These benefits are driving some compliance leaders to embark on a restructuring to centralize and consolidate their compliance testing and monitoring team. To accomplish this restructuring, compliance leaders need to consider their current monitoring and testing capabilities across the organization and identify what shifts and changes across its people, processes, and technology are needed to accomplish the centralization. This change typically requires the organization to break down previously existing test siloes within the business units or regulation-specific infrastructures. While there are many benefits to implementing a centralized monitoring and testing team, the fact remains that if organizational data is poor or incomplete, or if data cannot consistently be available to the team, the impact of restructuring will be limited.

— **How can we empower the first line of defense more?** To empower the first line of defense, the first line must feel vested in and "own" their compliance. Compliance leaders can encourage this ownership, in significant part, by apportioning responsibility to the first line to monitor their own compliance; periodically/regularly testing the first line's monitoring results; and then providing the first line with comprehensive feedback on their compliance efforts in a timely manner. For this strategy to work, the first line must be able to obtain data and any available KRI metrics specific to their business and operations, which will be foundational in the first line's design of a risk-based approach.

Once this foundation is established, compliance can expect the first line to implement a targeted, risk-based approach to assessing their compliance risks, to identify potential gaps, and to prioritize controls for enhancements and ways to potentially de-risk (as applicable). Overall, empowering the first line will yield a stronger compliance structure as well as greater compliance effectiveness and efficiencies through earlier evaluation of risks and control gaps.

— **How can we improve consistency and coordination in our reporting?** A consistent methodology and testing and monitoring terminology, applied across all risk assurance functions, better supports enterprise-wide reporting to the board and reporting feedback to the first line.

— By implementing a consistent (and aligned) methodology and terminology, compliance leaders are better able to design an Enterprise Risk Management (ERM)-type dashboard for presentation to their boards (and other stakeholders). A well-designed dashboard summarizes the compliance risks across the enterprise, provides a short description of those risks, identifies senior-level "ownership" of the risks, and (leveraging the consistent terminology) identifies where monitoring and testing coverage exist (across the three lines of defense). This integrated, enterprise-wide view helps compliance leaders demonstrate they have appropriate coverage and standards in place for monitoring and testing across all three lines of defense and supports their overall compliance priorities and strategies. It can also help illustrate that policies and standards are being followed and that appropriately skilled personnel are involved in efforts. By aligning to the ERM methodology, greater consistency in reporting and assessment of risks can also occur.

Similarly, a consistent approach can benefit reporting and feedback on monitored/tested risks to business process and risk owners and senior leaders within the first line where the compliance risks exist and are being managed.

Developing a risk-based compliance testing plan

To enhance the value their organizations derive from compliance monitoring and testing efforts, compliance leaders increasingly recognize the need to ground their efforts in their enterprise-wide compliance risk assessment.[9] By using the compliance risk assessment as the foundation for their testing and monitoring efforts, compliance leaders can design an annual plan that more strategically targets specific areas of risks, including the organization's highest risks or emerging risk areas. Since some organizations may have deeper and more robust analysis in their compliance risk assessments than do other organizations,[10] the benefit of using the compliance risk assessment will vary according to the detail and specificity. Regardless, for all organizations the compliance risk assessment should provide compliance leaders with a basis for defining their compliance risk universe in a consistent manner and can assist compliance leaders in identifying priority risks for inclusion in the testing plan. For example, the compliance risk assessment may identify certain jurisdictional risks, product and services risks, misconduct risk, consumer or customer risks, prior test results (including by audit and from regulatory exams), and changes in their operations, that should be considered in the planning process.

In furtherance of a risk-based monitoring and testing approach, compliance leaders are also progressively incorporating the following as inputs in their annual plans:

- Employee surveys which can also provide valuable intelligence as to the organization's highest risk compliance areas and further compliance leader's understanding of how their organization is doing in identifying and mitigating risks and how well the compliance structure operates.
- Hotline reports, e-mail, social media, and keyword searches.

Additional benefits of a well-designed, risk-based compliance testing strategy also include the following:

- More strategic optimization and allocation of subject matter resources
- Ability to craft a more proactive approach to the mitigation of compliance risk and trends across the organization
- A deeper understanding of the compliance program effectiveness

Compliance monitoring and testing hot spots

Some recent trends in the scope of compliance testing and monitoring programs include risk-based testing of:

- Third-party relationships based on a vendor risk assessment—this may include testing to confirm that the third party is meeting their legal, regulatory, and contractual obligations, and that their internal monitoring processes appear sufficient to identify compliance issues[11]
- Compliance policies and procedures to assess if implemented compliance processes align to the organization's documented approach and to understand/demonstrate that the compliance program is not just a "paper program"
- Consumer/customer complaints that could reflect compliance trends including in harms or misconduct
- Emerging compliance risks identified during the year, including based upon any regulatory enforcement actions or issued guidance within that time frame
- Root cause analysis and impact assessments of monitoring and testing results.

