KPMG

# Harnessing data and analytics to transform compliance

kpmg.com

# Executive summary

In the past 10 years, amazing advances in technology and automation have presented great opportunities for organizations to innovate and realize efficiencies. Yet, as technological capabilities expand, so too do regulatory expectations, including what compliance programs should be. Today's Chief Compliance Officers (CCOs) are expected to have certain data and analytics (D&A) available at their fingertips from across the enterprise, to recognize and question potential indicia or red flags that are visible in the data and also to utilize D&A to refine and focus their compliance efforts in a more risk-based manner. Recent Department of Justice (DOJ) guidance issued for fraud and compliance programs and the recent regulatory enforcement actions make clear that foundationally, regulators expect more. Proactive planning is needed today.

The question is, can your organization meet these heightened demands for compliance D&A? And how can you help your organization to prepare to meet regulatory expectations today and into the future. This paper sets forth five key areas that CCOs can utilize as they chart a course for more robust, and predictive, D&A capabilities. This includes:

1. Evaluating your compliance program data needs;
2. Assessing the data quality;
3. Sharing compliance data across the three lines of defense;
4. Integrating and automating data analytics for greater compliance insights;
5. Crafting predictive analytics that your organization needs.

The viewpoints presented in the following pages leverage the experience and insights of KPMG LLP's (KPMG) compliance professionals and our top-rated D&A practice, which Forrester ranked as the leading provider in the insights services market.[1]

[1] Forrester Wave: Insights Services Providers, Q1 2017

KPMG

# Regulatory and business drivers for data and analytics

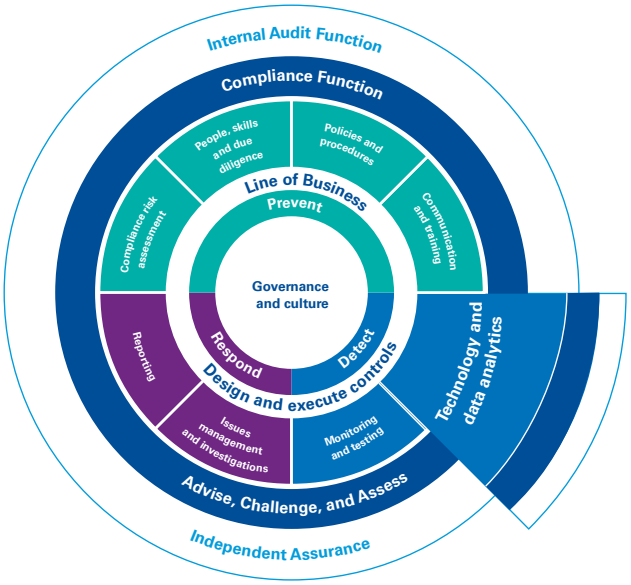
KPMG's compliance framework[2] highlights data and analytics as a core component of an effective compliance program. Yet increasingly, data and analytics underpin an entire compliance program and provide a mechanism for compliance functions to prevent, detect and respond to ethical misconduct issues and potential wrongdoing, as well as make more informed decisions. This includes:

— Greater understanding of risks and governance activities;

— More effective root cause identification;

— Better reporting of emerging risk metrics, compliance themes, and required regulatory reporting.

**The role of data analytics in a compliance program**




**Playing catch-up on compliance analytics**

KPMG's CCO Survey found that data analytics is one of the least mature components of most compliance programs.

— 51% of CCOs rank improving data quality for risk data aggregation and risk reporting as a top compliance challenge.

— Just 47% leverage data analytics and other technology processes to conduct root cause and trending analysis.

— Only 40% integrate KRIs and KPIs into broader governance, risk and compliance efforts.

— Only 48% utilize standardized KRIs and KPIs in the development of their compliance monitoring and testing approaches and plans.

While most CCOs realize the potential value to be gained by harnessing data analytics, they face practical, organizational, and technical challenges as they seek to tap into and analyze streams of business data to better track and address compliance risks.

