In pursuit of compliance metrics

kpmg.com

Executive summary

Effective compliance metrics support compliance efforts by providing a window into an organization's compliance risks and controls. Yet, the metrics must be accurate, comprehensive, and insightful to prevent misperception about compliance risks. Further, more predictive metrics that are aggregated from disparate data across an organization can provide a more pointed view of risk severity and hone in on compliance risks that might otherwise be buried.

It is vital that organizations evaluate, integrate, and (when valuable) automate metrics that provide insights into their compliance efforts in order to more effectively prevent, detect, and respond to current and future compliance risks. Such metrics can help compliance and business leaders identify gaps and areas where further operational controls can strengthen the control environment, while enabling the organization to move beyond compliance and realize greater value.

Using insights from discussions with executives and their stakeholders, this publication provides key takeaways to help compliance, business, and risk leaders initiate their next steps to bolster their metrics:

— **Confirm your compliance metrics goals** so you can prioritize enhancements that are directionally aligned to goals and business needs

— **Evaluate existing compliance metrics**, specifically key risk indicators (KRIs) and key performance indicators (KPIs) to better understand where your metrics are already strong, and where they can be improved or supplemented

— **Determine the compliance metrics to enhance** based upon a detailed analysis of factors, in order to realize greater value and risk coverage

— **Continuously improve and strengthen metrics** as part of the compliance journey.

Confirm compliance metrics goals

Key point:
To improve compliance risk management, organizations should use a range of metrics that incorporate operational and compliance data across all of their compliance activities enterprise-wide.

Metrics that are properly tailored to the organization and incorporate operational and compliance data[2] allow compliance and business leaders to craft a more risk-based approach to their compliance activities.

Well-designed metrics also help the organization's Board and other stakeholders evaluate compliance risks holistically and against the Board's stated risk tolerances.

Since there is no single metric that can be used to evaluate compliance, compliance leaders tend to rely upon a range of different metrics and incorporate pragmatic examples[3] alongside hard statistics to paint a more holistic picture of the "health" of their compliance program. Metrics should:

- Inform the Board of the organization's risks, controls (operating and design effectiveness), and mitigation efforts
- Cover the organization's highest compliance risks based upon severity, significance, and trends
- Cover all compliance activities (see the KPMG Compliance Program Framework on page 2 for topical areas)
- Include a diverse mixture: qualitative, quantitative, multi-dimensional, and predictive[4], as well as pragmatic examples.

[1] https://advisory.kpmg.us/risk-consulting/compliance-transformation/kpmg-chief-compliance-officer-survey.html

[2] Note: Reliance on operational data alone presents an incomplete view of compliance risks and program effectiveness that can inadvertently result in unknown/unmitigated risk exposure.

[3] Pragmatic examples can be quantifiable or may be more qualitative examples of "near misses," that reflect how compliance activities operate or which identify specific weaknesses in compliance efforts. In presenting this type of pragmatic example to the Board or other stakeholders, compliance leaders seek to explain what the root cause(s) of the compliance issue was, and the remediation steps taken/to be taken in such an instance.

[4] While predictive analytics may be aspirational for many organizations in certain industries, these type of metrics are quite valuable for evaluating compliance risks. Organizations can assess what kind of predictive metrics would be most beneficial to their organization when identifying how to prioritize enhancements to their metrics.

KPMG's CCO Survey: Metrics Focus

KPMG LLP (KPMG) surveyed the Chief Compliance Officers (CCOs) of organizations representative of the FORTUNE 100 to gather perspectives on their compliance journeys, including how metrics, and, specifically, KPIs and KRIs, can help ground their risk-based approach to compliance, and in furtherance of their business and operational goals.

How CCOs[1] are utilizing data and analytics for compliance purposes:

KPIs and KRIs as part of Governance, Risk, and Compliance efforts — **40%**

KPIs and KRIs to develop compliance monitoring and testing — **48%**

Data analytics to conduct root cause and trending analysis — **47%**

"While our survey indicates some CCOs incorporate data and metrics into their compliance programs, this is still an underdeveloped area. Organizations that do leverage metrics to monitor and measure their compliance programs are seeing tremendous value from these insights."

—Amy Matsuo
Principal, KPMG LLP

Evaluate existing compliance metrics

Key point:
Organizations should use a combination of metrics (one-dimensional, multi-dimensional, quantitative and qualitative) for compliance purposes that are tailored to their regulatory requirements and risks.

KPMG has developed a proprietary Compliance Program Framework rooted in governance and culture, and spanning the three lines of defense, that organizations can use to evaluate the scope and focus of their existing compliance metrics, any potential gaps in metrics, and the connectivity of metrics to compliance program activities and controls.

