How to Conduct a High-Quality Ethics and Compliance Program Evaluation

Anne R. Harris, Principal
Ethics Works, LLC

ETHICS WORKS

Overview

1. About Me
2. Why Conduct an E&C Program Evaluation?
3. Planning the Evaluation
   - Scope, Responsibility, Objectives
   - Process, Timing, Deliverables
   - Context
   - Applicable Standards
   - Available Resources
4. One Approach: Organize the Evaluation by the Elements of Effective E&C Programs
   - Key information to gather for each element
5. Reporting the Results

WHY CONDUCT AN E&C PROGRAM EVALUATION?

- To determine a baseline: where are we now and where do we want to go?
- To prepare for – or in the aftermath of – a merger or acquisition
- To respond to a mandate from a government agency
- To satisfy the recommended approach in applicable E&C program standards and guidelines
- To implement a regular process under the organization's continuous improvement efforts

PLANNING THE E&C PROGRAM EVALUATION SCOPE, RESPONSIBILITY, OBJECTIVES

- Define the scope
- Who will conduct the evaluation?
  - Internal vs External
  - Under Privilege?

Talk to Counsel

- What are the objectives of our E&C program?
  - *To prevent and detect illegal and unethical conduct*
  - *To respond effectively to incidents*
  - *To promote a culture of ethics and compliance*
  - *To continuously improve the program*
- What are the objectives for the evaluation?
  - Are we compliant with applicable standards?
  - Does our approach make sense for our organization?
  - Is it working? How well? What isn't working?
  - Are we focusing available resources on high risk areas?

May Depend on Purpose & Audience

PLANNING THE E&C PROGRAM EVALUATION PROCESS

- Develop the Process Plan
  1. Document & Data Review
     - Information about the organization + E&C-related documents and data
     - Training records, org charts, Helpline case lists, policies, communications
  2. Interviews with Key Individuals
     - Draft CEO Communications to Participants
     - Plan consistent interview questions; allow flexibility
     - Involve key functions/roles
       - Business Leaders - E&C Program Staff
       - Human Resources - Finance
       - Security - Internal Audit
       - IT Security - Legal

PLANNING THE E&C PROGRAM EVALUATION PROCESS

3. On-site Testing and Review
   - Review investigation files, Helpline case records
   - Follow up document requests
   - Determine if practices reflect policies and procedures
4. **Culture Assessment**: Surveys / Focus Groups
   - Draft CEO / Division Head communications to survey / focus group participants
   - Use standard, planned question sets
   - Organize focus groups to facilitate open communications
   - Preserve confidentiality of focus group discussions
5. Draft Report & Review
   - Request additional information and documents
6. Final Report
   - Summary presentation to Senior Leadership / Board

Timing

Sequence

Deliverables

Audiences

Planning the E&C Program Evaluation
Consider the Context

- Is the E&C program newly-launched or mature?
- Is the organization
  - small or large?
  - domestic or international?
  - geographically condensed or dispersed?
  - public or private?
- Within which industry or industries does the organization operate?
- What resources are available for the program?

Planning the E&C Program Evaluation
Examples of Standards / Guidelines

- U.S. Sentencing Guidelines, Chapter 8, Part B(2): "Effective Compliance and Ethics Program"
- OECD (Organisation for Economic Co-operation and Development) "Good Practice Guidance on Internal Controls, Ethics and Compliance"
- U.S. Department of Justice (DOJ), Criminal Division: "Evaluation of Corporate Compliance Programs" [not guidelines, but offer insight into DOJ views]
- U.S. Public Companies: Sarbanes-Oxley Act of 2002 (SOX)
- New York Stock Exchange(NYSE)-listed companies: NYSE Rule 303A.10 "Code of Business Conduct and Ethics
- National Association of Securities Dealers Automated Quotations (Nasdaq) exchange-listed companies: Nasdaq rule 4350(n) "Code of Conduct"
- U.S. Government Contractors: U.S. Federal Acquisition Regulation (FAR) Subparts 3.10 and 52.203-13, among others

