JANUARY 2021

COMPLIANCE & ETHICS PROFESSIONAL

CEP MAGAZINE

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

RENÉE WARDLAW
SENIOR DIRECTOR OF CORPORATE COMPLIANCE AND ASSOCIATE GENERAL COUNSEL FOR BRISTOL BAY NATIVE CORPORATION, ANCHORAGE, ALASKA, USA

ENHANCING PROCESSES IS JUST THE TIP OF THE ICEBERG (P10)

Returning to business travel: Mitigating risk for your employees (P16)

Protecting corporate data in the work-from-home era (P20)

Rethink your policy management system to strengthen your compliance program (P26)

Balancing effective compliance policies against the ubiquity of ephemeral messaging (P32)

SCCE®

We've moved!

Effective January 1, 2021

Society of Corporate Compliance and Ethics & Health Care Compliance Association's new address is:

6462 City West Parkway
Eden Prairie, MN 55344

While our address has changed, our member service contact information remains the same:

Phone: +1 952.933.4977
Toll-free: 1.888.277.4977
Fax: +1 952.988.0146
Email: helpteam@corporatecompliance.org

SCCE
Society of Corporate Compliance and Ethics

New year, new address for SCCE

by Gerry Zack

Think of this month's letter as part two of the letter I started last month. As we begin 2021, many of us are optimistic that better days lie ahead. When the COVID-19 pandemic became a serious threat last March, we did what many organizations did; we made a lot of quick decisions to protect our employees and our members, resulting in a remote workforce, the cancellation of in-person conferences, and gradual conversion to or development of virtual events. I discussed many of these changes last month.

Along the way, SCCE faced another decision. We were already well along in the development of a new headquarters we had purchased, having significantly outgrown our old and very outdated building. Should we have stopped immediately? The alarmists were saying things like, "COVID-19 changes everything. People will never return to an office environment." Should we have followed that logic and abandoned the build-out of the new office?

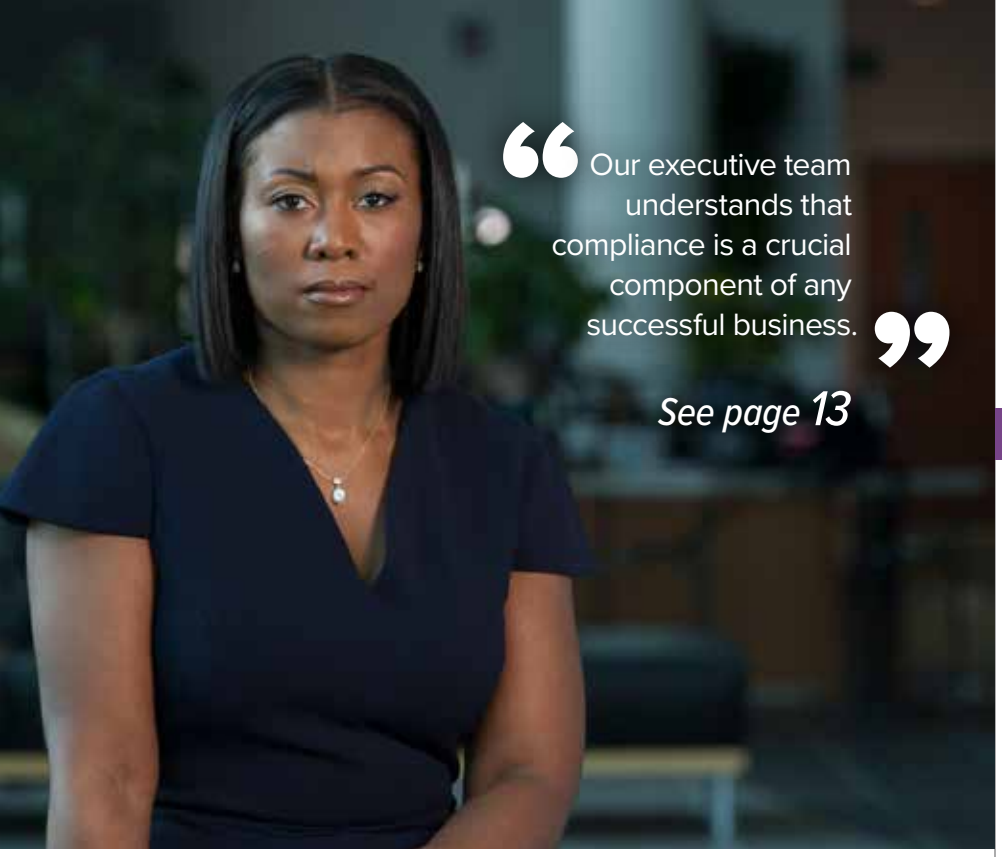
We decided to move ahead and finish the work, and the result is the new office address you'll see in this magazine, on our website, and on all of our materials beginning January 1. When people ask why, the answer is rather simple. First, people will want to return to an office. We've learned that remote working can be efficient, so there will be greater use of remote-working options. But there will be a desire and need for working together in an office once it becomes safe to do so.

And this leads me to the second, and more important, reason. When our employees return, whenever that is, we want them to be in an environment they enjoy, so they will be happy, productive, and proud of their organization. Our old office was overcrowded and inefficient in every respect. The new office will lead to improved productivity and increased capacity. In addition, we were able to incorporate several COVID-19 considerations into the design, enabling greater capabilities for social distancing and other health and safety measures.

The pandemic has been a setback for all of us. But rest assured that SCCE was well positioned to deal with it, and we have continued to take action so that when the craziness subsides and we gradually return to something resembling normal, this association will be stronger than before and able to serve the profession better for many years to come.

Gerry Zack
CCEP, CFE, CIA
Please feel free to contact me anytime to share your thoughts:
+1 612.357.1544 (cell)
+1 952.567.6215 (direct)
gerry.zack@corporatecompliance.org

@Gerry_Zack
/in/gerryzack



COMPLIANCE & ETHICS PROFESSIONAL

CEP

MAGAZINE

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

January 2021

Features

10 **Meet Renée Wardlaw: Enhancing processes is just the tip of the iceberg**
an interview by Adam Turteltaub

16 **Returning to business travel: Mitigating risk for your employees**
by Michael F. Savicki
Prepare now for the return of business travel to mitigate risk for employees and your organization.

20 **Protecting corporate data in the work-from-home era**
by Melody Haase
There is no one-size-fits-all solution to data loss, but there are key aspects to keep in mind.

26 **Rethink your policy management system to strengthen your compliance program**
by J. Veronica Xu
Policy management is an important facet of creating a culture of compliance.

32 [CEU] **Balancing effective compliance policies against the ubiquity of ephemeral messaging**
by Daniel J. Polatsek
Self-deleting message apps can be great for security—but also for concealing unlawful conduct.

Columns

1 **Letter from the CEO**
by Gerry Zack

15 **A view from abroad**
by Sally March

19 **The other side of the story**
by Shin Jae Kim

25 **EU compliance and regulation**
by Robert Bond

31 **Culture is all of our business**
by Nick Gallo and Gio Gallo

37 **Driven**
by Walter E. Johnson

53 **How to be a wildly effective compliance officer**
by Kristy Grant-Hart

66 **The last word**
by Joe Murphy

CEP Magazine (ISSN 1523-8466) is published by the Society of Corporate Compliance and Ethics (SCCE), 6462 City West Parkway, Eden Prairie, MN 55344. Subscriptions are free to members. Periodicals postage-paid at Saint Paul, MN 55112. Postmaster: Send address changes to ***CEP Magazine***, 6462 City West Parkway, Eden Prairie, MN 55344.

SCCE®
Society of Corporate Compliance and Ethics

+1 952.933.4977 or 888.277.4977 | corporatecompliance.org

Departments

5 **News**
7 **SCCE news**
9 **People on the move**
67 **Takeaways**
68 **SCCE upcoming events**
69 **2020 *CEP* index**

Articles

38 **Engage with your marketing team to avoid influencer marketing risks**
by Caroline Franco
Influencer marketing predates social media, and as the practice evolves, so do the risks.

44 [CEU] **Your organization has received a data access request. What now?**
by Patrick O'Kane
Is your company ready to handle a data access request under GDPR and the CCPA?

48 **New data reveal the growth of compliance in Latin America**
by Alejandra Montenegro Almonte and James Tillen
Explore the diverse and ever-changing compliance landscape in Latin America.

54 **Ensuring organizational justice for all**
by Emeka N. Nwankpah
Does your organization treat all investigations with fairness and consistency?

58 [CEU] **Is your company's job applicant-tracking system making compliant inquiries?**
by MaryEllen O'Neill
Examine your tracking system for job applicants. You may uncover some inappropriate — or illegal — practices.

CEP Magazine is printed with 100% soy-based, water-soluble inks on recycled paper, which includes 10% post-consumer waste. The remaining fiber comes from responsibly managed forests. The energy used to produce the paper is generated with Green-e® certified renewable energy. Certifications for the paper include Forest Stewardship Council (FSC), Sustainable Forestry Initiative (SFI), and Programme for the Endorsement of Forest Certification (PEFC).

VOLUME 18, ISSUE 1

Regional Compliance & Ethics Conferences

Updates on the latest news in regulatory requirements, compliance enforcement, and strategies to develop effective compliance programs. These one-day events include general and specialty sessions, as well as opportunities to network with industry peers.

Attendees will have the opportunity to earn live Compliance Certification Board (CCB)® continuing education units (CEUs).

Virtual and in-person conference formats vary.

January 8, 2021 • Asia VIRTUAL
January 22, 2021 • Southern California VIRTUAL
February 4, 2021 • South America VIRTUAL
February 11, 2021 • Middle East & Africa VIRTUAL
February 26, 2021 • Alaska VIRTUAL
March 5, 2021 • Minneapolis, MN VIRTUAL
March 26, 2021 • Boston, MA VIRTUAL
April 8, 2021 • Asia VIRTUAL
April 23, 2021 • Tampa, FL VIRTUAL
May 7, 2021 • Richmond, VA VIRTUAL
May 14, 2021 • San Francisco, CA VIRTUAL
June 18, 2021 • Nashville, TN VIRTUAL
July 16, 2021 • Chicago, IL VIRTUAL
August 13, 2021 • Atlanta, GA VIRTUAL
September 17, 2021 • Scottsdale, AZ VIRTUAL
October 8, 2021 • Washington, DC
October 22, 2021 • Dallas, TX
November 5, 2021 • Columbus, OH
November 12, 2021 • Seattle, WA
December 3, 2021 • Philadelphia, PA

Visit the website for more information
corporatecompliance.org/regionals

SCCE
Society of Corporate Compliance and Ethics

US sanctions Russian research facility for alleged cybercrimes

The United States Department of the Treasury's Office of Foreign Assets Control announced sanctions against the State Research Center of the Russian Federation FGUP Central Scientific Research Institute of Chemistry and Mechanics, or TsNIIKhM, on October 23.[1]

The research center is accused of using malware to target facilities in the Middle East in 2017 and again in the US in 2019. The attack in the Middle East focused on a petrochemical facility, while the US attacks were probes to identify security vulnerabilities in the domestic energy infrastructure.

"'The Russian Government continues to engage in dangerous cyber activities aimed at the United States and our allies,'" said Secretary Steven Mnuchin.[2] "'This Administration will continue to aggressively defend the critical infrastructure of the United States from anyone attempting to disrupt it.'"

Brazilian meatpacking company settles multiple investigations by US authorities

Brazil's J&F Investimentos and JBS SA agreed to pay fines to the United States Department of Justice and the Securities and Exchange Commission for bribery and insider trading.[3] J&F, owned by two Brazilian brothers, controls JBS, the largest meatpacking company in the world.

The brothers admitted to bribing Brazilian politicians in order to gain financing and other benefits for the company. The bribery scheme involved multiple subsidiaries of J&F, including Pilgrim's Pride. The DOJ fined the company $256 million, but half of the full penalty amount was credited to fines paid to the Brazilian authorities.

J&F now has extensive holdings in the US, and as equity analyst Marco Saravalle told *The Wall Street Journal,*[4] "The important thing about the company is that they have good operational assets and the executives are motivated to produce results for shareholders."

