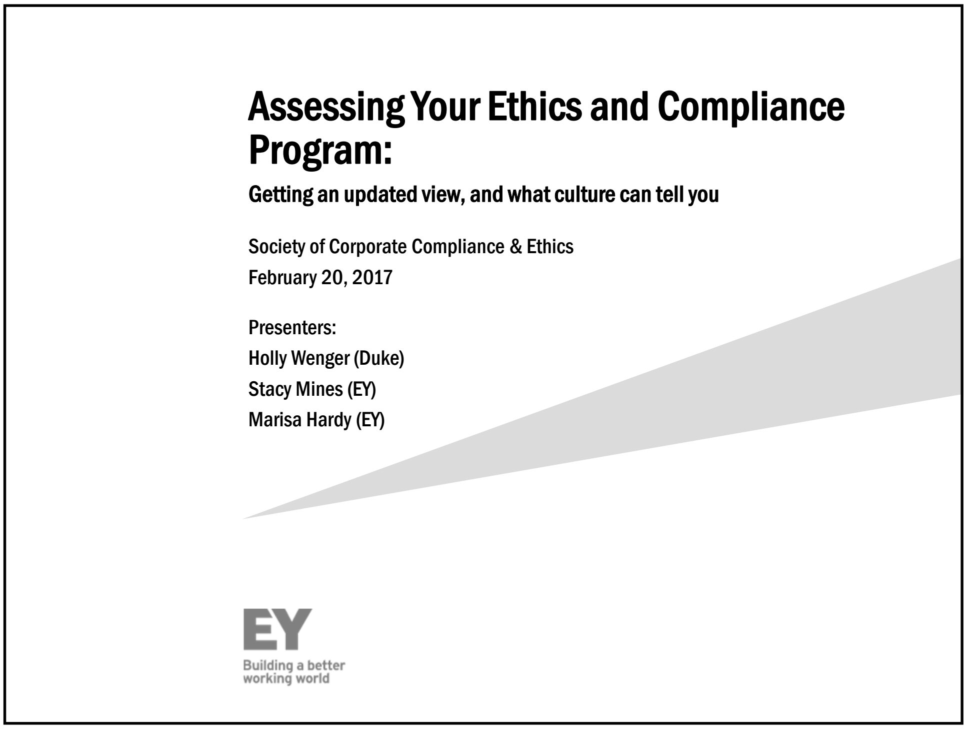
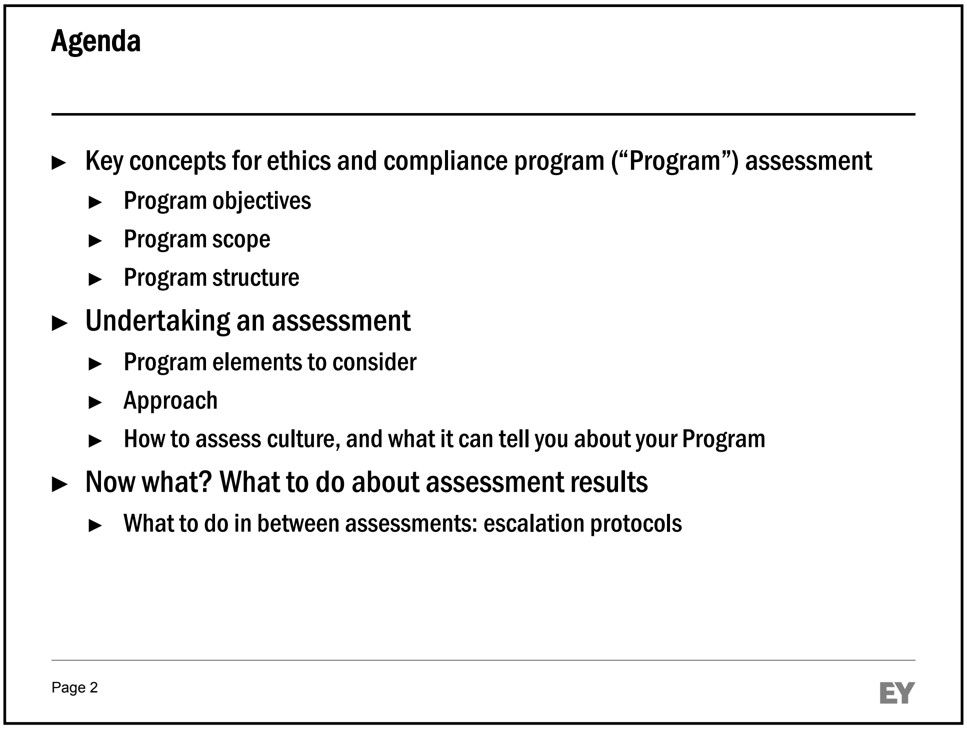


Assessing Your Ethics and Compliance Program:

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. 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

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

Compliance risk universe
*Illustrative utility company example

Legal and regulatory requirements

Competitive practices (FTC, DOJ)
- Antitrust
- Customer, competitor, supplier relations

Corporate governance (SEC)
- Board structure and processes
- Audit committee structure and processes
- Ethics

Employment (EEOC, DOL)
- Executive compensation
- Compensation
- Benefits
- Hiring
- Employee info privacy
- Reductions in force
- Whistleblower protection
- Harassment prevention
- Accommodation (discrimination prevention)
- Workplace violence
- Global migration (immigration)
- Contingent workforce
- Labor
- Leave
- Employment torts

