BUSINESS ETHICS LEADERSHIP ALLIANCE

ROUNDTABLE RECAP:

October 30th, 2019 Hosted by AARP

Participating Companies

AARP
Booz Allen Hamilton
CareFirst BlueCross BlueShield
Diebold Nixdorf
Dominion Energy
Eagle Bank
Hewlett Packard Enterprise
Hilton
Marriott International Inc.
Noblis
Otsuka America Pharmaceutical
salesforce.com, inc.
Sodexo
The AES Corporation
The Chubb Corporation
Under Armour
Washington Gas Light Company
WSP

Topic 1: **Overviews of AARP's new Chatbot and ERM Practices**

Discussion Leads: **Ellen Hunt**, Senior Vice President - Audit, Ethics & Compliance Officer, AARP and **Joe Pugh**, Enterprise Risk Management and Compliance Director, AARP

AARP pt. 1 Chatbot Discussion
Problem: AARP needed to have a better understanding of why people went to the Code of Conduct and what information they needed. They wanted to deliver information faster and make the experience easier.

Research: AARP looked at vendors and determined the cost and timeline would not work for them, so they explored internal options to create their own Chatbot. They started by analyzing their "Ethics Advice Database" which houses the questions and answers that have come into the Ethics & Compliance Office has dealt with since 2011 to start with the top 15 most frequently asked questions, and used Q&A Maker, a Microsoft product to develop questions and answers.

Launched Oct. 8th, 2019, the Chatbot has received nearly 300 questions as of Oct. 30th (over 3 times the number of questions the Ethics & Compliance Office receives in a typical year).

- AI helps it learn as it goes, utilizing Microsoft Q&A and Power BI; if it can't answer a question, askers are directed to the Ethics office
- Valuable analytics help them identify areas where they need to focus efforts if there are themes in questions
- Most popular questions are around gifts and entertainment and joining a board
- BAH is launching a chatbot soon as well that will cover their entire policy library; Accenture has a chatbot COBE as well

Related BELA Resources:
https://bela.ethisphere.com/canada_bringing-the-code-of-conduct-to-life/
https://bela.ethisphere.com/realogy-code-user-guide-mgr/
https://bela.ethisphere.com/accenture-code-of-ethics/

AARP Pt. 2 Enterprise Risk Management Discussion

Joe Pugh provided an overview of what got ERM started at AARP and where they are today, and today, they have:

- Portfolio view of critical enterprise risks
- Enterprise risk and strategy mapping
- Risk owner accountability
- Formal cadence and risk informed reporting
- Internal Audit Integration
- Board & Executive risk alignment
- Risk appetite dialog

Creating a Board & Executive Risk Partnership, began approximately 2014

- Risk Working Group made up of Board Members and Executive Team
- Education
- Risk Assessment Survey
- Joint Scenario Workshop – 90 minutes at a Board meeting with the goal to help the Board become more risk savvy (an outside vendor did help facilitate this)

Lessons Learned

- Keep it right size and simple
- Relationship building is never done, keep talking to folks about risk
- Keep your ERM eye on strategy, tie risks to strategies, what is being done to mitigate risk>
- Take the time to create a board executive risk partnership
- Ask the Board if they are *getting what they need and want to exercise their risk oversight responsibilities*?
- Don't forget your friends in internal audit; to help make sure your mitigations are more than just on a piece of paper

Questions to AARP

Q: How often are you doing your ERA
A: Annually

Q: Is your risk appetite statement a policy? A charter?
A: It is a Board approved statement that is shared with the Board annually

Q: How do you talk about risk mitigation from a budget perspective if you do talk about it?
A: It's factored into the equation, but also look at risk as an opportunity, it's all tied together

Q: Have you invested in an ERM GRC tool?
A: Not yet. Some in the room reported using Tableau. Not many in the room have GRC tools.

Related BELA Resources

Article https://bela.ethisphere.com/risk-management/
Global Ethics Summit session https://bela.ethisphere.com/continuous-improvement-from-risk-assessments-to-action-plans-and-everything-in-between/
Article https://bela.ethisphere.com/wp-content/uploads//Canada_effectively-assessing-and-managing.pdf

Topic 2: Scaling to Manage Third Party Risk, Starting with Anti-Corruption Assessments and Capability Building

Discussion Lead: **Leslie Benton**, Vice President, Ethisphere

Companies are spending a lot of time and people power onboarding third parties, they have (often) sophisticated due diligence programs, but issues keep occurring. How do we determine if what our third parties tell us in the DD questionnaire is accurate? What's the best way to check them against that, and how can we make sure we have the capacity to tackle issues that come up?

