KPMG's Chief Compliance Officer Survey results

Boosting the value of compliance in a changing regulatory climate

May 12, 2017

kpmg.com
Consider how the new U.S. presidential administration is changing the regulatory landscape and how this could impact Chief Compliance Officers’ (CCO) 2017 agendas

Discuss the demographics and structure of the Survey

Discuss Survey results by program component

Discuss better practices of compliance programs
The new administration’s impact on the regulatory landscape

The new administration’s goal is to reduce cross-industry regulations by 75%, creating uncertainty as to which regulations and to what extent they could be affected.

The new administration potentially brings:

- Repealing provisions or replacement of the Affordable Care Act
- $1 trillion in infrastructure investment funded by billions in tax breaks
- Dramatic tax reform leading towards a consumption tax
- Reducing CFPB oversight authority
- DOL Fiduciary Rule vote to rescind and compliance date pushback could affect consumer protection and the insurance sector
- Continued or enhanced focus on financial crimes, trade and economic sanctions (OFAC)
- Regulatory reform and stricter enforcement of the FDA
- Repealing provisions of the Dodd-Frank Act
- Regulatory agency leadership changes (Federal Reserve, SEC, CFTC, CFPB)

Key regulatory changes may include:

- Uncertainty
- Potential shift in government enforcement tone and priorities
- Need for organizations to recalibrate their risk management and compliance priorities
- Regulatory reform
- Opportunities to further automate compliance processes

75% reduction in regulations
Boosting the value of compliance in a changing regulatory climate

Organizations are investing more resources in regulatory technology (e.g., data analytics, surveillance, compliance automation, integration of programmatic areas) and compliance transformation as core capabilities and tools to enable a proactive response to compliance risks, rather than reactively defend. As organizations’ compliance risk management programs mature—become more effective, efficient, and sustainable—cost allocations move more toward integration and automation.

*Note: Budget allocations are illustrative based on KPMG experience.
KPMG’s CCO Survey examined the specific approaches to compliance that CCOs are taking in each of nine core compliance components depicted in KPMG’s proprietary Compliance Program Framework, in order to prevent, detect, and respond across their three lines of defense model.
Launched in the summer of 2016
Sent to 300 CCOs of the largest organizations, representative of the largest FORTUNE 100 U.S. companies

<table>
<thead>
<tr>
<th>Targeted industries</th>
<th>Compliance function size ranges</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Financial services—banking and capital markets and insurance (34%)</td>
<td>— Less than 25 individuals (40%)</td>
</tr>
<tr>
<td>— Healthcare and life sciences (21%)</td>
<td>— 25-74 individuals (23%)</td>
</tr>
<tr>
<td>— Consumer markets (13%)</td>
<td>— 75-250 individuals (21%)</td>
</tr>
<tr>
<td>— Industrial markets (8%)</td>
<td>— More than 250 individuals (16%)</td>
</tr>
<tr>
<td>— Energy (14%)</td>
<td></td>
</tr>
<tr>
<td>— Technology, media and telecommunications (10%)</td>
<td></td>
</tr>
</tbody>
</table>
CCOs identified their top compliance challenges for 2017

- 55% Ensuring accountability and compliance responsibilities
- 50% Transforming compliance effectiveness and sustainability
- 50% Improving data quality
- 39% Strengthening governance and culture
- 32% Managing surveillance, reporting, data, and controls
- 31% Managing cybersecurity and data privacy
- 19% Reforming compliance reporting
- 16% Managing cross-border regulatory change

In addition, 8% of respondents identified pressures from innovators and new entrants as challenges.
Survey findings
High, low, and average responses to each compliance component

1. Governance and culture
2. Risk assessment
3. People, skills, and due diligence
4. Policies and procedures
5. Communication and training
6. Technology and data analytics
7. Monitoring and testing
8. Issues management and investigation
9. Reporting

Consumer markets
Financial services
Healthcare and life sciences
Industrial markets
Energy and natural resources
TMT
Average of all responses
Core compliance component findings