Environmental (EPA)
- NEPA
- Air quality
- Water Quality
- Management systems and reporting
- Hazardous material management
- Laboratory practices
- Permit management

Financial
- SOX
- Tax
- Treasury

Fraud and corruption (DOJ)
- Foreign Corrupt Practices Act (FCPA)
- Insider transactions
- Anti-money laundering
- Financial statement fraud
- Occupational fraud (intellectual property, trade secrets)
- Corruption
- Revenue and expense recognition

Government contracts (DOD, OMB)
- US Government contracts
- Other jurisdictions (state and country)

Information management
- Records retention
- Freedom of Information ACT (FOIA)
- Data and record classification
- Information access
- Information availability and recovery
- Information management monitoring
- Information disposition
- Litigation discovery rules
- Data protection and privacy

Intellectual property (DOC)
- Copyright
- Trademark
- Trade secret
- Patent

International dealings/trade (FTC, DOC)
- Boycott
- Import
- Export

Workplace health/safety (OSHA)
- Security and Emergency Response (ESF)
- Employees
- Contractors

Product quality/liability
- Quality management system

NRC
- Nuclear operations and decommissioning
- New construction

State PUCs
- Base rate and other cost-recovery cases
- Inspection rules
- Regulatory proceedings and investigations
- Reporting requirements
- Retail choice rules
- Privacy rules

FERC
- Market manipulation
- Market behavior rules
  - Affiliate restrictions
  - Standards of conduct
- Wholesale market price reporting
- Compliance effectiveness

Commercial operations
- Participation in ISO and RTO markets
- Billing and payment, settlement
- Creditworthiness
- Capacity and supply obligations

NERC
- Critical infrastructure protection standards
- Reliability standards

CFTC
- Futures/derivatives/options trading
- Trading standards

Political activities
- Lobbying guidelines
- PAC contributions
- Employee's activities
- Time and expense reporting of meetings

Business requirements

Internally focused requirements
- Mission
- Values
- Code of Conduct
- Policies and procedures
- Quality management certifications (ISO, Six Sigma)
- Crisis preparedness

Externally focused requirements
- Corporate social responsibility
- Sustainability
- Public commitments
- Contractual obligations
- Vendor management
- Exchange listings

Voluntary standards
- US Federal Sentencing Guidelines
- Industry codes
- Trade associations

Emerging issues

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.

Illustrative US example

Why is Program scope so important?

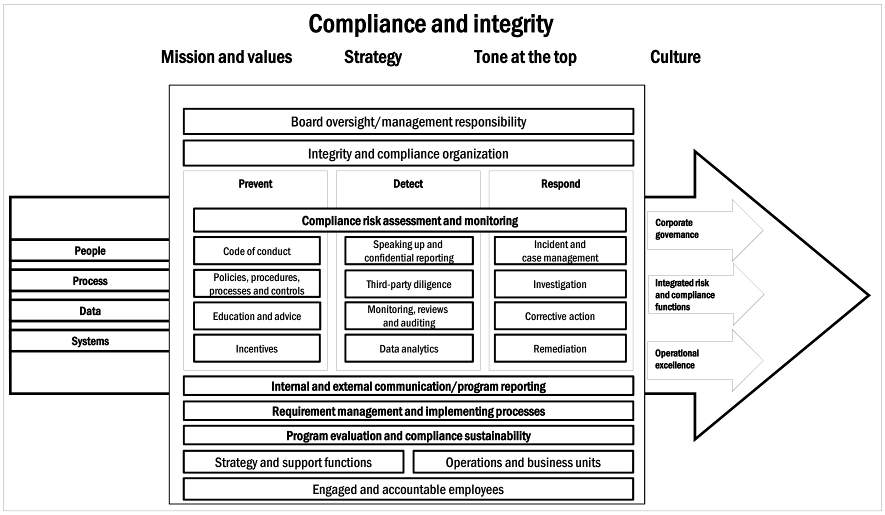
- U.S. Sentencing Guidelines, SEC, DOJ, and FERC set forth key elements of an effective compliance program; view is broad
- Effective, broad-based compliance programs may mitigate criminal penalty
- Role of Ethics and Compliance department is to provide reasonable assurance core compliance management 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

