Trends in Compliance and Ethics

Global Ethics & Compliance

November 13, 2015
Agenda

- Introductions
- Compliance Trends
  - PwC’s 2015 State of Compliance Survey: Key Themes
  - Conflict Minerals – an overview
  - Third Party Risk
Compliance Trends
PwC’s State of Compliance 2015 Survey

Key Themes

1. The compliance function should actively participate in the setting of corporate strategy.

2. Owners of compliance obligations should be aware of what “compliance” entails across the organization as well as understanding the scope of their own responsibilities.

3. The compliance function should collaborate with business owners of compliance obligations.

4. Compliance leaders should evaluate and potentially re-imagine the identity of their function.

5. Compliance officers should explore ways to increase operational efficiency and effectiveness.
**Theme 1:** The compliance function should actively participate in the setting of corporate strategy.

- 78% of CEOs are concerned about over-regulation.
- 38% of CCOs saw an increase in staffing, while 36% saw no change and 8% saw a decrease.
- 50% of CEOs expect to increase headcount.

*Source: PwC’s 2015 State of Compliance Survey*
The compliance function can be particularly valuable as companies experience significant growth.

What trend do you believe will be the greatest driver for change in compliance risk management over the next 10 years?

- Technological breakthroughs: 53%
- Shifts in economic power: 12%
- Accelerating urbanization: 1%
- Climate change: 2%
- Demographic shifts: 11%

What will your Chief Compliance Officer/Corporate Compliance function do to address these trends?

- Engage with new/ additional internal stakeholders: 51%
- Engage with new/ additional external stakeholders: 45%
- Build this trend into compliance risk metrics: 52%
- Embed new compliance risks into business strategy decisions: 55%

Source: PwC's 2015 State of Compliance Survey

*Confidential Information for the sole benefit and use of PwC's Client*
**Theme 2:** Owners of compliance obligations should be aware of what “compliance” entails across the organization as well as understanding the scope of their own responsibilities.

Note: This is a representation of the way responsibility is allocated at a small sample of companies. It is not a recommendation of how that responsibility should be allocated.
**Theme 3:** The compliance function should collaborate with business owners of compliance obligations.

Which of the following departments or functions serve on the Compliance Committee?

<table>
<thead>
<tr>
<th>Department/Function</th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance</td>
<td>85%</td>
<td>83%</td>
</tr>
<tr>
<td>Legal</td>
<td>82%</td>
<td>80%</td>
</tr>
<tr>
<td>Internal Audit</td>
<td>59%</td>
<td>63%</td>
</tr>
<tr>
<td>Finance</td>
<td>55%</td>
<td>52%</td>
</tr>
<tr>
<td>Human Resources</td>
<td>54%</td>
<td>52%</td>
</tr>
<tr>
<td>Risk Management</td>
<td>50%</td>
<td></td>
</tr>
<tr>
<td>Operations</td>
<td>45%</td>
<td>41%</td>
</tr>
<tr>
<td>Information Technology</td>
<td>40%</td>
<td>32%</td>
</tr>
<tr>
<td>Business Units</td>
<td>37%</td>
<td>31%</td>
</tr>
<tr>
<td>Sales and Marketing</td>
<td>22%</td>
<td>17%</td>
</tr>
<tr>
<td>Supply Chain</td>
<td>13%</td>
<td>12%</td>
</tr>
<tr>
<td>Procurement</td>
<td>13%</td>
<td>11%</td>
</tr>
<tr>
<td>Research &amp; Development</td>
<td>12%</td>
<td>9%</td>
</tr>
<tr>
<td>Investor Relations</td>
<td>9%</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>10%</td>
<td>12%</td>
</tr>
</tbody>
</table>

*Source: PwC’s 2015 State of Compliance Survey*
‘Best in class’ compliance functions focus on key strategic and emerging risks.

Select your top 3 areas in terms of future perceived level of compliance-related risk to your business over the next 5 years (i.e., to 2020)?

![Risk Chart]

Source: PwC’s 2015 State of Compliance Survey

‘Confidential Information for the sole benefit and use of PwC’s Client’
**Theme 4:** Compliance leaders should evaluate and potentially re-imagine the identity of their function, including its people.

Which of the following skillsets and experiences are represented in your organization’s Corporate Compliance function?