1. Governance and culture

Many organizations have:
1. Active board of directors
2. Established board committees
3. Involved and engaged CCOs

But mandates could be more robust

Percent | Target program continuum
---|---
87% | Employees understand the culture and expectations
94% | Board approves the program annually
82% | Enterprise-wide governance includes CCO

Percent | Governance and culture effectiveness
---|---
36% | CCOs that do not know line-of-business management takes ownership of culture and agenda
22% | CCOs that do not know they undertake compliance program reviews upon changes in the regulatory environment
31% | CCOs that do not communicate conduct and culture lessons

Regulators are increasingly focusing on whether organizations have a strong compliance culture, which is seen as an overarching control against misconduct.
2. Risk assessment

Core compliance component findings

The U.S. Sentencing Guidelines suggest that organizations assess their risk of criminal conduct and take appropriate steps to reduce the potential risks identified.

79% of CCOs have a formal risk assessment process; however, 24% do not, or do not know if they consider appropriate and effective internal controls.

Heavier regulated sectors are ahead, according to respondents.

- Utilize both qualitative and quantitative inputs
- Maintain an inventory of obligations
- Have a governance committee that reviews changes
Core compliance component findings

3. People, skills, and due diligence

Factor compliance into performance and compensation: 61%

Document roles and assignment: 71%

Ongoing skill assessments: 29%

Onboarding due diligence of employees and vendors: 82%
Core compliance component findings

4. Policies and procedures

Organizations have documented policies and procedures, and a code of conduct. KPMG’s CCO Survey found that they:

- Have a compliance program document with overview of program, policies, and procedures outlined: 84%
- Have policies and procedures align with mission, values, and vision: 94%
- Have their code of conduct accessible to all employees: 95%
- Have a process exist to update policies and procedures annually: 92%

Yet, processes exist to capture changes in laws, rules, and regulations for only 69% of respondents.
5. Communication and training

### Core compliance component findings

Most CCOs have a comprehensive training program for *individual employees:*

- **98%** Require compliance training include policies and procedures
- **94%** New employee training is tailored to responsibilities
- **84%** Training covers laws, rules, and regulations

**77%** of CCOs have clear lines of communication, enabling sharing of issues, lessons learned, and leading practices

However, many organizations could implement stronger training of *third parties:*

- **44%** of CCOs do not know or do not require third-party compliance training
6. Technology and data analytics (DA)

Move from **reactive** discovery and analytics to **proactive** identification of compliance issues

Organizations do not **fully take advantage** of DA

Technology and DA should be holistic, yet few CCOs report they:

<table>
<thead>
<tr>
<th>Conduct root cause and trending analyses</th>
<th>Utilize KRIs and KPIs to develop monitoring and testing approaches</th>
<th>Use KRIs and KPIs in broader compliance, risk, and governance efforts</th>
<th>Have technology that aligns with requirements without significant gaps</th>
<th>Analyze their technology infrastructure to confirm alignment with compliance requirements and identify gaps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than half for all</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Consumer markets
Average
TMT
Core compliance component findings

7. Monitoring and testing (M&T)

Robust M&T
Early identification of risks; risk trend identification and operational effectiveness is key

- **66%** Perform process and control testing as part of their M&T efforts
- **84%** M&T results are used to develop action plans
- **74%** M&T results communicated to the board and senior management
- **76%** Monitor and track regulatory changes
Core compliance component findings

8. Issues management and investigation

Protocols and mechanisms for investigating escalated activity and for all issues management (e.g., regulatory inquiries, subpoenas, etc.)

Investigation results can be an indicator of systemic or clustered issue (in organizational levels or departments)

- 77% of investigation metrics are used to inform and prioritize enhancements to the compliance program
- 65% have processes to assess the impact of issues, root causes, and cross-organizational impacts
- 76% of annual report of investigation metrics to the board of directors include root cause analysis and quantitative data
9. Reporting

Core compliance component findings

Compliance departments have the responsibility to periodically report to the governing authorities on the effectiveness of compliance programs.