ICO fines Marriott 18.4 million pounds for data breach

After extended investigations and negotiations, the United Kingdom's Information Commissioner's Office levied a fine of £18.4 million against Marriott International Inc. for a data breach that occurred in 2014.[5] The breach was one of the largest leaks of personal data in recent years, affecting more than 300 million guests. The breach affected Starwood Hotels and Resorts Worldwide Inc., which Marriott acquired in 2016.

The investigation was complicated by Brexit, the passage of the General Data Protection Regulation (GDPR), and the fact that Marriott was accepting responsibility for a breach that happened prior to the acquisition. The Information Commissioner's Office stated that the fine was under GDPR and in cooperation with European Union data protection authorities.

UK Serious Fraud Office releases DPA guidance

The United Kingdom's Serious Fraud Office published new guidance related to deferred prosecution agreements (DPAs).[6] The guidance, nested in the office's internal *SFO Operational Handbook*, offers insight into how the office will approach DPAs, what is required of companies that seek to enter such an agreement, and some of the standard requirements placed upon companies that do enter DPAs.

The guidance also clearly delineates the procedures involved in securing a DPA; what information, if any, is released to the public; how a DPA looks when entered into the legal record; and the criminal offenses to which DPAs can apply.

One of the most salient parts of the guidance, from a company's point of view, describes the procedures prosecutors must go through in order to determine whether a company should be prosecuted in court or whether the Crown should enter into a DPA.

Endnotes

1. Maggie Miller, "Treasury sanctions Russian group accused of targeting US critical facilities with destructive malware," *The Hill*, October 23, 2020, https://bit.ly/2Jhofdf.
2. United States Department of the Treasury, "Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware," news release, October 23, 2020, https://bit.ly/3oDTAax
3. Harry Cassin, "Brazil holding company agrees to pay $285 million to settle FCPA violations," *The FCPA Blog*, October 14, 2020, https://bit.ly/3kItn8l.
4. Luciana Magalhaes, Samantha Pearson, and Jacob Bunge, "Meat Giant JBS's Owner Settles U.S. Corruption Charges," *The Wall Street Journal,* October 14, 2020, https://on.wsj.com/31WR0mf.
5. Jonathan Armstrong and André Bywater, "Client Alert: ICO Fines Marriott £18.4m after Data Breach," Cordery Compliance, November 3, 2020, https://bit.ly/3oSh5wC
6. United Kingdom Serious Fraud Office, "Deferred Prosecution Agreements," *SFO Operational Handbook*, accessed November 9, 2020, https://bit.ly/3eftBRY.

VIRTUAL

Compliance & Ethics Essentials Workshop

Be a more effective member of your compliance team. Attend our new virtual Compliance & Ethics Essentials Workshop for an introduction to compliance and ethics taught by industry leaders. The curriculum focuses on the core elements of an effective compliance program to help you build a foundation for your career.

Workshops are limited to 150 participants. Register early to secure your spot!

In addition to the valuable education this program provides, participants also will be able to earn all of the continuing education units (CEUs) required to sit for the Certified Compliance & Ethics Professional (CCEP)® exam. Interested in elevating your career? To learn more about eligibility and other Compliance Certification Board (CCB)® exams, visit corporatecompliance.org/certification.

Topics include:

- Introduction and background to compliance and ethics programs
- Standards and procedures
- Governance, oversights, and authority
- Risk assessment
- Due diligence in delegation of authority
- Communication and training
- Incentives and enforcement
- Monitoring, auditing, and reporting systems
- Investigations
- Response to wrongdoing
- Program improvement
- Overview of FCPA, UK bribery, conflict of interest, and privacy and data security
- Key skills necessary for compliance professionals

UPCOMING WORKSHOPS

January 11–14, 2021 ▪ March 1–4, 2021

Learn more
corporatecompliance.org/essentialsworkshops

SCCE® Society of Corporate Compliance and Ethics

SCCE Association News

SCCE Compliance & Ethics Essentials Workshops

corporatecompliance.org/essentialsworkshops

SCCE's Compliance & Ethics Essentials Workshops provide a comprehensive introduction to the elements of a compliance program. These virtual programs are ideal for individuals with less than two years of experience in compliance, including those that have just entered compliance for the first time.

The four days of training are designed to help new compliance professionals develop and improve their compliance skills and become more effective members of the compliance team.

Attendees will have the opportunity to earn 21.6 live Compliance Certification Board (CCB)® continuing education units (CEUs) from their desk, enough to sit for the Certified Compliance & Ethics Professional (CCEP)® exam.*

Workshops are limited to just 150 participants. Don't wait to enroll.

Upcoming workshops

- January 11–14, 2021
- March 1–4, 2021

Learn more:
www.corporatecompliance.org/essentialsworkshops

*To see all the requirements to sit for the certification exam, including work experience, please visit *www.corporatecompliance.org/certification*.

Stay informed

The Compliance & Ethics Blog

Read educational insights and compliance news from industry professionals or share your knowledge with the compliance and ethics community by submitting an article.

Compliance Perspective Podcasts

Listen to the insights of compliance and ethics experts as they discuss everything from assessing risk, understanding the latest regulations, reporting to the board & training your workforce.

Subscribe to Compliance Perspectives here:

iTunes
apple.co/1TCNS24

Email
bit.ly/podcastsub

Android
bit.ly/1Z3S2la

Learn more
complianceandethics.org

SCCE
Society of Corporate Compliance and Ethics

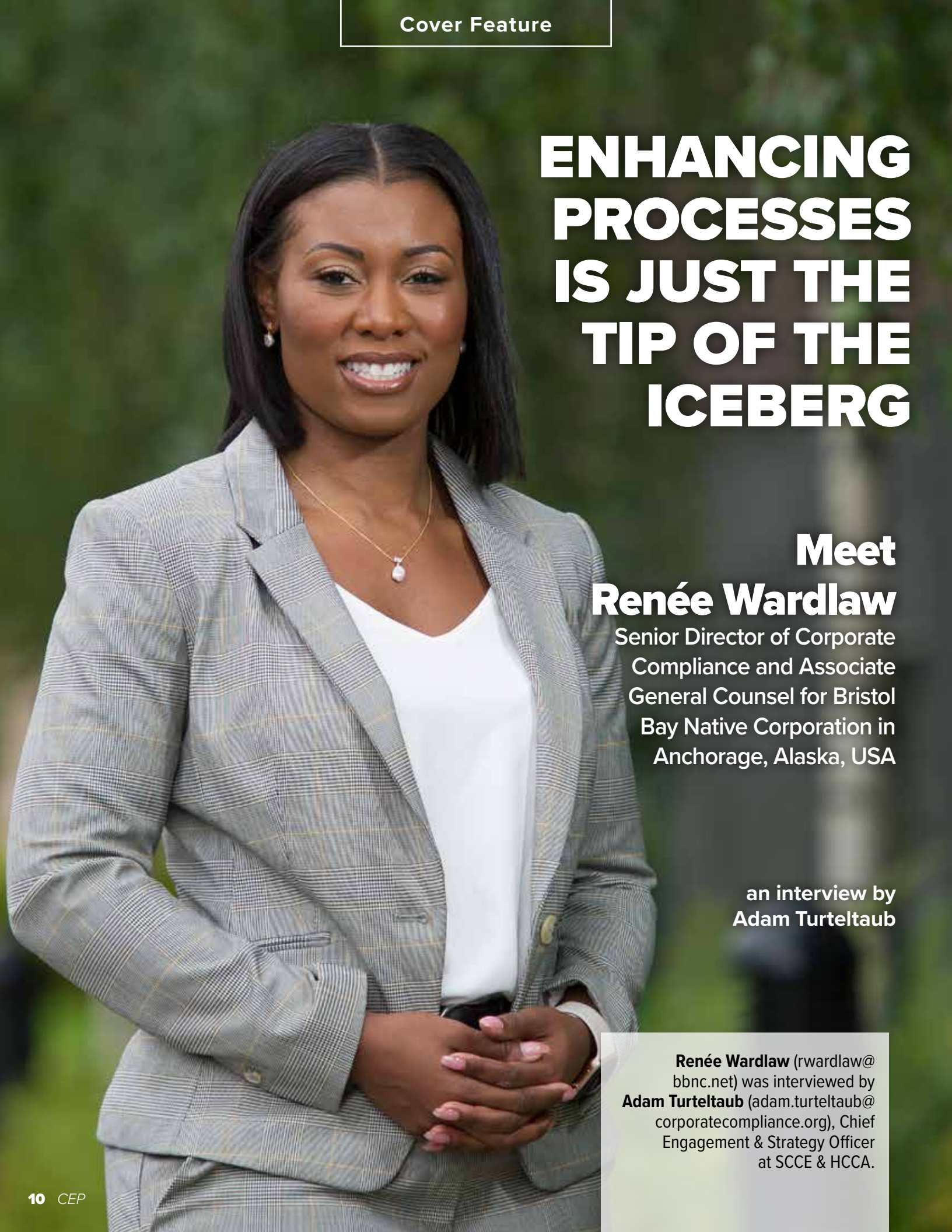
PEOPLE *on the* MOVE

WHERE'S YOUR CAREER TAKING YOU?

If you've received a promotion or industry award, accepted a new position, or added a new staff member to your compliance department, let us know! It's a great way to keep the compliance community up to date.

To submit your news, visit **http://bit.ly/2snNxdJ** or email *margaret.martyr@corporatecompliance.org*

- **Aida M. Lebbos** has joined the University of Maryland Global Campus as associate vice president, institutional compliance and risk, in Adelphi, Maryland, USA.
- In Purchase, New York, USA, **Allison Kiene** has been appointed Argo Group's new group general counsel.
- New York-based Gemini Trust Co. LLC announced the appointment of **Andy Meehan** as chief compliance officer of Asia-Pacific region.
- **Ashley Carr** is the new director of code enforcement for the city of Clarksburg, West Virginia, USA.
- In Madison, Wisconsin, USA, **Katie Ignatowski** has been promoted to chief compliance officer for the University of Wisconsin system.



ENHANCING PROCESSES IS JUST THE TIP OF THE ICEBERG

Meet Renée Wardlaw

Senior Director of Corporate Compliance and Associate General Counsel for Bristol Bay Native Corporation in Anchorage, Alaska, USA

an interview by Adam Turteltaub

Renée Wardlaw (rwardlaw@bbnc.net) was interviewed by **Adam Turteltaub** (adam.turteltaub@corporatecompliance.org), Chief Engagement & Strategy Officer at SCCE & HCCA.

AT: First, it would be good if you could give an overview of the Bristol Bay Native Corporation's purpose and structure. It's unique.

RW: Unique is an understatement. Bristol Bay Native Corporation (BBNC) was established by the Alaska Native Claims Settlement Act of 1971 with the mission of "Enriching Our Native Way of Life." Headquartered in Anchorage, Alaska, BBNC works to protect the land in Bristol Bay, celebrate the legacy of its people, and enhance the lives of its shareholders — the Native people of Southwest Alaska's Bristol Bay region. BBNC has five separate and distinct business lines, which include industrial services, government services, construction, tourism, and seafood. Our businesses are diversified with successful operations that house subject matter expertise in specific industries. While we are a for-profit corporation, we are unique in that our shareholders receive dividends derived from business profits. We are proud to work in partnership with our subsidiaries to ensure that all employees are operating with integrity and fulfilling BBNC's mission to enrich the lives of our shareholders.

AT: Like many other native organizations, you are also a government contractor. What kind of complexity does that add to the compliance program?

RW: It is a bit complex, but I'll try to explain it simply. Alaska Native corporations are eligible to participate in the Small Business Administration (SBA) 8(a) Business Development Program and, by federal statute, are deemed socially and economically disadvantaged. BBNC has been involved in government contracting since early 2000 and has been fortunate to have minimal turnover in key leadership. Those key leaders have in-depth technical and management experience to navigate the regulations and complexities pertaining to government contracting. Applicable laws are routinely updated and strictly enforced with severe penalties for offenses. It is critical to have a compliance program that meets mandatory requirements: qualified personnel, processes and policies, mandated training, internal controls, and reporting obligations. Our code of ethics provides an overarching resource to all employees and includes a specific section on the importance of business ethics and integrity in government contracting. Additionally, we have a network of employees enterprise-wide who have expertise in specialized areas of government contracting in the SBA 8(a) program.