Key concepts for program assessment

Program structure

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



Compliance and integrity

Mission and values

Strategy

Tone at the top

Culture

Board oversight/management responsibility

Integrity and compliance organization

Prevent

Detect

Respond

Compliance risk assessment and monitoring

Code of conduct

Policies, procedures, processes and controls

Education and advice

Incentives

Speaking up and confidential reporting

Third-party diligence

Monitoring, reviews and auditing

Data analytics

Incident and case management

Investigation

Corrective action

Remediation

People

Process

Data

Systems

Corporate governance

Integrated risk and compliance functions

Operational excellence

Internal and external communication/program reporting

Requirement management and implementing processes

Program evaluation and compliance sustainability

Strategy and support functions

Operations and business units

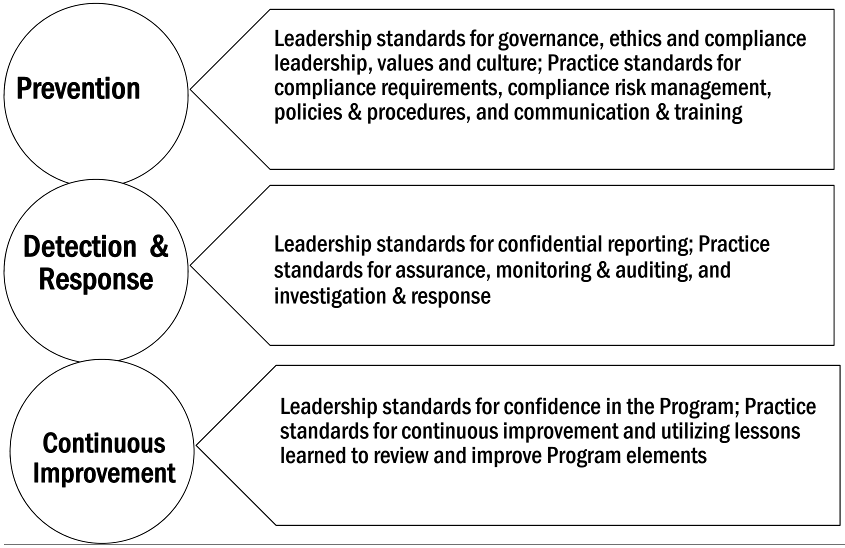
Engaged and accountable employees

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

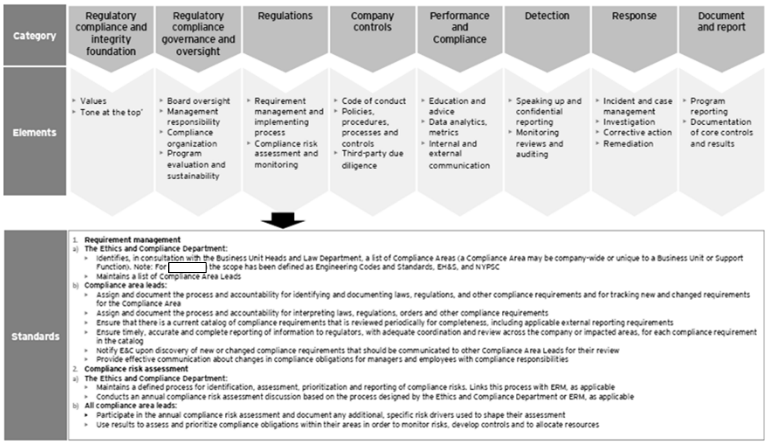
Leadership standards for confidential reporting; Practice standards for assurance, monitoring & auditing, and investigation & response

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.**



Category	Regulatory compliance and integrity foundation	Regulatory compliance governance and oversight	Regulations	Company controls	Performance and Compliance	Detection	Response	Document and report
Elements	Values Tone at the top'	Board oversight Management responsibility Compliance organization Program evaluation and sustainability	Requirement management and implementing process Compliance risk assessment and monitoring	Code of conduct Policies, procedures, processes and controls Third-party due diligence	Education and advice Data analytics, metrics Internal and external communication	Speaking up and confidential reporting Monitoring reviews and auditing	Incident and case management Investigation Corrective action Remediation	Program reporting Documentation of core controls and results

Standards

1. **Requirement management**

a) **The Ethics and Compliance Department:**
- Identifies, in consultation with the Business Unit Heads and Law Department, a list of Compliance Areas (a Compliance Area may be company-wide or unique to a Business Unit or Support Function). Note: For [redacted] the scope has been defined as Engineering Codes and Standards, EH&S, and NYPSC
- Maintains a list of Compliance Area Leads

b) **Compliance area leads:**
- Assign and document the process and accountability for identifying and documenting laws, regulations, and other compliance requirements and for tracking new and changed requirements for the Compliance Area
- Assign and document the process and accountability for interpreting laws, regulations, orders and other compliance requirements
- Ensure that there is a current catalog of compliance requirements that is reviewed periodically for completeness, including applicable external reporting requirements
- Ensure timely, accurate and complete reporting of information to regulators, with adequate coordination and review across the company or impacted areas, for each compliance requirement in the catalog
- Notify E&C upon discovery of new or changed compliance requirements that should be communicated to other Compliance Area Leads for their review
- Provide effective communication about changes in compliance obligations for managers and employees with compliance responsibilities

2. **Compliance risk assessment**

a) **The Ethics and Compliance Department:**
- Maintains a defined process for identification, assessment, prioritization and reporting of compliance risks. Links this process with ERM, as applicable
- Conducts an annual compliance risk assessment discussion based on the process designed by the Ethics and Compliance Department or ERM, as applicable

b) **All compliance area leads:**
- Participate in the annual compliance risk assessment and document any additional, specific risk drivers used to shape their assessment
- Use results to assess and prioritize compliance obligations within their areas in order to monitor risks, develop controls and to allocate resources

Using your framework for assessments

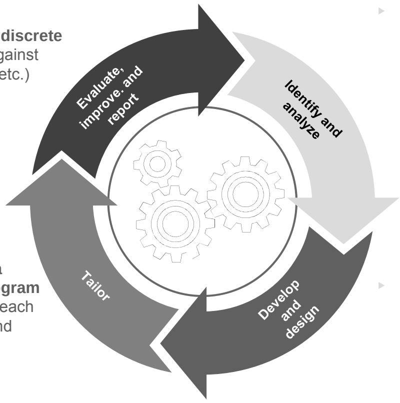
- Assess against your framework
  - Keep in mind your framework should be designed to incorporate external guidance (i.e., Federal Sentencing Guidelines and FERC guidance)
- Ensure assessment tools are tied to your framework
- Benefits
  - Allows for third party and internal assessment of progress against 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.)