KPMG recently surveyed CCOs of organizations representative of the FORTUNE 100 to gather their perspectives on their compliance journey, including the use of data analytics.

[2]The KPMG framework integrates the U.S. Federal Sentencing Guidelines suggestions for compliance programs as a foundation, and goes beyond those concepts to incorporate regulatory requirements and guidance from cross-industry regulators and leading compliance initiatives.

## Data and analytics – The underpinning of an effective compliance program

**Making the business case for further investment**

Data and analytics can provide CCOs and key stakeholders with a 360-degree view of potential compliance and ethics exposures. When data can be harnessed from disparate systems, compliance leaders are better equipped to holistically evaluate their compliance programs' effectiveness and to identify real-time actionable indicators of risk and performance. This allows compliance leaders, and other stakeholders such as senior management and the Board of Directors to have greater transparency (and assessment) of enterprise-wide compliance risks, to further embed accountability across the first line of defense, and to more strategically deploy resources and investments.

Boards of Directors often find themselves dependent on compliance and other stakeholders' metrics to assess the health of their compliance programs. When metrics or key risk indicators (KRIs), in particular, are decentralized, Board of Directors often find it more challenging to understand the scope of the risks present and to form a cohesive and accurate view of compliance risks. Siloed views of risks can inadvertently underestimate risk impacts or probabilities of harms. Therefore, the Board of Directors must have access to metrics that it can question and utilize in order to:

- Better safeguard its organizations against regulatory and compliance risks;
- Remain vigilant in identifying risks;
- Have confidence that the organization is operating in a safe and sound manner;
- Be alert to whether the business, risk and compliance functions are addressing current as well as emerging risks in a timely manner.

Often, how organizations prioritize investment in data and analytics is impacted by the risk management priorities of the Board of Directors, the organization's culture, revenue drivers, relative risk exposure and cost models.

**KRIs and KPIs:**
KRIs and KPIs are often critical predictors of events that might increase the organization's risk exposure and strong early warning signs of potential problems to come so they can be monitored and mitigated. For this reason, KPIs and KRIs can be catalysts, enabling compliance leaders to make smarter compliance decisions and more effectively manage compliance risks.

# Evaluating your compliance program data needs

When it comes to data analytics, many compliance leaders are challenged first and foremost with where to start. Organizations today collect and store massive amounts of data—financial data, transaction data, employee data, customer data, IT data, third-party data, and more. While compliance leaders recognize how critical data is to their compliance efforts and how valuable it can be in understanding organization-wide risk and opportunities for strategic and proactive compliance efforts, more than a few acknowledge the sheer amount of data is overwhelming, and how easy it is to get lost searching for correlations and trends with no discernable benefit at the end of the day. Many CCOs also find it challenging to understand what data is indicative of compliance program health or should be utilized to predict future risks.

For CCOs looking to evaluate their compliance program data needs, the items below can be informative first steps:

— **Refer to the organization's compliance risk assessment**
CCOs should focus data-related efforts on their most critical compliance risks. The organization's compliance risk assessment should establish the compliance risk universe and what the organization understands its most critical risks to be, based upon probability and impact. In this way, the risk assessment should provide parameters for what risks need to be measured, monitored, or controlled, and where investment in data analytics can be most beneficial. The risk assessment may also reveal what data might have integrity or accuracy issues that should be considered for remediation.

— **Review existing compliance metrics**
Reference to the list of the existing KRIs and KPIs that the organization tracks and reports on can help the compliance leader:

  – Understand what risk information is already being collected and what is the current state of knowledge of compliance risks;
  – Confirm the KRIs/KPIs remain appropriate for measuring and evaluating compliance risk;
  – Assess what additional data might help to enhance the board and senior management's understanding of the organization's compliance risks and how they are being managed, including emerging or trending risks.

