


**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

---

Page 2 EY

---

---

---

---


---

---

---

---

**Key concepts for program assessment**  
**Program objectives**



Page 3 EY

---

---

---

---

---

---

---

---

## 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 written guidance for compliance to employees and third parties acting on behalf of the company
- 3 Provide assurance to employees and third parties that they can rely on the company as a safe environment, and these issues will be resolved fairly
- 4 Foster a culture where acting ethically and in compliance with company values is highly regarded
- 5 Attract customers, business partners and employees, because the company demonstrates high ethical standards
- 6 Ensure the company takes a risk-based approach to alignment of resources



Page 4

EY

---

---

---

---

---

---

---

---

---

---

## 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?



Page 5

EY

---

---

---

---

---

---

---

---

---

---

## Key concepts for program assessment

### Program scope



Page 6

EY

---

---

---

---

---

---

---

---

---

---

## Compliance risk universe \*Illustrative utility company example

Legal and regulatory requirements		Business requirements	
<b>Competitive practices (FTC, DOJ)</b> <ul style="list-style-type: none"> <li>Antitrust</li> <li>Consumer, competitor, supplier relations</li> </ul>	<b>Fraud and corruption (DOJ)</b> <ul style="list-style-type: none"> <li>Foreign Corrupt Practices Act (FCPA)</li> <li>Insider transactions</li> <li>Anticorruption requirements</li> <li>Financial statement fraud</li> <li>Occupational fraud (intellectual property, trade secrets)</li> <li>Corruption</li> <li>Revenue and expense recognition</li> </ul>	<b>NRC</b> <ul style="list-style-type: none"> <li>Nuclear operations and decommissioning</li> <li>New construction</li> </ul>	<b>Internally focused requirements</b> <ul style="list-style-type: none"> <li>Market</li> <li>Values</li> <li>Code of Conduct</li> <li>Privacy and protection</li> <li>Quality management certification (ISO, Six Sigma)</li> <li>Green preparedness</li> </ul>
<b>Corporate governance (SEC)</b> <ul style="list-style-type: none"> <li>Board structure and processes</li> <li>Anti-corruption structure and controls</li> </ul>	<b>Government contracts (DOCS OMB)</b> <ul style="list-style-type: none"> <li>US Government contracts</li> <li>Other jurisdictions (state and country)</li> </ul>	<b>State PUCs</b> <ul style="list-style-type: none"> <li>State rate and other cost-recovery cases</li> <li>Regulatory proceedings and investigations</li> <li>Reporting requirements</li> <li>Real-time rates</li> <li>Priority rules</li> </ul>	<b>Externally focused requirements</b> <ul style="list-style-type: none"> <li>Stakeholder responsibility</li> <li>Public commitments</li> <li>Contractual obligations</li> <li>Vendor management</li> <li>Exchange listings</li> </ul>
<b>Employment (EEOC, DOL)</b> <ul style="list-style-type: none"> <li>Executive compensation</li> <li>Compensation</li> <li>Benefits</li> <li>Wage</li> <li>Employee life/privacy</li> <li>Production in force</li> <li>Whistleblower protection</li> <li>Harassment prevention</li> <li>Accommodation (discrimination covered)</li> <li>Workplace violence</li> <li>Child labor (immigration)</li> <li>Contract labor</li> <li>Employment terms</li> </ul>	<b>Information management</b> <ul style="list-style-type: none"> <li>Records retention</li> <li>Freedom of Information Act (FOIA)</li> <li>Data and record classification</li> <li>Information access</li> <li>Information availability and recovery</li> <li>Information management monitoring</li> <li>Information disposition</li> <li>Information retention rules</li> <li>Data protection and privacy</li> </ul>	<b>FERC</b> <ul style="list-style-type: none"> <li>Market manipulation</li> <li>Benefits</li> <li>Utility restrictions</li> <li>Standards of conduct</li> <li>Wholesale market price reporting</li> <li>Compliance effectiveness</li> </ul>	<b>Voluntary standards</b> <ul style="list-style-type: none"> <li>US Sentencing Guidelines</li> <li>Industry codes</li> <li>Trade associations</li> </ul>
