Evolution of a Compliance & Ethics Program

Keri Grafing
Sr. Director, Global Compliance & Ethics, Best Buy

Agenda

Structuring for success
Maturing the program
Developing KRIIs and metrics
Building relationships with influencers
Structuring for Success

How do we create a stronger platform for our compliance functions to better mitigate the risks and drive an ethical culture?
Where we were …

Compliance as an extension of Legal

Reporting to General Counsel

Siloed metrics

Disjointed compliance capabilities

Competing risk voices

Perceived as barrier to business

“We need a function that is truly focused on the compliance function, not compliance just as an extension of the legal job.”

-Todd Hartman
Chief Risk and Compliance Officer, Best Buy
Where we are now.

- Compliance as an extension of legal
- Reporting to General Counsel
- Disjointed compliance capabilities
- Competing risk voices
- Siloed metrics
- Perceived as barrier to the business

Separate and more inclusive compliance function, integrated with Fraud, Risk and Info Security

- Reporting to the Audit Committee with dotted line to Chief Financial Officer
- Enterprise-wide comprehensive metrics
- Centralized capability with one budget
- Holistic enterprise risk management
- Perceived as a partner to the business

New Structure for Success

Enterprise Risk & Compliance Organization

- Audit Committee
- Chief Financial Officer
- Chief Risk & Compliance Officer

Global Compliance & Ethics
- Whistleblower Hotline
- Ethics Office Policies
- Compliance Risk Management
- Product Safety & Compliance
- FCPA Program

Enterprise Privacy
- CCPA, HIPAA, Customer and Employee Data Privacy Programs
- Privacy & Info Sec Policies
- Information Records Management

Global Threat Detection & Response
- Fraud Prevention & Detection
- Digital Forensics & Investigation
- Data Loss Prevention
- Business Continuity and Disaster Recovery
- Crisis Response
- Campus Security

Enterprise Information Protection
- Information Security
- Threat & Vulnerability Management Program
- Network Security
- Security Architecture
- Information Security Assessment and Reporting
- Third Party Due Diligence and Risk Assessments
- Insurance Risk Management

Enterprise Risk Management
- Third Party Due Diligence and Risk Assessments
- Project Management
- Data Analytics

Business Operations
- Training and Communication
- Change Management & Process Improvement
Restructure Advantages

- Compliance teams can act as objective assessor with a lens separate from Legal
- Faster issue escalation to the Board and higher enterprise profile
- More comprehensive data provides holistic view of risks
- More efficient and more informed allocation of resources

Enterprise Risk & Compliance Organization Mission

To help drive ethical culture into each leader’s business and to help identify, assess, and mitigate material risk and compliance issues.
Maturing the Compliance & Ethics Program

Questions we asked ourselves

1. Do we have a culture that values the importance of ethical behavior?
2. Do we have a culture where concerns can be reported without fear of retaliation?
3. Do we have the ability to identify issues that may arise?
4. Do we have the right reporting channels in place?
A culture that values ethical behavior has...

- A strong tone at the top
- A robust ethics training & awareness program
- Integration into business strategy and inclusion of ethics in performance expectations
- Strong prevention, detection & response programs

Tone at the Top

- Do executive leaders have a strong record for **setting ethical tone** and speaking to the importance of acting ethically?

- Are leaders willing to engage their teams in **ethics-based discussions**?

- Do we **equip leaders with the right tools and data** to enable and encourage ethics-based conversations?

- Are ethical behaviors specifically included in our **written expectations for leaders**?
Training & Awareness

• Do we have an engaging and relevant annual ethics training required for all employees?
• Do our employees favorably rate our compliance and ethics trainings?
• Do employees know where to locate the Code of Ethics and are they familiar with it?
• Do employees know how to raise ethical concerns?
• Are ethical expectations communicated when new employees and officers on onboarded?

Integrating into Business Strategy and into Performance Appraisals

• Do we have frequent and substantive contact with executive leaders?
• Do we have a voice in the business teams’ operations and strategic initiatives?
• Are ethical behaviors included in the performance appraisal process?
**Prevention, Detection & Response**

- Do we **promptly respond** to compliance and ethics concerns and escalate high-risk ones?
- Are employees who report concerns **satisfied** with the process and outcome?
- Are employees aware of and believe the company supports its **Anti-Retaliation Policy**?
- Do business teams that own a compliance capability have a strong compliance program with frequent **auditing of operations**?
- Do we have **compliance champions** throughout the organization embedded in various business units?