— **Assess the organization's existing infrastructure against future compliance risk management goals**
Organizations differ significantly in their reliance upon technology to support their compliance efforts. Particularly in lesser or multiregulated industries, with smaller corporate compliance functions (if any), organizations may have manual processes in place for aggregating data and analyzing it, whereas more heavily regulated industries are shifting to greater integration of technology and harmonizing the technology across the enterprise.

An understanding of the organization's current state of data analytics and senior leadership's goals for future data analytic capabilities should help to frame the effort that the organization is seeking to undertake, and can be a valuable input in defining realistic time frames and costs for completion, as well as to help create a road map that is right-sized for the organization. Identification of a future state can also inform the core milestones that need to be achieved in a road map. A well-defined road map can help the organization migrate to a more data-driven metrics environment in a controlled way that may not significantly impact the organization's business.

# Assessing the data quality

**Data quality issues**

— Incomplete data: A lack of historical or detailed data, or limited availability and access to data maintained in disparate systems

— Inconsistent data: A lack of standardized data across the organization's technology infrastructure, often with data having different currency

— Poor data integrity: Data entered manually may be subject to human error, with fields populated incorrectly

For many organizations, data is unverifiable, old, inaccurate, or absent, due to manual data entry processes. In addition, organizations may have duplicate records of data, or inconsistencies in data across its systems. All of these issues can make it difficult to derive meaning and insights from the data, thereby reducing compliance leaders' confidence in their ability to rely upon the analytics when making strategic decisions or to assessing compliance trends.

Yet, in order to derive meaning from data analytics, a compliance leader must be comfortable with the availability, integrity, and accuracy of data that is needed to understand and assess compliance risks enterprise-wide.

One way for compliance leaders to address the data quality challenge is to conduct data quality assessments across the organization to better understand data they are using to monitor compliance efforts. Some organizations use "data quality scorecards" which rate the quality of business units' data.

A data quality assessment can enable the compliance leader to evaluate the compliance impact, including the ability to monitor compliance risks and aggregate data for further analysis.

KPMG

# Sharing data across the three lines of defense

Data ownership can be a major challenge for compliance functions seeking to obtain needed data and develop analytics from various owners across the enterprise. This is because in many organizations, the data the compliance function needs to formulate meaningful metrics and understand compliance trends, including predictively, is owned by individuals or units that sit outside the compliance function. For example, the data owner may be a business line, operation unit, information technology (IT), or human resources.

As a result, the data owner may be sensitive to how their data will be used, once they provide it, especially if there are privacy concerns. Further, data owners and stakeholders may also be protective of the data and fear losing control of how the data will be analyzed and applied. They also tend to be quite vested in ensuring the reliance placed on the data is appropriate. Because of this, compliance functions in siloed or decentralized organizations report it can be difficult to obtain the necessary data they need from data owners to evaluate their compliance program, understand their risks, and prioritize enhancements.

Yet, this is one of the most important inputs to a compliance program today—data. The effectiveness of the program depends upon available data that has integrity and can be culled from disparate sources, and aggregated enterprise-wide for a holistic view of compliance risks. Therefore, collaboration and coordination with the data owners, wherever they sit in the organization, is no longer an option, it is essential.

To the extent an organization has a data governance model in place, this can help to reassure the data owners and stakeholders that the data will be used consistent with the agreed upon model. To the extent possible, as part of the collaboration and partnership, the compliance function can also share with the data owners the reasons why the data is needed and what it will be used for. Through an "open door policy," all stakeholders can share information specific to the data that can bring them together in their shared goal of enhancing compliance, understanding risks and managing those risks. To the extent there is a benefit to the data owner as well, compliance's ability to share those perceived benefits can also help to engage those parties and make the business case. For example, sharing data enterprise-wide may enable the compliance function to provide the business or operations with comparisons to the other lines. This helps them manage an aspect of their compliance risks or to further understand those risks. Likewise, a trend may be identified in the data from one business line and be able to predictively help another business line.