AT: I want to focus for a bit on you and your experiences. Normally, graduate degrees don't come up in these interviews, but you have both a JD and an MBA. There are lots of lawyers in compliance, but not as many MBAs as there probably should be. How does the MBA inform the way you approach compliance issues?

RW: Having multiple interests can be a gift and a curse. I obtained my JD and MBA in a joint program at American University in Washington, DC. I have always been interested in business. I believe that compliance professionals are an essential resource for successful business operations. I first try to approach any compliance issue by looking at the perspective of the various stakeholders involved in the matter, along with BBNC's policies. Because I have an MBA, I feel I can better appreciate the business perspective and efficiently resolve questions or concerns about a proposed resolution. This augments my role as not only an issue spotter but also a problem solver.

I am sure that fellow compliance professionals will agree with me that all prosecutors are compliance champions, whether they realize it or not.

AT: You also had experience working as a prosecutor, working as an assistant attorney general in Alaska. How well do you think prosecutors at the state level appreciate compliance programs?

RW: I am sure that fellow compliance professionals will agree with me that all prosecutors are compliance champions, whether they realize it or not. As an assistant attorney general, I represented the Alaska Division of Banking and Securities.

A civil or criminal matter would come to the division's attention, and then we would investigate the issue and process the matter for resolution. From time to time, a matter would push the division to draft new statutes or regulations

to accomplish a widespread fix to an underlying issue. I gained a wealth of experience in statute and regulation writing and internal investigations. This knowledge provided me with an excellent foundation for working in a diversified corporate environment.

Prosecutors and compliance professionals engage in a similar loop of proactive measures focused on reducing and resolving risks. I believe prosecutors appreciate the importance of compliance programs and value their function to reduce and resolve civil or criminal matters.

We want to make sure that employees not only know the rules for business but that they also know how to make ethical and compliant business decisions.

AT: Let's go back to your day-to-day work. BBNC operates in almost all 50 states and nearly 16 countries. How does it stay interconnected to ensure all its employees are operating with integrity?

RW: Connecting with others is my favorite part about being a compliance professional for BBNC. We have grown leaps and bounds over the past 10 years, and are proud of our growth and commitment to integrity in the US and abroad. Because its employee population spans the globe, BBNC uses technology as a tool to ensure its employees have the most up-to-date resources available to them. We maintain an electronic policy library, including an interactive code of ethics, and use an electronic learning management system to create and deploy customized trainings in various areas. At BBNC, we want to make sure that employees not only know the rules for business but that they also know how to make ethical and compliant business decisions.

In alignment with the most recent Department of Justice guidance for corporate compliance programs,[1] BBNC and its subsidiaries use a risk-based approach to create and maintain right-sized compliance programs. Where some of our businesses have more significant risks and regulatory oversight, it is important to rely on qualified personnel within the specific business to develop and maintain appropriate compliance programs. We strive to be in partnership with subject matter experts to ensure we are delivering the right amount of compliance to reduce overall risks to operations.

AT: BBNC headquarters are in Anchorage, Alaska, which is a remote location. How does it ensure its leaders incorporate ethics and compliance into their business operations?

RW: Being in alignment with leadership has proven to be a great asset to BBNC's compliance and ethics initiatives. For the past 11 years, BBNC, with the support of the executive team and board of directors, hosts an Annual Leadership & Compliance Conference. The conference brings together BBNC leadership from across the country to receive training in leadership, compliance, and ethics. The conference attendees are charged with sharing the training with their employees. Sharing information from the top ensures that the message of compliance and ethics is spread to all employees. BBNC has never wavered from its commitment to operating with integrity as it is continued on a trajectory of growth.

This year, we supplemented our conference with our first Spotlight on Compliance, which was a weeklong series of events, release of tools and materials, and outreach to each of our employees. The Spotlight on Compliance allowed BBNC to deliver the message that each of us is the *i* in "integrity." We are looking forward to this being an annual event.

AT: What comprises BBNC's compliance department?

RW: The compliance department is overseen by the chief compliance officer (CCO), who reports to the general counsel. I, as the senior director of compliance, report to the CCO, and I am charged with carrying out the compliance program, including developing and tracking training, policy management, investigations, and compliance-driven incentives. Our compliance specialist provides administrative support to the team. Our records and information management team, which manages the life cycle of records for the organization and its subsidiaries, is also a part of the compliance department.

AT: How does BBNC's leadership support compliance within the organization?

RW: Leadership is not only about talking the talk but also about walking the walk. The executive team is committed to an ethical corporate culture. BBNC promotes a servant-leadership philosophy, which focuses on the development of good corporate citizens who are empowered to make ethics and compliance a part of their everyday life. Our executive team understands that compliance is a crucial component of any successful business and models supportive leadership throughout the organization, holding themselves to the highest standards. Their support of the compliance department and active participation in the Annual Leadership & Compliance Conference is a true demonstration of talking the talk and walking the walk.

AT: Finally, let's look to the future. How do you see compliance evolving over the next few years?

RW: The most exciting aspect of being a compliance professional is the never-ending areas where compliance and ethics can enhance existing processes. I see compliance becoming more integrated into the day-to-day business decisions of a successful corporation. I believe that compliance professionals can bring significant value to their business operations by promoting electronic collaboration tools. Ultimately, compliance is grounded in genuine and authentic relationships with others. So long as compliance professionals stay connected to the business operations they serve, they will be valued members of a successful business team.

AT: Thank you, Renée!

Endnotes

1. U.S. Dep't of Justice, Criminal Div., *Evaluation of Corporate Compliance Programs* (Updated June 2020), http://bit.ly/2Z2Dp8R.

Save the Date

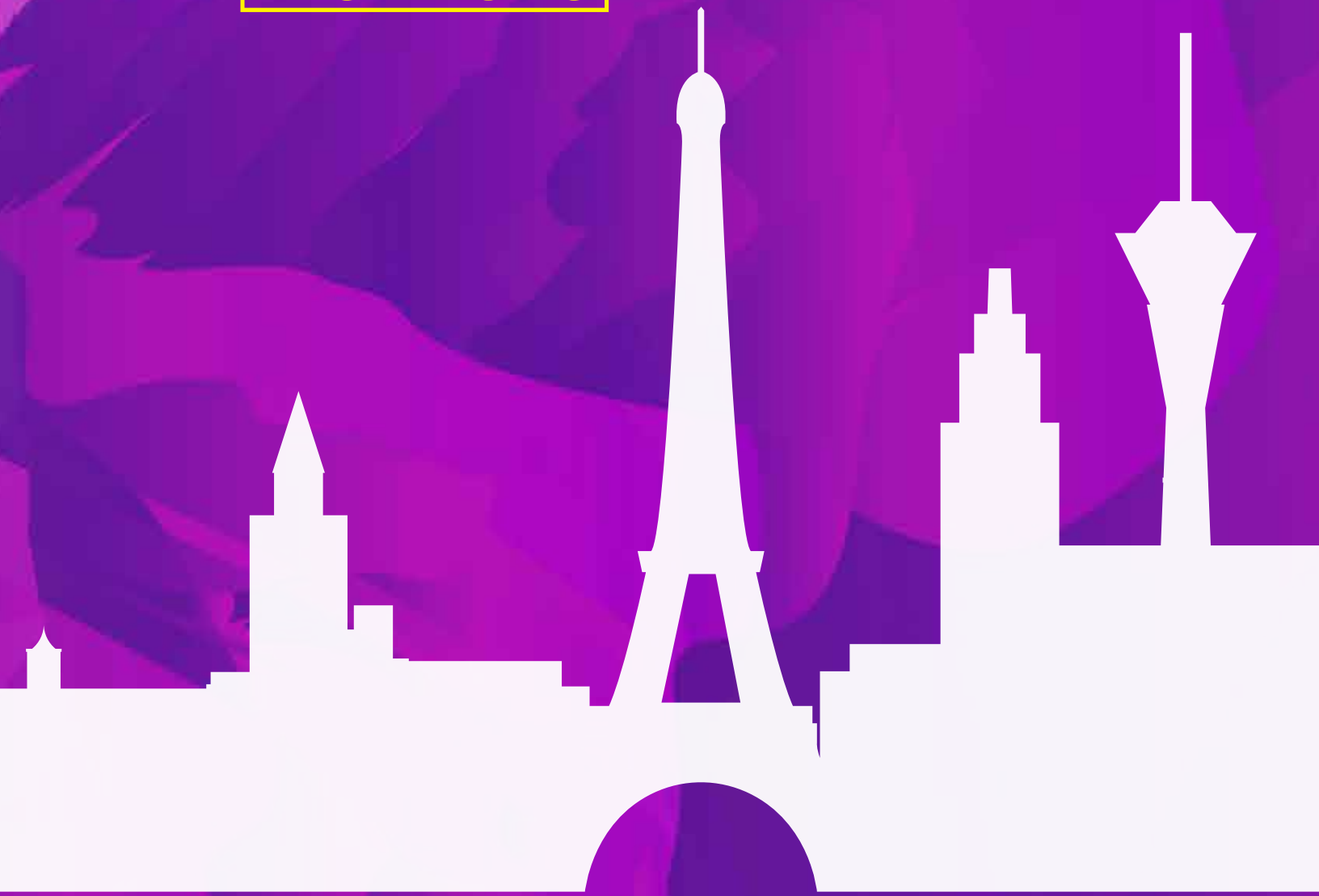
2021 CEI

September 19-22

LAS VEGAS

20 YEARS ANNIVERSARY

Compliance & Ethics Institute



Learn more
corporatecompliance.org/2021CEI

SCCE
Society of Corporate Compliance and Ethics

Personal impact statement

by Sally March

On December 31, the UK's Brexit transition period comes to an end. As I write this, the representatives of the UK and EU are still talking about whether a trade deal can be reached and, if so, what it will look like. With no clarity and only days left to prepare, on top of the fluid responses here and in other countries to COVID-19, we have uncertainty squared. Also, though I am writing before the US election has been certified, the count kept us on the edge of our seats. In uncertain times, psychologists advise us to focus on the things we can control.

Business pundits are advising senior executives to focus on purpose. As one of these firms puts it, "What is your company's core reason for being, and where can you have a unique, positive impact on society?"[1] Employees feel that purpose is important, yet most say that if their company has a purpose statement, it isn't having an impact. We've seen some good examples in the past year of companies that do have a clear purpose and whose leaders use that to make tough decisions in tough times. Unilever, for example, has clear purpose, values, and principles, and as part of its commitment to communities, it has been promoting good hand-washing habits around the world for years. In 2020, they brought their experience to schools in the UK, helping teachers when schools reopened.

Not all of us can have input on our corporate purpose statement, but each of us can, and should, be clear about our own purpose. It's probably not in a job description, but understanding how our role fits in with the organization's objectives is a good start. Ask, "Where can I have a positive impact?" At this stage, mine is to inspire the new generation of ethics and compliance professionals to think beyond boundaries. And for leaders, helping team members understand their unique purpose will help them focus on things they can control in these uncertain times. CEP

Sally March

(sjmarch10@gmail.com) is Director, Drummond March & Co, in London, UK.

Endnotes

1. Arne Gast et al., "Purpose: Shifting from why to how," *McKinsey Quarterly*, April 22, 2020, https://mck.co/3jY6pbO.

RETURNING TO BUSINESS TRAVEL: MITIGATING RISK FOR YOUR EMPLOYEES

by Michael F. Savicki

Michael F. Savicki

(michael.savicki@amexgbt.com) is Vice President for Risk, Compliance & ESG—The Americas, and Global Head of Privacy & Commercial Compliance at American Express Global Business Travel.

The disruption of recent months has forced companies around the world to rewrite business plans and alter operations. Perhaps most significant has been the unprecedented migration of workers to virtual, work-from-home environments, necessitated by travel restrictions and the widespread lockdown of citizens. But as the rules curtailing people's movement are eased, much has been written and said about the best way to get people back to their offices.

One topic not discussed as much as it should be is the return of business travel. While the number of flight bookings remain generally low, there has been a recent uptick in some locations. In October 2020, for example, more than a million passengers passed through the Transportation Security Administration checkpoints for the first time since the lockdown began.[1] Companies, therefore, would be well advised to start preparing.