**Tone at the Top**
- CEO and CFO video messages in annual training
- Targeted anti-retaliation training for leadership
- Ethical toolkits for leaders

**Training & Awareness**
- Rebrand whistleblower hotline
- Code of Ethics overhaul
- Audience-specific live ethics trainings and road show
- Annual eLearning training focused on topical issues

**Prevention, Detection & Response**
- Clarified escalation and investigation protocols for high-risk investigations
- Resources for reporters and subjects of an investigation
- Coaching and Corrective Action Guidelines implemented
How did we get here?

Where we're at → Identify the gaps → Incorporate best practices → Where we want to be

Let's talk about what's possible:

Developing KRI & Metrics
Developing KRI and Metrics

Key Risk Indicator (KRI): Metric used to provide a signal of changing risk exposure in various areas of the organization. Metric helps inform whether the frequency/severity of the risk is changing.

**Lead Indicator**
- **Predictive** in nature – Can provide advance warning to management about possible change in level of risk exposure
- **Example**: Number of people trained

**Lag Indicator**
- **Reactive** in nature - Provides information about the impact of the risk after it has happened
- **Example**: Number of incidents reported

Identifying KRI

1. **Identify and define the specific risk**
   - What type of event may result in a loss?
   - Example: Information Security Risk: Loss of confidentiality, integrity, or availability of systems or data originating from a system security incident or cyber-attack.

2. **Define sources/causes of risk**
   - What is the event trigger?
   - Example: Loss of confidentiality of data due to the impact of a third party.

3. **Define KRI & type (lead/lag)**
   - What metric can inform if there is an increase or decrease in risk?
   - Example: % of vendors assessed with high (residual) risk as a part of the Third Party Risk Assessment (TPRA)

4. **Define KRI source, target, & frequency**
   - What is the source, target, and the frequency of reporting?
   - Example:
     - Source: TPRA Team
     - Target: 10%
     - Frequency: quarterly
**Compliance & Ethics Team KRI Example**

1. **Identify and define specific risk**
   - Unethical employee behavior that creates a risk/event.

2. **Define sources/causes of the risk**
   - Lack/weakness of training
   - Poor leadership/tone at the top
   - Human behavior
   - Financial incentive/performance

3. **Define KRI (and target, source, frequency)**

<table>
<thead>
<tr>
<th>Human Behavior KRIs</th>
<th>KRI Definition</th>
<th>Type</th>
<th>Source</th>
<th>Actual</th>
<th>Target</th>
<th>Frequency</th>
<th>Status**</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethical culture survey results</td>
<td>Lead</td>
<td>Ethisphere</td>
<td>___</td>
<td>At or above Ethisphere benchmark</td>
<td>Annual</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Hotline Reports</td>
<td>Lag</td>
<td>Metrics dashboard</td>
<td>___</td>
<td>Equal to or less than prior year’s YTD</td>
<td>Quarterly</td>
<td>--</td>
<td></td>
</tr>
</tbody>
</table>