Based on their compliance exposure, risk profile, and tolerance, compliance leaders should consider if including any of these topics in their monitoring and testing programs makes sense.

[9] Note: Although not a focus point of this discussion, compliance leaders can also benefit from considering and consulting the organization's ERM risk assessment when developing their annual testing plans.

[10] The regulatory requirements and expectations applicable to an organization, tend to impact the level of specificity compliance leaders document in the organization's compliance risk assessment as well as the extent of linkages between the risk assessment and the compliance monitoring and testing approaches. For some organizations facing less regulatory scrutiny in this program component, compliance risk assessments tend to remain targeted to specific known regulatory risks (e.g., anti-bribery and corruption, third-party programs, trade sanction or fraud), and monitoring and testing plans tend to be reactive to past risks identified.

[11] Note: There should also be alignment between compliance testing plans and overall vendor management efforts.

The role of technology and data analytics in monitoring and testing

As organizations seek to measure their compliance program effectiveness through testing and monitoring, they typically look to their available data to inform their testing strategy. Specifically, data is foundational to a compliance leader's understanding of the organization's compliance risks and to implementing a risk-based approach to testing, with prioritization of the greatest risks. Yet, for many compliance leaders, their available data is lacking—it may have questionable integrity and/or accuracy or may not be able to be aggregated enterprise-wide. This is particularly prevalent in organizations that have inherited a technology infrastructure that is decentralized and siloed. In such instances, the organization likely has multiple technology systems, and separate efforts are untaken by each business unit or function with each having their own data scientists for their specific testing and monitoring efforts. Consequently, their management reporting is often driven by manual input and data interpretations. Limited work flow functionality exists, impacting the analytics that can be performed to identify trends, or to segment by risk factors enabling proactive maintenance of risks.

Without proper aggregated data for analysis, compliance leaders are flying (somewhat/at least partially) blind in developing their risk-based testing and monitoring approaches for the year. Consequently, these organizations often recognize that their first priority in realizing better monitoring and testing capabilities is to understand and potentially enhance their technology infrastructure. In so doing, they can derive more robust data to inform their monitoring and testing efforts and create a more seamless, ongoing, consistent, and sustainable monitoring testing process. For these organizations, it is common to see compliance leaders focused on:

- **Developing a better understanding of their data and Infrastructure:** Since technology is only as good as the data it uses, compliance leaders are increasingly testing their data to garner a better understanding of data quality; identifying where pockets of data need to be further remediated based on the value of the data and the potential risks; assessing whether there are gaps or inconsistencies in data feeds or inputs; and analyzing the root causes of any issues. As such, conducting data quality assessments across their three lines of defense is at the forefront of many compliance leaders' efforts.

  Also, to deepen their understanding of their technology infrastructure, compliance leaders can engage with cross-disciplinary stakeholders to document their current-state capabilities. This includes, in part, an overview and inventory of the data and technology architecture that supports the organization's compliance efforts across the enterprise; the scope of the current data analytics capabilities; the automated monitoring and testing capabilities; and the business requirements. This documented analysis can then be utilized in designing more tailored monitoring and testing of automated controls within the infrastructure, and be leveraged to identify priority areas for enhancements.

- **Better data coordination across the three lines of defense:** As compliance leaders look to enhance their coordination across the three lines with respect to data extractions and usage, they are focused on designing coordinated processes for data requests, data extractions, and data use as well as the implementation of shared repositories and tools to house the data across the organization. This type of coordinated and integrated approach to data extraction and collection can help minimize multiple requests for similar data from the IT or operations teams involved in the data extractions. It can also help provide a consistent starting point for all testing and a consistent understanding of controls implemented across the enterprise. It may be that existing Governance Risk and Compliance (GRC) systems provide an acceptable unified platform for sharing this data, although compliance leaders often find the systems lack repository capabilities and sometimes do not meet their compliance needs for specific data analytics.

