Evolution of a Compliance & Ethics Program

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

BEST BUY

Agenda

Structuring for success

Maturing the program

Developing KRIs and metrics

Building relationships with influencers

BEST BUY

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

BEST BUY

"

"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	Separate and more inclusive compliance function, integrated with Fraud, Risk and Info Security
Reporting to General Counsel	Reporting to the Audit Committee with dotted line to Chief Financial Officer
Siloed metrics	Enterprise-wide comprehensive metrics
Disjointed compliance capabilities	Centralized capability with one budget
Competing risk voices	Holistic enterprise risk management
Perceived as barrier to the business	Perceived as a partner to the business

BEST BUY

New Structure for Success

Enterprise Risk & Compliance Organization

Audit Committee

Chief Financial Officer

Chief Risk & Compliance Officer

| Global Compliance & Ethics	Enterprise Privacy	Global Threat Detection & Response	Enterprise Information Protection (Info Security)	Enterprise Risk Management	Business Operations
▪ Whistleblower Hotline	▪ CCPA, HIPAA, Customer and Employee Data Privacy Programs	▪ Fraud Prevention & Detection	▪ Information Security	▪ Enterprise Risk Assessments and Reporting	▪ Training and Communication
▪ Ethics Office Policies	▪ Privacy & Infor Sec Policies	▪ Digital Forensics & Investigation	▪ Threat & Vulnerability Management Program	▪ Third Party Due Diligence and Risk Assessments	▪ Change Management & Process Improvement
▪ Compliance Risk Management	▪ Information Records Management	▪ Data Loss Prevention	▪ Network Security	▪ Insurance Risk Management	▪ Project Management
▪ Product Safety & Compliance		▪ Business Continuity and Disaster Recovery	▪ Security Architecture		▪ Data Analytics
▪ FCPA Program		▪ Crisis Response			
		▪ Campus Security			

BEST BUY

8

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.
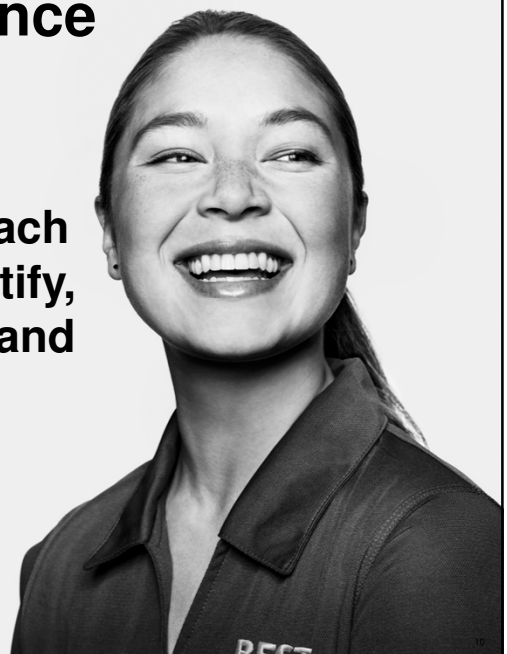
Maturing the Compliance & Ethics Program

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?
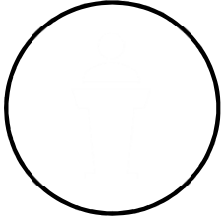
4.

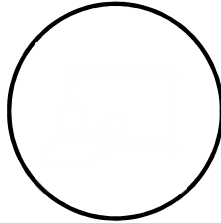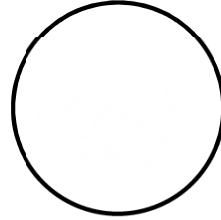Do we have the right reporting channels in place?

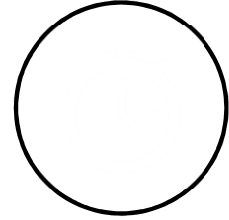# A culture that values ethical behavior has…

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**?
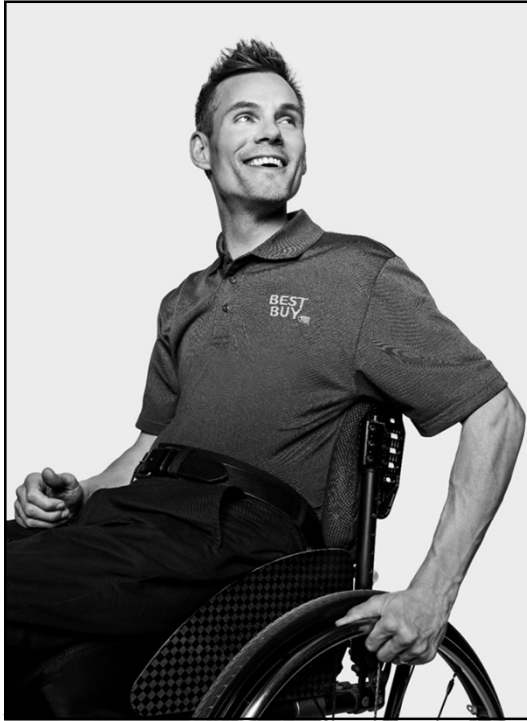
Training & Awareness

- 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**?