- Compliance or ethics background: 80%
- Legal background: 80%
- Audit background: 65%
- Regulatory compliance experience: 64%
- Industry expertise: 55%
- Business operations background: 55%
- Finance background: 43%
- HR background: 28%
- Data analysis experience: 33%
- Technology acumen: 33%

Source: PwC’s 2015 State of Compliance Survey
**Theme 5:** Compliance officers should explore ways to increase operational efficiency and effectiveness.

**Does your Chief Compliance Officer/Corporate Compliance function actively measure compliance cost to your organization?**

- 41% Yes
- 35% No
- 24% Don't know

**What elements does your Corporate Compliance function consider to help define aggregate compliance cost when determining budgets or articulating program value?**

<table>
<thead>
<tr>
<th>Element</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct operating costs</td>
<td>74%</td>
</tr>
<tr>
<td>Compliance-related initiatives</td>
<td>69%</td>
</tr>
<tr>
<td>Systems and tools</td>
<td>57%</td>
</tr>
<tr>
<td>Third party (e.g., contingent workers, contractors, consulting fees)</td>
<td>55%</td>
</tr>
<tr>
<td>Indirect operating costs</td>
<td>51%</td>
</tr>
<tr>
<td>Direct cost of non-compliance</td>
<td>36%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
</tr>
<tr>
<td>Don't know</td>
<td>12%</td>
</tr>
</tbody>
</table>

*Source: PwC’s 2015 State of Compliance Survey*
Technology has the potential to add significant value to compliance management.

Why doesn’t your Corporate Compliance function use a dedicated GRC technology tool?

- We make do with other in-house tools
- GRC technology is not a priority for us
- We don’t have budget for GRC technology
- None of the GRC technology tools we have seen meet our needs
- GRC tools are too expensive
- We don’t have time to analyse and select a GRC technology vendor
- We don’t have the technical expertise to effectively use GRC technology tools

Source: PwC’s 2015 State of Compliance Survey
Compliance teams need data that measures how well the business manages compliance risk.

How, if at all, does your organization use data analytics in its corporate compliance and ethics program?

- For internal reporting: 53%
- For trending and comparisons: 39%
- To monitor for inappropriate or suspicious activity: 37%
- To track regulatory compliance (e.g., meeting compliance deadlines): 35%
- For visualization and dashboarding: 28%
- For transaction monitoring: 28%
- For external reporting: 20%
- We receive automated data outputs: 20%
- We do not use data analytics in our corporate compliance and ethics program: 17%
- We access data from portable devices (e.g., smartphone, tablet): 8%
- Don't know: 14%

Source: PwC's 2015 State of Compliance Survey

*Confidential Information for the sole benefit and use of PwC's Client*
Top 5 ways that compliance professionals can become C-suite stars . . .

1. **Actively express an interest** in participating in strategy decisions, and proactively articulate to the CEO the strategic value that compliance can deliver.

2. **Review the strategic plan** and develop ideas for addressing new or unusual compliance risks, or leveraging them to gain competitive advantage.

3. **Forge close relationships with key business leaders** throughout the company and offer insights to help the business identify and mitigate risks related to compliance issues.

4. **Define (or redefine) the scope of compliance** across the organization and build partnerships with compliance owners within the business to ensure that all issues are being managed effectively.

5. **Implement efficiency initiatives** to improve the effectiveness of the compliance function and reduce compliance-related costs.
**Temporary stay on disclosing conflict status**

- Included in the SEC’s communication that suspended the conflict status labelling requirement
- Has caused some confusion over whether this guidance overrides the Rule’s requirement for the audit in CY2015
- On August 18th, the U.S. Court of Appeals for the D.C. Circuit upheld their original decision that the labelling requirement is unconstitutional.
- On October 2, 2015, SEC and Amnesty International filed petitions requesting an en banc rehearing of the April 2014 and the August 2015 D.C. Court of Appeals panel decisions, in an effort to reverse the ruling that struck down portions of the conflict minerals rule as unconstitutional.

“Pending further action, an IPSA will not be required unless a company voluntarily elects to describe a product as “DRC conflict free” in its Conflict Minerals Report.”

--SEC statement, April 29, 2014
SEC High Level Requirements

S1502 essentially requires a new level of transparency and risk management across company supply chains.

What are conflict minerals?
Conflict minerals, per S1502, are tantalum, tin, tungsten and gold (“3TG”) that may be necessary to the production or functionality of a company’s products.

