Assessing Your Ethics and Compliance Program:
Getting an updated view, and what culture can tell you

Society of Corporate Compliance & Ethics
February 20, 2017

Presenters:
Holly Wenger (Duke)
Stacy Mines (EY)
Marisa Hardy (EY)

Agenda

► Key concepts for ethics and compliance program (“Program”) assessment
  ► Program objectives
  ► Program scope
  ► Program structure
► Undertaking an assessment
  ► Program elements to consider
  ► Approach
  ► How to assess culture, and what it can tell you about your Program
► Now what? What to do about assessment results
  ► What to do in between assessments: escalation protocols
Key concepts for program assessment
Program objectives

Objectives of an ethics and compliance program

An ethics and compliance program must be well-designed, applied in good faith, and actually implemented across the organization.

1. Provide assurance to shareholders and the board of directors that the company complies with its legal obligations.
2. Communicate expectations and provide workable solutions for compliance by employees and third parties acting on behalf of the company.
3. Provide assurance to employees and third parties that they can raise concerns in a safe environment, and those issues will be resolved timely.
4. Foster a culture where acting ethically and in compliance with company values is highly regarded.
5. Ensure the company takes a risk-based approach to alignment of resources.
6. Attract customers, business partners and employees, because the company demonstrates high ethical standards.

---
Six key questions

Ethics and compliance officers should be able to answer six key questions through their Programs.

1. What are our most significant ethics and compliance risks?
2. Who is accountable for managing them?
3. What are they doing?
4. Is it working?
5. How do we know?
6. Do we have appropriate data and records management practices?

Key concepts for program assessment
Program scope
Duke's independent monitor has been complimentary of the Company's efforts to break down compliance silos.

### Compliance risk universe

#### Legal and regulatory requirements

<table>
<thead>
<tr>
<th>Category</th>
<th>Subcategories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Competitive practices</td>
<td>(FTC, DOJ)</td>
</tr>
<tr>
<td>Corporate governance</td>
<td>(SEC)</td>
</tr>
<tr>
<td>Employee</td>
<td>(EEOC, DOL)</td>
</tr>
<tr>
<td>Environmental (EPA)</td>
<td>(US)</td>
</tr>
<tr>
<td>Financial</td>
<td>(SEC)</td>
</tr>
<tr>
<td>Government contracts</td>
<td>(DOD, OMB)</td>
</tr>
<tr>
<td>Intellectual property</td>
<td>(DOC)</td>
</tr>
<tr>
<td>International dealings/trade</td>
<td>(FTC, DOC)</td>
</tr>
<tr>
<td>Workplace health/safety</td>
<td>(OSHA)</td>
</tr>
<tr>
<td>Product quality/ liability</td>
<td>(FDA)</td>
</tr>
</tbody>
</table>

#### Business requirements

<table>
<thead>
<tr>
<th>Category</th>
<th>Subcategories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internally focused requirements</td>
<td>(Mergers)</td>
</tr>
<tr>
<td>Externally focused requirements</td>
<td>(Corporate governance)</td>
</tr>
<tr>
<td>Voluntary standards</td>
<td>(Sustainability)</td>
</tr>
<tr>
<td>Emerging issues</td>
<td>(Six Sigma)</td>
</tr>
</tbody>
</table>

#### Why is Program scope so important?

- U.S. Sentencing Guidelines, SEC, DOJ, and FERC set forth key elements of an effective compliance program; view is broad
- Effective, broad-based compliance programs may mitigate criminal penalty
- Role of Ethics and Compliance department is to provide reasonable assurance core compliance management practices are in place — i.e., provide independent oversight
- Duke’s enterprise compliance program initially identified 21 compliance risk areas, including FERC, NERC, Nuclear, State Regulatory, Aviation, Tax, Anti-corruption, Political Activity, Supply Chain, Labor and Employment, SOX, and Federal and State Contracting
- Duke’s independent monitor has been complimentary of the Company’s efforts to break down compliance silos
It is crucial to develop an ethics and compliance framework to ground your Program; that’s what you should assess against.
A framework provides a comprehensive view of your Program structure

Benefits of having a Program framework

A Program framework drives a common view of ethics and compliance across all risk areas. It provides a comprehensive approach for defining accountabilities, core program elements, and key standards.

