Douglas Hileman Consulting, LLC
www.douglashileman.com
April 2024

Compliance Week 2024: It's a Wrap
Thought-Provoking Highlights

Douglas Hileman, CRMA, CPEA, FSA

Compliance Week 2024 is a wrap. Three days packed with content, networking, and useful perspectives. I led a three-hour workshop on Leveraging COSO's ICSR[1] for Compliance and Value. Attendees were impressive and engaged. I was gratified that so many said they found it practical and helpful. The entire conference met the same high standard[2]. Here are a few of my favorite quotes[3] and takeaways.

"Lies compound. They take you further and further from where you want to be." @TraciBrown was a keynote speaker on body language and lying. Good expertise to have for compliance, audit, and investigation professionals. She is energetic, the tips were practical and the session was entertaining. Her book **How to Detect Lies, Fraud and Identity Theft** is a delightful read, and a good reference (for work *and home*?).

"Legal's primary role is defending the company. The role of Compliance is to help provide transparency." @MaryShirley, Head of Compliance a #Masimo.

If the roles are combined, it can create a conflict. Legal can be inherently defensive, looking for exactly what is necessary. Compliance may wish to promote efforts on compliance, improvements, engagement and ethics. Stakeholders view the functions differently. If it's the same person, they don't know exactly who they are talking to, thereby limiting the openness and effectiveness of the communications.

[1] I am an author of COSO's "Achieving Effective Internal Control over Sustainability Reporting (ICSR)," supplemental guidance released March 2023.
[2] To see what you missed: https://www.national.complianceweek.com/agenda/
[3] Quotes may not be exact, but the best I remember them. Hey – I was listening!

“Align KPIs with business objectives. The percentage of people completing training doesn’t help achieve a business objective.” Mary Shirley again! [Her book “Level Up” is great.]

In the example above, executive management and the board will expect 100%, or very close to it. This resonated with me, for KPIs in Sustainability and climate (including GHG emissions). The same may be true for safety statistics, results of supplier audits, This can be on your function’s internal dashboard, but reconsider how they align with the level of discussion in the C-suite and board. GHG emissions are top of mind, with global, U.S.[4], state [California] and B2B drivers. In initial stages of companies’ journey, compiling the GHG emissions inventory is an accomplishment. KPIs on the inventory and impacts of early improvements may be useful. Companies may set targets, either voluntarily or to achieve compliance or requirements set by key business partners. New objectives align with the changing business environment: specific categories of Scope 3 emissions; reduce emissions in cost-effective ways; maintain or improve customer relations; avoid shareholder filings; develop and commercialized new products and services.

“The biggest way to unlock value is by mindset, not with your head in Excel.” @NickGallo at #Ethico.

He describes his role as a “Return on Integrity Coach.” How many times have we done the right thing, and felt like an acorn falling onto the lush floor of a forest? It was something small, it didn’t make a noise, and nobody was around to see it. If the acorns don’t fall, eventually there is no more forest. Note that Nick’s mindset does not require a degree, license, certificate or course. It’s an attitude we can take anywhere.

[4] The SEC released a final rule on climate-related disclosures on March 6, 2024. Less than a month later, the SEC announced it would voluntarily stay the rules pending judicial review; this is the status at this writing. Many requirements of SEC’s rule are similar to those imposed via other jurisdictions and channels. It’s still worth watching.

"It's risk management, not list management."

I wish I had noted attribution for this catchy phrase. Risk is a key driver for Sustainability reporting and disclosures, notably those directed at the general capital markets. SASB developed the Sustainability [disclosure] Standards using the definition of "materiality" from the U.S. Supreme Court – exactly the approach used for financial topics. If you aren't following these criteria for materiality, you could be at risk from failure to disclose decision-useful information on material risks. Risk is in every regulatory and disclosure framework for climate. It's one of four pillars of TCFD (now embedded in ISSB S-2) and California's SB 261. It's a section of the SEC climate disclosure rule. Enterprise Risk Management begins with identifying risk. It's not uncommon to prepare a risk register, document what you're already doing – and stop. This is not risk management. Conference sessions covered cybersecurity, climate, sustainability, and (no surprise) AI. This is an excellent reminder for all.

"Tone at the top needs reverberation in the middle, and an echo from the bottom." The Institute of Internal Auditors publishes "Tone at the Top" every other month. Deloitte says the tone at the top is the first ingredient in a world class ethics and compliance program[5]. The term rose in popularity from accounting firms in the wake of the Enron and WorldCom scandals. More than a decade earlier, Peter Drucker authored remarks that morphed into "culture eats strategy for breakfast."

With the proliferation of Sustainability reporting and disclosure standards in the last ~decade, there is more emphasis on the board's role, senior management role, and governance. However, for many years I have seen lofty statements come from high in the organization – and stop. It gets tangled in "the muddle in the middle." Those on the shop floor (the first line in the three lines model) see mixed messages and hypocrisy. The quip is a reminder for anyone in governance, risk, compliance or audit to ensure alignment at all levels of the organization.

[5] See https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-tone-at-the-top-sept-2014.pdf; accessed 4/10/2024

“Much is written about a ‘speak-up culture’; it won’t work unless you also instill a ‘listen-up culture.’” @NicoleFrew of Scotia Bank (Toronto) made this point. Thought-provoking yet simple.

Engineers warned not to launch the space shuttle Challenger in weather below the design capabilities of O-rings. Higher-ups didn’t listen, and many of us viewed the tragedy live in 1986. In 2002, Cynthia Cooper uncovered fraud at WorldCom during an internal audit. She spoke up, but found no listeners. There are many examples of high profile failures with these attributes. I’m reminded of the Safety Pyramid with a broad layer of simple occurrences (unsafe act) at the bottom, with incrementally smaller layers of more impactful occurrences (near miss, property damage). The apex of the pyramid is a highly undesirable occurrence (fatality, explosion). The “compliance apex” is getting bigger, with hefty fines for data breaches, privacy, AML, environmental, SEC disclosures, OFAC and more. In writing the COSO ICSR supplemental guidance, the author team reminded reminded each other that the famous COSO cube is “porous.” Internal controls have several uses, and for several groups. I think of a Compliance (and Ethics) communications culture triangle. Drafting off Nicole’s point, it needs to be porous to be effective.

COMPLIANCE WEEK
NATIONAL
• 2024 •
WORKSHOP D
Leveraging COSO ICSR for Compliance and Value in Sustainability Reporting
D
Additional Registration Required. Look for this symbol on your badge to attend.
VIEW ROUNDTABLE TOPICS

Contact doug@douglashileman.com for more: COSO ICSR workshops; support in compliance/ risk/ reporting/ audit/ audit readiness/ climate.