Update your travel policy

In the past, travel policy reviews commonly took place once a quarter, or even once a year. Today, employers need processes that enable a regular review and update of their travel policy. While doing so, companies must understand the need to protect both the well-being of employees and their own corporate reputation. For example, employers may insist all employees use masks or facial coverings for air and rail travel regardless of whether it is mandated by the operator or relevant authority. At the same time, a company could allow a business traveler to book an airline that employs an open middle seat policy even if it's not the lowest fare available on a particular route. In the policy update, employers could also stress the need to follow the

Centers for Disease Control and Prevention (CDC) best practice guidance for overnight hotel stays and dining out while traveling.

Monitor government mandates prior to booking

Federal, state, and local governments have responded to COVID-19 with restrictions designed to stop the spread. These requirements continue to change on a regular basis. For example, certain states in the northeast of the United States have enacted mandatory two-week quarantine requirements for travelers from the majority of other states, and all nonessential travel remains prohibited between the US, Canada, and Mexico. The CDC, on the other hand, recently announced a more nuanced approach by indicating that it will no longer require all flights carrying airline passengers arriving from, or those who recently had a presence in, mainland China, Iran, the Schengen region of Europe, the UK/Ireland, and Brazil to land at one of 15 designated US airports and will halt enhanced entry health screening for these passengers.[2] Instead, the CDC indicated that it would be implementing a new enhanced risk-mitigation strategy to reduce the risk of travel-related disease transmission by prioritizing other public health measures, including (i) increased education and outreach, (ii) contact tracing, (iii) increased testing, and (iv) post-arrival recommendations for monitoring and potential quarantine, among other activities.

Accordingly, employers must make sure travelers can access up-to-date information about travel restrictions, including border closures, entry requirements, and quarantine measures, in addition to having a documented internal approval process in place prior to booking. Because these regulatory developments are constantly evolving, global travel management companies (TMCs) are uniquely placed to help travel managers keep travel policies current while making sure travelers stay well informed prior to and during their business trip.

Monitor travelers while traveling

Employers should be particularly mindful of their duty of care obligations for their travelers, as there are many areas to address. For starters, employers should strongly encourage travelers to book travel within the company's existing tools and policies and provide personal protective equipment or ensure that the selected supplier will do so for the journey. Employers should also, either directly or via their TMC, ensure their travelers are fully aware of all risk-mitigation best practices while traveling. For example, the US government, via the departments of Transportation, Homeland Security, and Health & Human Services, issued nonbinding guidance that highlighted best practices and key mitigation strategies for travelers, airlines, and airports.[3] The guidance stressed the need for individual traveler education, face masks or facial covering throughout the journey, and use of apps to facilitate contactless travel to the greatest extent possible.

In addition, an employer's global security team or TMC should have tools that locate employees traveling on business, such as tracing corporate card swipe data or geo-tracking via a mobile app on a company device. Should an event occur, employers will want to contact their travelers and will need immediate access to this information. Finally, if an employee falls ill during a trip, employers will need the right insurance and a way to efficiently repatriate the individual.

Communicate with employees following the trip

After a traveler returns home, employers should have a documented process for employees to report any illness prior to returning to the office. If an employee returns from the trip feeling ill or with potential symptoms, employers should encourage them to seek medical assistance and/or quarantine.

After a traveler returns home, employers should have a documented process for employees to report any illness prior to returning to the office.

Stay on top of the requirements

At its core, business travel is a force for good. The restart of travel will accelerate the economic recovery needed to get the world moving again. Employers should be aware and mindful of the various government and supplier requirements, develop internal policies and procedures, and

partner with an experienced global TMC to support the end-to-end business travel experience for their travelers.

If an employee returns from the trip feeling ill or with potential symptoms, employers should encourage them to seek medical assistance and/or quarantine.

About the author

Prior to joining American Express GBT, **Michael F. Savicki** was senior attorney – compliance & corporate governance at Sikorsky Aircraft Corporation; secondee counsel at Deutsche Bank's Litigation and Regulatory Enforcement Group; and senior litigation associate at Fried, Frank, Harris, Shriver & Jacobson LLP. He began his legal career as a law clerk at the United States Second Circuit Court of Appeals. He is a graduate of Tulane Law School and Connecticut College and a member of the Connecticut, Massachusetts, and New York state bars. This article reflects his personal views.

Endnotes

1. Transportation Security Administration, "TSA screens over 1M passengers on a single day for the first time since March," news release, October 19, 2020, https://bit.ly/3lkWQVV.
2. Centers for Disease Control and Prevention, "Federal Government Adjusts COVID-19 Entry Strategy for International Air Passengers," news release, September 9, 2020, https://bit.ly/3lcQbxe.
3. U.S. departments of Transportation, Homeland Security, and Health & Human Services, *Runway to Recovery: The United States Framework for Airlines and Airports to Mitigate the Public Health Risks of Coronavirus*, July 2020, https://bit.ly/36j2gdV.

Takeaways

- Governments have responded to COVID-19 with various restrictions designed to stop the spread. These requirements continue to evolve.
- Considering the increase of air travelers passing through security checkpoints, companies should develop the end-to-end business travel experience for their travelers.
- Organizations' travel policies need to be regularly reviewed and updated to protect both the well-being of employees and their own corporate reputations.
- A documented internal approval process should be in place prior to booking and provide employees with up-to-date travel requirements, including border closures and quarantine measures.
- Employers should be mindful of their duty of care obligations and require travelers to book using the company's tools and policies for oversight purposes.

Operation Car Wash affects compliance programs

by Shin Jae Kim

Petrobras was under the spotlight of Operation Car Wash — an unprecedented corruption scandal in Brazil. Once a beloved Brazilian company, Petrobras suffered a big hit, and its market value reduced dramatically. Failures and weaknesses of its internal controls to prevent and detect ethical deviations became evident. To rebuild its reputation and market trust, Petrobras went through a transition phase and has been investing in the implementation of an effective corporate governance system and improvement of its compliance program.

Marcelo Zenkner, chief governance and compliance officer of Petrobras, told me that, in response to the facts disclosed in Operation Car Wash, Petrobras had to work fast to mitigate risks by creating a robust compliance system, which included new controls and procedures. This phase generated the perception by some of increased bureaucracy and loss of agility. In a second phase, the company moved to an effective integrity system, where compliance became instilled in every employee in the company.

Another initiative adopted by Petrobras is the third-party due diligence. This procedure scores third parties based on integrity risk or *Grau de Risco de Integridade* (GRI) and attributes low, medium, and high GRIs to potential suppliers. The result of this GRI assessment is used by Petrobras to select or ban third parties to participate in public tenders conducted by Petrobras. If a company is attributed with a high GRI score, the company is automatically blacklisted from participating in public tenders and cannot be selected as a Petrobras supplier. If this is the case, however, the company may still choose to present further information and evidence of its compliance program and/or remediation of red flags identified during the integrity due diligence to have its GRI score reviewed.

Recently, many companies have been seeking judicial measures against Petrobras' blacklisting as a result of a high GRI.[1] Courts (both judicial and administrative bodies)[2] have ruled both in favor of and against the GRI system adopted by Petrobras, but the matter has not been faced by Brazilian high courts, and it is too early to predict what will be the majority position in this regard. Certainly, this new procedure adopted by Petrobras will have a domino effect on its supply chain, particularly on the implementation of strong compliance programs.

Shin Jae Kim
CCEP, CCEP-I
(skim@tozzinifreire.com.br) is the head of the Compliance & Investigation practice at TozziniFreire Advogados in São Paulo, Brazil.

Endnotes

1. Robson Bonin, "Petrobras rejects contractors for 'high integrity risk,'" *Veja*, updated October 17, 2020, https://bit.ly/38D4gAn.
2. Valor Econômico, "Justice puts Petrobras Compliance in check," Meritum, October 24, 2018, https://bit.ly/3pjWG3A.

PROTECTING CORPORATE DATA IN THE WORK-FROM-HOME ERA

by Melody Haase

Melody Haase

(melody@4discovery.com) is the Head of Client Success at 4Discovery, a digital forensics firm based in Chicago.

/in/melodyannhaase

Work restrictions created by COVID-19 forced companies worldwide to quickly adopt technologies and fundamentally change the way they do business. In October 2020, McKinsey & Company released the results of a survey that showed companies exponentially adopted digital technologies to do business, and these same companies do not expect that to change.[1] However, in a rush to adopt new technologies during a crisis, companies were often focused on business continuity rather than security.

Security companies around the globe have reported increases in ransomware, data breaches via email, and unauthorized access of systems. Data breaches of all shapes and sizes can fundamentally impact a company's ability to do business and/or its reputation. Many articles about data security are focused on outrageous statistics and horror stories of businesses shutting their doors because of a security incident. Rather than focusing on scary statistics and costly solutions, this article will focus on general security concepts and some common things companies can do to enhance corporate data privacy during the work-from-home era. By the end of this article, readers will be better informed and more prepared to take the next steps to protect corporate data.

Understanding the threat landscape

Security threats can largely be placed into two categories: internal threats and external threats. Internal threats typically arise because of some sort of employee behavior, whether intentional or not. This can take many forms, such as an employee who becomes the victim of a phishing attack, a rogue employee who steals data, or an employee who carelessly leaves

sensitive files in an unsecured location. External threats are actors outside of the organization that are aimed at gaining access to corporate systems and data. Typically, they gain access to systems by leveraging poor security practices, malware, or exploits. Luckily, many of the tools used to thwart bad actors can be used to mitigate both internal and external threats.

Additionally, every company has different clients, employee bases, and thresholds for risk tolerance. This can affect how each company views security. There is an age-old debate in the security industry about security vs. convenience. For those promoting security, there is a push for more protections and steps to access systems. For those who promote convenience, there is a push for less security to make systems easier to access for the sake of business convenience. However, there are always implications to these decisions that may require companies to change the way they do business.

A great example of how to think about security vs. convenience is using the practice of blacklisting IP addresses by country. Blacklisting is the process of blocking items. In this context of IP addresses, it means that you can choose to block all IP addresses coming into your systems from hacking hotspots like Russia or China. If a company only does business inside of the United States and only has employees inside of the United States, it may be a feasible option to turn off the rest of the world's IP address range. However, it may be more complicated and less feasible for a global business to employ these same policies to reduce risk because it may affect its ability to provide system access to its customers and employees.

Physical security has drastically changed

Before COVID-19, companies were accustomed to all of the physical and environmental security in their facilities. Security cameras were online to monitor physical activities inside of locations. Badge access was required to enter buildings. Shredding boxes were placed around locations to ensure sensitive data was disposed of properly. Printers asked for passwords before printing to prevent the wrong person from picking up sensitive documents. Locked file cabinets were housed in offices to prevent access to sensitive files. Doors were placed on offices and conference rooms to prevent people from hearing confidential phone calls.

Work from home has completely upended the physical security environment. When COVID-19 hit, many individuals were not prepared to work from home. Many people did not even have workstations or desks. Many homes do not have security cameras or require badge access. Shredding, printers with password access, and locked file cabinets are likely not available. Spouses often share workspaces and hear each other's conversations. If the company is allowing Bring Your Own Device (BYOD), it also means that the computer being used for work may or may not have shared access between numerous individuals in the house. While companies may not be able to control this environment, they can, at a minimum, provide training to employees, as well as provide them with more secure ways to access systems.

Security requires a shift in mindset

In order for companies to transition traditional security practices to work from home, more emphasis must be placed on giving employees tools to be successful with their personal security, including training them on basic security practices. Many corporate security exercises contain information about and examples explaining what to do inside of an office and the corporate environment. However, this training typically does not include information on keeping data secure in an unsecured environment like a typical home setting.

Training should be changed to focus on the employee's home security practices and how they relate to corporate data security. Some items employees should be educated on are:

- Changing standard settings on routers and modems;
- Checking and strengthening security settings on their operating systems, web browsers, and other applications;
- Limiting the number of applications they install to prevent application-level security issues;
- Creating unique usernames and passwords for devices and accounts that house corporate data;
- Spotting phishing and malware attack threats that they may encounter;
- Protecting physical access to devices containing corporate data;
- Disposing of documents in line with corporate policies; and
- Reporting security incidents to the appropriate parties.

Employees should be reminded of security often. They must be reminded that they are constantly interacting with confidential

corporate data and should act accordingly. If the company has a corporate newsletter or bulletin, dedicating a portion of it to security practices can be extremely beneficial. It can help reinforce the items learned during training as well as provide employees updates about changes in the corporate security environment.