CCOs agree:

- 84% of enterprise-wide compliance reports are reported to the board.
- 82% of reporting supports the organization’s risk appetite and strategic efforts.

Yet, only 47% reported having an integrated enterprise-wide reporting system (including compliance monitoring).

CCOs also note the need for a common reporting dashboard.
Core compliance component findings

Third-party risk management

There is a rising global regulatory expectation and scrutiny of organizations’ third-party relationships

Third parties are involved in more than 75% of corruption cases*

However:

— Only 52% have a process to confirm third parties adhere to compliance due diligence requirements

— Only 56% require their third parties participate in compliance training (at inception and annually)

— Only 31% have implemented an enterprise-wide tool to manage their third-party risks

*According to: Anti-Bribery and Corruption: Rising to the challenge in the age of globalization, KPMG in Switzerland, 2015
How can Internal Audit help?
## Better practices

### Preventive practices

<table>
<thead>
<tr>
<th>Risk assessment</th>
<th>Policies and procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Help with internal collaboration</td>
<td>— Review compliance policies and procedures as part of audit planning to understand compliance expectations</td>
</tr>
<tr>
<td>— Work with other assurance teams to integrated</td>
<td>— Understand how policies and procedures have been “operationalized” in the first line of defense</td>
</tr>
<tr>
<td>risk assessment programs to work toward a</td>
<td></td>
</tr>
<tr>
<td>consistent view of risk</td>
<td></td>
</tr>
<tr>
<td>Governance and culture</td>
<td>People, skills, and due diligence</td>
</tr>
<tr>
<td>— Add culture considerations to existing audits</td>
<td>— Consider compliance considerations and controls when assisting with due diligence efforts</td>
</tr>
<tr>
<td>— Perform stand-alone culture audits</td>
<td>— Test for understanding of compliance and related controls when executing audits</td>
</tr>
<tr>
<td>— Expand audit universe to consider the compliance</td>
<td></td>
</tr>
<tr>
<td>program and its individual elements</td>
<td></td>
</tr>
<tr>
<td>Training</td>
<td></td>
</tr>
<tr>
<td>— Participate in compliance training as required</td>
<td></td>
</tr>
<tr>
<td>— Review / test for completion of mandatory training</td>
<td></td>
</tr>
<tr>
<td>across the organization</td>
<td></td>
</tr>
</tbody>
</table>
### Technology and data
- Identify opportunities to develop data analytics into the risk assessment and testing programs.
- Develop continuous auditing / continuous monitoring routines to address compliance risk during audits and transition to the business for ongoing monitoring.

### Monitoring and testing
- Drive coordination among the three lines of defense.
- Linkage of testing to an integrated risk assessment, focusing on areas of highest risk and exposure.
- Coverage inclusive of data and technology.

### Issues management and investigation
- Appropriate, risk-based structure.
- Root cause analysis.
- Identification of thematic trends.
- Defined protocols.

### Detective & responsive practices

#### Detective practices

- **Technology and data**
  - Identify opportunities to develop data analytics into the risk assessment and testing programs.
  - Develop continuous auditing / continuous monitoring routines to address compliance risk during audits and transition to the business for ongoing monitoring.

- **Monitoring and testing**
  - Drive coordination among the three lines of defense.
  - Linkage of testing to an integrated risk assessment, focusing on areas of highest risk and exposure.
  - Coverage inclusive of data and technology.

#### Responsive practices

- **Issues management and investigation**
  - Appropriate, risk-based structure.
  - Root cause analysis.
  - Identification of thematic trends.
  - Defined protocols.

- **Reporting**
  - Review comprehensive to include:
    - Investigations.
    - Retaliation monitoring.
    - Program efficacy.
    - Performance metrics.
    - Training and certifications.
Questions?
For more information, contact:

Julie Gerlach  
Managing Director, Advisory  
T: 404-222-3389  
E: jgerlach@kpmg.com

Ric Kimball  
Principal, Advisory  
T: 404-222-3407  
E: ekimball@kpmg.com
Thank you