What is the goal of s1502?
S1502 seeks to reduce funding for armed groups in the DRC and surrounding countries. Companies are required to perform due diligence and report on whether the 3TG in their products may have been sourced from the DRC region, and if so, if they are conflict free. Note that the regulation does not restrict sourcing from the region. This is a transparency requirement only.

When is the reporting due??
The Form SD (and, if applicable, CMR) are due May 31st for the prior calendar year.

~1,265
Issuers filed a Form SD

~ 1,000
Issuers included a Conflict Minerals Report (over 75%)

6
Issuers obtained an audit of their Conflict Minerals Report

Figures are based on CMRs filed as of 7/15/2015
Summary of SEC Rule – Audit Requirement

- The Conflict Minerals Report, when required, must include an independent audit report to express an opinion or conclusion covering:
  - Whether the design of the due diligence framework conforms, in all material respects, with a nationally or internationally recognized framework (e.g., OECD), and
  - The accuracy of the description in the CMR of the DD measures undertaken
- Generally Accepted Government Auditing Standards (Yellow Book) established by GAO apply. Audit could be either:
  - Attestation Engagement (must be performed by CPA), or
  - Performance audit (not required to be conducted by CPA)
- For companies using their financial statement auditor, the IPSA is considered a non-audit service subject to pre-approval by the Audit Committee
- Some level of independence required to be the IPSA auditor
**Program Assessment or Mock Audit**

<table>
<thead>
<tr>
<th>Program Assessment</th>
<th>Mock Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Assessment of the company’s Conflict Mineral compliance program and activities,</td>
<td>• Focuses on preparedness of the company to meet the 2 objectives in scope</td>
</tr>
<tr>
<td>broadly</td>
<td>of the future IPSA</td>
</tr>
<tr>
<td>• Covers both areas of compliance as well as areas in scope of the audit</td>
<td>• Execute the audit methodology</td>
</tr>
<tr>
<td>• Can include program design and/or execution (minimally a sample of 1)</td>
<td>• Assess Company’s due diligence framework is designed in conformity, in</td>
</tr>
<tr>
<td></td>
<td>all material respects, with the criteria set forth in the OECD</td>
</tr>
<tr>
<td></td>
<td>• Company’s description of the due diligence measures is consistent, in</td>
</tr>
<tr>
<td></td>
<td>all material respects, with the due diligence process the Company</td>
</tr>
<tr>
<td></td>
<td>undertook</td>
</tr>
</tbody>
</table>
Third Party Risk

Increased reliance on Third Parties represents a unique compliance challenge.
Third Party Risk Management

Third party risk management is focused on understanding and managing risks associated with third parties with which the company does business and/or shares data.

**Third Party Risk Management Framework**

Third party risk management is focused on understanding and managing risks associated with third parties with which the company does business and/or shares data.

**Third Parties**
- Vendors
- Suppliers
- Joint Ventures
- Business Channels
- Marketing Partners
- Affiliates
- Broker Dealers
- Regulated Entities

**The PwC TPSRM Framework**

**Risk Considerations**
- Reputational
- Privacy
- Operational
- Regulatory / Compliance
- Financial
- Termination
- Business Continuity
- Subcontractor
- Country
- Technology
- Information Security
- Concentration

*Confidential Information for the sole benefit and use of PwC’s Client*
Managing Risk Associated with Third Parties