Traditionally, organizations may have developed metrics that focus on select compliance efforts such as certifications of compliance with the Code of Conduct, training completions and monitoring and testing results. Supplemental metrics across *all* compliance activities are increasingly used to enable organizations to more holistically assess their compliance efforts.[5] This includes metrics covering compliance culture, technology infrastructure, data validation efforts, and the operational effectiveness of their controls.

Types of metrics

Organizations should use compliance metrics that are tailored to their regulatory requirements and that help to evaluate compliance risks across their organization's products, jurisdictional presence, and processes.

Effective compliance metrics should be easy to measure and provide meaningful insight

Ideally, organizations should utilize a combination of the following types of metrics:

- **One-dimensional:** These metrics are based on one data attribute, such as number of compliance trainings completed late, or number of Code of Conduct acknowledgments outstanding. One-dimensional metrics can provide a basic insight into the effectiveness of compliance efforts.
- **Qualitative:** These metrics are comprised of intangible, abstract, and subjective measures based on an individual's judgment and perspective. They can be used to evaluate "soft" or "entity-wide" controls that are not quantitative.
- **Quantitative:** These metrics are tangible and concrete metrics that are easily measured in the form of quantity or time and easily expressed in numbers and/or data results. Quantitative metrics are sometimes called backward-looking metrics.
- **Multi-dimensional:** These metrics are based on multiple data attributes and therefore can offer greater insights into the effectiveness of compliance efforts as they are more detailed.
- **Predictive:** These metrics leverage past data and trends (including patterns and abnormalities) to make predictions about compliance risks in the future. They can be built and implemented as data capture and availability issues are resolved.

[5] Source: Compliance and Ethics Professional, *Collecting and evaluating effective compliance program metrics*, Tim Hedley and Ori Ben-Chorin (December 2015)

KPMG

Determine compliance metrics to enhance to realize greater value and risk coverage

Key point:
In identifying ways to enhance their compliance metrics, organizations should consider if their existing metrics adequately address their regulatory risks in the jurisdictions where they operate; Board interest in specific compliance topics; the organization's compliance goals; the data they have available; and, the functionality of their technology and tools for metrics generation and reporting.

When developing compliance metrics, compliance leaders should have a strong understanding of their existing state and desired future state as well as the organization's risks and the Board's risk tolerance. In addition, engaging in upfront strategic discussions with cross-functional stakeholders in the business and operations can help compliance leaders to ensure alignment in goals and allow a concerted approach at the inception of any project. The following list can assist compliance leaders in working with their stakeholders to scope their metrics needs and functional abilities, which should then inform their strategy and plan.

— **The organization's regulatory requirements and expectations in all jurisdictions where it operates:** Compliance leaders should review their existing compliance metrics, in conjunction with cross-functional stakeholders, to better understand if they adequately cover the organization's risk areas. In reviewing these metrics, compliance leaders should identify what risk information they already collect about their compliance with each of their regulatory requirements (across finance, operations, human resources, legal. etc.). From this, they can then determine what additional data would enhance their knowledge of how they are complying with their regulatory obligations, and whether data needs to be, and can be, further aggregated for a more complete understanding and assessment.

— **Board interest in compliance topics:** Compliance leaders should also evaluate what information their Board, business, risk, and operational leaders need to know; the Board's risk tolerance; and senior management's desired proactiveness. Collectively, this may inform the investments the organization is willing to undertake to enhance its metrics.

— **The organization's compliance goals:** Some organizations are evaluating their current abilities to implement predictive analytics. Developing predictive analytics can require significant investment in technology and resources, particularly when implementing intelligent automation that will identify real-time compliance risk scenarios. Therefore, it is important to understand the organization's compliance goals and vision for how (and whether) predictive metrics should be developed. This can also help compliance leaders to prioritize implementation of those predictive metrics that are thought to be most impactful to the organization's compliance efforts.

— **The data available within the organization, integrity of the data, and existing technology infrastructure:** Compliance leaders need to be cognizant of the data they are relying upon. If the data quality is poor or unreliable, any metrics or use of the data downstream will be based upon potentially faulty premises, and will be likewise unreliable. Even when data is reliable, compliance leaders can be challenged by differences in data collection across the organization, with certain risk indicators collected by some units but not others, preventing an aggregate view of compliance risk.[6]

[6] https://advisory.kpmg.us/risk-consulting/compliance-transformation/harnessing-data-analytics-to-transform-compliance.html

Compliance automation

Predictive analytics, dashboards, and data visualization are becoming increasingly important tools for organizations to manage compliance risks more proactively, embedding compliance operationally, and encouraging business decisions that consider the organization's compliance obligations. Organizations can use data visualization and predictive analytics to evaluate the likelihood of future occurrences to better track and monitor their conduct and culture risks using techniques such as data mining, statistical modeling, machine learning, and artificial intelligence.