**Lessons learned – Siloed data can distort compliance risks**

Otherwise, the compliance function—and the Board of Directors—may not formulate an enterprise-wide view of its compliance risks (or a subset of risks), or a true understanding of the operating effectiveness of its controls across the organization. This can unintentionally cause the compliance function (or the Board) to have a view of risk that is not accurate. Without a holistic view of risks enterprise-wide, the Board of Directors can be hindered in its oversight and governance, and lack an accurate view of its risk profile. Failure by the compliance function to obtain business line data and analyze it comprehensively can hinder compliance effectiveness and the organization's ability to know, and mitigate, its compliance risks.

If necessary, compliance functions ought to be prepared to escalate forcefully when business lines, operational units, risk management function, human resources or others in the organization are not complying with data requests, and when collaborative efforts are not resulting in timely action. This can be based upon a materiality assessment of the data and the need.

## Data governance models

As organizations seek to further leverage the data they have enterprise-wide, a centralized data governance model can provide foundational support to this effort. A data governance model can take different forms, but it is essentially a model for how the organization will manage its data quality, security, privacy, compliance, standardization, and consolidation. It is supported by people, processes, standards and technology. Standards may include the following:

- **Data naming:** conventions for standard words, abbreviations, structure and sequence, etc.
- **Data definition:** norms of clarity, completeness, and enterprise/global perspective
- **Data models:** with conventions for model notation, levels of models (conceptual, logical, physical), data abstraction, data normalization, and dimensionality
- **Data access:** conventions for requesting, approving, establishing, and removing data access capabilities
- **Data sensitivity:** especially standard classifications of data sensitivity—public, private, restricted, and classified, for example—and the means by which specific data items are classified
- **Data security:** including conventions for securing data in transit, acceptable use of storage devices, etc.
- **Data exchange:** including those standards that improve the ability of partners (internal and external) to exchange data efficiently and accurately[3]

Depending upon the goals of the program, a data governance model may also provide a means for data integration (helping to build connections among disparate data sources and resolve conflicts), data exchanges, and root cause analysis (to find and fix the root causes of data quality defects, data security failures, etc.). While compliance usually does not own a data governance model or framework, along with other stakeholders it can be an impactful participant, contributor and supporter of the process. In some organizations, compliance may also be part of a data governance council.

## The benefits of a data governance model

One benefit of central stewardship of data is that it requires all of the organization's different data owners to come together to design and execute the governance structure. In addition, it typically leads to a greater level of diligence and assessment of the data quality, accessibility to the data across the organization, and ultimately transparency. Collectively, these attributes build trust in, and a better understanding of, the available data within the organization that compliance leaders, as well as other stakeholders, need. It also creates greater consistency—e.g., the data is known, there is one version of the truth from the data, and the data should be able to be reconciled back to the business's view of its compliance risks.

[3] For further information see Data Governance Infrastructure by Dave Wells, KPMG, published October 1, 2010.

KPMG

# Integrating and automating data analytics for greater compliance insights

As organizations take note of guidance on fraud programs quietly issued by the DOJ in February 2016, it becomes clear that the yardstick against which compliance programs are measured is shifting. As a result, the data analytics expected to evidence program effectiveness and garner greater compliance insights, are likewise moving.

Compliance leaders who are alert to these regulatory developments, see integration across the three lines of defense, as well as human resources, legal, technology and other units as needed (now more than ever) to develop a more accurate perspective of compliance risks. Further, these compliance leaders recognize further integration and aggregation of data is needed to avoid unintentionally "underestimating" compliance risks that are buried in segregated units or operations and considered to be isolated. When risks are siloed, those having a systemic impact, in aggregate, can also be missed.

In contrast, compliance leaders who continue to view their data in siloed isolation, risk unintentionally burying or undervaluing risk indicators because they appear insignificant in isolation.