Consider Best Practices, not just minimum compliance

PLANNING THE E&C PROGRAM EVALUATION
EXAMPLES OF STANDARDS / GUIDELINES - CONTD

- U.S. Health Care providers: Centers for Medicare and Medicaid Services, "Compliance Program Policy and Guidance" relative to 42 CFR §§422.503 and 423.504
- United Kingdom: The Bribery Act 2010
- Brazil: Clean Company Act 2014
- Spain: Article 33 bis of the Spanish Criminal Code 2015
- General Data Protection Regulation, effective May 25, 2018 for orgs that collect or process personal data of individuals in the EU
- Several sets of integrity / anti-corruption program guidelines published by international Non-Governmental Organizations (NGOs) including the United Nations Global Compact, the World Bank, and the World Economic Forum
- Many regulations applicable depending on industry: Automotive, Health Care, Oil and Gas, Manufacturing, Pharmaceuticals, Transportation, and so on

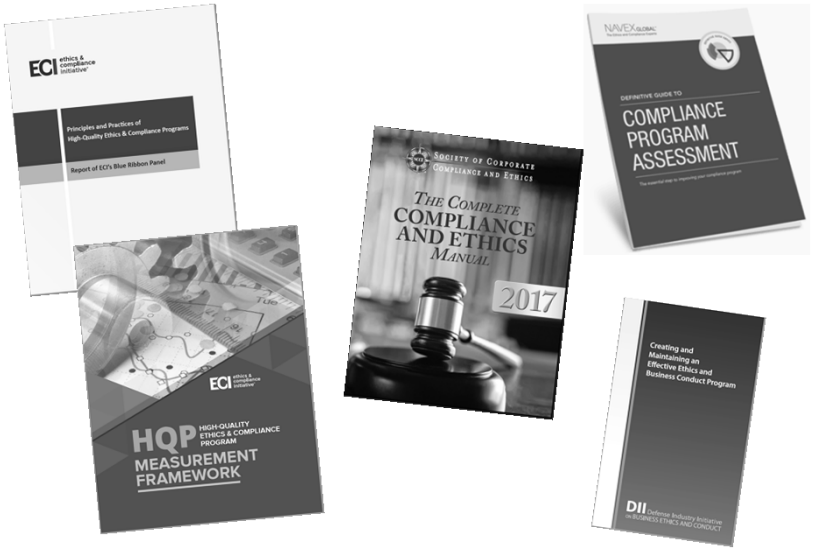
SOME PUBLICLY-AVAILABLE RESOURCES TO HELP

- Convercent, "A Practical Guide to Compliance Program Review and FSGO Benchmarking," 2015.
  - https://www.convercent.com/resource/convercent-practical-guide-to-program-review.pdf
- Dubinsky, Joan Elise and Alan Richter. "Global Ethics and Integrity Benchmarks" 2015. available at http://www.qedconsulting.com/products/section2j.php
- Meacham, James, and the SAI Global Advisory Services Team, "Compliance and Ethics Program Best Practices: Assessing Your Program and Moving It Up the Maturity Curve." 2014, SAI Global LTD.
  - http://www.ethic-intelligence.com/wp-content/uploads/2014-SAI-Global-Program-Assessment-Maturity-Curve.pdf
- OECD "Good Practice Guidelines on Internal Controls, Ethics, and Compliance," 2010.
  - http://www.oecd.org/daf/anti-bribery/44884389.pdf

Some Publicly-Available Resources to Help – contd

- U.K. Ministry of Justice, "The Bribery Act 2010 Guidance," 2011
  - https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf
- U.S. Department of Justice, Criminal Division, Fraud Section: "Evaluation of Corporate Compliance Programs," 2017.
  - https://www.justice.gov/criminal-fraud/page/file/937501/download
- U.S. Department of Justice, Criminal Division and the U.S. Securities and Exchange Commission, Enforcement Division: "A Resource Guide to the U.S. Foreign Corrupt Practices Act," 2012.
  - https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf
- U.S. Sentencing Commission Federal Sentencing Guidelines for Organizations
  - http://www.ussc.gov/guidelines/2016-guidelines-manual/2016-chapter-8

