The Compliance Journey

Navigating Through the Challenges and Opportunities

Overview

Understanding Regulatory Requirements and Enforcement Priorities

The Role of Compliance: Expense Pressures, Metrics and Reporting, Getting to Proactive

The Compliance Vision: Prioritizing Investments in Your Compliance Program
Understanding Regulatory Requirements and Enforcement Priorities

The Culture of Compliance

The importance of fostering a proactive culture of compliance in today’s highly regulated environment is critical to long-term growth and success. Organizations need to move from a high risk reactive approach to a proactive culture of ethics and compliance.

**Heighened Regulations**
- Stricter enforcement of FCPA by the US DOJ and SEC
- FCPA and other anti-bribery and corruption regulations
- Federal Trade Commission Act
- False Claims Act

**Tougher Business Environment**
- Pricing pressures in developed markets (e.g., US and W Europe)
- Access and funding challenges in developing and emerging markets

**Increased Stakeholder Expectations**
- Customers have higher expectations for services/products
- Payers seek greater efficiency
- Professionals need support
- Shareholders demand higher returns

**Increased Public Scrutiny**
- Demand for greater corporate transparency, access to key data, and better understanding of relationships between customers and organizations

**Diminished Reputations**
- Some companies perceived as untrustworthy
- Ongoing compliance failures attract attention
Understanding Regulatory Requirements and Enforcement Priorities

A Sustainable Approach to Regulatory Compliance

- The pace and complexity of regulatory change, coupled with the increase in regulatory scrutiny and enforcement action by relevant authorities, continues to make compliance a top concern for organizations.

- Compliance Transformation is the continual evolution and alignment of an enterprise’s compliance activities with their internal risk profile and tolerance, culture, strategic and financial objectives, business, operating, functional, and human capital models.

Compliance Transformation Framework

Organizations need to be able to deploy change and adapt their people, processes, and technology in support of the compliance activities to address continually changing internal and external environments.

- Governance and Culture
  - Mission/vision/values statements
  - Entity-wide policies & procedures (e.g., code of conduct)
  - Policies & procedures with embedded compliance requirements
  - Policy management
  - Regulatory change management

- Regulatory Compliance
  - Periodic reporting to management & the Board
  - Required regulatory reporting
  - Technology to support compliance program (testing, training, etc.)
  - Predictive measures: key risk indicators (KRIs) / key performance indicators (KPIs)
  - Root cause analysis & trending

- Risk Management
  - Inventory regulations
  - Categorize inherent compliance risk
  - Assess residual risk
  - New product review

- Issues Management & Remediation
  - Issues management & investigation
  - Response plan and process for investigating alleged non-compliance
  - Issues management & investigation
  - Response plan and process for investigating alleged non-compliance

- Ethics & Compliance Program Management
  - Senior executive commitment
  - Program effectiveness incentives
  - Performance management & compensation
  - Disciplinary enforcement & accountability

- Third-Party Risk Management
  - Third-party compliance due diligence & management
  - Third-party participation in training programs
  - On-going skills assessment

- Monitoring & Testing
  - Transactional, process & control testing
  - Periodic compliance program evaluation

- Government Investigations
  - Responding to government investigations/exams/inspections
  - Rebutting regulatory change
  - Confronting breaches of ethics or compliance

- Culture of Compliance
  - Culture / tone of compliance & regulatory change
  - Regular & frequent training
  - Third-party participation in training programs
  - Monitoring & tracking of regulatory change
WASHINGTON D.C., JAN. 12, 2017 — "The Securities and Exchange Commission today announced its Office of Compliance Inspections and Examinations’ (OCIE) 2017 priorities. Areas of focus include electronic investment advice, money market funds, and financial exploitation of senior investors. The priorities also reflect a continuing focus on protecting retail investors, including individuals investing for their retirement, and assessing market-wide risks."