- Sets accountability for cross-cutting elements such as compliance risk assessment and Helpline process (response and remediation)
- Identifies those accountable for compliance programs in key risk areas
- Establishes universal standards with accountabilities and process steps
- Provides tools for management reporting and oversight
- As enforcement guidance evolves, requirements and expectations are incorporated into the framework and standards, and are communicated uniformly to compliance risk areas
Framework and standards:
Coverage

**Prevention**
Leadership standards for governance, ethics and compliance leadership, values and culture; Practice standards for compliance requirements, compliance risk management, policies & procedures, and communication & training

**Detection & Response**
Leadership standards for confidential reporting; Practice standards for assurance, monitoring & auditing, and investigation & response

**Continuous Improvement**
Leadership standards for confidence in the Program; Practice standards for continuous improvement and utilizing lessons learned to review and improve Program elements

Framework and standards example

A compliance framework sets accountability for cross-cutting Program elements. In addition, a compliance framework identifies those accountable for managing compliance obligations in core risk areas and operations. This is essential as the compliance group does not manage day-to-day compliance obligations — that work is done in the operating units. A framework would have core categories focused on prevention, detection, and response, underlying elements and related standards (sample standards provided in one area as an example only). The core elements and standards are developed based on each organization’s structure, culture, and underlying decisions regarding program scope and responsibilities.
Using your framework for assessments

► Assess against your framework
  ► Keep in mind your framework should be designed to incorporate external guidance (i.e., Federal Sentencing Guidelines and FERC guidance)
► Ensure assessment tools are tied to your framework
► Benefits
  ► Allows for third party and internal assessment of progress against core program elements at the compliance risk level – not just at enterprise level
  ► Utilizes an optional maturity model to facilitate continuous improvement
  ► Provides tools for management reporting and oversight
  ► Assessing against your framework helps ensure that when you design improvement plans, they are tied to the structure you have in place and communicated to all stakeholders

The value of Framework and Assessments
It pays to be prepared!

► Duke has stayed in the driver’s seat on the development and implementation of the framework rather than being told by the IM what to do and when
  ► Demonstrates commitment to a compliance culture
► Improves even the most mature compliance programs and provides a path for less mature programs to evolve
► Facilitates sharing of best practices and lessons learned among compliance professionals
  ► Created a Compliance Council comprised of the compliance area lead for each identified compliance risk area
  ► Commitment to IM was twice a year meetings but Council members requested quarterly meetings in 2017 based on benefits gained in 2016
► For the first time, identified in 2016 the top 10 enterprise compliance risks based on a common, repeatable process and developed appropriate mitigation
Program lifecycle

- Regularly evaluate effectiveness of overarching framework.
- On phased cycle, assess discrete compliance risk areas against framework (identify gaps, etc.)
- Each compliance risk area builds its own tailored program to fit its risk profile, meeting each element of the framework and standards.
- Regularly re-assess compliance and ethics risks to ensure appropriate coverage, considering changes in regulatory requirements, audit findings, actual cases (externally and internally).
- Update framework to reflect changes in business or operations, new compliance risks, and/or enforcement guidance.

Undertaking a Program assessment
What is the purpose of a Program assessment?

- Assess the design and operation performance of the ethics and compliance infrastructure – including the compliance function and processes – relative to legal/regulatory requirements and leading practices
- Help management to identify and prioritize opportunities to enhance culture and infrastructure, including integration, alignment, and coordination across organizational boundaries
- Establish a baseline for assisting management with ongoing ethics and compliance monitoring and continuous improvement
- Help management identify opportunities to embed and sustain risk management activities throughout the organization

The following framework elements should be included in an assessment

<table>
<thead>
<tr>
<th>Ethics and integrity</th>
<th>Oversight</th>
<th>Supporting elements</th>
<th>Prevention</th>
<th>Detection</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Values</td>
<td>Board oversight</td>
<td>Internal and external communication</td>
<td>Code of conduct</td>
<td>Speaking up and confidential reporting</td>
<td>Incident and case management</td>
</tr>
<tr>
<td>Culture</td>
<td>Management responsibility</td>
<td>Program evaluation and sustainability</td>
<td>Compliance risk assessment</td>
<td>Monitoring, reviews and auditing</td>
<td>Corrective</td>
</tr>
<tr>
<td>Tone at the top</td>
<td>Compliance organization and structure</td>
<td>Policies, procedures, processes and controls</td>
<td>Education and Training</td>
<td>Data collection and analytics</td>
<td>Enforcement, remediation and reporting</td>
</tr>
<tr>
<td></td>
<td>Program coordination and integration within the enterprise</td>
<td>Incentives</td>
<td>Incentives</td>
<td>Requirement management and implementing process</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Program reporting</td>
<td>Third-party due diligence</td>
<td>Third-party due diligence</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Requirement management and implementing process</td>
<td>Requirement management and implementing process</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Foundational approach for Program assessments**