- Regularly **re-assess compliance and ethics risks** to ensure appropriate coverage, considering changes in regulatory requirements, audit findings, actual cases (externally and internally)

- **Each compliance risk area builds its own tailored program** to fit its risk profile, meeting each element of the framework and standards

- 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?

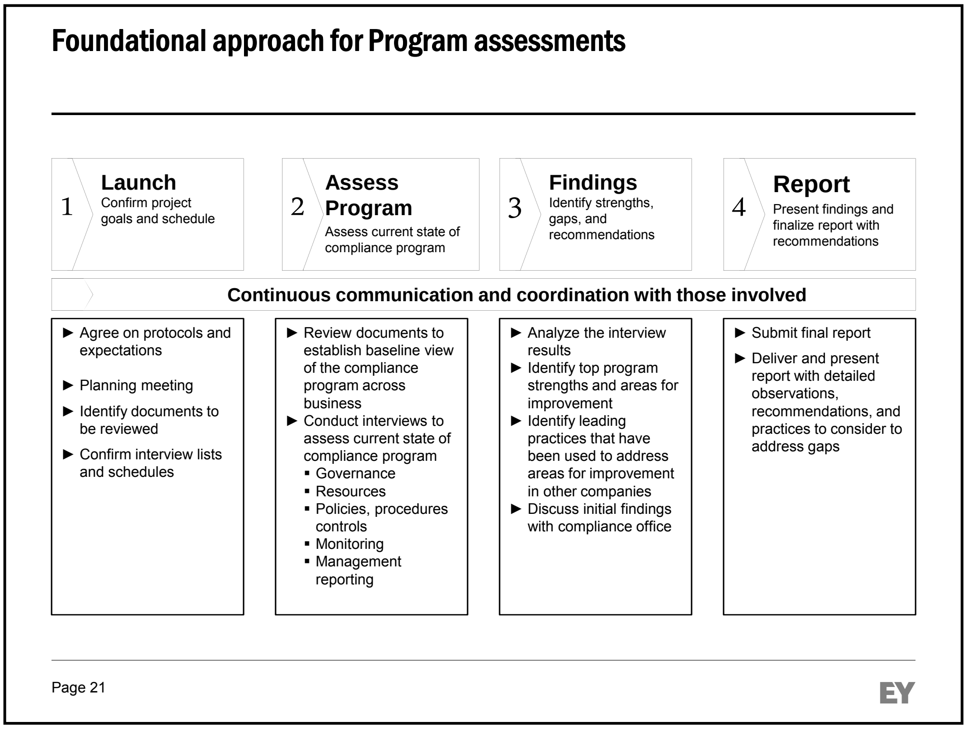
- ► Assess the design and operation performance of the ethics and compliance infrastructure – including the compliance function and processes – relative to legal/regulatory requirements and leading practices
- ► Help management to identify and prioritize opportunities to enhance culture and infrastructure, 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

EY

The following framework elements should be included in an assessment

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

EY



Foundational approach for Program assessments

1 **Launch**
Confirm project goals and schedule

2 **Assess Program**
Assess current state of compliance program

3 **Findings**
Identify strengths, gaps, and recommendations

4 **Report**
Present findings and finalize report with recommendations

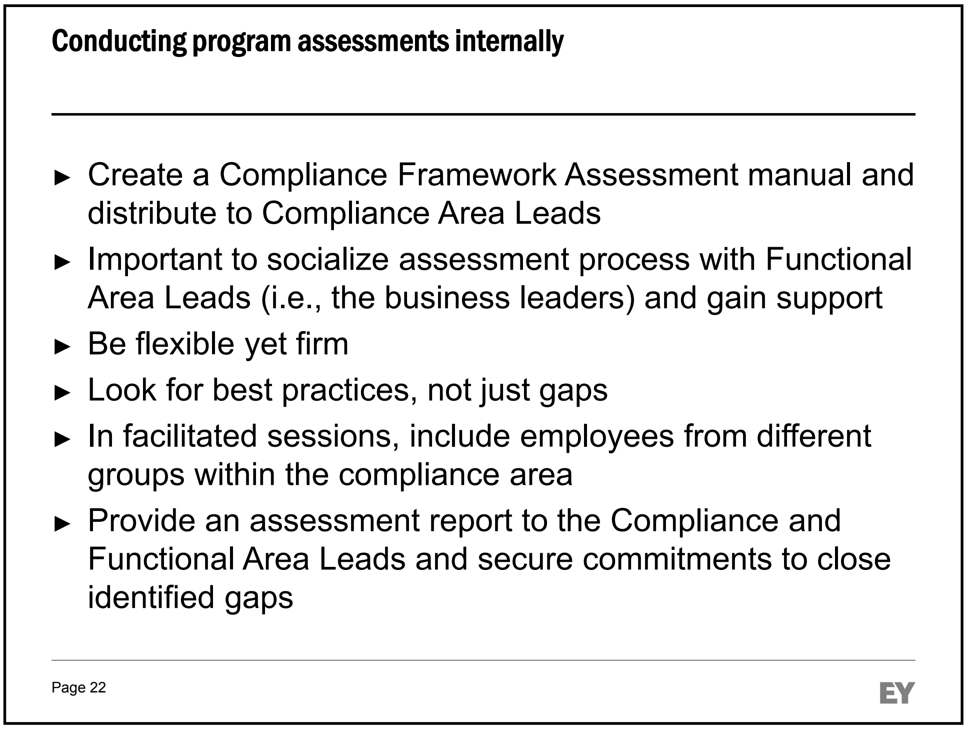
Continuous communication and coordination with those involved