The U.S. Department of Health and Human Services, Office of Inspector General released its Work Plan for fiscal year 2017. It focuses on the following areas:

- physical security
- information security
- contracts and grants
- Overseas contingency operations (OCO), including programs and operations in front-line states such as Afghanistan and Pakistan

In 2016, the Department of Justice (DOJ) brought 13 corporate FCPA enforcement actions (the second-largest number of all-time behind 2010 in which the DOJ brought 17 corporate FCPA enforcement actions).
Expense Pressures

The Cost of Compliance

One of the major challenges firms face is the continued scarcity of skilled compliance personnel, forcing firms to do more with less and putting a focus on the development of existing staff. Consistent with 2015 results, two-thirds (67 percent) of firms overall are expecting senior staff to cost more in 2016, largely due to the demand for skilled staff and knowledge (84 percent), and the need for additional senior staff to manage volumes of regulatory requirements (59 percent).

- Thomson Reuters’ Cost of Compliance 2016 Report

- A benchmark study of 46 multinational organizations was conducted by Tripwire and Ponemon Institute LLC in January 2011 to determine the organization’s compliance efforts including the cost of non-compliance with laws, regulations, and policies. The study revealed that:
  - The cost of non-compliance was 2.7 times the cost of compliance.
  - The average cost of compliance was US$3.5 million, and the average cost of non-compliance related problems was nearly US$9.4 million.

- In 2016, the federal government finalized 411 regulations, published $164.2 billion in compliance costs and imposed 120.8 million in net paperwork burden hours.

Metrics and Reporting

How Compliance Leaders View Their Programs

KPMG’s 2016 Compliance Transformation Survey examined the progress that major organizations across multiple industries are making in their compliance journeys. Across the nine compliance components, organizations report the least progress with respect to technology and data analytics. Some key findings include:

- More focus required on third parties. Only half of organizations have a process to confirm that third-party vendors adhere to compliance due diligence processes, and just 31 percent manage third-party risk and issue tracking through an enterprise-wide tool capable of monitoring KPIs and KRIs.

- Opportunities to leverage technology. While 69 percent of CCOs say their organization leverages technology to support its compliance initiatives, only 47 percent say they use data analytics and other technology processes to conduct root cause and trending analysis.

- Keeping pace with regulatory changes. Only 27 percent of CCOs strongly agree that the compliance department has a change management process in place to identify and incorporate changes in laws and regulations.

- Widespread use of enterprise-wide compliance reporting. 84 percent of organizations provide reports on the enterprise-wide state of compliance including culture, conduct, governance, and key issues. In contrast, only 47 percent of CCOs say their company has an enterprise-wide reporting system that is integrated across functions and business units and with compliance monitoring.

"Our dashboards are so advanced, they automatically filter out any bad news."

""
Compliance Visualization & Analytics

Through leveraging data from multiple disparate data sources, design a customized solution that provides data-driven intelligence and actionable insights to more effectively manage and embed key components of a robust compliance and ethics governance function. Initial key focus areas include investigations, retaliation monitoring, due diligence, and training.

Data Analytics and Reporting Dashboards

Metrics and Reporting

Determining Metrics That Matter

What is the challenge?
- Identifying and evaluating metrics that evaluate the effectiveness of the compliance program initiatives

What does the Board want?
- Metrics that are measured over time to flag high-risk areas and benchmark the performance of the program against regulatory and evaluative frameworks
- Metrics that demonstrate program effectiveness and compare compliance initiatives against those at peer organizations

What does the Board not want?
- Basic quantitative program metrics such as the number of calls to the organization’s ethics hotline, the number of investigations launched and closed, the number of training courses completed, and the number of internal audit findings

"We’re really struggling with finding what metrics really do demonstrate that a compliance program is effective.

— FORTUNE 350 CCO"

"We’ve got a few metrics that we’ve been using... but I’m not sure that’s a real tie to the effectiveness of the program. It’s just something that we’ve been having a difficult time coming up with.