16
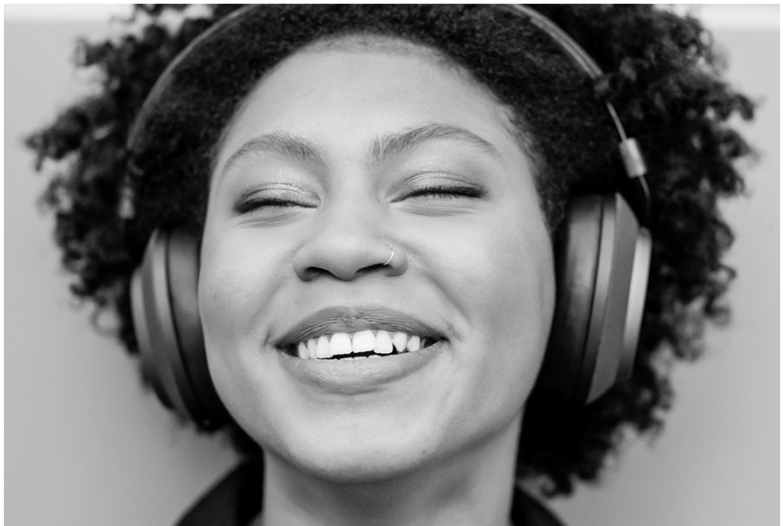
Prevention, Detection & Response

- 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?

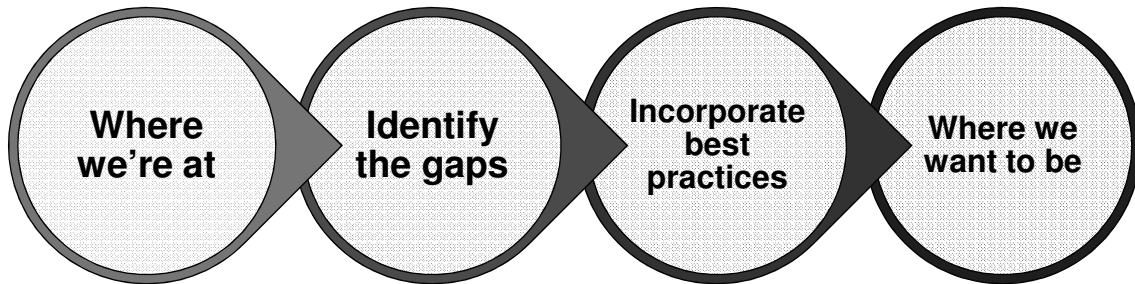| Tone at the Top	Training & Awareness
• CEO and CFO video messages in annual training • Targeted anti-retaliation training for leadership • Ethical toolkits for leaders	• Rebrand whistleblower hotline • Code of Ethics overhaul • Audience-specific live ethics trainings and road show • Annual eLearning 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 KRIs & Metrics

Developing KRIs 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

BEST BUY

BEST BUY INTERNAL USE ONLY. DO NOT COPY, PUBLISH OR DISTRIBUTE. THE MATERIAL IN THIS DOCUMENT IS CONFIDENTIAL TO BEST BUY.

Identifying KRIs

1.	**2.**	**3.**	**4.**
Identify and define the specific risk	Define sources/ causes of risk	Define KRI & type (lead/lag)	Define KRI source, target, & frequency
What type of event may result in a loss?	**What is the event trigger?**	**What metric can inform if there is an increase or decrease in risk?**	**What is the source, target, and the frequency of reporting?**
Example • **Information Security Risk:** Loss of confidentiality, integrity, or availability of systems or data originating from a system security incident or cyber-attack.	**Example** • Loss of confidentiality of data due to the **impact of a third party.**	**Example** • **% of vendors assessed with high (residual) risk** as a part of the Third Party Risk Assessment (TPRA)	**Example** • Source: TPRA Team • Target: 10% • Frequency: quarterly

BEST BUY

Compliance & Ethics Team KRI Example

1.   2.   3.