<b>Environment (EPA)</b> <ul style="list-style-type: none"> <li>Asbestos</li> <li>Water quality</li> <li>Management systems and reporting</li> <li>Hazardous material management</li> <li>Laboratory practices</li> <li>Pest management</li> </ul>	<b>Intellectual property (DOC)</b> <ul style="list-style-type: none"> <li>Copyright</li> <li>Trademarks</li> <li>Trade secret</li> <li>Patent</li> </ul>	<b>Commercial operations</b> <ul style="list-style-type: none"> <li>Participation in RTO and RTO markets</li> <li>Buy and sell power, settlement</li> <li>Capacity and supply obligations</li> <li>Counterparty</li> <li>Critical infrastructure protection standards</li> <li>Reliability standards</li> </ul>	<b>Emerging issues</b> <p>Aside from mandatory requirements, organizations make choices regarding their brand, their values and the commitments they make to customers, business partners, employees and other stakeholders. Although voluntary, consequences for non-compliance could be more serious than non-compliance with mandatory requirements.</p>
<b>Financial</b> <ul style="list-style-type: none"> <li>SOX</li> <li>Tax</li> <li>Treasury</li> </ul>	<b>International dealings/trade (FTC, DOJ)</b> <ul style="list-style-type: none"> <li>Export</li> <li>Import</li> <li>Embargo</li> </ul>	<b>NERC</b> <ul style="list-style-type: none"> <li>Grid infrastructure protection standards</li> <li>Reliability standards</li> </ul>	<b>Emerging issues</b> <p>Aside from mandatory requirements, organizations make choices regarding their brand, their values and the commitments they make to customers, business partners, employees and other stakeholders. Although voluntary, consequences for non-compliance could be more serious than non-compliance with mandatory requirements.</p>
	<b>Workplace health/safety (OSHA)</b> <ul style="list-style-type: none"> <li>Safety and Emergency Response (SERF)</li> <li>Employees</li> <li>Contractors</li> <li>Product quality/ability</li> <li>Quality management system</li> </ul>	<b>CFTC</b> <ul style="list-style-type: none"> <li>Financial/institutions/trading</li> <li>Trading standards</li> </ul>	<b>Emerging issues</b> <p>Aside from mandatory requirements, organizations make choices regarding their brand, their values and the commitments they make to customers, business partners, employees and other stakeholders. Although voluntary, consequences for non-compliance could be more serious than non-compliance with mandatory requirements.</p>
	<b>Political activities</b> <ul style="list-style-type: none"> <li>Lobbying guidelines</li> <li>SEC guidelines</li> <li>Employee activities</li> <li>Time and expense reporting of meetings</li> </ul>	<b>Political activities</b> <ul style="list-style-type: none"> <li>Lobbying guidelines</li> <li>SEC guidelines</li> <li>Employee activities</li> <li>Time and expense reporting of meetings</li> </ul>	<b>Emerging issues</b> <p>Aside from mandatory requirements, organizations make choices regarding their brand, their values and the commitments they make to customers, business partners, employees and other stakeholders. Although voluntary, consequences for non-compliance could be more serious than non-compliance with mandatory requirements.</p>