Additional High-Quality Resources



One Approach: Organize the Evaluation by the Elements of Effective E&C Programs

1. Organization, Leadership and Governance
2. Risk Assessment
3. Standards of Conduct, Policies and Procedures
4. Communications and Training
5. Integration with HR/Performance Management Processes
6. Reporting, Investigations and Corrective Action
7. Monitoring, Auditing, and Program Evaluation
8. Culture of Ethics and Compliance
9. Third-Party Risk Management

1. Organization, Leadership & Governance

- *The organization's governing authority / Board of Directors should exercise knowledgeable, reasonable oversight over the E&C program.*
- *The CECO should report at a high level of the organization, with direct access and periodic reporting responsibility to the Board, and have sufficient resources to operate the E&C program effectively. The CECO should have authority and independence.*
- *Senior leadership should demonstrate commitment to, and foster throughout the organization, a culture of ethical business conduct and a commitment to comply with the law.*

- Board of Directors
  - What is their understanding and engagement re E&C program?
  - Does the organization provide the Board periodic education/training relative to their responsibility for E&C program oversight?
  - What is the frequency / content / quality of information reported to Board or appropriate subcommittee?
  - Is there a procedure for concerns to be raised directly to the Board or subcommittee?

1. ORGANIZATION, LEADERSHIP & GOVERNANCE - CONTD

- CEO/Senior Leadership
  - How do they demonstrate commitment to E&C?
  - In what ways does the CEO support the CECO's efforts to implement an effective program?
  - Is there a senior leadership oversight body, e.g., E&C Steering Committee? What is its function?
- CECO
  - Experience and qualification for the role?
  - Reporting relationship?
  - Direct line of communication to Board/Audit Committee?
  - Sufficient resources? Authority?
- E&C Program organization
  - Sufficient staff?
  - Ethics Liaisons or other creative staffing approaches?
  - How are E&C staff in remote locations supported?

How are E&C staff Selected, Trained, & Evaluated?

2. RISK ASSESSMENT

- *Periodic risk assessment should be conducted to determine the likelihood and impact of unethical or illegal conduct.*
- *Based on its findings, the E&C program should be modified, or its resources be refocused, to mitigate the most significant risks.*

- Does the organization conduct E&C risk assessments?
- Does the risk assessment effectively flag the highest risk areas based on the nature of the business?
- How does the organization address identified high risk areas?
- Are the results of the risk assessment used in planning processes for E&C program objectives, budgets, etc.?

3. Standards of Conduct, Policies & Procedures

- *Written Code of Ethics and Conduct and Policies and Procedures*
- *Should clearly communicate behavioral expectations, including consequences for violations*
- *Should be understandable, comprehensive, useful, accessible*

Code of Conduct

- Does the organization have stated Values? Does the Code support and reinforce the Values?
- Does the Code address all the relevant topics and policy areas?
- Is it engaging and easy for anyone to understand?
- Is it communicated to employees and others effectively?
  - Is it available in all applicable languages?
  - How is it distributed to employees and others?
- Is there a process for periodic reminders or re-commitment to compliance?

Reflective of Culture

3. Standards of Conduct, Policies & Procedures - continued

Policies and Procedures

- What is the process for developing and approving policies?
- What is the process for updating or maintaining policies?
  - As the law or regulations change
  - As the organization changes
- Are policies and procedures clear and understandable?
- How are they communicated to various audiences?
- How are people trained on policies?
- Who is responsible for enforcing compliance with policies?