Automation can help organizations further refine their compliance metrics to target their compliance risks. To do so, leaders may need to:

- Aggregate critical data elements from across the organization into a single source and dashboard, including data relevant to culture, for internal and external reporting purposes
- Use cognitive technologies to tag, label and combine structured and unstructured data
- Build predictive analytical models for more proactive identification of issues and risks
- Identify favorable scenarios and models for more risk-based and predictive transaction and sanctions monitoring (e.g. third-party vendor management, anti-bribery and corruption risks)
- Use sentiment analytics and decision science to stratify or classify data for enhanced data analysis
- Create or test data feeds, data lineage, production work flow, edit checks/controls, and report submissions using data quality rules engines.

A firm understanding of what data exists and is available across an organization, and the integrity of that data, is key to forming a realistic current-state analysis of the organization's metrics as a baseline for further enhancements. An organization may need to enhance existing data and remediate the data before it can design metrics that are truly valuable to its stakeholders and indicative of compliance effectiveness and health.

- **Technology and tools for metrics development and reporting:** As discussed earlier, KPMG's Compliance Transformation survey found that many organizations do not leverage technology to support their compliance initiatives as extensively as they could.

  Increasingly, organizations are using technology to generate reporting dashboards that synthesize compliance metrics and can paint a more holistic and consistent view of compliance risks enterprise-wide. In aggregating data enterprise-wide, dashboards help leaders obtain a more comprehensive vision of their compliance risks, instead of siloed views, which can undervalue risk indicators in isolation. From this vantage point, senior leaders are better equipped to monitor their compliance risks in a more targeted manner, strategically focus on improving compliance activities where they most need it, and remain vigilant in addressing their trending risks enterprise-wide. They can also allocate their human and monetary resources using a more risk-based approach.

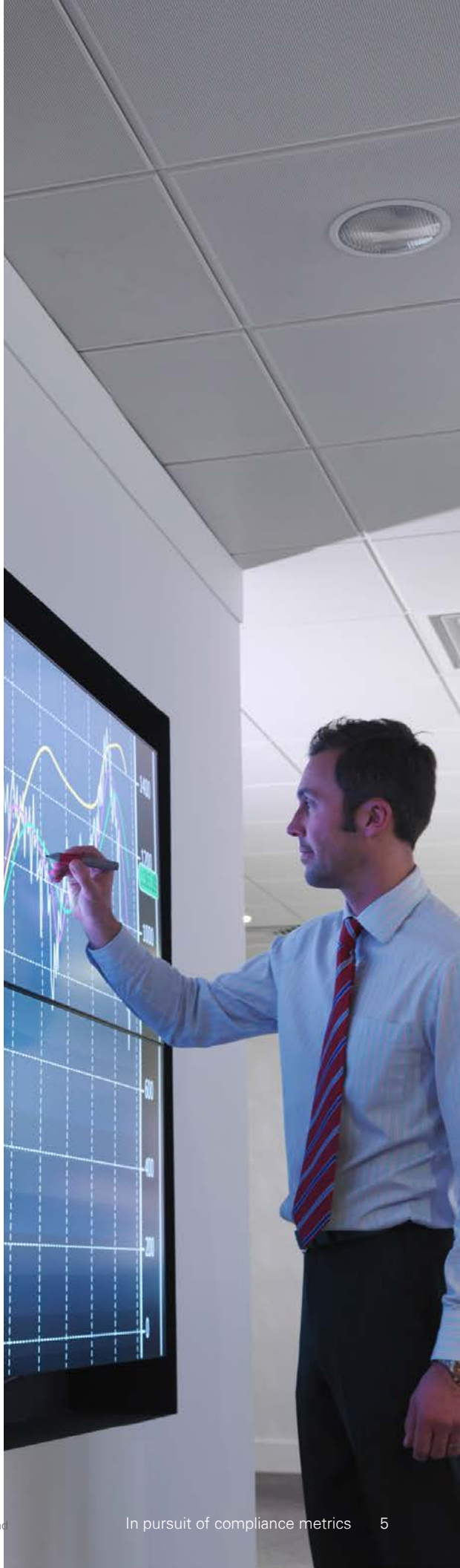
Continuous improvement and strengthening of compliance metrics

Key point:
Organizations should *continuously* reassess their compliance metrics and refine them so they can better manage their evolving compliance risks, identify business or operational enhancements to support compliance, and realize greater value from their compliance investments.