- ► 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



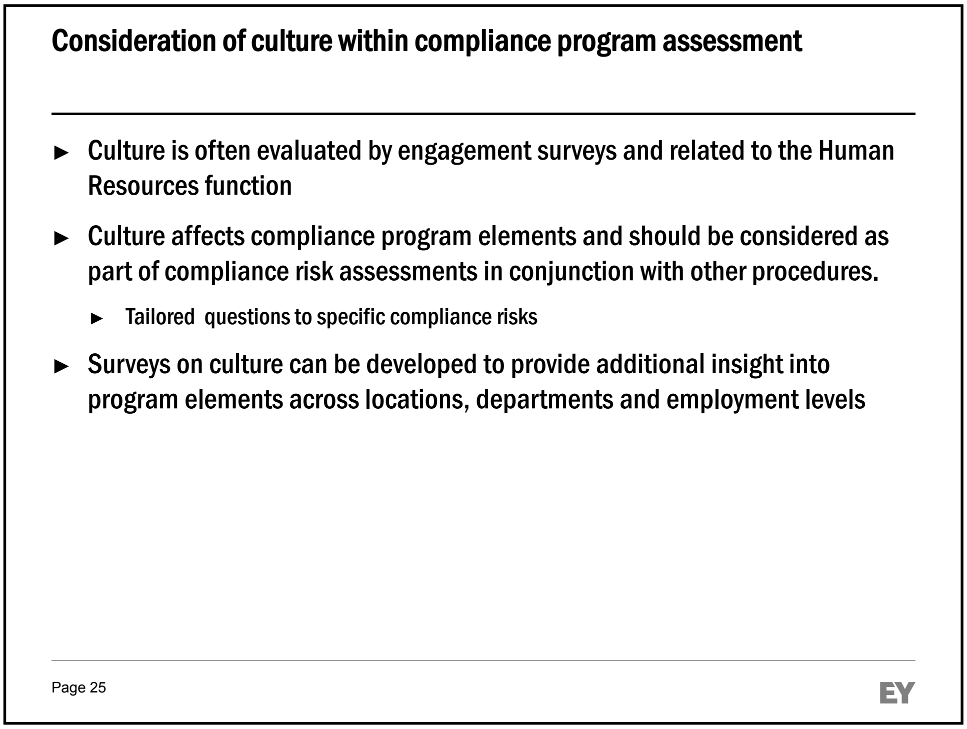
Conducting program assessments internally

- ► 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

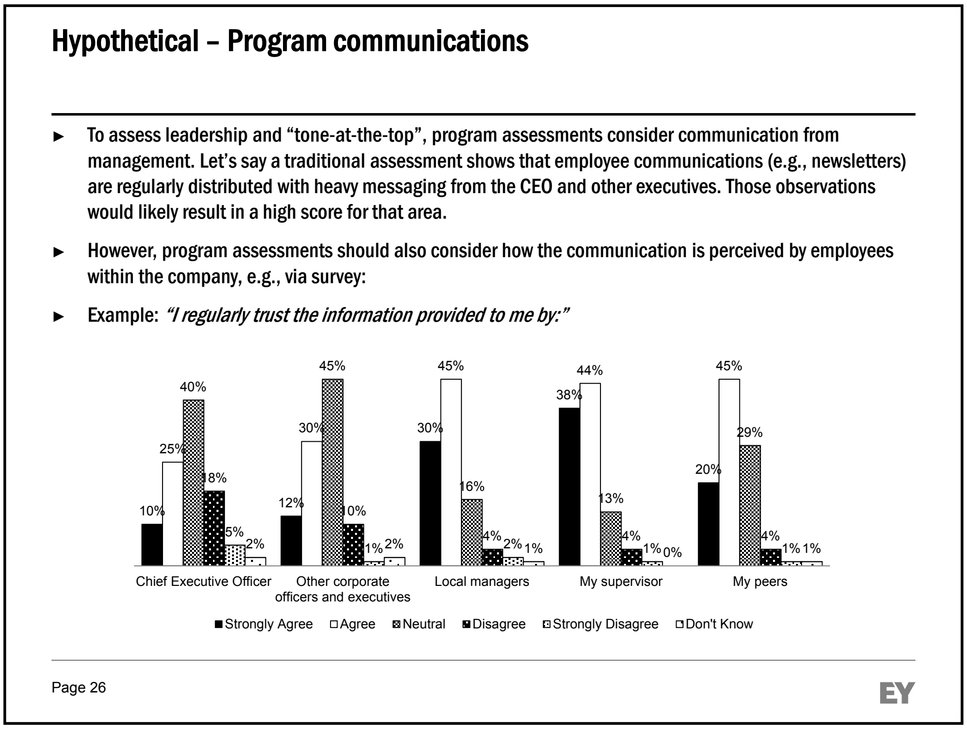
- Incomplete reporting to the board and senior leadership
- Lack of consistent ethics and compliance risk assessment process
- Absence or immaturity of consistent investigation protocols for all of the various parties conducting investigations
- Policy management is deficient (e.g., minimum review cycle, 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