Page 7

EY

## 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

Page 8

EY

## Key concepts for program assessment Program structure



Page 9

EY

**It is crucial to develop an ethics and compliance framework to ground your Program; that's what you should assess against.**

---

---

---

---

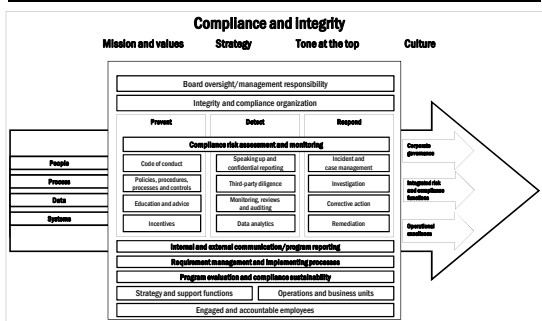
---

---

---

---

**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

---

---

---

---

---

---

---

---



**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

---

---

---

---

---

---

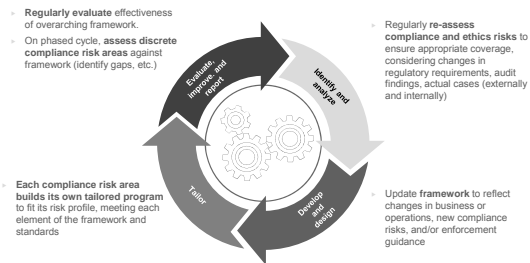
---

---

---

---

**Program lifecycle**



---

---

---

---

---

---

---

---

---

---

**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**

Ethics and integrity	Oversight	Supporting elements	Prevention	Detection	Response
<ul style="list-style-type: none"> <li>• Values</li> <li>• Culture</li> <li>• Tone at the top</li> </ul>	<ul style="list-style-type: none"> <li>• Board oversight</li> <li>• Management responsibility</li> <li>• Compliance organization and structure</li> <li>• Program coordination and integration within the enterprise</li> <li>• Program reporting</li> </ul>	<ul style="list-style-type: none"> <li>• Internal and external communication</li> <li>• Program evaluation and sustainability</li> </ul>	<ul style="list-style-type: none"> <li>• Code of conduct</li> <li>• Compliance risk assessment</li> <li>• Policies, procedures, processes and controls</li> <li>• Education and Training</li> <li>• Incentives</li> <li>• Third-party due diligence</li> <li>• Requirement management and implementing process</li> </ul>	<ul style="list-style-type: none"> <li>• Speaking up and confidential reporting</li> <li>• Monitoring, reviews and auditing</li> <li>• Data collection and analytics</li> </ul>	<ul style="list-style-type: none"> <li>• Incident and case management</li> <li>• Corrective</li> <li>• Enforcement, remediation and reporting</li> </ul>