— FORTUNE 350 CCO"
Metrics and Reporting

Metrics That Matter Are Those That Are Important To Your Organization

- One-Dimension vs. Multi-Dimension Metrics
- Qualitative / Subjective Metrics
- Predictive Metrics
- “Near Miss” Metrics

Types of Metrics: One-Dimension vs. Multi-Dimension Metrics

<table>
<thead>
<tr>
<th>One-Dimensional Metric</th>
<th>Multidimensional Metrics...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of calls to the Ethics hotline</td>
<td>Nature of allegations (e.g., by type of allegation)</td>
</tr>
<tr>
<td></td>
<td>Nature of allegations of noncompliance/misconduct (per risk area/per quarter/per business unit/per geographic location, etc.)</td>
</tr>
<tr>
<td></td>
<td>Number of allegations resulting in an internal investigation (e.g., per quarter, as well as per operating unit, per geographic location, per department, per line of business, etc.)</td>
</tr>
<tr>
<td></td>
<td>Number of days to respond to an allegation for each reporting mechanism (e.g., hotline, Webline, telephone, verbal to supervisor/manager, etc.)</td>
</tr>
<tr>
<td></td>
<td>Number of allegations made anonymously versus self-identified personnel</td>
</tr>
<tr>
<td></td>
<td>Number of allegations per reporting mechanism (e.g.,...</td>
</tr>
</tbody>
</table>
Types of Metrics: Qualitative / Subjective Metrics

- Helpful in evaluating “soft” entity-wide controls that do not lend themselves easily to a quantitative analysis
  - Collect through fielding an internal employee perception survey that seeks to evaluate a variety of data points, including employee comfort level in utilizing available advice and reporting mechanisms; propensity to use one mechanism over another; and perception of the “ethical tone at the top” from senior leaders, local managers, and supervisors, etc.

- Evaluating behaviors and perceptions
  - ≈75% of employees observed misconduct within their organizations in the past 12 months
  - >50% stated what the observation could potentially cause a significant loss of public trust if discovered
  - Driving forces behind misconduct include:
    1) pressure to do “whatever it takes” to meet targets; and
    2) not taking the code of conduct seriously
  - ≈50% of employees were uncertain that they would be protected from retaliation and more than half suggested a lack of confidence that they would be satisfied with the outcome

Types of Metrics: Predictive Metrics

- Predictive metrics or “forward-looking” can alert the organization as to future or emerging risks
- Future metrics are increasingly becoming important to track, and the table below provides a number of examples of such forward-looking metrics:

<table>
<thead>
<tr>
<th>“Forward-Looking” Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase in vendor dependencies may suggest a greater risk from diminished control</td>
</tr>
<tr>
<td>An increase in the growth rate of the number of locations/manufacturing centers or customer interaction channels may suggest a greater future risk</td>
</tr>
<tr>
<td>An increase in the number of regulatory changes may suggest a greater risk resulting from increased complexity</td>
</tr>
<tr>
<td>An increasing trend in negative customer survey results may suggest increasing risk in the corresponding product or business</td>
</tr>
<tr>
<td>Aggressive profitability targets compared to past performance may suggest increasing risk from actions needed to meet goals</td>
</tr>
<tr>
<td>Missed remediation time lines may suggest risk management and resource issues</td>
</tr>
<tr>
<td>A lack or delay in timely risk-specific training events may suggest an increased risk resulting from lack of technical compliance knowledge</td>
</tr>
<tr>
<td>Declining average years of experience for employees in key business units may suggest diminishing risk-specific technical compliance skills</td>
</tr>
</tbody>
</table>
Metrics and Reporting

Types of Metrics: “Near Miss” Metrics

- If your compliance program was able to thwart misconduct before it ever happened, isn’t that a measure that your compliance program is working properly?
  - One way of capturing in metric form that misconduct was foiled is to capture the number of calls to the hotline (or perhaps the number of customer complaints) in a particular compliance area, both before and after, risk mitigation activities had occurred.

- Evaluate every opportunity for capturing “near miss” metrics and reporting on them to the Board and/or Board committees and, if necessary, also to the regulators, in order to substantiate a claim that organizational controls are working as intended.