A primer on BYOD

At the beginning of COVID-19, many employees that typically worked in secure corporate environments were sent home to work on home computers, personal cell phones, and home networks. From a security standpoint, BYOD is not recommended. It is a great area of risk, and policies and practices related to BYOD are riddled with issues. There are simply too many variations on BYOD for an in-depth analysis in this article. However, because of BYOD's risk, it is necessary to stop and consider it as part of a general security plan.

These personal devices often have no form of mobile device management or data loss prevention software installed on them, both of which provide an extra layer of protection to corporate data and accounts by allowing corporate information technology (IT) to have some administrative oversight of the device and the data contained on the device. When companies allow individuals to use their own devices for work without any protections, the company ultimately loses control of that device and the data stored on it.

Because the employee owns the device and controls access to the device, it becomes complicated and can even become a legal battle to perform basic functions such as protecting data for litigation holds and retrieving data for internal investigations. Similarly, employees control security patches and have the ability to install whatever software they want. This can allow insecure devices to connect to corporate infrastructure and create additional security incidents. Most importantly, employees can commingle personal and professional data on any of their devices and accounts.

Often, BYOD policies, processes, and procedures do not require employees to sign a declaration certifying they have deleted corporate data from the device and/or their personal accounts upon the termination of their employment. This declaration is beneficial to collect in the event litigation for theft of corporate data needs to occur. At a minimum, every company should stop and consider its current BYOD practices, conduct a risk assessment regarding the safety and security of the data accessed by BYOD users, check if its policy is currently updated for COVID-19-related activities, and ensure the policy addresses how to retrieve and/or certify the destruction of corporate data at the end of the work-from-home period or upon termination of employment.

Security starts at the top

While the first part of this article focused on employees and the home environment, the major component of corporate security comes from within. Corporate security is best implemented, practiced, and enforced when it comes from the highest leadership levels. Communication about security and buy-in needs to happen at all levels of the organization to ensure that all security policies and practices are followed. How do you create a culture of security?

Start by conducting an assessment of your policies and procedures. Each of them needs to be updated to adjust for employees who are now potentially working in unsecured areas using unauthorized equipment and accounts. Simultaneously, the incident response playbook should be reviewed and updated to ensure parties still have a streamlined way to respond to incidents. Once updated, these policies and procedures should be redistributed to employees for review.

This should all be pushed out with an enhanced work-from-home training program as described above. Provide employees with common examples of security mistakes, how they affect the business, and how they could have been prevented with stronger security practices. These exercises do not need to be extravagant. Simply focus on the most important areas of data security for your organization.

A cycle of continuous security improvement

A security assessment of the organization's current technology environment needs to be conducted. Network infrastructure, individual devices, and online accounts all have potential security issues that need to be checked. At 4Discovery, most of the security incident response cases we have worked on thus far had a simple root cause, such as a security setting that was never changed when a system was implemented, a system that was unpatched, or reusing an administrator username and password throughout an entire infrastructure.

IT should constantly be in a cycle of continuous security improvement as a common course of practice. Below are some helpful practices to combat common weaknesses used by attackers to gain access to systems.

Take password protection seriously
One of the most common methods used in data breaches is password compromise. Ensure all default administrator usernames and passwords have been changed for off-the-shelf devices. Create unique administrative usernames and passwords for individual pieces of infrastructure. All accounts must require strong passwords that are long and use a variety of characters. Along those same lines, password changes should be mandatory on a routine basis to prevent any user credentials that may have appeared in past data breaches to be used to access systems.

Use multifactor authentication everywhere possible
Multifactor authentication (MFA) should be required for all accounts that have the option. MFA is the process by which a user needs at least two things to enter a system. Some commonly used forms of MFA are two-factor authentication text message codes, and hardware- or software-based tokens. While two-factor authentication text codes are not recommended as a best practice for MFA, simply having them in lieu of nothing adds an additional layer to account security.

Employ the POLP
Simply looking at all of the account settings in systems and evaluating them using the principle of least privilege (POLP) can help immensely when strengthening systems. POLP simply means that individual users only need, and thus should only have access to, the least amount of system access necessary to perform a task. Reducing people's access to systems and data limits the ability of bad actors to move throughout corporate systems using their accounts. It also hinders rogue employees who may attempt to access and exfiltrate confidential data.

Control all programs and settings
Use gold images and control the device from the start. Gold images are the standard settings and programs that are deployed on corporate assets. By using a gold image, IT can more quickly set up new machines while customizing settings to least privileges before deployment. When creating a standard, think about how much of the internet employees need to access. Do they need the ability to install software, and are they going to need to plug in USB devices? These are all common ways people exfiltrate data and attempt to cover their tracks. You can also combine this practice with POLP role-based permissions, common data loss prevention software, and/or device management solutions to maintain more control over the devices and data.

Interrogate and harden all default settings
Many systems and applications come with minimal security settings for the sake of convenience for the average user while sacrificing some security. This is done with the expectation that the user or administrator will strengthen the settings as necessary. This can be as simple as ensuring the firewall is not speaking to the entire internet, making applications ask for camera and microphone permission, and turning on logging and monitoring. The goal is to prevent bad actors from having easy access and provide IT with the tools they need to monitor attacks.

Individual users only need, and thus should only have access to, the least amount of system access necessary to perform a task.

Continuously update systems
Setting a routine software update schedule every week is crucial. As an example, WannaCry and other ransomware forms were able to spread throughout the globe because systems went without patches for over two months. Years later, many systems still had not applied the patch Microsoft issued in March of 2017.[2] If companies would have taken the proactive steps to fix their systems, the vulnerability would have been patched, and system access never would have occurred.

Encrypt traffic with a VPN
While an organization may not be able to control an employee's home router settings, it can provide a safe way for its

employees to access systems. Setting up a virtual private network (VPN) to route internet traffic from the machine to its destination will help prevent attackers from accessing unencrypted data in transit. This way, in the event there is an unsecure network connected to a corporate asset, there is an extra level of data protection.

Preparing for the inevitable

The fact of the matter is that every company will suffer data loss at some point. Once an incident occurs, it is important to respond and recover from the event in a timely fashion. Aside from having an up-to-date incident response playbook, the three most important things postincident are logging, backups, and insurance.

Often, systems have settings for logging that are turned off by default. By turning on logging, analysis can be performed on system access to understand how the system and data were accessed and/or exfiltrated. Because many incidents happen months prior to the time they were noticed, archiving logs before they age and roll off in the system can provide a historical library for later analysis.

Similarly, systems have settings for backups that are not enabled by default. Turn on backups and use the 3-2-1 backup rule. Keep at least three copies of your data, in two different mediums, with at least one of them kept off-site. Backups are critical in the event of attacks like ransomware, so they should also be routinely tested to ensure they are good backups. Having recent backups minimizes data loss and provides the capability to get systems back up and running in the wake of an attack. Along the same lines, make sure to take a forensic image or remove the hard drive from the computers of departed employees to preserve historical data.

Insurance is a great tool in risk mitigation related to security incidents. Generally, there are cyberliability, cyberinsurance, and business interruption policies that may apply to these events. Each policy covers different aspects of data loss. When speaking with your insurance carrier and counsel, make sure to ask about what is being covered by the policy and what duties you have under the policy. This way, you can see what other risks you may need to mitigate with your internal policies and procedures or an outside vendor.

There is no one-size-fits-all solution

This article's advice is meant to be a primer to help organizations understand the risks associated with data loss. It is ultimately up to each organization to decide what is best for its operations. Talk with your leadership, compliance, and IT teams to develop a solution that is the right fit for your organization.

Endnotes

1. Laura LaBerge, Clayton O'Toole, Jeremy Schneider, and Kate Smaje, *How COVID-19 has pushed companies over the technology tipping point—and transformed business forever*, McKinsey & Company, October 5, 2020, https://mck.co/3eCj17K.
2. Sean Gallagher, "WannaCry? Hundreds of US schools still haven't patched servers [Updated]," Ars Technica, May 21, 2019, https://bit.ly/3p462QM.

Takeaways

- Security practices must be shared, embraced, and followed by all.
- If it is in practice at your organization, stop to consider if Bring Your Own Device is still the right option.
- Aim for continuous improvement in your information technology department.
- Be prepared with logging, backups, and insurance.
- Choose the solutions that are right for your organization.

Age-appropriate design and privacy

by Robert Bond

In the European Union, children's data need to be processed in line with the General Data Protection Regulation (GDPR), and organizations that offer goods and services to children must now also take into account the Age Appropriate Design Code,[1] which has recently been published by the UK regulator, the Information Commissioner's Office. Children are considered to be all individuals under the age of 18.

The same rights and protections apply to children under the GDPR as apply to adults. However, extra care is needed here when fulfilling the data controller obligations, and different steps will have to be taken to ensure children obtain the correct level of protection. The code offers practical guidance on how to meet these obligations. The main tenets are:

- The controller must always keep the best interests of the child as the primary consideration when designing and developing online services likely to be accessed by a child.
- It is important to identify possible risks to children, which arise out of the processing, and to put in place mitigation to minimize those risks.
- Controllers must be clear, open, and honest with children about data processing.
- There must be no detrimental use of children's data.
- A risk-based approach must be taken to identify a user's age and ensure that the standards in the code are effectively applied to child users.
- Settings should be high privacy by default apart from in limited circumstances.
- Controllers should proactively ensure they are only collecting the minimum data possible and only share the data where there is a compelling reason to do so.
- Controllers should provide prominent and accessible tools to help children exercise their data protection rights.

What this means in terms of specific, practical steps:

1. **Data protection impact assessments**: Organizations that process children's data should consider the risks posed to these children. A data protection impact assessment is a useful tool for identifying risks and how to mitigate them.
2. **Transparency**: If the data controller knows that children visit its site, include a child-friendly privacy notice, which can be linked to the main privacy notice, that is written in simple language that a child of the average age would understand.
3. **Cookies**: As most children will just accept whatever default settings are provided, it is important that the defaults provide the child with adequate protection regarding the use of their personal data.
4. **Other rights (e.g., right of access, right of erasure)**: Children may need some extra assistance in taking advantage of these rights.

Robert Bond

(robert.bond@bristows.com) is Senior Counsel & Notary Public at Bristows LLP in London, UK.

Endnotes

1. Elizabeth Denham, "Age appropriate design: a code of practice for online services," Information Commissioner's Office, accessed November 4, 2020, https://bit.ly/3esxx1u.

RETHINK YOUR POLICY MANAGEMENT SYSTEM TO STRENGTHEN YOUR COMPLIANCE PROGRAM

by J. Veronica Xu

J. Veronica Xu
Esq., CHC, CHPC, CCEP
(veronica.xu@saberhealth.com) is the Chief Compliance Officer for Saber Healthcare Group headquartered in Cleveland, Ohio, USA.

"Mom, help! Where can I find the weekly schedule online?" "Mom, the portal doesn't work." "Mom, what's the difference between a 'private source' and a 'secondary source?'"

These are the questions I have been recently asked by my 10-year-old who is acclimating to doing schoolwork online, and I am sure this resonates with many parents facing similar pleas for help on a daily basis. As the nation is combating COVID-19, numerous schools have adjusted their teaching mode and moved everything online. As a result, parents or guardians have inevitably become teachers' assistants and technical support for their young children grappling with virtual learning.

Since the beginning of the pandemic, many things have changed in our lives, welcomed or not. Compliance's work is no exception. My son's questions prompted me to ponder: Do our employees know where to find policies and obtain information? Can our employees easily access our policy system when working remotely? Do they understand the content of the policies? Is our policy system ready for all the changes and challenges that the pandemic has brought forth?

Policies are an essential part of a compliance program. They are — by their inherent nature — meant to help guide employees in dealing with issues encountered in business operations to enhance safety, ensure quality, and reduce the number of incidents and violations of laws and regulations. In my opinion, as an integral component of a compliance program, policies are a triangular framework that consists of three basic elements: (1) a policy management and review process, (2) a policy library and database system, and (3) policy training and education (Figure 1). All three elements are closely correlated and ultimately affect the overall success of your policy implementation and level of compliance.

This article is intended to share some practical tips to help you and your team improve, communicate, and use your policy system as part

of your effort to strengthen your compliance program.