Therefore, in order to aggregate data that could reflect on the health of the compliance program, and to report on their risks in a united way, many compliance leaders are scoping out data aggregation tools, data visualization tools, and reporting dashboards. Dashboard reporting solutions range from inexpensive basic platforms to more robust tools with greater functionality and requiring greater investment and tailoring. Often times, compliance's budget significantly guides the decision on what tool to invest in or utilize.

In addition, it is important for compliance leaders to consider their goals when they purchase and implement a dashboard reporting tool. Some compliance leaders invest in these tools with a short term view to automate some previously manual processes while others are looking for a long term solution for three to five years or longer.

Regardless of the vision, it is important that as the organization matures, the compliance function can support this maturation with further integration of data analytics and metrics, and further automation. Compliance's needs should be defined and should guide the tool selection process.

**Making sense of data using dashboards**

Data visualization tools and reporting dashboards are often highly sought after by compliance leaders who seek a deeper understanding of the organization's compliance program effectiveness.

For example, to identify transactions that may be higher risk for potential anti-bribery and corruption violations, a compliance leader may look to business data such as the highest selling salespersons and compare this list of individuals to disparate expense detail over a certain dollar threshold, which could be for the entertainment of government officials. By targeting data from many different disparate systems, an organization can monitor using more data points that can collectively help identify the highest risk transactions to focus review on.

**Data integration can help the compliance function focus on riskier transactions**

Data integration enhances risk coverage and therefore identification of risks. Integrating the data allows analysis to become more nuanced, gradually increasing compliance's ability to identify higher-risk transactions.

KPMG

## The quest for predictive analytics

Compliance leaders increasingly recognize the need to design and implement analytics that enable compliance to be more predictive in assessing their risks and risk trends. To some degree, this shift is driven by regulatory expectations which reinforce the need for organizations to conduct root cause analysis, identify systemic issues, remediate control deficiencies or failures, and to explain their actions in these areas. It is in these respects that predictive analytics can be particularly useful. To maximize the benefit obtained, some leading organizations are building analytics directly into their compliance processes in order to identify risk scenarios in real time and to enhance their risk coverage in a cost-effective way. For this reason, compliance leaders usually see the value of becoming more predictive and utilizing technology to achieve this.

However, whether compliance leaders have the budget to invest in developing predictive analytics that are tailored to their compliance risks and risk profile is another story. For compliance leaders in this situation, with limited funding, this is the one definite area where compliance leaders need to invest to prepare for the future, even if implementation will happen incrementally over time. The ability of organizations to more efficiently identify and manage their compliance risks across the organization will be a key differentiator in the business and success in the future.

**Next generation analytics – Using HR data to inform an understanding of compliance risks**

- Upward feedback results for employees in leadership roles
- Number of employees subject to coaching by business unit or jurisdiction/region (in absolute terms and percentages)
- Growth in coaching year-over-year
- Increase in resignations of high performers by business unit or region/jurisdiction year-over-year or at a cyclical time of year
- Rise or decline in turnover in a business unit or region/jurisdiction compared to others enterprise-wide and year-over-year
- Rise or decline of more than a predefined percentage in terminations and resignations in a business unit or region/jurisdiction compared to others enterprise-wide and year-over-year
- Higher risk employee due diligence results