Interactive Code
Links to Policies

COMMON E&C-RELATED POLICIES AND PROCEDURES

- Anti-Bribery, Anti-Corruption
- Background Checks
- Business Continuity
- Community Involvement/Social Responsibility
- Communications – Internal and External
- Conflicts of Interest
- Corporate Opportunities
- Anti-Discrimination and Harassment
- Drug-Free Workplace
- Environmental Compliance
- Equal Employment Opportunity/Diversity
- Export-Import Compliance
- Fair Competition and Anti-Trust
- Anti-Fraud
- Gifts and Hospitality
- Health and Safety
- Insider Trading
- IT Security
- Performance Management
- Physical Security
- Political Contributions & Activities
- Privacy of Personal Data
- Product Safety
- Proprietary and Confidential Information
- Protection of Company Assets
- Purchasing/Procurement
- Quality
- Records Retention
- No Retaliation / Whistleblower Protection
- Smoke-Free Workplace
- Social Media
- Third Party/Supplier Compliance
- Travel and Entertainment
- Use of Electronic Assets/Internet Use
- Workplace Violence Prevention

4. COMMUNICATIONS AND TRAINING

❖ *Employees and other stakeholders should receive periodic and effective communications and training, about the Code of Conduct and ethics and compliance policies and procedures, that is appropriate to their roles*

Awareness

- Is there a multi-year Communications and Training Plan?
- Is it informed by the Risk Assessment? Does it focus on high risk areas?

How to Seek Help

Communications

- Is there an ethics and compliance web portal?
- What periodic communications are issued to increase awareness?
- Are there E&C-related communications from the CEO and other senior leaders?
- Does the organization communicate real E&C cases and outcomes, disguised to protect identities?

4. COMMUNICATIONS AND TRAINING - CONTINUED

Training

- Quality, Method, Frequency, & Audience of the Code of Conduct Training?
- Targeted compliance training for specific audiences/topics?
- How is the effectiveness of training evaluated?
- How is training completion tracked?

Consequences of Failure to Complete

- How is training conducted for remote employees or others who may be difficult to reach?
- What does the organization do about ethics and compliance training for
  - New Hire Orientation
  - New Supervisors
  - Middle and Upper Management
  - Board of Directors
  - Suppliers and other Third Parties
- Training for supervisors and managers on how to respond when employees raise E&C questions and concerns?

5. INTEGRATION WITH HR/PERFORMANCE MANAGEMENT PROCESSES

- *Reasonable steps should be taken to prevent people with a history of ethical misconduct or legal violations from being placed in positions of authority.*
- *The organization should promote and incentivize ethical and compliant conduct.*
- *Appropriate disciplinary / corrective action should be taken in the event of illegal or unethical conduct.*

WALKING THE WALK

- How does the organization promote ethical conduct?
- Are E&C incorporated in performance management / incentive compensation processes?
- What is the due diligence process to screen candidates for hiring into positions of authority (substantial discretion in acting on behalf of the organization)?
- Does the CECO verify that corrective/disciplinary action is taking place when warranted?
- Is disciplinary action applied consistently, regardless of the organizational level of the violator?
- What processes are in place to prevent retaliation?

6. Reporting, Investigations and Corrective Action

- *The organization should make available one or more communications channels, such as a Helpline, through which employees and others can raise E&C concerns confidentially and/or anonymously and without fear of retaliation*
- *Concerns should be investigated thoroughly, fairly and promptly.*
- *If unethical or illegal conduct is found to have occurred, the organization should promptly take appropriate corrective and/or remedial action – including action to prevent similar misconduct in the future.*

Helpline / Confidential Communications Channels

- Helpline?
  - Internal or external? 24/7? Languages? Toll-free + web?
  - Does it offer both confidential and anonymous reporting options?
  - How is it promoted/encouraged?
  - Do communications explain exactly what happens when someone calls the Helpline so people know what to expect?
  - Is it used?
- Communicated to suppliers, customers, agents, sales representatives, others?
- Other communications channels available?

6. Reporting, Investigations and Corrective Action - continued

Investigations & Case Management

Trust

- Standard, written investigations protocol?
- Who conducts investigations? How are they trained?
- Are investigations prompt, thorough, and fair?
- Does the organization have written case management standards (e.g., guidelines for communicating with the reporting party, maintaining confidentiality, case closure timing targets)?
- Root cause analysis to determine why misconduct occurred?
- How does the organization analyze reports and case data for trends and red flags? How does it use reports and case data for reporting to senior leadership and the Board?