Organizations must reassess and refine their existing inventory of compliance metrics to address evolving risks. They should also use the data underlying the metrics to identify business or operational enhancements in furtherance of compliance efforts, including training, investigations, customer complaints and to the extent applicable, sales practices. Conducting regular evaluations of the organization's compliance metrics can help leaders to reaffirm the metrics they use; address business, market and regulatory trends; and ensure that metrics remain aligned to the organization's highest risks and are not obsolete, or fading in importance of value.

In addition, quality control testing of the data sources and feeds that underlie the organization's compliance metrics is also important. Testing helps to validate that the data is complete, accurate, and has integrity, especially when there are changes to the data or the technology systems. Seemingly innocuous changes made for operational reasons can impact the data feeding into the metric or cause the data to be dropped, diminishing the value of the metric and its use. Sometimes these changes can actually expose the organization to additional regulatory risk.

Further, as part of their continuous improvement efforts, compliance and business leaders can benefit from considering what the metrics reflect about the program's health and what additional metrics can impact that evaluation. Through a review of metrics, compliance leaders can identify instances for follow-up, a quick refresher, or additional communication to reinforce a particular issue. Governance remains key.



Conclusion

In a world where 2.5 quintillion bytes of data[7], are produced daily, organizations face the daunting task of analyzing key business, customer and employee behaviors, both for business strategy and to provide risk-based compliance insight. Well-designed metrics can empower business, compliance and risk leaders to execute their responsibilities more soundly; present appropriate information to management and the Board; evaluate alignment of compliance efforts with business goals and strategies; and further the organization's overall compliance risk management. Well-developed compliance metrics also enable organizations to improve their ability to prevent, detect, and respond effectively and efficiently.

Visit kpmg.com/us/regandcompliancetransformation to learn more about how KPMG can help support your organization in moving beyond compliance.

Case study: Creating metrics and reporting to evaluate conduct and culture

A large financial institution sought to evaluate its conduct and culture risk across its business areas, products and geographies. The institution's leadership looked to better evaluate these risks, and report such metrics appropriately to management, executive leadership and the Board.

With the support of KPMG, the institution developed metrics and reporting that would help enable it to conduct an enterprise-wide assessment of its conduct and culture risks, which considered regulatory expectations and leading practices. The metrics and reporting included:

— A rationalization of the institution's existing risk inventory and hierarchies

— Design of a consistent taxonomy for evaluating conduct and culture using a point system and aggregation approach

— A formalized methodology, establishing categories and factors of risks and controls to be evaluated, and a scoring methodology that aligned to the institution's operational and compliance risk assessments.

After establishing the metrics and reporting, KPMG also assisted the institution in conducting its conduct and culture risk assessment, in identifying gaps that could be remediated, and provided recommendations for control enhancements.

The institution not only gained greater visibility into its conduct and culture risks at the enterprise and across jurisdictions, products, and business areas, but also developed a sustainable approach to its conduct and culture data analysis, measurement and reporting.

[7] IBM Consumer Products Industry Blog, *2.5 quintillion bytes of data created every day. How does CPG & Retail manage it?* (April 24, 2013)

KPMG

Sample metrics

Type of metric	Data source types	Sample metrics
One-dimensional/quantitative	Investigations	Number of calls to the ethics hotline during an established time frame
One-dimensional/predictive	Expenses	Increases to volumes/magnitude of gifts/entertainment
One-dimensional/predictive	Third Parties	Increases to higher risk-ranked third-party intermediary engagements/ transactions
One-dimensional/qualitative	Policy	Detail and descriptions of exceptions to policy (e.g., failure to pre-clear, after-the-fact violations)
One-dimensional/qualitative	Business Performance	Progress to plan metrics (highlighting achievement to plan metrics for the compliance program and operational effectiveness)
One-dimensional/predictive	Business Performance	Sales targets/growth rate spikes and evaluation of business units and jurisdictions that continuously meet the spikes within a certain low percentage or numerical range
One-dimensional/predictive	Complaints	Customer service complaints using keyword searches
One-dimensional/quantitative	Customers	Number of new accounts with shell companies with billing addresses in secrecy jurisdictions
One-dimensional/quantitative	Monitoring/Testing	Number of outstanding risk mitigation program actions
One-dimensional/qualitative	Customers	Target customer demographics (e.g., age, wealth, financial sophistication)
One-dimensional/qualitative	Employee	Upward or 360 feedback for supervisors, and variations from an established average
One-dimensional/predictive	Business Performance	Claims handling; uphold rates and speed of payment (Insurance)

Sample metrics (cont.)