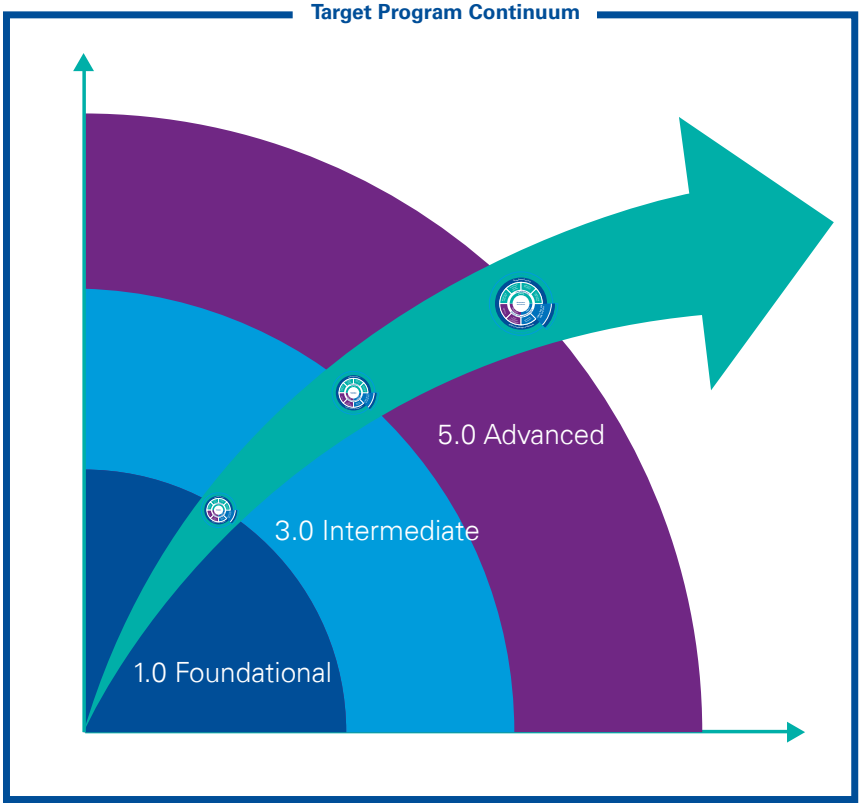
# Enhancing data analytics

Compliance leaders may decide to launch phased or incremental projects to enhance their data analytics capabilities. This may be based on where the organization is in the compliance maturation continuum, its desired state, and its risk tolerance.

**In a predictive analytics world, the value of "rear-view mirror" data should not be underestimated**

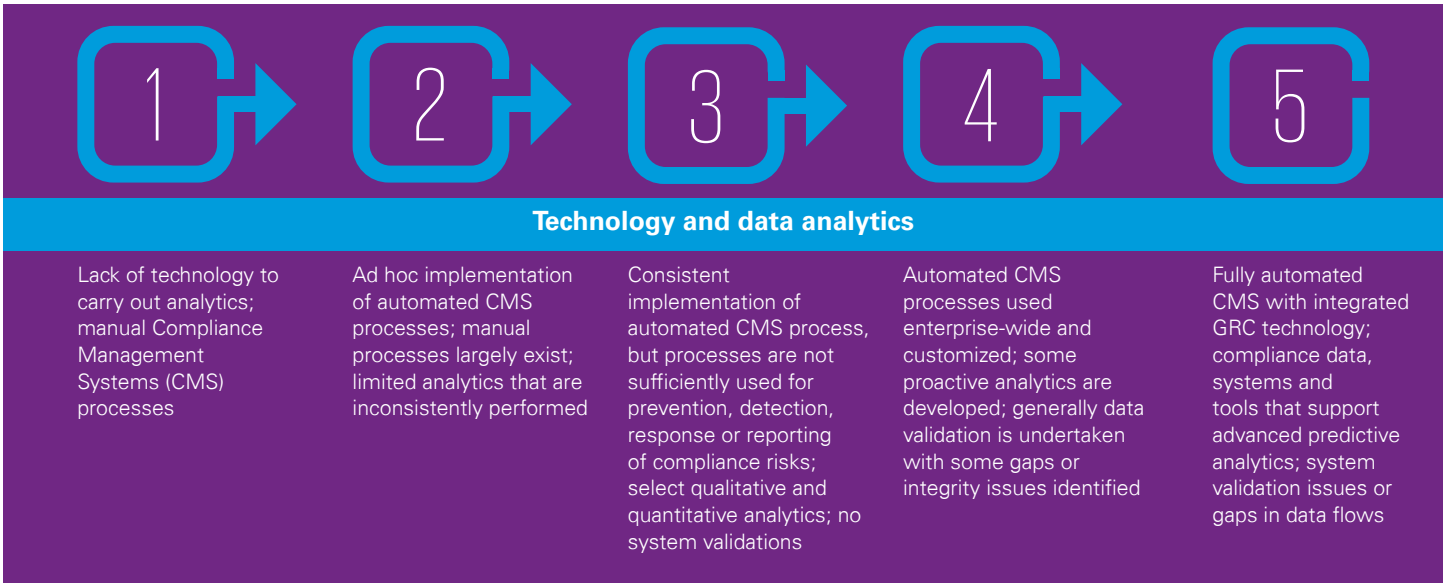
As organizations shift to more predictive analytics, they should continue to utilize and recognize the value of the "rear view mirror" data they already collect. Historical data is still needed to respond to regulatory inquiries and recognize trends (especially at public organizations), and can be valuable in identifying foreseeable future events and trends. It also allows compliance to back-test forward-looking, predictive models that they are considering implementing.