The following are examples of Third Party due diligence assessments performed on potential and existing third parties to understand the existing control environment and capabilities.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Information Security &amp; Privacy</th>
<th>Physical Security</th>
<th>Subcontractor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology Architecture</td>
<td>Security policies</td>
<td>Fire Suppression</td>
<td>Third Party Relationship Management</td>
</tr>
<tr>
<td>Assets utilized</td>
<td>Encryption</td>
<td>Server Security &amp; Conditions</td>
<td>Sub-Service Third Party Relationships</td>
</tr>
<tr>
<td>Technology Roadmap</td>
<td>Logical access Control</td>
<td>Data Centers</td>
<td>Logical access Control</td>
</tr>
<tr>
<td>Technological capabilities</td>
<td>Customer contact</td>
<td>Backup Power Sources</td>
<td>Monitoring, communication and connectivity</td>
</tr>
<tr>
<td>System Development Lifecycle (SDLC)</td>
<td></td>
<td>Asset management</td>
<td></td>
</tr>
<tr>
<td>Audit trail</td>
<td></td>
<td>Key Card &amp; Facility Access</td>
<td></td>
</tr>
<tr>
<td>Application management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring, communication and connectivity</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Country</th>
<th>Reputational</th>
<th>Financial</th>
<th>Business Continuity &amp; Resiliency*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Political</td>
<td>Litigation or ethical flags</td>
<td>Going concern</td>
<td>Recovery</td>
</tr>
<tr>
<td>Geographic</td>
<td>Media coverage</td>
<td>Liquidity</td>
<td>Data Backup Management</td>
</tr>
<tr>
<td>Regulatory</td>
<td>OFAC or other factors</td>
<td>Leverage</td>
<td>Offsite storage</td>
</tr>
<tr>
<td>Legal</td>
<td></td>
<td>Profitability</td>
<td>Media and vital records</td>
</tr>
<tr>
<td>Economic</td>
<td></td>
<td>Transaction Processing</td>
<td>Data integrity</td>
</tr>
<tr>
<td>Travel Safety</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operational</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>People</td>
<td>Anti-Bribery</td>
</tr>
<tr>
<td>Process</td>
<td>Anti-Money Laundering</td>
</tr>
<tr>
<td>Financial Reporting</td>
<td>Sales &amp; Marketing Activities</td>
</tr>
<tr>
<td>Subcontractors</td>
<td>Transparency Reporting</td>
</tr>
<tr>
<td>Concentration</td>
<td>Anti-corruption</td>
</tr>
<tr>
<td></td>
<td>PCI</td>
</tr>
</tbody>
</table>

*Business Continuity Management includes Business Contingency (“BC”) planning and Disaster Recovery (“DR”)

PwC

*Confidential Information for the sole benefit and use of PwC’s Client
**Third party inventory, stratification and on-going assessment model**

The inventory, risk rating and on-going testing model enables a focus on efforts to establish the third party inventory, oversee services with higher levels of inherent risk. The model relies on the existing third party inventory and new third parties as an input, as well as an area of refresh to ensure the third party inventory is kept complete and accurate on an on-going basis. The model also drives the on-going due diligence process based on the inherent risk and the business facts of the services provided.
# Third Party Risk Management – Program governance structure

A TPRM strategy is supported by three lines of defense – the first line lies within each individual Line of Business and is empowered by the second line who owns the provision of ongoing guidance, tool support, and facilitation of cross-business collaboration. The third line is responsible for evaluating the design and operating effectiveness of the Program.

## First Line of Defense
- Primary responsibility for compliance and owner of risk
- BU managers and third party relationship owners are responsible for identifying, assessing and mitigating risk associated with their business
- Implement internal controls and practices are consistent with company-wide policies & procedures
- Promote a strong risk culture and sustainable risk-return decision making

## Second Line of Defense
- Independent compliance framework, policy & oversight
- Business partners work with the BU’s to identify, assess and mitigate all risks
- Design and assist in implementing company-wide risk framework and oversee enterprise risks
- Provide independent risk oversight across all risk types, business units and locations
- Perform quality assurance reviews and other targeted oversight practices to ensure that the line of business is compliant with internal policies/ external regulations

## Third Line of Defense
- Independent assurance
- Independently test, verify and evaluate risk management controls against internal policies
- Report upon effectiveness of the program

---

<table>
<thead>
<tr>
<th>Board of Directors</th>
<th>Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Audit</td>
<td>Enterprise Risk Committee</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Legal &amp; Compliance</th>
<th>Management &amp; Oversight</th>
<th>Operational Risk Oversight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third Party Management Office</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sourcing</th>
<th>Subject Matter Specialists</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procurement</td>
<td>Contracts Management</td>
</tr>
<tr>
<td>Sourcing</td>
<td>InfoSec, Privacy, PhySec, BCM, TP Compliance, TPRM, HR, Credit/Finance, Reputational Risk, Technology, Operational Risk</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Unit Sponsor</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Third Parties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subcontractors</td>
</tr>
</tbody>
</table>
**Bio’s**

**Thack Skidmore**
Director, Performance Governance Risk and Compliance
PwC LLP
Irvine, California
Thack.skidmore@pwc.com
+1 949.437.5607

**Cynthia Keith**
Manager, Risk Assurance
PwC LLP
San Diego, California
cynthia.g.keith@pwc.com
+1 858.677.2675
Thank you