- **Assessment of compliance controls:** Compliance leaders are seeking to understand if their existing compliance controls are based upon outdated data and risk assessments, determined at a point in time. If so, they may have unintended and hidden compliance risks, and compliance controls may require further augmentation to reduce risks. This can be process-level controls in the first line or second line controls.

In contrast, organizations with a more mature technology infrastructure and data capabilities can more easily use data across their enterprise on their compliance risks to inform their monitoring and testing strategies. In their compliance journey, these organizations typically seek to realize more value from their enhanced technology infrastructure, including by:

- Validating data feeds into and out of their various systems
- Developing more predictive analytics in order to proactively identify potential misconduct
- Enhancing the risk and performance indicators they derive, by aggregating data from disparate data sources that may seem disconnected or unrelated, but combine to paint a more robust vision of the organization's risks. For example, compliance leaders may opt to enhance the organization's technology to facilitate greater identification of behavior patterns that indicate a high risk of corruption or noncompliance in distribution channels; or seek to improve the data integrity of its transactional coding of payment to better monitor its third-party and anti-bribery and corruption risk and trends therein. In both examples, organizations will benefit from improved visibility of their risks, and better monitoring and testing controls.

Increasingly, compliance leaders recognize the need for data analytics and an adequate technology infrastructure to support their compliance efforts, and specifically their compliance testing and monitoring efforts. With the recognition that resources and funding are limited, compliance leaders need to allocate funding to the technology enhancements that will yield the greatest benefit to their compliance program. Understanding their current state can significantly help these leaders strategically prioritize potential data and infrastructure enhancements; design a future state that is realistic (from a time line and investment perspective) and develop a well-thought-out plan to bridge the gap, in conjunction with all relevant stakeholders.

Data considerations:

- **Multiple Systems and Platforms** – Products are administered on different systems, creating inconsistent data taxonomies.
- **Incomplete data** – Lack of historical or detailed data, and limited availability and access of data maintained in disparate systems.
- **Data inconsistency** – Lack of standardized data usages, inaccurate data, or duplicate records, reviews and work flow review may be challenging to complete with a high degree of consistency (still leaving potential exposure).
- **Data integrity** – Data is entered into the system manually and could be subject to human error. Fields could be left blank or populated inappropriately.
- **Structure/unstructured** – Different types of data are often difficult to analyze with traditional data analysis models.

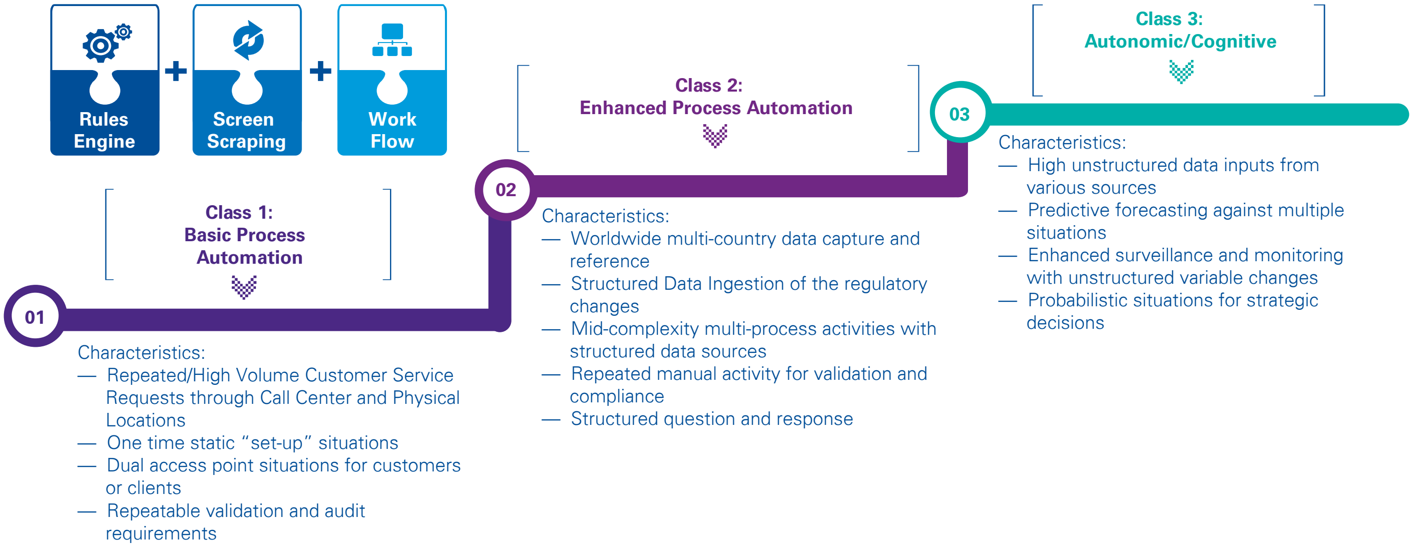
Predictive analytics becomes a priority, and use of digital labor is on the rise