Leslie shared some statistics from a recent Ethisphere and Kroll survey (linked in the resources section below):

- Third-party violations top the list of perceived risks to an organization's anti-bribery and corruption program, representing 35 percent of responses
- Almost a quarter of respondents report that they do not feel confident in their organization's ability to catch third-party violations of anti-bribery and corruption laws
- 45 percent of respondents work with at least 1,000 third parties per year
- 58 percent of respondents reported that they uncovered third-party violations of anti-bribery and corruption laws after the completion of their initial due diligence

Discussion around training third parties around the room. Challenges/obstacles mentioned were lack of budget; too many third parties to do it – not scalable or cost effective. Leslie shared that what she's seeing most often is often training modules initially that are retaken on some regular cadence (annually or every two years). One attendee said they train at onboarding, then re-screen and train every three years.

The group discussed monitoring third parties in some way (using a combo of data analytics, the business relationship owner staying close, audits, and other tools) is much more expected by regulators (for larger companies) but smaller companies aren't formally monitoring, though they may do a contract refresh periodically.

Challenge from the room – what if your employment department pushes back on training third parties? A: Leslie said she's not seeing this very often because guidance exists that specifically says in certain situations you should provide training. In some sectors like financial, training is required by statute and regardless of industry, often there is a bigger risk in not training third parties.

For many companies, when you are in risky areas, or in a risky business, you want to help your third parties build capability. These companies might not have significant internal resources and may welcome this kind of engagement from their large customer.

One idea from the room: your agreement may give you the right to audit, and performing a cross-functional audit of a third party might be appreciated by that third party if they don't have that capability.

How do you make sure the follow through is meaningful? The "effectiveness" piece is challenging according to many in the room.

The attendees discussed how you may be able to leverage external assessments done by third parties on your vendors. If the vendor has had one – that is something you can look to. Leslie discussed ISO37001 as a tool that exists. Is that something that you might ask about? More and more certifications are happening outside the US, particularly in Latin America and Asia.

Related BELA Resources:
Ethisphere and Kroll ABC report cited above https://bela.ethisphere.com/ethisphere-kroll-2018-abc-report/
Better Safe than Sorry article https://insights.ethisphere.com/wp-content/uploads/Leslie_S2019.pdf
Global Ethics Summit session https://bela.ethisphere.com/2019-ges-supply-chain-monitoring/
Global Ethics Summit session https://bela.ethisphere.com/2019-ges-intelligence-behind-due-diligence/
Training Third Parties *https://bela.ethisphere.com/training-3rd-parties-what-works-what-doesnt-and-where-its-going/*

Topic 3: Compliance Monitoring, the Second Line of Defense

Discussion Lead: **Melanie Hilley,** Chief Ethics and Compliance Officer, Deputy General Counsel, Booz Allen Hamilton

Monitoring – how do you know all the pieces of the program you've built are working? In auditing they often talk about the three lines of defense: 1) Everyone in your organization – following the policies, etc.; 3) are auditors and they serve an independent purpose too, but that middle line of defense 2) is "what you are doing along the way" – how are you keeping track of it so you can report out on it; and how is it integrated into your enterprise risk framework?

You have to start somewhere – that may mean a Microsoft Office suite and a tableau license, but you have to start somewhere.

What are your top risks – start there and document them for the programs you are building a monitoring program around.

Map them to what your controls are – this is time consuming, but you must start here; and get to know it well, this is your foundation

There are three kinds of monitoring activities

1) Core risk monitoring
2) Process monitoring activity – for example, your hotline, does it work? Can people get to it? If you built a portal people use for approvals, is it functioning
3) Trend monitoring – are certain things getting better or worse over time

Document what of the above you are already monitoring and in a perfect world what you would be monitoring ("If I could know anything about what is going on with XYZ, what would I want to know"

BAH identified 180 Compliance Monitoring Activities – the **WHAT**

Next think about **HOW**: questionnaires, data, external sources

- Design how you will report out. These can be tiered depending on who needs to see what, what is relevant to them, what needs to be escalated. BAH uses Tableau to design dashboards to help the audience visualize the data in their risk framework in a red-yellow-green format
    - The full report gets shared with audit and ERM – question to the room – who else should see it? Who gets what? The Board audit committee sees a portion of the risk activities as well; leveraged with stories of what could happen.

Related BELA Resources:

Global Ethics Summit Session https://bela.ethisphere.com/2019-ges-engaging-key-stakeholders/
Sample dashboards https://bela.ethisphere.com/holland-america-dashboard/
Monitoring https://bela.ethisphere.com/aecom-data-analytics/