Element 1: Policy management and review process

First and foremost, a company must have policies. Governmental guidelines[1] and regulations have long established and highlighted the importance of policies and written standards for companies. As the very first element of a compliance program, policies play instrumental roles in structuring a company's business practices and ethical framework. In fact, they are the foundation of a company's operations, from employee attendance and anti-discrimination to personal protective equipment, donning and doffing procedures, and workplace safety. Here are some key factors to be considered in a policy management and review process.

Development of policies

- **Inventory and assessment of needs: Know what you have and need.** Create an inventory of the company's policies, and make a list of policies that are mandated by regulatory requirements and are significant to your company's operations. Institute the policies that are must-haves and retire those that are outdated or no longer pertinent. Avoid having a policy for everything because it is impractical and often causes an undue burden on the company to devote resources to maintain them.
- **Collaboration: Know who the subject matter expert is.** To effectively engage people and track progress, the compliance team can work with designated personnel (e.g., a policy director) or launch a task force consisting of representatives from key departments. Depending on the size of the company, you may consider forming a policy committee with clear delineation of duties.
- **Content: Know what is in your policies.** The devil is in the details, so the content of policies must be assessed to ensure its applicability, accuracy, and consistency with regulatory requirements and business needs. For instance, temperature taking and employee testing are now the mandatory safety measures in many industries, and thus should be reflected in the respective policies. Moreover, it is equally important to use concise language and keep the message brief. Policies are meant to provide guidance to employees in an effective manner rather than testing employees' academic levels or knowledge base. Therefore, simple and clear verbiage is preferred. It is not uncommon that companies hire lawyers to write their policies, but not all the readers can comprehend legal jargon like "prima facie" and "malfeasance." Also, avoid using abbreviations and acronyms, since not all employees, especially new hires, are familiar with the defined terms used among team members.
- **Format: Know what your policies look like.** Standardize the form and keep the format consistent to make it understandable. Policies should be published in a searchable format for easy reference. Policies are not marketing materials, although they can be. Rather, they address and identify risks; they are used as practical guides for employees who need an answer or solution to a situation. Simplicity is the key. The pragmatic value always outweighs a fancy format.

Review and management

Policy management plays a fundamental role in the long-term success of the company's business practices. Whether your organization uses spreadsheets, paper, or other basic methods, it is imperative that there is a process in place. It requires continuous attention, cross-functional collaboration, and a sustainable approach that focuses

Figure 1: The three elements of a compliance policy system

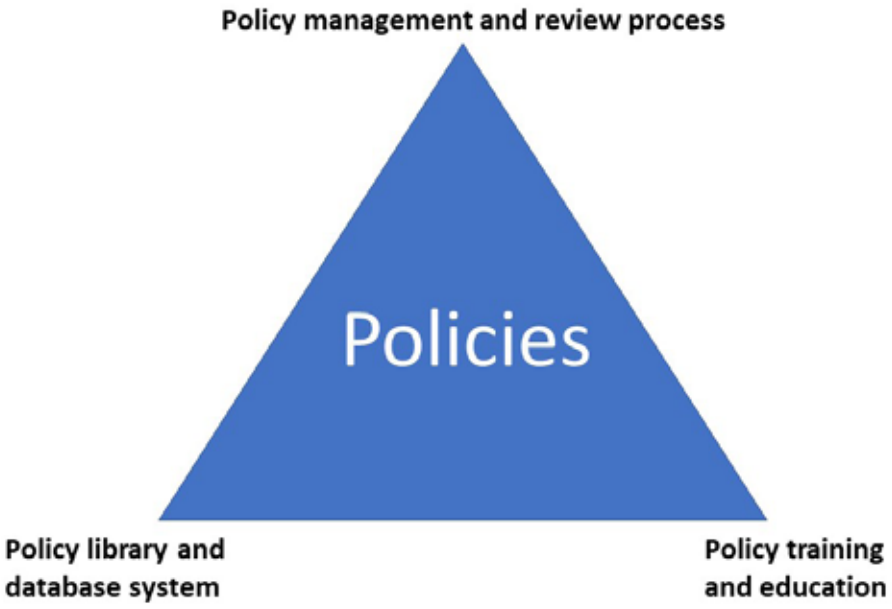


Table 1: Example of a table for managing policy review schedules.

Category*	Department	Responsible party (Name)	Due date/Annual review date
Workplace safety	Risk Management	Last name, first name	January 10th
Anti-discrimination, anti-harassment, and anti-retaliation	Human Resources	Last name, first name	February 10th
Conflict of interest and vendor relations	Purchasing and Procurement	Last name, first name	March 10th

** If the number of policies is limited, then each policy can be listed in the table above. However, if the number exceeds a certain limit (e.g., 500 policies or more), it may be infeasible to list every single policy in a table. Instead, categorizing them will be more efficient.*

on departmental contribution, buy-in, and teamwork. It takes an integrated approach to achieve the end goal. With diligent review and continual assessment, policies and management thereof can be enhanced, thus making compliance more dynamic, effective, vigorous, and engaging.

Develop an overarching framework. Mapping out the process and schedule — including categorizing policies and specifying the subject matter experts who will be responsible for reviewing their respective policies, due dates, and/or the policy review frequency — can be helpful for the compliance team to oversee and track progress. Regardless of whether your company uses a software program to conduct policy reviews, creating a review schedule can be beneficial, as it summarizes and highlights the major focus areas. It can be a simple table with particular policies in each month or quarter sorted by department or policy category (Table 1).

On the departmental level, each team can itemize all of their specific policies in their own documents. Unfortunately, policy review and management is that type of necessary ritual that is hard to maintain but easy to break. Creating a policy review schedule can help the policy owners internalize the process and truly make it a habit (Table 2).

Lastly, people tend to stop noticing things when they see them all the time, including policy reviews. To bring in new ideas and attain insightful input, try inviting a different person to read the policies. With a fresh set of eyes and different perspectives, you may receive an unexpected harvest. Also, inviting members of the workforce who are directly affected by the policies to participate in the review process and seeking their constructive feedback will be another way to assess and validate the clarity, intelligibility, and practicality of the policies.

Element 2: Policy library and database system

After the initial work of establishing policies, an organization needs to have a system where it can maintain and publicize them. Because certain industries are scrutinized more than others, such as healthcare and banking, the companies in those industries are notorious for routinely producing large binders of policies in order to keep up with the ever-changing rules and business environment.

The tricky part is this: In the midst of the pandemic, when employees are working remotely, how can a company effectively update its policies and make them available in a timely fashion? Printing everything out is a practice of yesterday. It has become imperative that each company, especially the ones with multiple office locations and branches across the region or worldwide, maintain a virtual policy library/database where people can access it without any geographic or time limitation.

When developing or evaluating a platform, we need to keep end users in mind (i.e., employees who access it on the front end and policy owners who need to track and maintain policies on the back end). Many other pieces, like online access, system integration, status tracking, and automatic notification, should also be taken into consideration. Whether you have developed a policy system, are shopping for one among a variety of options on the market, or are evaluating an existing system, these assessment questions should be asked.

Cost and budget

What is the cost of initial setup and annual upkeep? Since this is likely to be one of the critical deciding factors in whether the company chooses a particular platform — in-house or outsourced — having a general idea about the cost required (including time commitment, labor, technical upgrade, regular maintenance, etc.) to set up and maintain the virtual policy library and database system is helpful in allocating adequate resources and selecting appropriate tools.

How much is budgeted for this? You may need to examine the manpower and resources available for this project.

Format and platform

Are your policies saved on a shared drive? Are they managed by different departments in separate locations? Or are they published through an online portal? Do you use a software program to handle policies? From a practical standpoint, having numerous policies and saving them in scattered places will not only confuse employees but also cause major disruptions to business operations. Outdated versions could be used, or employees may not know about the existence of the policies at all. Keeping all of them in one centralized location can reduce confusion and frustration.

Is the system able to store archived policies? For reference or other various reasons, keeping a record of retired policies and archiving them is a common practice that many companies follow. Hence, the system's ability to archive retired policies is a huge plus, especially for record-keeping and litigation purposes.

System integrity and security

Does the system allow a number of administrators to have overarching control over the system to ensure the security and integrity of the system? What measures are implemented to prevent unauthorized users from changing settings or content of the policies? Like any other database, safeguards must be established to maintain the integrity of the policy library and database system.

Automation of the process

How does the system track reviews and revisions? Can automatic notifications and reminders be set up and sent to personnel responsible for the policy review? The system's ability to automate and streamline the process rather than requiring your team to manually triage and assign will certainly help the team overcome a big hurdle. It will add tremendous value to the system if it can track and evidence all policy development, review, revisions, and updates.

Accessibility and user-friendliness

Does it require user login credentials? Login credentials can be a double-edged sword. Depending on the industry your company is in and the labor force you have, you may or may not want to require login credentials. With a majority of the workforce working remotely, more than ever employees rely on policies for guidance. Easy access and user-friendliness of the system are also key to an effective policy system.

Can the policy library be easily accessed anywhere in the region where your business footprint reaches? Is there a limit on the number of concurrent users? Like everyone else, we all have experienced technical glitches at one time or another and shared the same frustration as my 10-year-old son. To avoid employees losing faith or patience in your system, establish a stable policy system.

Does the system have a strong key word search capability? More often than not, when employees are searching for a company policy, it is because they are facing a question that needs to be answered. It is highly unlikely that they would know the exact policy name. In fact, they may only have a term or phrase in mind relating to the question they are currently facing. Therefore, a robust search feature will be a big help.

Just because the compliance team is not physically in the office does not mean the compliance work stops. Making policies easily accessible to employees is one of the effective ways to promote compliance. While some changes may be temporary, others may become permanent. An online policy library/database that employees can easily access will likely stick around.

Since each company's line of business and its compliance team's approach vary, there is no one-size-fits-all solution. But, hopefully, the aforementioned factors can assist you with developing, selecting, or evaluating a suitable system for your company.

Table 2: Example of a department-specific table for managing policy review schedules.

Policy name (Compliance policy)	Responsible party (Name)	Month of review
Code of conduct	Last name, first name	January
Hotline policy	Last name, first name	February
HIPAA privacy policy	Last name, first name	March

Element 3: Training and education on policies

Establishing policies and maintaining them are just the first two steps leading to a lasting and effective policy program. Today's risk landscape is more uncertain and perplexing than ever, regardless of the industry you are in. Given new regulations like data privacy laws, bribery and anti-corruption rules,

and many others, our employees are being tested, overwhelmed, and exhausted by every new risk lurking around every corner. As a major pillar, policies provide guiding principles to employees, but if employees do not know about the policies and tools that the company has devised, they can't use them. Training and educating employees on the policies is often a missing link. Laws and regulations provide that companies must take steps "to effectively communicate the standards, policies, and procedures" to the entire workforce.[2] Without proper training and guidance, employees would be drowned in an ocean of risk that would gain in velocity and ferocity with no relief in sight.

Training for the workforce

Knowledge is power. The more employees know about the policies and system, the more they tend to use them. Helping employees find the answers they need via effective tools and resources can considerably reduce the company's exposure to disputes, lawsuits, and sanctions. Below are some ideas for your reference.

- Develop a cheat sheet or reference guide for the workforce that lists the link(s) to major policies and the contact information of responsible parties.
- Provide periodic training on policies to raise employees' awareness, highlight available resources, and demonstrate the company's commitment to compliance.
- Incorporate policy information into routine conference calls and virtual meetings.

Training for policy owners

It is vital for policy owners to understand the policies' importance and the review thereof, so it is highly recommended that your company conduct periodic training on regulatory changes and business updates to keep policy owners abreast of the processes and procedures in place.

Training is not about educating alone; rather, it is also a way of communicating messages. We want employees to know that no matter what our new normal may look like, the compliance team is here to help and support them. One of the ways to achieve it is to make policies readily available and easily accessible to employees when they need them.

Take this opportunity

Change always pushes us to think, act, evaluate, and re-think. In the wake of COVID-19 and in our new working world, compliance will need to reassess its strategic approach, redesign processes, revamp measures, remind employees of the company policies, and reiterate the company's commitment to compliance. Policy management is one of the steps we take, and it is crucial to a successful business operation as well as an effective compliance program. The development, review, management, implementation, and communication of the policies will not only ensure your company is compliant with regulatory requirements that mandate a sound policy system be maintained, but they will also help cultivate a corporate culture of compliance that leads the company to achieve its objectives by mitigating risks. CEP

Endnotes

1. "Compliance Guidance," Department of Health & Human Services, Office of Inspector General, accessed November 4, 2020, https://bit.ly/34FpMR2.
2. 42 C.F.R. § 483.85.