Lack of Fear

Corrective & Remedial Action

- What procedures exist to ensure that appropriate corrective action is taken, including action to prevent similar misconduct from occurring in future?
- Is disciplinary action applied consistently, regardless of the level of the offender?
- What policies and processes are in place to prevent retaliation?
- Does the organization take reasonable steps to prevent similar misconduct from recurring?

7. Monitoring, Auditing and Program Evaluation

- *The organization should implement internal controls, such as monitoring processes, to verify that its business is being conducted in compliance with the Code and its standards, as well as auditing processes to detect unethical and illegal conduct.*
- *Resources allocated to monitoring and auditing functions should be determined based on E&C risk assessment findings.*
- *Periodic audits and assessments should contribute to the ongoing evaluation of the effectiveness of the E&C program and improvements should be implemented accordingly.*

- Is the Internal Audit function independent?
- What processes are used to detect unethical and illegal conduct?
- Does the organization periodically review business practices, Code of Conduct, policies, procedures and internal controls?
- Following unethical or illegal conduct events, are existing internal controls or processes reviewed and improved?
- Does IA periodically test the Helpline?
- Does the organization periodically evaluate the effectiveness of the E&C program?
- What metrics / measurements are used to evaluate the program's effectiveness?

8. Culture of Ethics and Compliance

- *The organization should promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.*

- What is the Tone from the Top?
- Do leaders "walk the walk" in addition to "talking the talk"?
- Are organizational leaders held accountable for promoting an ethical and compliance culture?
- How does the organization make sure that middle management and supervisors remain consistent with the desired ethical culture and the Tone from the Top?
- Do people contact the CECO seeking guidance?
- Do employees express confidence that they can raise E&C concerns without fear of retaliation?
- Do employees raise E&C concerns and questions?
- Do employees perceive that the organization conducts business in ways consistent with its Values?
- Does the organization do E&C culture assessments? How? What are the results?
- How does the company "operationalize" E&C?
- Are the consequences for ethical failure clearly understood?
- Do employees perceive that ***procedural justice*** exists in the organization?

Fairness in Workplace Processes & Outcomes

9. THIRD-PARTY RISK MANAGEMENT

- *The organization should take steps to protect itself from ethics and compliance risks that may arise from its relationships with third parties, including suppliers, sales representatives, and agents.*

- Does the organization:
  - conduct effective risk-based due diligence when entering into business relationships with third parties?
  - hold third parties responsible for compliance with its Code of Ethics and Conduct? How?
  - have a Supplier Code of Conduct?
  - offer assistance to suppliers / third parties to help them establish and manage their own E&C programs?
  - communicate about its Helpline or other confidential/anonymous communication channels to third parties to encourage them to report concerns?
- How does the organization monitor ethics and compliance risks in these ongoing relationships?

REPORTING THE RESULTS

- Written report most common
  - High-Level Presentation Only increasingly requested – with appendices
  - Executive summary presentation for senior leadership and/or the Board of Directors

Format Depends on Audience + Purpose

- Include:
  - list of interviewees, but not focus group participants
  - recommendations for improvement, action plans including timing based on priority, plans to track progress
  - recommended plan for future evaluation processes

- Conduct a separate debrief including "lessons learned" review with E&C staff

Reporting the Results to Senior Leadership and the Board of Directors

Be Prepared to Address

- Are we doing the things we need to do to meet compliance requirements? Can we "check the boxes?"
- Beyond that, are we effectively fostering a culture of integrity?
- Are we, in fact, focusing our resources on our highest-risk areas?
- What's working? What's not working? How do we know?
- How do we compare to our benchmark/comparator organizations?
- What was the most surprising result of the assessment?
- What are the top 3-5 priority recommendations for improvement and why? What's the risk of inaction?

Costs

A High-Quality E&C Program Evaluation is…

is one that brings useful value to the organization by helping leadership effectively mitigate risks and enhance ethical culture, thereby supporting its success.

One size does not fit all. Listen well and consider the organization's

- **Risks**
- **Resources**
- **History**
- **Unique characteristics**
- **People**
- **Industry**
- **Program Maturity**

Thank You!