Knowing what events or risks have materialized in the past continues to be of significant relevance and can be a valuable source for compliance leaders in identifying focal areas in which to further build out their predictive analytic capabilities.



When it comes to data analytics, there is a wide variation of where organizations sit on KPMG's overall compliance maturity model. This involves many components from processes, to automation, to technology and more, as depicted in the sample chart of maturations below.

**Enterprise-wide compliance program assessment – Maturity model**




A compliance data analytics assessment and consideration of the overall maturity model can help compliance leaders recognize the current state of their capabilities versus where they would ideally like to be in a future state. The maturation model can also assist compliance leaders in pinpointing steps they need to take in the future. Compliance leaders should have a firm understanding of what targeted future state they want, the investment required to achieve it, and the projected impact on the organization's compliance.

Further, as compliance leaders look to enhance the data analytics they use to boost their compliance efforts, they should also look across their entire compliance program framework and assess additional enhancements needed for program alignment. This includes considering the connections between each of the components of the compliance program framework.

For example, enhancing compliance data analytics typically requires changes to the technology infrastructure, and could impact the risk assessment, monitoring and testing efforts, governance and other compliance program components. This also means continuously monitoring the analytics utilized in order to ensure the analytics remain calibrated to risk changes and trends, as well as to update and invest in further analytics as the organization's risk profile or tolerance changes. This is part of an effective compliance journey.

# Making the next move

It is clear that in today's compliance environment, data analytics is an essential ingredient in an organization's ability to understand its compliance program effectiveness, to proactively respond to compliance trends and also to reactively identify and evaluate root causes of wrong-doing. Given the growing importance of data and data analytics to a compliance program, it is no surprise that compliance leaders frequently identify data analytics as a priority investment for their organizations in 2017 and 2018.

As a magnitude of possibilities emerges in data analytics capabilities, often supported by digital labor (machine learning), compliance leaders should strategically assess—in conjunction with other stakeholders—how to best expand their use of data analytics that support their compliance program and enable them to better evaluate their effectiveness and trending risks. The value of investing in the right data analytics today cannot be overstated.

# Contact us

**Amy Matsuo**
**Principal, Advisory**
**Compliance Transformation Solution**
**Global and National Leader**
**Financial Services Lead**
**T:** 919-380-1509
**E:** amatsuo@kpmg.com

**Richard Girgenti**
**Principal, Advisory**
**Compliance Transformation Solution**
**Executive Sponsor**
**Americas Forensic Leader**
**T:** 212-872-6953
**E:** rgirgenti@kpmg.com

**Julie Gerlach**
**Managing Director, Advisory**
**Compliance Transformation Solution**
**National Co-leader**
**T:** 404-222-3389
**E:** jgerlach@kpmg.com

**Authored by Julie Gerlach, Nicole Stryker, Amy Matsuo and Ray Dookhie.**

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

**kpmg.com/socialmedia**