* Percentage of agree/strongly agree
** Red/Yellow/Green

**KRI and Metrics**

<table>
<thead>
<tr>
<th>Cause</th>
<th>KRI</th>
<th>Type</th>
<th>Source</th>
<th>Actual</th>
<th>Target</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack/weakness of training</td>
<td>Training completion rates</td>
<td>Lead</td>
<td>ERC T&amp;C team</td>
<td>___</td>
<td>90%</td>
<td>Annual</td>
</tr>
<tr>
<td>% of employees who score 80% or higher</td>
<td><strong>Lack of participation</strong></td>
<td>Lead</td>
<td>ERC T&amp;C team</td>
<td>___</td>
<td>80%</td>
<td>Annual</td>
</tr>
<tr>
<td>Overall satisfaction score of 3 or higher</td>
<td><strong>Lack of understanding</strong></td>
<td>Lead</td>
<td>Learning Network</td>
<td>___</td>
<td>4.5/5.0</td>
<td>Annual</td>
</tr>
<tr>
<td>Ethical culture survey leadership results**</td>
<td><strong>Ethical culture</strong></td>
<td>Lead</td>
<td>Ethisphere</td>
<td>___</td>
<td>At or above benchmark</td>
<td>Annual</td>
</tr>
<tr>
<td>% of officers engaging in C&amp;E messaging</td>
<td>C&amp;E Team</td>
<td>___</td>
<td>65%</td>
<td>Annual</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Growth in # of Level 3 investigations</td>
<td>Lag</td>
<td>EthicsPoint</td>
<td>___</td>
<td>0</td>
<td>Quarterly YOY</td>
<td></td>
</tr>
<tr>
<td>Growth in # of substantiated Level 3 allegations</td>
<td>Lag</td>
<td>EthicsPoint</td>
<td>___</td>
<td>0</td>
<td>Quarterly YOY</td>
<td></td>
</tr>
<tr>
<td>Turnover rate</td>
<td>HR</td>
<td>___</td>
<td>30%</td>
<td>Quarterly</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethical culture survey results</td>
<td>Lead</td>
<td>Ethisphere</td>
<td>___</td>
<td>At or above benchmark</td>
<td>Annual</td>
<td></td>
</tr>
<tr>
<td>Hotline reports and overall reporting trends</td>
<td>Lag</td>
<td>Metrics dashboard</td>
<td>___</td>
<td>Equal to or less than prior year’s YTD</td>
<td>Quarterly</td>
<td></td>
</tr>
<tr>
<td>Increased % of STI based on NPS score or increased number of people who have NPS as a component of their STI</td>
<td>Lead</td>
<td>TBD</td>
<td>___</td>
<td>0</td>
<td>Annual</td>
<td></td>
</tr>
<tr>
<td>Increase in # of store contests</td>
<td>Retail Ops</td>
<td>___</td>
<td>Equal to or less than prior year’s YTD</td>
<td>Quarterly</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KPIs/scorecards for retail teams</td>
<td>Chris Schmidt</td>
<td>___</td>
<td>0</td>
<td>Open</td>
<td></td>
<td></td>
</tr>
<tr>
<td># of hotline reports with issue type of “Pressure”</td>
<td>Lag</td>
<td>Metrics dashboard</td>
<td>___</td>
<td>Equal to or less than prior year’s YTD</td>
<td>Quarterly</td>
<td></td>
</tr>
</tbody>
</table>
Developing C&E KRI and Metrics

Pulling data from categories like:

- AP Investigation data
- eLearning/training completion rates
- Internal survey data
- Whistleblower data
- Weights & Measures data
- HR/ER investigations data
- Internal Audit findings
- Other audit data
- OSHA citations
- POS exception reporting
- NOVs (Notices of Violations)

Let's talk about what's possible:

Building Relationships with Influencers
Ethical Culture Assessment to Identify Gaps

Engaging with Leaders

- As we know, ethical culture filters from the top down
- Create an environment where leaders feel vested in the Compliance & Ethics program
- Use data and risk assessments to demonstrate to leaders how compliance & ethics is critical to their business
  - Ethical Culture Survey
  - Metrics dashboard
Building Relationships with Key Influencers

<table>
<thead>
<tr>
<th>Compliance Committee</th>
<th>Compliance Assurance &amp; Monitoring Program</th>
<th>Enterprise Investigations Committee</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Who:</strong> Officers with compliance or risk functions</td>
<td><strong>Who:</strong> Managers and directors with compliance functions or who are needed partners</td>
<td><strong>Who:</strong> Lead investigator from Ethics, ER, Fraud, AP, and IS and their manager</td>
</tr>
<tr>
<td><strong>Purpose:</strong> To educate leaders across the enterprise about compliance risk and get them on board with mitigating it</td>
<td><strong>Purpose:</strong> To educate mid-level leaders across the enterprise about risk and get their assistance in mitigating it</td>
<td><strong>Purpose:</strong> To gain consistency in investigations and remediations; gain high-level buy-in re the processes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy Governance Board</th>
<th>International Partners</th>
<th>Senior Leaders 1:1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Who:</strong> Officers whose teams own compliance policies</td>
<td><strong>Who:</strong> Counterparts and leaders of international business units</td>
<td><strong>Who:</strong> Executive team and senior leaders</td>
</tr>
<tr>
<td><strong>Purpose:</strong> To gain consistency provide governance in policy lifecycle; to gain buy-in from leaders on importance of policies to a C&amp;E program</td>
<td><strong>Purpose:</strong> To gain consistency in process; to understand and help enhance tone at the top and drive ethical and compliant culture</td>
<td><strong>Purpose:</strong> To provide leaders tools for talking points with teams and to help leaders feel vested in C&amp;E program and part of the solution</td>
</tr>
</tbody>
</table>

Fostering a Culture of Integrity

“In looking for people to hire, you look for three qualities: **integrity, intelligence,** and **energy.** And if you don’t have the first, the other two will kill you. You think about it; it’s true. If you hire somebody without [integrity], you really want them to be dumb and lazy.”

- Warren Buffett
Thank you.