Metrics and Reporting

The Purpose of Reporting

- Demonstration of the monitoring efforts being conducted with respect to compliance program initiatives
- Provides the Board with a snapshot of the implementation and successes/shortfalls of the compliance program initiatives
- Metrics should be shared with the Board 3-4 times a year
- Board’s Oversight Responsibilities
  - A Board must act in good faith in the exercise of its oversight responsibility for its organization, including making inquiries to ensure (1) a corporate information and reporting system exists and (2) the reporting system is adequate. To assure the Board that appropriate information relating to compliance with applicable laws will come to its attention timely and as a matter of course.
Metrics and Reporting

Monitoring Efforts & Reporting Metrics to the Board

Metrics Should Reflect:
- Risks to the organization and the compliance initiatives designed to mitigate risks
- Implementation plans for compliance initiatives and success of implementation
- Reports should include metric objectives and a scorecard to reflect progress and successes of particular initiatives
- Incentives to promote compliance (i.e., compensation linked to performance on key compliance initiative metrics)

What to Report to the Board:
- Annual, semi-annual or quarterly reports
- Risk assessments and work plans
- Audit status reports
- Proactive vs. reactive information
- Prioritize risks

Monitoring Efforts: How to Present to the Board

Use of Dashboards and Scorecards
- Utilize objective scorecards that demonstrate how well management is executing the compliance program, mitigating risks, and implementing corrective action plans
  - Dashboards can contain key financial, operational, and compliance indicators to assess risk, performance against budgets, strategic plans, policies and procedures, or other goals and objectives.
  - Remember to strike a balance between too much and too little information
- Report information on internal and external investigations, serious issues raised in internal and external audits, hotline call activity, all allegations of material fraud or senior management misconduct, and all management exceptions to the organization’s code of conduct and/or expense reimbursement policy.
- Address significant regulatory changes and enforcement events relevant to the organization’s business.
- Create a usable scorecard today and then refine it based on experiences
  - Start with 3-5 metrics and fully integrate them before refining
  - Use clear factual data points that are made transparent across the organization to achieve business goals and desired outcomes
  - Focus on content over format

Reminder
- An effective system used every day is better than the almost-perfect system that never leaves the drawing board
**Effective Communication of Compliance to the Board**

**How to acquire the attention of the Board:**

- Reminder that U.S. Sentencing Guidelines require Boards to “...exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program”
- Without proper oversight and monitoring of the compliance program, organizations may face much larger penalties in the event that problems are identified
- Note that metrics provide a high level narrative of the status and success of the compliance program, and thus serve to generate further action and budgetary allotments
- Mandatory certifications for Corporate Integrity Agreements, including Board Members

**Metrics and Reporting**

One Size Does Not Fit All:

- The Guidelines allow for variation according to “the size of the organization”
- Boards must have an understanding of the dynamic regulatory environment in order to be able to ask more pertinent questions of management and make informed strategic decisions regarding the organizations’ compliance programs
  - Boards should be aware of, and evaluate, the adequacy, independence, and performance of different functions within an organization on a periodic basis

**Getting to Proactive**

From Reactive to Proactive

Despite increasing governmental scrutiny and sanctions on organizations, few have prioritized creating a proactive culture of ethics and compliance. A reactive focus on compliance significantly increases an organization’s risk of sanction.