Type of metric	Data source types	Sample metrics
One-dimensional/qualitative	Culture	Examples of "tough" business examples that senior leadership has had to make; deals or mergers that were rejected or high-level employees who were terminated, because of compliance concerns
One-dimensional/qualitative	Monitoring/Testing	Examples of root cause analysis in "significant" investigations and examples of missed opportunities
One-dimensional/qualitative	Monitoring/Testing	Test results of controls tested for operational effectiveness (or pragmatic example results)
One-dimensional/predictive	Third Parties	Numbers and trends in third-party relationships that appear to be shell companies or connected to politically exposed persons
One-dimensional/predictive	Investigations	Spikes in volume of reports to escalation channels within a specific date range of compliance trainings
One-dimensional/qualitative	Employee	Employee, trade, transactional, operational metrics for employees at "higher" risk of compliance violations
One-dimensional/qualitative	Employee	Employee transactions that are consistently slightly below organizational or regulatory thresholds (organizations to identify the value deviation)
Multi-dimensional/quantitative	Business Performance	Percentage changes in account movements within an established time frame of reporting deadlines; percentage of funds misallocated during this time (e.g. five days) and later reversed
Multi-dimensional/quantitative	Complaints	Number of customer complaints by topic matter, compared to prior months or years or other divisions
Multi-dimensional/quantitative	Monitoring/Testing	Number of issues self-identified by the first line and timeliness of issues identified

KPMG

Sample metrics (cont.)

Type of metric	Data source types	Sample metrics
Multi-dimensional/qualitative	Employee	Compensation/bonus/raises/hiring/terminations/rotation in conjunction with compliance scorecard of individuals
Multi-dimensional/quantitative	Business Performance	Number of exceptions approved for higher-risk business processes and change over a set time, based upon a norm value expected
Multi-dimensional/quantitative	Monitoring/Testing	Number of findings (audit, compliance monitoring, testing or validation), and trends in each effort year over year by materiality and by region or office or unit; remediation time frames and trends
Multi-dimensional/quantitative	Monitoring/Testing	Number and severity of outstanding compliance issues by the first line and timing of resolution of these issues
Multi-dimensional/quantitative	Complaints	Number and percentage of complaints alleging aggressive sales tactics, with variations among units or jurisdictions identified
Multi-dimensional/quantitative	Employee	Turnover rates for compliance and relevant control function personnel and trends year over year, including termination rates
Multi-dimensional/quantitative	Monitoring/Testing	Number of approval and certification exceptions including year over year trends and trends in timelines for remediation
Multi-dimensional/predictive	Business Performance	Spikes in operational production of a certain percentage that correspond to time frames of, or divisions with, high regulatory obligations
Quantitative/predictive	Employee	Recruitment offer rejections and early resignations
Predictive/quantitative	Legal	Number of lawsuits by topic and growth year over year

Contact us

Amy Matsuo
Principal, Advisory
Regulatory & Compliance Transformation (R&CT) Solution Global and National Leader
T: 919-664-7302
E: amatsuo@kpmg.com

Regina Cavaliere
Principal, Advisory
R&CT Healthcare and Life Sciences Co-Lead
T: 973-912-5947
E: rcavaliere@kpmg.com

Dan Click
Managing Director, Advisory
R&CT Consumer, Retail and Industrial Manufacturing Lead
T: 313-230-3240
E: dclick@kpmg.com

Carolyn Greathouse
Principal, Advisory
R&CT Technology, Media and Telecommunications Lead
T: 314-244-4096
E: cgreathouse@kpmg.com

Stacey Guardino
Partner, Advisory
R&CT Insurance Lead
T: 212-954-4950
E: sguardino@kpmg.com

Julie Luecht
Principal, Advisory
R&CT Energy Lead
T: 713-319-3721
E: jluecht@kpmg.com

Anthony Monaco
Partner, Advisory
R&CT Government Lead
T: 212-872-6448
E: amonaco@kpmg.com

Todd Semanco
Partner, Advisory
R&CT Financial Services Lead
T: 412-232-1601
E: tsemanco@kpmg.com

Jennifer Shimek
Principal, Advisory
R&CT Healthcare and Life Sciences Co-Lead
T: 973-912-6167
E: jshimek@kpmg.com

Acknowledgements: authored by Ursula Nigrelli, Amy Matsuo, Nicole Stryker, and Robin Augie with contributions by Deborah Bailey, Lisa Newport, and Karen Staines.

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

kpmg.com/socialmedia