Identify and define specific risk	Define sources/causes of the risk	Define KRI (and target, source, frequency)
Unethical employee behavior that creates a risk/event.	1. Lack/weakness of training 2. Poor leadership/tone at the top 3. Human behavior 4. Financial incentive/ performance	

Human Behavior KRIs

KRI Definition	Type	Source	Actual	Target	Frequency	Status**
Ethical culture survey results	Lead	Ethisphere	—	At or above Ethisphere benchmark	Annual	--
Hotline Reports	Lag	Metrics dashboard	—	Equal to or less than prior year's YTD	Quarterly	--

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

KRIs and Metrics

Cause		KRI	Type	Source	Actual	Target	Frequency
Lack/weakness of training	Lack of participation	Training completion rates	Lead	ERC T&C team	—	90%	Annual
	Lack of understanding	% of employees who score 80% or higher	Lead	ERC T&C team	—	80%	Annual
		Overall satisfaction score of 3 or higher		The Learning Network	—	4.5/5.0	Annual
Poor leadership/tone at the top		Ethical culture survey leadership results*	Lead	Ethisphere	—	At or above benchmark	Annual
		% of officers engaging in C&E messaging		C&E Team	—	75%	Annual
		Growth in # of Level 3 investigations	Lag	EthicsPoint	—	0	Quarterly YOY
		Growth in # of substantiated Level 3 allegations		EthicsPoint	—	0	Quarterly YOY
		Turnover rate		HR	--	30%	Quarterly
Human behavior		Ethical culture survey results	Lead	Ethisphere	—	At or above benchmark	Annual
		Hotline reports and overall reporting trends	Lag	Metrics dashboard	---	Equal to or less than prior year's YTD	Quarterly
Financial incentive/performance		Increased % of STI based on NPS score or increased number of people who have NPS as a component of their STI	Lead	TBD	—	0	Annual
		Increase in # of store contests		Retail Ops	—	Equal to or less than prior year's YTD	Quarterly
		KPIs/scorecards for retail teams		Chris Schmidt	—	0	Open
		# of hotline reports with issue type of "Pressure"	Lag	Metrics dashboard	—	Equal to or less than prior year's YTD	Quarterly

Developing C&E KRIs 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.

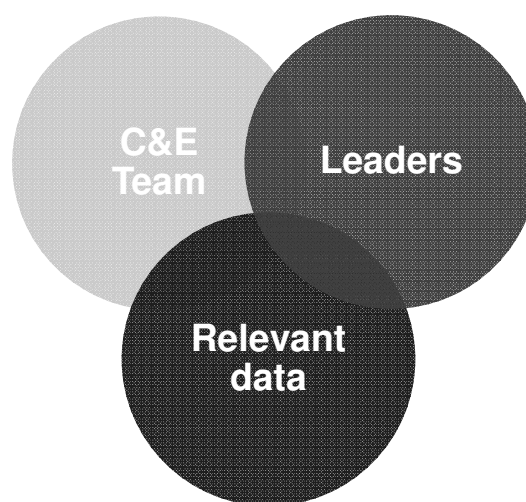# Building Relationships with Influencers

Ethical Culture Assessment to Identify Gaps

27

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

  - o Ethical Culture Survey
  - o Metrics dashboard

C&E Team

Leaders

Relevant data

BEST BUY

BEST BUY INTERNAL USE ONLY. DO NOT COPY, PUBLISH OR DISTRIBUTE. THE MATERIAL IN THIS DOCUMENT IS CONFIDENTIAL TO BEST BUY. 28

14

Building Relationships with Key Influencers

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

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

29

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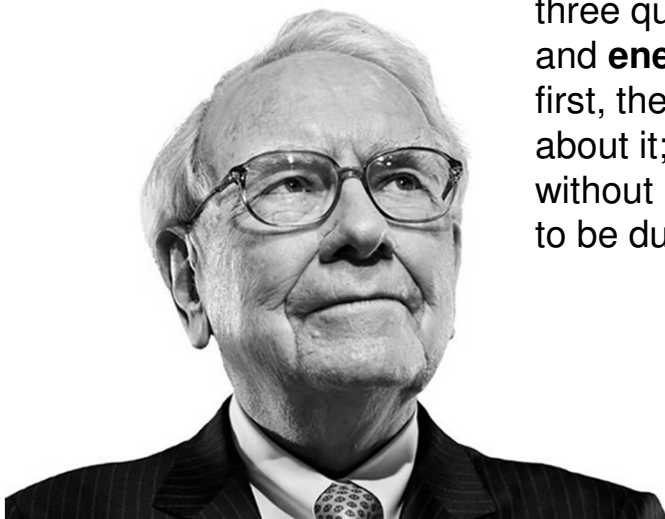
" In looking for people to hire, you look for three qualities: **integrity**, **intelligence**, and **energy**. And if you don't have the first, the other two will kill you. You think about it; it's true. If you hire somebody without [integrity], you really want them to be dumb and lazy**.** "

- Warren Buffett

30

15

Thank you.

31