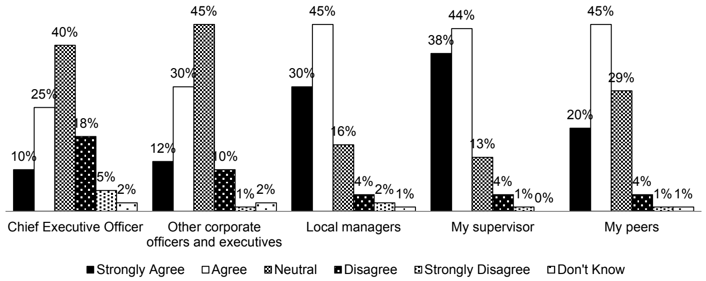


Hypothetical – Program communications

- 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:"*

Hypothetical – Program communications (cont'd.)

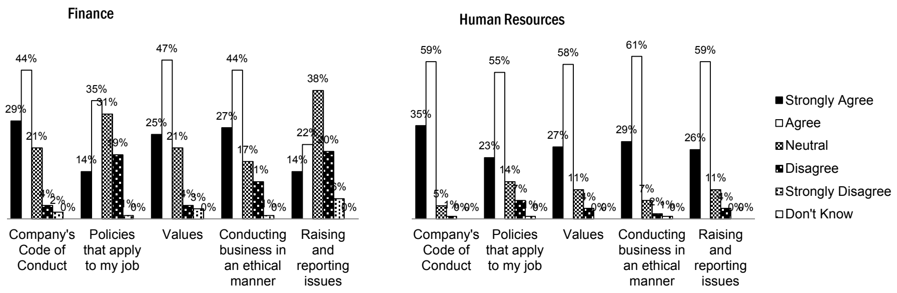
- Example: *"I regularly trust the information provided to me by:"*

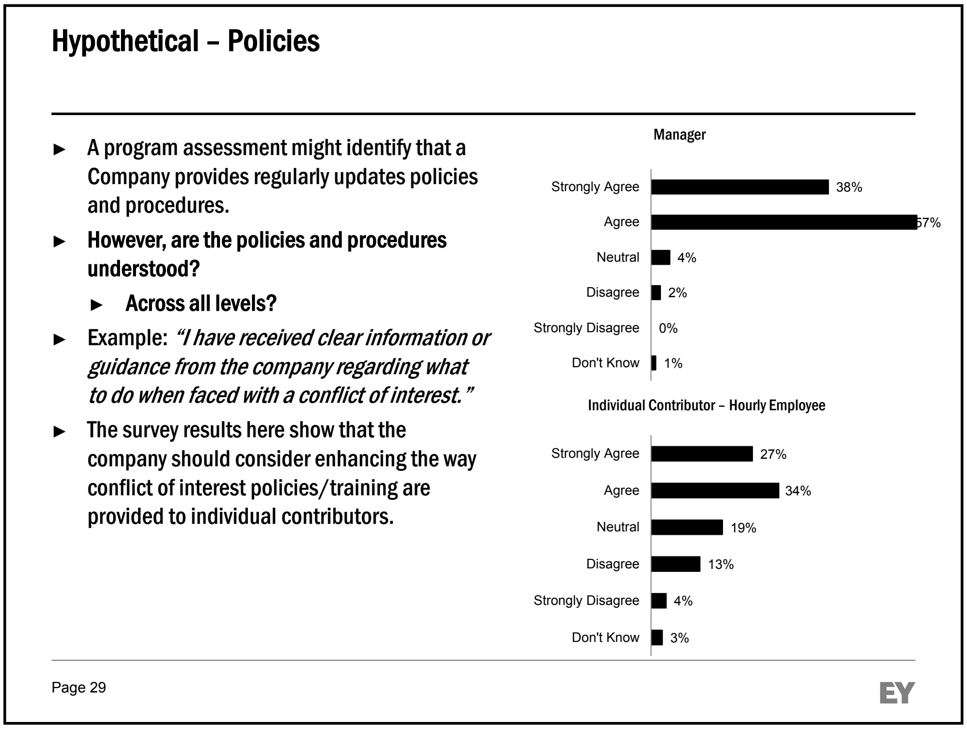


- It looks like messaging would be most effective coming from local managers or supervisors. So, although some messaging should still come from executives, the company should consider distributing other key messaging through local managers or supervisors.
- Given the level of neutral-to-disagree responses 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…"*