Takeaways

- Policies are a triangular framework that consists of three elements: (1) a policy management and review process, (2) a policy library and database system, and (3) policy training.
- Policy management plays a fundamental role in structuring a company's business practices and ethical framework, so it is essential to the company's long-term success.
- Policy management requires continuous attention, cross-functional collaboration, and a sustainable approach that focuses on departmental contribution, buy-in, and teamwork.
- Making policies easily accessible to employees is one of the effective ways to promote compliance.
- Establishing policies and maintaining them are the first two steps leading to a lasting and effective policy program; training on policies is also crucial.

Are you policing your way to a better culture?

by Nick Gallo and Gio Gallo

Welcome to the first installment of "Culture is all of our business"!

We are each responsible for not only the objective actions we take but also the subjective impressions that our actions, communications, and influence leave with the employees around us. Unfortunately, years of focus on policy enforcement and behavior prevention have left many of us fighting an impression that ethics gets in the way of business. Regardless of your definition of culture,[1] the culture of each division and behavior of each employee likely have a large impact on the whole organization. So consider the tone, approach, and focus of the compliance team that *are* in your control!

Ask how your efforts may feel solely like policing:

- How focused are you on "*polic*"-ies? They are, of course, essential! But do employees see the other side of you?
- Do employees primarily see your team as enforcing, restricting, and getting people in trouble?
- Do employees with "nothing to hide" anticipate a positive interaction when they see a calendar invite or email from compliance?

Consider what you expect in a police state: Proscribed behaviors, erratic enforcement, stiff consequences, and a reactionary black market. Now look for ways you can balance the culture of enforcement with the impression that you're helping the whole company achieve its mission:

- Learn about the perceptions that employees have of your activities. Tweak them without renovating the whole program (e.g., swap out a vendor, launch existing programs differently).
- Become a student of culture and leadership. Build a strong, cohesive team within your department that can shift the tone (e.g., celebrate wins, recognize positive behavior, and formally define your culture).
- It's not enough to say "someone requires this so you must do it," so treat required behaviors as if they are optional (in the spirit of behavioral economics[2]), and *influence* people to comply before they're threatened. Contextualize your efforts and the reasons behind them. Localize training, policies, and enforcement to subcultures (e.g., location, division).
- Ask for help from your compliance and ethics peers and colleagues in different divisions. It's a great way to build relationships, get ideas, and strengthen your own brand.

Stay tuned for more discussions about the potential for growth as you build on the objective expertise you have in compliance to truly transform your workplace into a more fair, safe, and thriving place to live and work — through the power of culture!

Nick Gallo

Gio Gallo

Nick Gallo *(ngallo@complianceline.com) and* ***Gio Gallo*** *(ggallo@complianceline.com) are Co-CEOs of ComplianceLine and lifelong students of healthy workplace cultures, based in Charlotte, North Carolina, USA.*

Endnotes

1. "Workplace Culture," The Great Game of Business, accessed November 4, 2020, https://bit.ly/36jafI7.
2. Dan Ariely, "Column: You Are What You Measure," *Harvard Business Review*, June 2010, https://bit.ly/3euqzZZ.

BALANCING EFFECTIVE COMPLIANCE POLICIES AGAINST THE UBIQUITY OF EPHEMERAL MESSAGING

by Daniel J. Polatsek

Daniel J. Polatsek

(daniel.polatsek@icemiller.com) is a Chicago-based partner in Ice Miller's White Collar Defense and Investigations Groups, where he oversees internal investigations and handles sensitive corporate governance and litigation matters for both public and private companies.

As we enter into the first quarter of 2021, the available evidence indicates that remote work is going to remain part of the work-life balance for much of this year. The US workforce continues to face unexpected pay cuts, furloughs, and layoffs, while senior executive teams and upper management face pressures to meet revenue expectations and budgeted projections for both shareholders and Wall Street.

For many companies, these economic pressures require reductions in force, consolidating greater authority within a smaller workforce and executives who have less time to supervise and approve operational decisions. The dilemma now is how the private sector responds to the challenge of having to do more with less but just as fast.

The answer, in part, is better, faster, and more secure communication platforms, but the technologies that make speed and efficiency possible, such as ephemeral messaging (i.e., mobile-to-mobile transmissions that are designed to self-delete from the recipient's screen after the message has been viewed) and employee use of personal devices for business, raise complicated issues for compliance departments seeking to manage risk without overmanaging business solutions that allow companies to stay productive.

Compliance programs in the pandemic

Over the past year, the Department of Justice has made clear that the pandemic will not excuse a substandard compliance infrastructure.[1] Companies are still required to tailor compliance programs designed to prevent, detect, and remediate unlawful conduct. This was most recently discussed in the virtual town hall held by representatives of the Department of Justice, the Securities and Exchange Commission, and the Federal Bureau of Investigation on May 20, 2020. These agencies made clear that while the pandemic is a challenging environment for compliance programs, the pandemic is not a defense to inadequate compliance protocols resulting in unlawful conduct.[2] Following the virtual town hall this past May, the Department of Justice also issued its updated *Evaluation of Corporate Compliance Programs* guidance in June 2020.[3] The guidance touched upon several different factors necessary for an effective compliance program. One key takeaway was that an organization's compliance program must be rationally tailored to the risks inherent to that organization's business operations. Put another way, *how and why* a company designed its compliance program can be an important factor in whether the company is afforded leniency

later by a regulator if one or more of its employees is involved in unlawful conduct.

The necessity of internal investigations

If the past is prologue, companies will continue to have to investigate civil and criminal conduct such as conflict of interest schemes, trade secret misappropriation, public corruption, price fixing, embezzlement, and insider trading, to name a few. Each scheme dictates its own appropriate investigatory methodology and constituent audiences, but the objectives remain the same: stop potential unlawful conduct, understand the nature and extent of the unlawful conduct, lawfully mitigate the legal and business risks arising from the unlawful conduct, and prevent the same or similar unlawful conduct from reoccurring. Meeting the foregoing objectives during an internal investigation is accomplished through an examination of the available evidence that generally hails from two sources: (1) witness interviews and (2) documentary evidence (i.e., electronic and hard-copy documents and communications). When witnesses cannot or will not fill in the details of a fraud scheme or other unlawful conduct, transactional records, hard-copy documents, and electronic communications are critical to filling in the information gaps.

Those overseeing an internal investigation, such as in-house counsel, audit committees, boards of directors, and other authorized stakeholders, must frequently assess whether the current circumstances warrant voluntary disclosure of the conduct being investigated to a regulator. Among other important considerations is whether a company's voluntary disclosure would allow it to seek leniency; cooperation credit; or, in a best case scenario, avoid any adverse consequence all together. The extent to which a company may be extended leniency within the context of a voluntary disclosure can be linked, in part, to its own root cause analysis of the underlying unlawful conduct. In other words, the degree to which leniency is extended to a company may be contingent on the company's efforts to understand the who, what, where, when, and how behind the unlawful conduct being investigated. Stated differently, corporate leniency extended by a regulator may be measured, in part, by how much a company can inform the government about what happened.

Once a voluntary disclosure is made and leniency is sought through cooperation credit or another avenue, it should be anticipated that a company's compliance program will be evaluated with respect to its capabilities to prevent and detect unlawful conduct through its preexisting compliance policies. Because ephemeral messaging is quickly becoming an integral part of how employees in corporate America communicate, companies can expect regulators to inquire about ephemeral messaging, the compliance policies underlying its use, and the policies underlying its preservation and collection during an investigation.

Challenges posed by ephemeral messaging

Although there are several different forms of ephemeral messaging that appear on social media and work-related platforms (e.g., Snapchat, WhatsApp, Wickr), the common denominator to all of these applications is the self-delete function after the communication is opened and read by the recipient. Because these communications are designed to be peer-to-peer communications, they generally do not travel through employer servers and are oftentimes encrypted, making the recovery of these communications by a private employer extraordinarily difficult if not impossible without prior protocols in place.

The value to ephemeral messaging is found in its speed, efficiency, and security. Unlike email, ephemeral messaging is very similar to having a brief in-person conversation that allows you to get to the point quickly and avoids the exchange of time-consuming formalities of an in-person conversation. Ephemeral messaging also allows the sender to entertain multiple different conversations at once. Another benefit to ephemeral messaging is the security found in its end-to-end encryption, which is useful when sensitive, proprietary, or other confidential business information must be discussed in real time. It is also attractive given the proclivity of malware, ransomware, and other types of data breaches targeting the private sector.

But the very same things that make ephemeral messaging an attractive form of communication can become critical gaps in a company's compliance infrastructure. Specifically, ephemeral messaging is a particularly good tool for concealing unlawful conduct because it is exceptionally difficult to monitor or recover these communications. As a result, should ephemeral messaging serve as the primary form of communication in perpetrating an unlawful activity, it is possible that, without the right protections, a thorough internal investigation and root cause analysis cannot be adequately performed — meaning, potentially unlawful conduct cannot

be remediated as quickly or as fully as it may have otherwise been — and this compliance gap could potentially interfere with the degree of leniency or cooperation credit granted to a company by a regulator when a voluntary disclosure is made. Depending on the size and scale of the unlawful conduct at issue, the consequences could be very impactful.

In *A Resource Guide to the U.S. Foreign Corrupt Practices Act, Second Edition*, the Department of Justice states part of obtaining leniency for the commission of unlawful conduct involving violations of the Foreign Corrupt Practices Act (FCPA) must include a thorough analysis of causes of the underlying unlawful conduct with a goal of timely and appropriately remediating those causes to prevent similar misconduct from occurring again.[4] It is also expressly stated that companies seeking leniency for FCPA violations must implement appropriate guidance and controls on the use of ephemeral messaging applications that could undermine a company's ability to retain business records or communications or otherwise comply with the company's document retention policies or legal obligations. While not as explicit in its policy pronouncements, the Antitrust Division of the Department of Justice has made it clear that it will be looking at whether a company's compliance policies are designed to address not only the technical changes regarding a company's business operations, but whether its compliance policies are also designed to address new methods of electronic communications that are being used and if those methods increase the risk of antitrust violations or undermine preexisting compliance policies.

What the foregoing makes clear is that there is an expectation from at least some divisions within the Department of Justice that compliance policies should be proactively managing the risks technologies like ephemeral messaging pose, such that its use will not allow it to be used to exploit unlawful purposes or unduly interfere with a company's ability to perform an adequate root cause analysis. A fair inference from the foregoing is that regulators will view ephemeral messaging as business records similar to other communications or documents that must be maintained, preserved, or recovered as part of an internal investigation or response to a grand jury subpoena.

Companies that support the widespread use of ephemeral messaging but do not take proactive steps to address or mitigate the risks in employing this communication platform may be viewed skeptically or, in a worst case scenario, willfully blind if the failure to address this type of communication platform is conspicuously absent. This would seem particularly true for companies where bid rigging, bribery, price fixing, or FCPA violations are a concern.

Compliance options

Because the potential consequences of serious unlawful conduct can be transformational with respect to stakeholder relationships, reputation, and civil and criminal enforcement, it makes sense for compliance departments to address the use of ephemeral messaging head-on. A starting point can be the rapport between compliance personnel and senior management. Understanding how and why ephemeral messaging is used and by whom within the organization will illustrate why it is important and where the greatest risks lie. Memorializing this internal risk assessment can explain how and why certain decisions were made about the compliance policies governing the permissible uses of ephemeral messaging. Put another way, a company can set forth the basis of the business justification for using ephemeral messaging and why its use makes sense within the context of the risks it poses to a compliance program.

For example, access to ephemeral messaging might have a number of valid business reasons for a manufacturer with international clients, but where outside consultants or other third-party intermediaries are used internationally or where foreign governmental approval is required, such use of ephemeral messaging would warrant careful scrutiny. Therefore, with respect to ephemeral messaging, compliance programs can provide guidance on:

- The types of information that can and cannot be transmitted through ephemeral messaging.
- Which persons within the company are specifically authorized to use ephemeral messaging and those who are not, and
- The types of work-related communications that are prohibited for this communication platform.