<table>
<thead>
<tr>
<th>1</th>
<th>Launch</th>
<th>Confirm project goals and schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Assess Program</td>
<td>Assess current state of compliance program</td>
</tr>
<tr>
<td>3</td>
<td>Findings</td>
<td>Identify strengths, gaps, and recommendations</td>
</tr>
<tr>
<td>4</td>
<td>Report</td>
<td>Present findings and finalize report with recommendations</td>
</tr>
</tbody>
</table>

**Continuous communication and coordination with those involved**

- Agree on protocols and expectations
- Planning meeting
- Identify documents to be reviewed
- Confirm interview lists and schedules
- Review documents to establish baseline view of the compliance program across business
- Conduct interviews to assess current state of compliance program
- Governance
- Resources
- Policies, procedures controls
- Monitoring
- Management reporting
- Analyze the interview results
- Identify top program strengths and areas for improvement
- Identify leading practices that have been used to address areas for improvement in other companies
- Discuss initial findings with compliance office
- Submit final report
- Deliver and present report with detailed observations, recommendations, and practices to consider to address gaps

---

**Conducting program assessments internally**

- Create a Compliance Framework Assessment manual and distribute to Compliance Area Leads
- Important to socialize assessment process with Functional Area Leads (i.e., the business leaders) and gain support
- Be flexible yet firm
- Look for best practices, not just gaps
- In facilitated sessions, include employees from different groups within the compliance area
- Provide an assessment report to the Compliance and Functional Area Leads and secure commitments to close identified gaps
Examples of common gaps identified in ethics and compliance program assessments

- Incomplete reporting to the board and senior leadership
- Lack of consistent ethics and compliance risk assessment process
- Absence or immaturity of consistent investigation protocols for all of the various parties conducting investigations
- Policy management is deficient (e.g., minimum review cycle, tracking reviews, and ensuring policies do not conflict)
- Unclear roles and responsibilities particularly regarding compliance requirement intake
- Lack of documented compliance processes

Culture considerations as part of your assessment
Consideration of culture within compliance program assessment

- Culture is often evaluated by engagement surveys and related to the Human Resources function.
- Culture affects compliance program elements and should be considered as part of compliance risk assessments in conjunction with other procedures.
  - Tailored questions to specific compliance risks.
- Surveys on culture can be developed to provide additional insight into program elements across locations, departments and employment levels.

Hypothetical – Program communications

- To assess leadership and “tone-at-the-top”, program assessments consider communication from management. Let’s say a traditional assessment shows that employee communications (e.g., newsletters) are regularly distributed with heavy messaging from the CEO and other executives. Those observations would likely result in a high score for that area.
- However, program assessments should also consider how the communication is perceived by employees within the company, e.g., via survey:
  - Example: “I regularly trust the information provided to me by:”

![Survey Results Chart]

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree
- Don’t Know
Hypothetical – Program communications (cont’d.)

► Example: "I regularly trust the information provided to me by:"

- It looks like messaging would be most effective coming from local managers or supervisors. So, although some messaging should still come from executives, the company should consider distributing other key messaging through local managers or supervisors.

► Given the level of neutral-to-disagree responses regarding messaging coming from executives including the CEO, the ethics and compliance office should partner with key stakeholders to address that finding.

Hypothetical – Program training

► Program assessments include a review of training materials and the process of updating for new policies or regulations. A typical assessment would include review of these materials. If they all appear to be in place and updated, it might seem as if this element is well-established.

► However, are there could be high risk components of the training program that require additional focus or attention. E.g., is ample training provided across all departments?

► Example: "In the past two years, I have received sufficient and useful training that covers and includes..."
Hypothetical – Policies

A program assessment might identify that a Company provides regularly updates policies and procedures.

However, are the policies and procedures understood?

Across all levels?

Example: “I have received clear information or guidance from the company regarding what to do when faced with a conflict of interest.”

The survey results here show that the company should consider enhancing the way conflict of interest policies/training are provided to individual contributors.