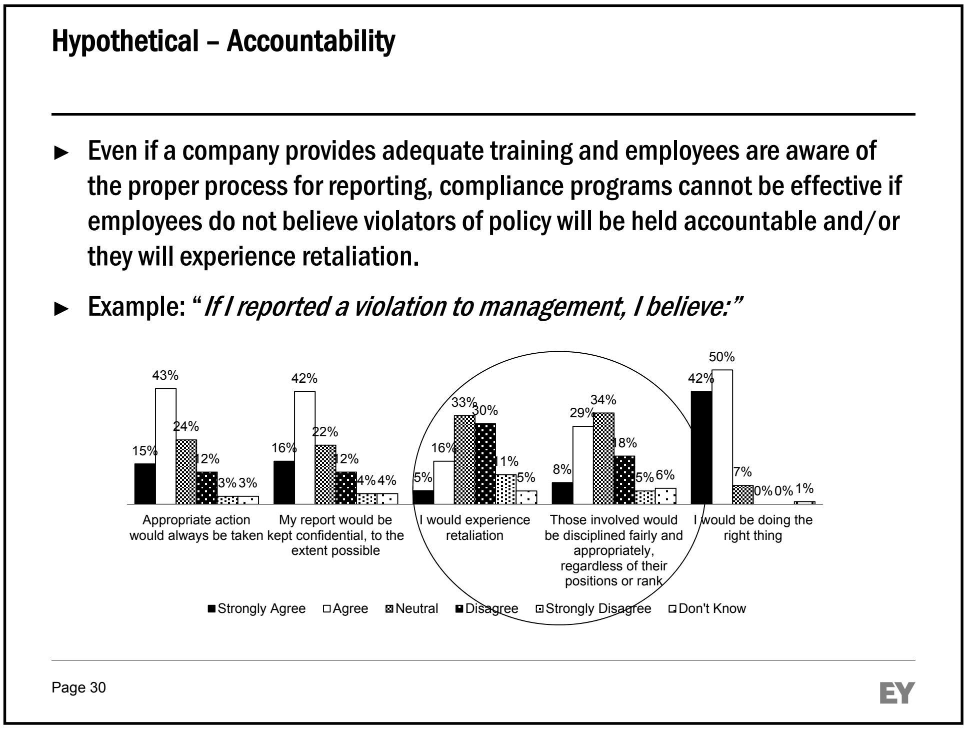




Hypothetical – Policies

- ► 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.

EY



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:"*

EY

Getting senior leadership to understand that compliance and ethics don’t “just happen”

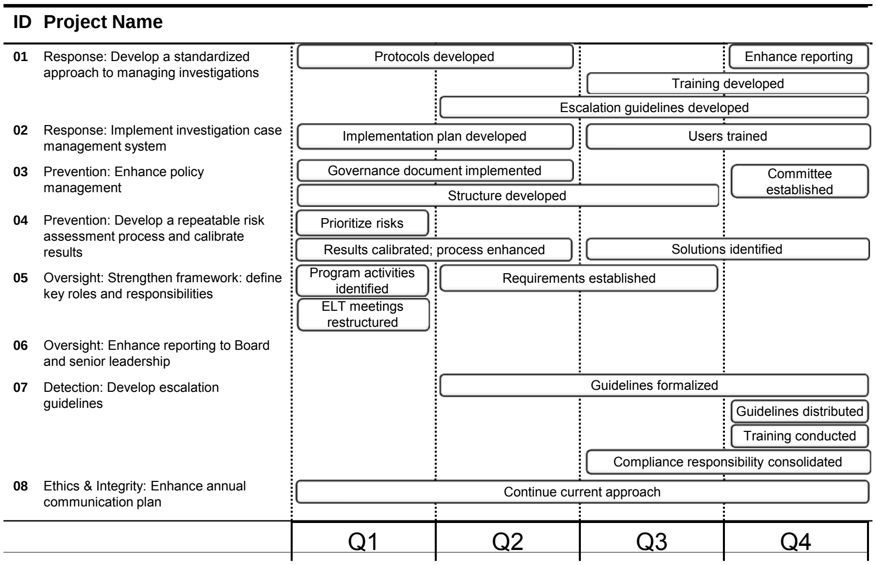
- May find gaps between executive expectations and employee understanding or perceptions
- Creating a culture of compliance is a relentless job and it starts at the top
  - Have a communication plan
  - Make leadership messaging easy

Now what?
What to do with assessment results

Close gaps: develop improvement plans

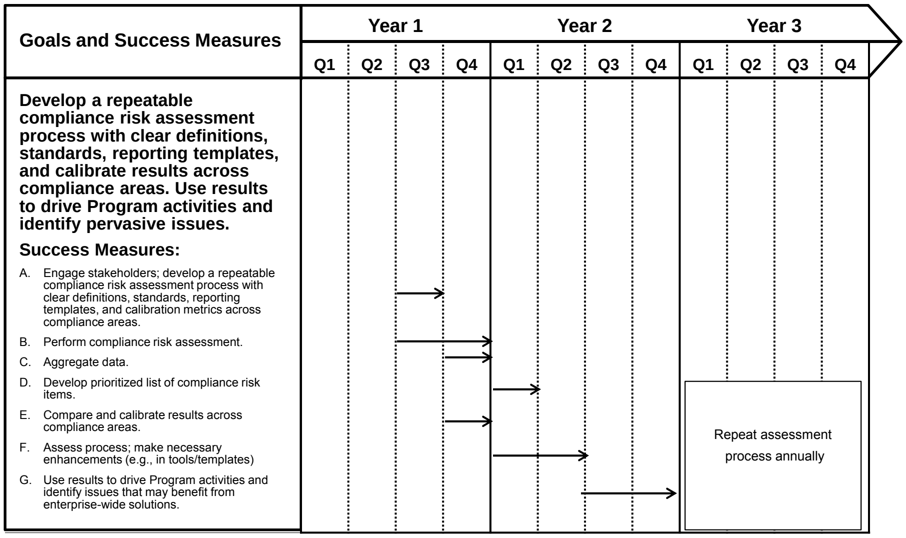
- Create a roadmap for prioritized improvement opportunities
- Work with compliance area leads and/or risk owners to develop improvement plans
- Monitor improvement on a consistent basis
- Share lessons learned

Example roadmap (Program)



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

Example roadmap (Prevention – compliance risk assessment)



Goals and Success Measures

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.