**WHAT HAVE WE FOUND?**

<table>
<thead>
<tr>
<th>Inconsistent behaviors and messages from leadership</th>
<th>Staff and Management are not held accountable for negative behaviors</th>
<th>Culture initiatives are oriented towards remediation rather than prevention</th>
<th>Compliance driven culture change is not always actively business-led</th>
<th>Lack of understanding of the underlying assumptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Observed behaviors are contrary to what is expected of staff</td>
<td>• The approach towards rewards and penalties is not applied consistently</td>
<td>• Ethics and compliance culture and risk management is inconsistently prioritized</td>
<td>• Ethical and compliance culture initiatives have been focused on achieving quick wins through tactical and sporadic initiatives</td>
<td>• The need to deepen the ethical culture is not always actively business-led</td>
</tr>
<tr>
<td>• Leadership creates a perception that ethical culture and risk management is inconsistently prioritized</td>
<td>• Ethics and compliance culture and risk management is inconsistently prioritized</td>
<td>• The need to deepen the ethical culture is not always actively business-led</td>
<td>• Remediation approaches tend to be focused on the past rather than looking forward into the future</td>
<td>• There is a lack of focus on identifying the underlying assumptions of ethics and compliance culture, which drive behaviors and business outcomes</td>
</tr>
<tr>
<td>• A failing to effectively cascade the appropriate tone from the top</td>
<td>• Financial metrics such as revenue and profit take priority over a more balanced scorecard of metrics, ethics, and attention to risk</td>
<td>• The need to deepen the ethical culture is not always actively business-led</td>
<td>• Second line of defense teams frequently do not have experience working in the businesses that they oversee</td>
<td>• Staff do not understand what the commercial and regulatory requirements mean for them in their roles</td>
</tr>
<tr>
<td>• Leadership is defining compliance cultural expectations but not communicating to staff</td>
<td>• The need to deepen the ethical culture is not always actively business-led</td>
<td>• The need to deepen the ethical culture is not always actively business-led</td>
<td>• Training initiatives foster a “check the box” mentality vs. actually educating the employee</td>
<td>• Internal controls are not embedded beyond policy, processes and procedures</td>
</tr>
</tbody>
</table>

**THEME**

Inconsistent behaviors and messages from leadership

- Staff and Management are not held accountable for negative behaviors
- Culture initiatives are oriented towards remediation rather than prevention
- Compliance driven culture change is not always actively business-led
- Lack of understanding of the underlying assumptions
The Compliance Vision

Prioritizing Investments in Your Compliance Program

Balancing Priorities for Compliance Functions

- With pressure now mounting for change, many compliance leaders are taking a critical look at their functions and related areas of focus. And what they are finding is that they have become outdated—and in some cases, oversized.

- In the pursuit of achieving a "gold standard" of compliance (as laid out by various enforcement actions, deferred prosecution agreements, and corporate integrity agreements)—they have allowed their functions to grow in size and complexity. However, changes are often not aligned with the internal risk tolerance of the company or emerging trends in the regulatory and political landscape.
  
  - Most compliance functions are now suffering from significant overlap and redundancy, as well as outdated requirements that fail to mitigate the intended risk or effect a change in behavior within the business to align with the risk tolerance of the company.
  
  - Valuable resources are soaked up chasing down insignificant infractions and policing the policy.
The Compliance Vision

Balancing Priorities for Compliance Functions

Not surprisingly, many of the leading compliance functions across the United States and around the world are now rethinking their approaches to delivering on objectives. And while each is taking a customized approach to transforming its compliance programs and revisiting its strategies, our experience suggests that the most successful programs aim for three main outcomes:

1 – Becoming more Practical

- Key stakeholders are challenging the status quo and questioning the realized value of their programs in comparison to strategic compliance and commercial objectives. They recognize they will never have a perfect program and are, therefore, sharpening their focus on identifying and addressing the right risks for their particular business and markets. This, in turn, has allowed them to realign their resources to focus on higher-priority areas that create significant risks for the business.

2 – Realigning Responsibility

- Rather than enforcing a policy-driven program, many of the leading organizations are now shifting toward a principles-based program that essentially shifts responsibility for compliance back to the business. They are recognizing that compliance is an everyday priority that should be ingrained within all levels of the company. And so, they are giving the business the guidance, training, and support required to achieve compliance and allowing them to adapt the processes to their daily jobs. In doing so, they are spending less time policing the business and more time on their own business objectives.

3 – Focusing Resources

- Leading organizations are finding opportunities to release their resources from low-value tasks. Some are leveraging data analytics to improve efficiency and reduce manual processes. Others are rationalizing processes to eliminate duplication. The key is that these resources are now being tasked to higher-value activities that focus on the most important risks and critical processes for the business. By doing so, they are spending more time on the most significant risks and increasing alignment with the go-forward strategy of the company.

Questions?
Thank you