---

---

---

---

---

---

---

---

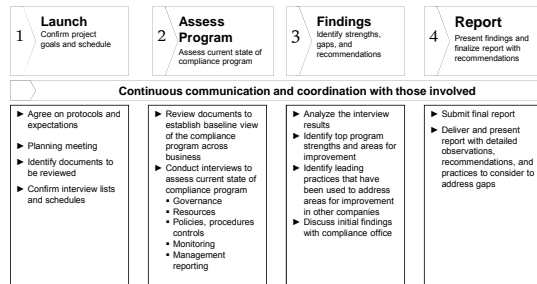
---

---

---

---

**Foundational approach for Program assessments**




---

---

---

---

---

---

---

---

---

---

---

---

**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

---

---

---

---

---

---

---

---

---

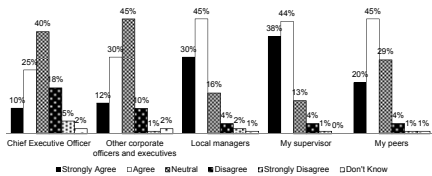
---

---

---

**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:”*




---

---

---

---

---

---

---

---

---

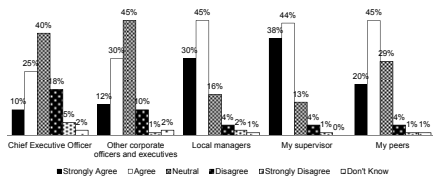
---

---

---

**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.

---

---

---

---

---

---

---

---

---

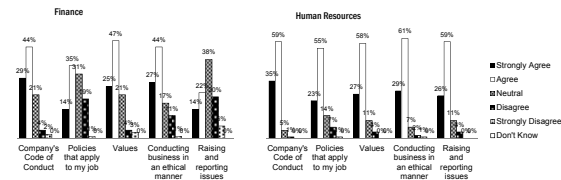
---

---

---

### 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..."*



---

---

---

---

---

---

---

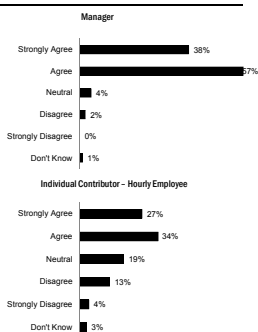
---

---

---

### 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.



---

---

---

---

---

---

---

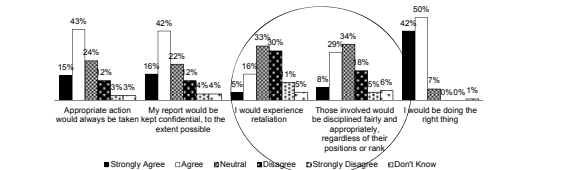
---

---

---

### 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

---

---

---

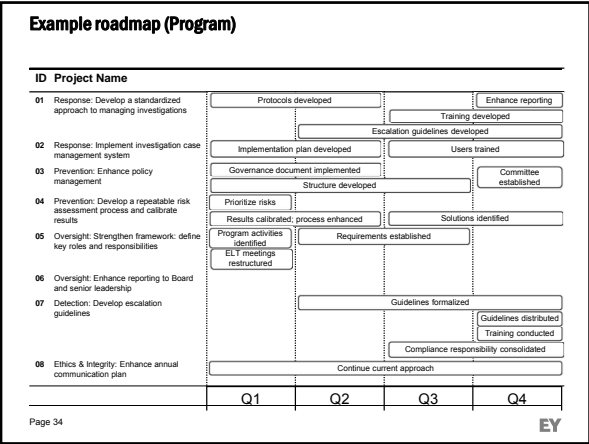
---

---

---

---

---




---



---



---



---



---



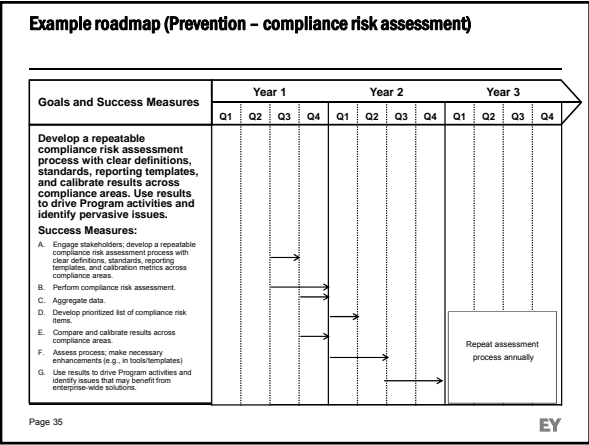
---



---



---




---



---



---



---



---



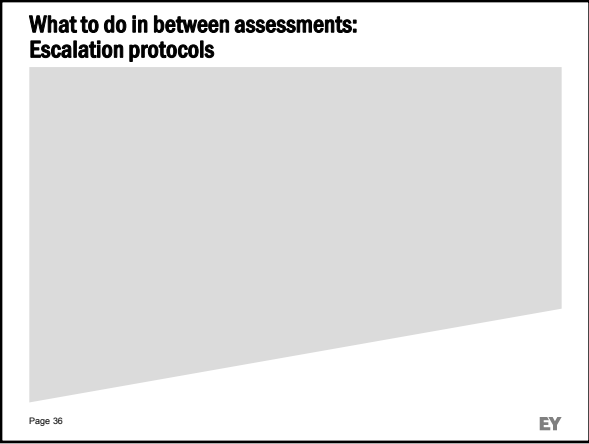
---



---



---




---



---



---



---



---



---



---



---

**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

---

---

---

---

---

---

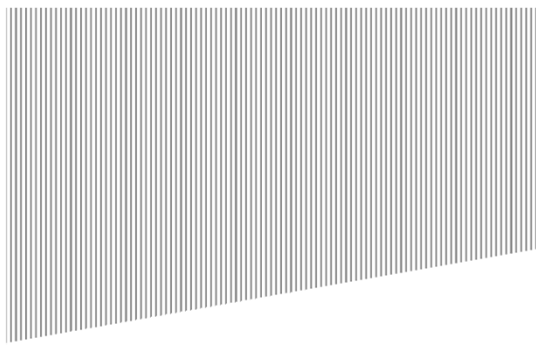
---

---

---

---

**Q&A / Closing**



---

---

---

---

---

---

---

---

---

---

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who learn to believe in our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit [ey.com](http://ey.com).

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2013 Ernst & Young LLP. All Rights Reserved.

WIR no. 1311-1189002

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

---

---

---

---

---

---

---

---

---

---