The idea of predictive analytics is to bring together disparate data for a more robust and sophisticated assessment of risks. For example, to employ predictive analytics, 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 jurisdictions. By aggregating the disparate data, the analysis becomes "richer" and visually the metrics point out "higher risk" areas for targeted monitoring. A similar approach can be applied for managing third party risks, and FCPA risks, among others. Without such aggregation, many compliance leaders continue to view their data in isolation where, unintentionally, risk factors can be buried or may appear insignificant.

Compliance leaders across industries also recognize that predictive analytics are a useful and valuable means to better allocate resources using a risk-based approach and as one tool to target higher risk areas for mitigation. Since predictive analytics can be costly to design, implement, and evaluate, compliance leaders tend to be very strategic in incorporating predictive analytics into their monitoring efforts. First, they identify the targeted compliance risks they want to mitigate; the data (and systems) that may be available and implicated in this risk (as well as data that does not yet exist); and the additional pieces of data that they will ultimately need to have available to use in their predictive analytics monitoring. Once a strategy is designed, the organization can start to build the intelligence capabilities it needs for proactive signaling of future risks.

This is particularly true in the financial services industry, where compliance leaders are increasingly focused on designing and implementing robust predictive analytics, driven by regulatory expectations as well as by historical risk exposure from "rogue" employees.[12] In addition, these compliance leaders are also intensifying their efforts to further cognitive automation, integrate digital labor, and establish an enterprise-wide regulatory automation infrastructure. Digital labor incorporates both technology and predictive elements and can enable an organization to progress from utilizing automated controls in its testing and monitoring efforts to digitizing the process and test work to ultimately creating cognitive abilities within a regulatory automation infrastructure.[13]

Implementing Digital Labor



Class 1:
Basic Process Automation

Characteristics:
— Repeated/High Volume Customer Service Requests through Call Center and Physical Locations
— One time static "set-up" situations
— Dual access point situations for customers or clients
— Repeatable validation and audit requirements

Class 2:
Enhanced Process Automation

Characteristics:
— Worldwide multi-country data capture and reference
— Structured Data Ingestion of the regulatory changes
— Mid-complexity multi-process activities with structured data sources
— Repeated manual activity for validation and compliance
— Structured question and response

Class 3:
Autonomic/Cognitive

Characteristics:
— High unstructured data inputs from various sources
— Predictive forecasting against multiple situations
— Enhanced surveillance and monitoring with unstructured variable changes
— Probabilistic situations for strategic decisions

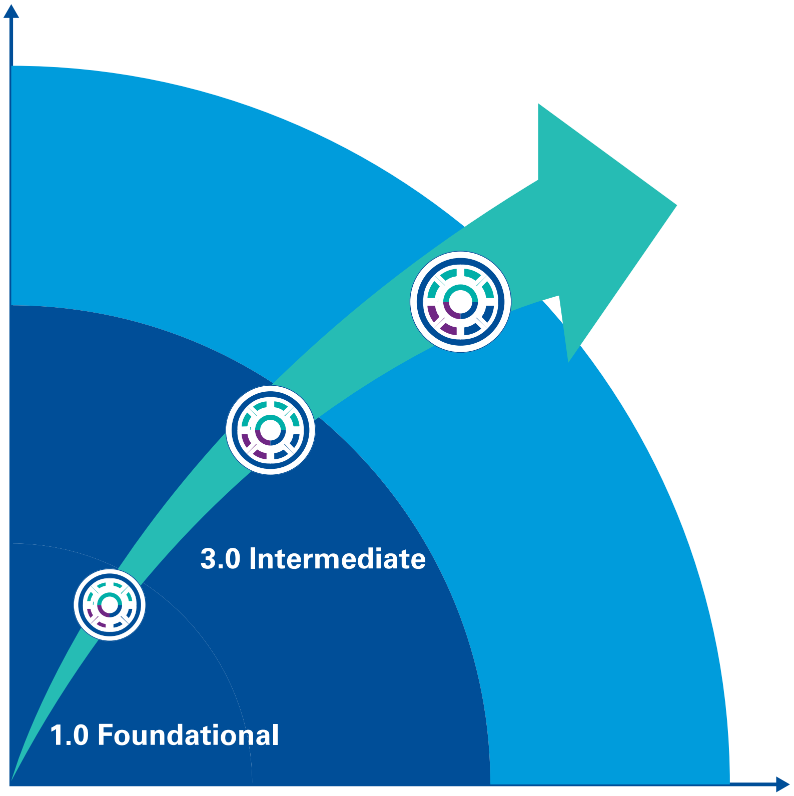
[12] For further insights pertaining to the financial services industries in monitoring and testing and specifically innovations in data and technology, see https://advisory.kpmg.us/content/dam/kpmg-advisory/risk-consulting/pdfs/2016/transformation-to-proactive-insights.pdf