Success Measures:

A. Engage stakeholders; develop a repeatable compliance risk assessment process with clear definitions, standards, reporting templates, and calibration metrics across compliance areas.

B. Perform compliance risk assessment.

C. Aggregate data.

D. Develop prioritized list of compliance risk items.

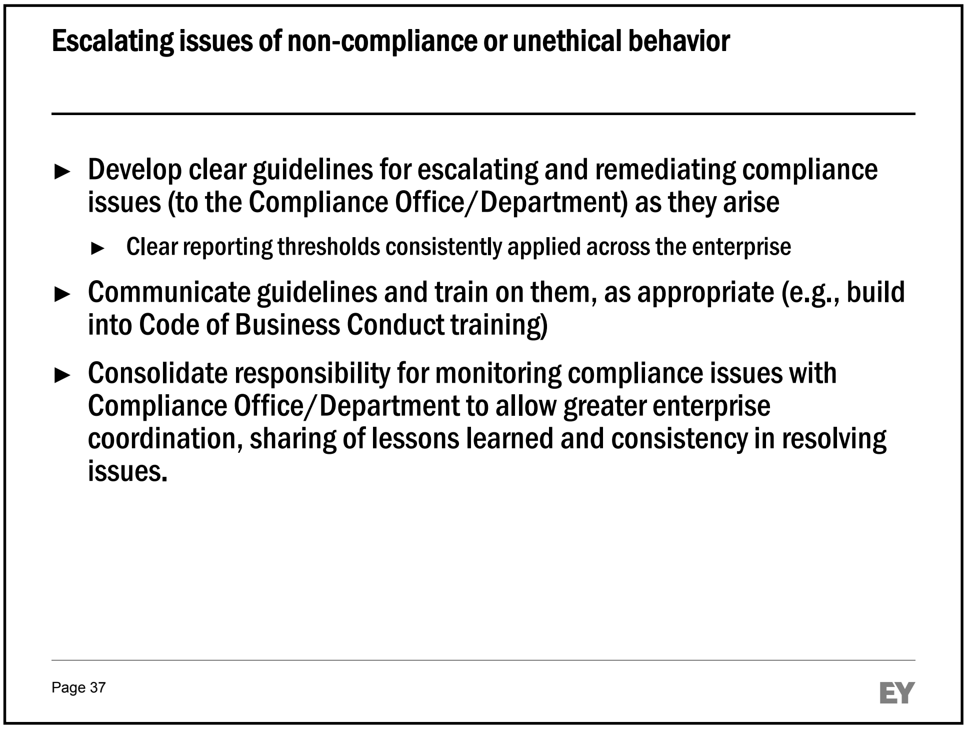
E. Compare and calibrate results across compliance areas.

F. Assess process; make necessary enhancements (e.g., in tools/templates)

G. Use results to drive Program activities and identify issues that may benefit from enterprise-wide solutions.

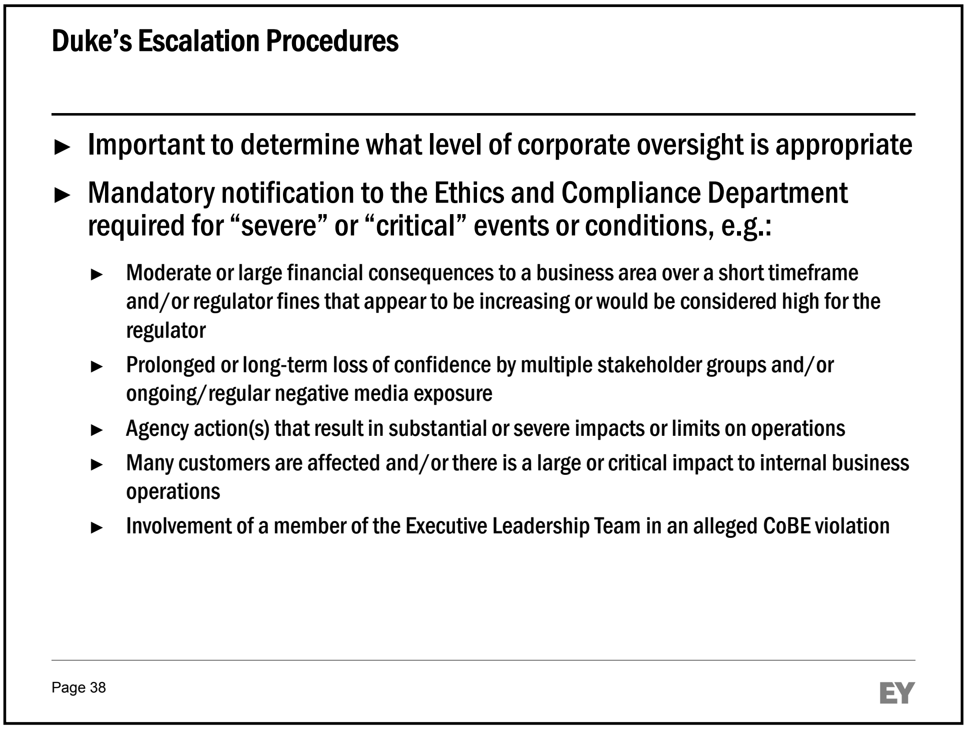
Repeat assessment process annually

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

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 team to deliver on 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.

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

WR no. 1311-1169002

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.