Hypothetical – Accountability

Even if a company provides adequate training and employees are aware of the proper process for reporting, compliance programs cannot be effective if employees do not believe violators of policy will be held accountable and/or they will experience retaliation.

Example: “If I reported a violation to management, I believe:”
Getting senior leadership to understand that compliance and ethics don’t “just happen”

► May find gaps between executive expectations and employee understanding or perceptions
► Creating a culture of compliance is a relentless job and it starts at the top
  ► Have a communication plan
  ► Make leadership messaging easy

Now what?
What to do with assessment results
Close gaps: develop improvement plans

► Create a roadmap for prioritized improvement opportunities
► Work with compliance area leads and/or risk owners to develop improvement plans
► Monitor improvement on a consistent basis
► Share lessons learned

Example roadmap (Program)

<table>
<thead>
<tr>
<th>ID</th>
<th>Project Name</th>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Response: Develop a standardized approach to managing investigations</td>
<td>Protocols developed</td>
<td>Training developed</td>
<td>Escalation guidelines developed</td>
<td></td>
</tr>
<tr>
<td>02</td>
<td>Response: Implement investigation case management system</td>
<td>Implementation plan developed</td>
<td>Users trained</td>
<td></td>
<td></td>
</tr>
<tr>
<td>03</td>
<td>Prevention: Enhance policy management</td>
<td>Governance document implemented</td>
<td>Structure developed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>04</td>
<td>Prevention: Develop a repeatable risk assessment process and calibrate results</td>
<td>Prioritize risks</td>
<td>Results calibrated; process enhanced</td>
<td>Solutions identified</td>
<td></td>
</tr>
<tr>
<td>05</td>
<td>Oversight: Strengthen framework: define key roles and responsibilities</td>
<td>Program activities identified</td>
<td>Requirements established</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06</td>
<td>Oversight: Enhance reporting to Board and senior leadership</td>
<td>ELT meetings restructured</td>
<td>Guidelines formalized</td>
<td></td>
<td></td>
</tr>
<tr>
<td>07</td>
<td>Detection: Develop escalation guidelines</td>
<td></td>
<td>Guidelines distributed</td>
<td>Training conducted</td>
<td></td>
</tr>
<tr>
<td>08</td>
<td>Ethics &amp; Integrity: Enhance annual communication plan</td>
<td></td>
<td>Compliance responsibility consolidated</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Example roadmap (Prevention – compliance risk assessment)

<table>
<thead>
<tr>
<th>Goals and Success Measures</th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Q1</td>
<td>Q2</td>
<td>Q3</td>
</tr>
<tr>
<td>Develop a repeatable compliance risk assessment process with clear definitions, standards, reporting templates, and calibrate results across compliance areas. Use results to drive Program activities and identify pervasive issues.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Success Measures:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Engage stakeholders: develop a repeatable compliance risk assessment process with clear definitions, standards, reporting templates, and calibration metrics across compliance areas.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B. Perform compliance risk assessment.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C. Aggregate data.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D. Develop prioritized list of compliance risk items.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E. Compare and calibrate results across compliance areas.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F. Assess process; make necessary enhancements (e.g., in tools/templates).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G. Use results to drive Program activities and identify issues that may benefit from enterprise-wide solutions.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Repeat assessment process annually.

---

## What to do in between assessments: Escalation protocols

...
Escalating issues of non-compliance or unethical behavior

► Develop clear guidelines for escalating and remediating compliance issues (to the Compliance Office/Department) as they arise
  ► Clear reporting thresholds consistently applied across the enterprise
  ► Communicate guidelines and train on them, as appropriate (e.g., build into Code of Business Conduct training)
  ► Consolidate responsibility for monitoring compliance issues with Compliance Office/Department to allow greater enterprise coordination, sharing of lessons learned and consistency in resolving issues.

Duke’s Escalation Procedures

► Important to determine what level of corporate oversight is appropriate

► Mandatory notification to the Ethics and Compliance Department required for “severe” or “critical” events or conditions, e.g.:
  ► Moderate or large financial consequences to a business area over a short timeframe and/or regulator fines that appear to be increasing or would be considered high for the regulator
  ► Prolonged or long-term loss of confidence by multiple stakeholder groups and/or ongoing/regular negative media exposure
  ► Agency action(s) that result in substantial or severe impacts or limits on operations
  ► Many customers are affected and/or there is a large or critical impact to internal business operations
  ► Involvement of a member of the Executive Leadership Team in an alleged CoBE violation
Q&A / Closing