[13] Specifically, KPMG considers there to be three classes within a digital labor approach: Class 1 – basic process automation; Class 2 – enhanced process automation; and Class 3 – full automation with cognitive abilities.

Enhancing compliance monitoring and testing

Compliance leaders often decide to launch phased or incremental projects to enhance the organization’s compliance monitoring and testing approach. This may be based on where the organization is in the maturation continuum, its desired state, and the aggressiveness of the planned changes and enhancements.

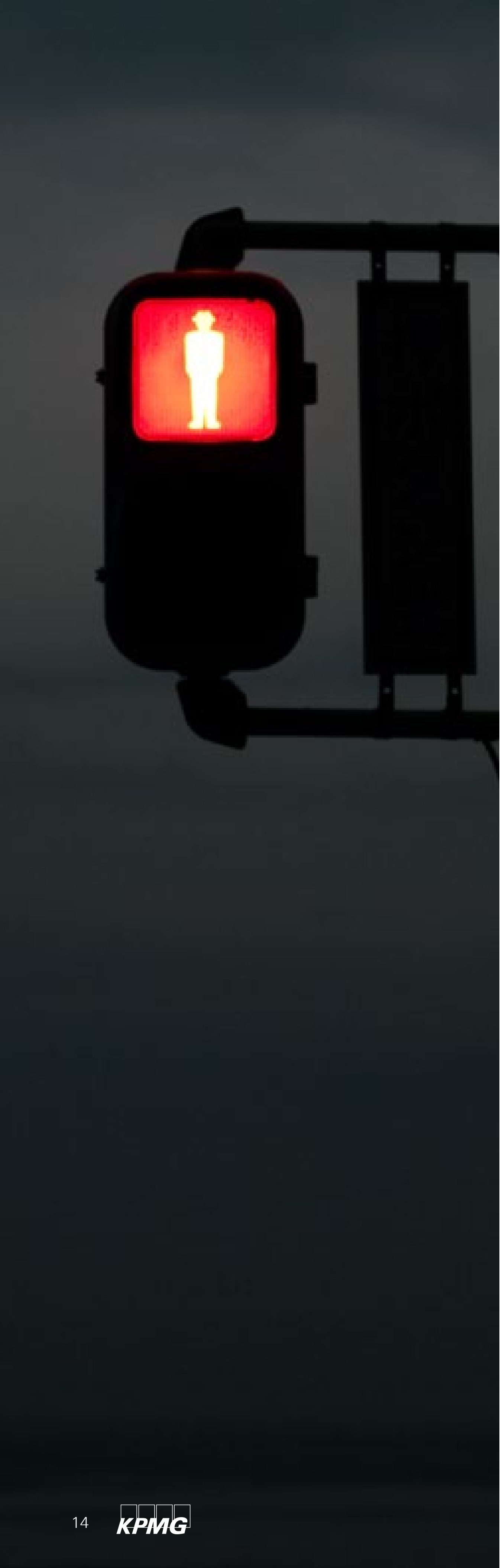
Target program continuum



Some characteristics that reflect where an organization sits on the maturation scale are depicted below:

Monitoring and Testing				
Foundational	**Developing**	**Intermediate**	**Mature**	**Advanced**
— Basic compliance monitoring and testing exists — The organization has implemented a highly manual process to identity and respond to risk(s) as they arise	— Siloed teams exist in LOBs or operations, with limited resources and SME support — Monitoring and testing is regulation-based with no enterprise-wide aggregation — Irregular monitoring — Insufficient testing for risks — Processes differ from policy and procedure	— Small team in compliance with limited scope and resources — High-level policies and procedures documented and implemented, and processes for some centralized monitoring — Testing occurs regularly but with limited control effectiveness; developing a disciplined and coordinated enterprise-wide risk assessment — Developing enhanced automation of monitoring and testing practices across the organization	— Centralized, established monitoring and testing team with dedicated resources — Detailed and documented policies, procedures, and processes all in alignment with minor exceptions — Ongoing, frequent enterprise-wide testing occurs including of design and effectiveness	— Well-established, centralized monitoring and testing team with SMEs; robust monitoring and testing policies, procedures, and processes all in alignment with no exceptions — Predictive and reflective, leveraging technology, data, and understanding of risk — Enterprise-wide testing based on annual risk-based plan and ad hoc adjustments to address emerging risks — Detailed control testing linked to regulatory risk — Algorithms and decision trees link operations to predictive compliance metrics — Data-driven environment (data aggregation of common risk taxonomies) to facilitate timely issue identification, root cause analysis and remediation, and reporting

As compliance leaders look to enhance their organization's compliance monitoring and testing, they must look across the entire compliance program framework to assess the needed enhancements. They should first consider what targeted future state they want, the investment required to achieve it, and the projected impact on the organization's compliance. Enhancing compliance monitoring, testing, and auditing typically requires changes to the technology infrastructure, data quality and/or accessibility as well as implementation of new controls and processes. Compliance leaders thus need to consider the connections between each of the components of the compliance program framework. As compliance testing enhancements are made or as testing results identify issues, part of an effective compliance journey includes not just addressing enhancements or issues in a silo, but also considering comprehensive linkage across all components of the framework. This linkage is particularly important to the compliance risk assessment process as changes to strengthen a compliance monitoring and testing program should have an impact on the compliance risk assessment—typically reducing residual risk.



Considerations Checklist

- If not already in place, consider implementing consistent terminology across your organization to clearly denote what responsibilities each line of defense has in the compliance program (e.g., quality assurance reviews, monitoring, surveillance, auditing).
- Understand how your compliance function prioritizes risks for testing and monitoring purposes and evaluate if enhancements should be undertaken.
- Assess whether there are any gaps or overlaps in your testing coverage across the three lines of defense and whether this is intentional (compensating controls) or if testing coverage can be adjusted to enable greater efficiencies.
- Understand what communication and coordination occurs among your three lines of defense in their testing roles and assess if this should be further enhanced.
- Assess your resource allocation approach for compliance monitoring and testing across your three lines of defense and whether your staffing model can be adjusted for greater efficiency and to better utilize the subject matter knowledge of those resources.
- Understand how your organization's data integrity and system infrastructure impact your monitoring and testing work, including your ability to monitor compliance risks and aggregate data for meaningful, valuable metrics.
- Identify any predictive analytics that you may want to consider to improve your risk-based identification and monitoring of compliance risks.
- Evaluate whether centralization of monitoring and testing efforts within your organization would be beneficial to achieve greater consistency, efficiency, and effectiveness.
- Understand what you are reporting to the board of directors and other stakeholders about what your monitoring and testing assessments and findings consist of and whether it they are aligned with your regulators' requirements and expectations.
- Evaluate the effectiveness of your monitoring and testing efforts.

Conclusion

Compliance leaders are improving their ability to use the three lines of defense to derive valuable insight into an organization's control and risk environment and to understand the overall effectiveness, sustainability, and agility of its compliance program. Further, many compliance leaders are transitioning to an approach centered on data and analytics, recognizing that a monitoring program inclusive of data analytics offers many benefits and enhances compliance effectiveness. These benefits can include reduction of duplicative activities and strengthening of existing activities to meet regulatory requirements; better and more meaningful reporting of emerging risk metrics, compliance themes, and required regulatory reporting; connectivity and alignment to issues management where compliance issues are inventoried, prioritized, remediated, and reported; further enablement of technology and data analytics to support root cause identification; and greater understanding of data and risk to anticipate impacts and govern activities.

Contact us

Todd Semanco
T: 412-232-1601
E: tsemanco@kpmg.com

Amy Matsuo
Compliance Transformation Leader
T: 919-380-1509
E: amatsuo@kpmg.com

Julie Gerlach
T: 404-222-3389
E: jgerlach@kpmg.com

Rich Girgenti
Compliance Transformation Sponsor
T: 212-872-6953
E: rgirgenti@kpmg.com

Acknowledgements: authored by Nicole Stryker and Phil MacFarlane; content contributors: Ray Dookhie, Karen Staines, and Melissa Mastro

kpmg.com/socialmedia

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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.