Consideration can also be given to tailoring in-person training and/or narrowly tailored Webex module training to ensure each individual authorized to use ephemeral messaging does so in a manner consistent with company policy. In this way, ephemeral messaging is not unlike other important compliance policies governing the receipt or use of gratuities, reimbursable business development expenses, and appropriate political contributions.

On an enterprise level, the compliance department can partner with the information technology

department to understand available options that allow internal ephemeral messaging without sacrificing record retention. At a minimum, this partnership can develop internal protocols to suspend the use of ephemeral messaging in the event unlawful conduct is discovered, investigated, or must be voluntarily disclosed to law enforcement. Litigation hold notices should also explain how a litigation hold affects individual use of ephemeral messaging.

Other controls can include policies that prohibit using ephemeral messaging with external business partners or using software that allows only company-sanctioned ephemeral messaging applications to be downloaded on employer-issued mobile devices or computers.

Unique challenges of personal mobile devices

Companies should anticipate that employees will use their personal mobile devices for work, which includes the use of ephemeral messaging. As a result, guidance on what applications and what content are permissible for conducting work-related communications on a personal mobile device should be given similar to that of other company policies governing the use of ephemeral messaging. Where company-issued mobile devices are issued to employees, companies can install mobile management software for monitoring employee communications and publish an express list of prohibited applications that cannot be used to conduct company business.

Because personal mobile devices contain both personal information and business-related communications, they can be particularly vexing from a compliance standpoint. Therefore, companies are well advised to have an express policy mandating employees read, certify, and consent to a policy that includes some or all of the following:

- If company business is conducted on a personal mobile device, an employee cannot later deny that employer access to the business-related data stored on that device.
- That the employee understands they have no expectation of privacy in the work-related content on a personal mobile device.
- That the employee further agrees that the user's work-related content may be monitored, reviewed, copied, and disclosed without the consent or approval of the employee at the employer's discretion.

This same message should be reiterated in the company employee handbook and, where required, posted on internal bulletin boards.

Ensure your program is taking ephemeral messing into account

While not easy, compliance solutions exist for navigating the use of ephemeral messaging and the use of personal devices in a remote work environment. Even in a remote work environment, during an extended pandemic, be proactive in understanding how and why ephemeral messaging is needed and used, and the unique risks to the company. CEP

The opinions expressed are those of the author alone and do not reflect the view of the Ice Miller LLP. This article is for general information purposes only and is not intended to be and should not be taken as legal advice.

Endnotes

1. U.S. Dep't of Justice, Criminal Div., *Evaluation of Corporate Compliance Programs* (Updated June 2020), http://bit.ly/2Z2Dp8R.
2. Timothy D. Belevetz, Guillermo Christensen, Daniel Polatsek, and Meredith Wood, "DOJ, SEC & FBI Host Virtual Town Hall on Foreign Bribery and Health Care Fraud Enforcement," Ice Miller, May 21, 2020, https://bit.ly/32u6Btx.
3. U.S. Dep't of Justice, Criminal Div., *Evaluation of Corporate Compliance Programs*.
4. U.S. Dep't of Justice and the Enforcement Div. of the U.S. Securities and Exchange Comm'n, *Resource Guide to the U.S. Foreign Corrupt Practices Act, Second Edition*, July 2020, https://bit.ly/2FBw5g7.

Takeaways

- Communication between compliance personnel and management should be established to assess the utility and risk of the use of ephemeral messaging and personal mobile devices.
- Internally memorialize the business justification for using ephemeral messaging and personal mobile devices within the context of the risks.
- In-person and webinar training on the permissible and prohibited uses of ephemeral messaging and personal mobile devices for company business should be considered.
- Compliance departments should partner with information technology to understand the capabilities of its own record retention and ability to suspend ephemeral messaging for an investigation.
- Companies should have an express privacy policy mandating employees' consent to the company's monitoring and collection of ephemeral messages and company communications on personal devices.

Compliance Resources

ON DEMAND

Whether you are looking for analysis of the last regulatory updates, or guidance on how to improve your compliance program – COSMOS search can help. Search across our growing archives of member magazines, newsletters, books, conference presentations, and session recordings to provide the trusted answers you need – when you need them most.

COSMOS®
Navigate the Compliance Universe

compliancecosmos.org

SCCE®
Society of Corporate Compliance and Ethics

Reassessing your professional purpose

by Walter E. Johnson

"Appreciate where you are in your journey, even if it's not where you want to be. Every season serves a purpose." – Author unknown

Many compliance and ethics practitioners are trying to navigate life, career, and our evolving profession. Our journey is a rewarding one, accompanied with challenges to help us face the next experience.[1] My dad used to say, "If you don't learn the lessons of each experience, you may find yourself repeating them until you do." He also used to say that these three questions will help you know if you are on the right track.

Why are you here?

This question is applicable to almost any scenario, point, and time. When applied to career, authors Paul Tieger and Barbara Barron-Tieger of *Do What You Are*[2] state that you are on the right track when you experience the following:

- Looking forward to going to work,
- Feeling often energized by what you do,
- Feeling like your contribution is respected and appreciated,
- Feeling proud when describing your work to others,
- Enjoying and respecting the people you work with, and
- Feeling optimistic about your future.

Whom are you seeking?

This question is about the audience. Our profession has multiple audiences, including customers, patients, regulators, sales representatives, shop managers, analysts, and more. Each relationship requires different delivery and engagement. You must know:

- Who your audience is,
- What to communicate to them,
- When to communicate to them,
- Where to reach your audience, and
- How to communicate to them.

What are you expecting?

This question is about influence and is interdependent with the previous question. Desired results are earned, and the key components of a person who can effectively influence their audience include the ability to *model* integrity, *motivate* others through respect and positive feedback, *mentor* others to believe in themselves and overcome challenges, and *multiply* or produce more leaders and expected results.[3]

With so much uncertainty around us, purpose may be easily forgotten or lost. For those who are trying to find their purpose, maybe now is the ideal time.

Walter E. Johnson
CCEP, CCEP-I, CHC, CHPC
(walter.johnson@inova.org) is Assistant Privacy Officer at Inova in Falls Church, Virginia and an Adjunct Professor of Business Ethics at University of Maryland Global Campus (UMGC).

The author's expressed views are his own and do not necessarily represent the views of Inova and UMGC.

Endnotes

1. Rick Warren, *The Purpose Driven Life: What on Earth Am I Here For?* (Grand Rapids: Zondervan, 2002).
2. Paul D. Tieger and Barbara Barron-Tieger, *Do What You Are: Discover the Perfect Career for You Through the Secrets of Personality Type* (New York: Little, Brown and Company, 1992).
3. John C. Maxwell and Jim Dornan, *Becoming a Person of Influence: How to Positively Impact the Lives of Others* (Nashville: HarperCollins Leadership, 1997).

ENGAGE WITH YOUR MARKETING TEAM TO AVOID INFLUENCER MARKETING RISKS

by Caroline Franco

Caroline Franco

is Ethics and Compliance Manager in the European Regional Operating Unit of Boehringer Ingelheim in Amsterdam.

/in/carolinefranco1

With the increasing threats of banner blindness and ad blockers, influencer marketing has been constantly on the rise and has established itself across all industries. This marketing technique enables companies to collaborate with individuals with specialized knowledge, expertise, authority, and/or reach on social media by leveraging their unique voice and message-delivery styles. These individuals — called influencers — insert brands or products in their social media posts to initiate electronic word-of-mouth engagement with a tuned-in audience — their followers.

Harvard Business School predicts marketers to spend $15 billion on this method by 2022,[1] which means that influencer marketing commences to preempt traditional advertising budgets. However, influencer marketing poses regulatory and reputational risks and has the potential to hurt the core values of your organization. It is therefore time for the compliance profession to help our organizations navigate through the ethics and compliance risks. In this article, I will walk through the differences between influencer marketing and more traditional techniques while focusing on content management, remunerations, disclosure requirements, and crisis management.

But first... what is so special about influencer marketing?

The concept of leveraging someone outside a company or a fictional character to endorse a brand is nothing new. Back in the 20th century, Coca-Cola used Santa Claus to endorse its drinks; Tony the Tiger endorsed Kellogg's cereals. Later on, brands leveraged celebrities. For example, Pepsi partnered with Michael Jackson.

While these characters might not have been called influencers at the time, their use had and still has the same objective: emotionally drive the buying decision process through the buyer's connection with the influencer.

Influencer marketing on social media, however, has different characteristics. The striking difference is that influencers established themselves on social media thanks to their content. They created their own "brand" via their posts, and companies need to find a way to organically and authentically fit into their feed. In addition, most influencers reserve the right to post in their own words and tone about brands or products, commonly referred to as their "voice." This involves the creation of a great deal of intellectual property, such as posts, pictures, images, words, and influencers' name and image to name a few. This specific aspect of influencer marketing calls for tailored contracts or terms of service agreements.

In addition to the posts, influencers have a constant and real-time dialogue or "engagement" with their followers via comments on posts and direct messages. Capturing engagement becomes crucial to understand customers and even follow up directly with them. Many companies push, for example, paid ads on the social media accounts of individuals who like or comment on influencers' posts related to their campaigns. However, capturing engagement raises many questions: Does the influencer or the marketer own the data related to the campaign? Given privacy laws, can the data be shared freely with marketers? Does the European Union's General Data Protection Regulation, the California Consumer Privacy Act, and other privacy laws apply? Does it depend on the country of the company or the country of the influencer? How about of the country of the follower?

To address these questions, we need to lead ethical and compliance discussions with our marketers to understand their campaigns and establish processes and controls. How these elements are set up and negotiated could ultimately affect the value of campaigns. All that said, it is impossible to understand the value of such campaigns without speaking about the costs associated.

How much do influencers cost?

Google this question and you will not be short of resources and companies providing you with numbers. Most of them base their compensation grids on benchmarking data and propose two models: paying per post or per followers' engagement. While both methods have their pros and cons, ethically, our profession should question these payments and their validity.

I'm not saying that influencers shouldn't be compensated fairly for their work: It takes time and effort to develop carefully curated accounts, but paying individuals might not always be needed or result in good press. Take the recent example of the city of Philadelphia in the United States. The city council paid influencers to post about staying home and washing hands during the COVID-19 pandemic.[2] This resulted in discussions about the use of public funding on this tactic and if these dollars could have been better suited on other public services.

Another risk of such campaigns could be that the influencers' opinions become void when the public finds out how much they were paid and ends up undermining the brand. These discussions are triggered mostly when compensation is disclosed to the public. Currently, this does not happen frequently. However, in some countries, it does more and more through scandals or via authorities' decisions. For instance, in December 2019, France published a new decree requiring pharmaceutical, generic drug, and medical device companies to disclose any payments made to French social media influencers.[3] While this might seem isolated, other countries are debating similar regulations. Therefore, it is recommended to proactively have these compensation discussions with marketing colleagues to plan for the future.

Best practice suggests companies communicate disclosure expectations with the influencers either via training and/or contracts.

Disclosure requirements

Since the beginning of influencer marketing, regulators have tried to increase transparency and educate consumers. As ethics professionals,

we can only agree this is necessary. One way is to make public disclosure of payments to influencers, as was done in France. This has substantial effects on privacy and is not required in most countries. Instead, authorities have focused mostly on disclosing the relationship only. This disclosure is incumbent on the influencer and the brand; however, influencers might not always be up to date with legal requirements. Best practice suggests companies communicate disclosure expectations with the influencers either via training and/or contracts. UK[4] and US[5] authorities have developed infographics to help share these requirements in layman's terms. However, in practice, this is more complicated. How can we ensure that influencers who, most of the time, want to create their own content do this disclosure appropriately? For example, in 2017, the German drugstore Rossmann was convicted by the Higher Regional Court in Germany for not properly identifying that content was sponsored.[6] Rossmann's posts were marked with the hashtag "#ad," but the Court ruled that it was not clear enough, as #ad was only in second place out of six hashtags.

The first step to successfully and legally work with influencers is to train employees on which relationships should be disclosed: not only monetary relationships (including in-kind compensation, such as free products and employment) but also personal and family relationships. In addition, it is important to explain how to disclose these relationships. Authorities worldwide focus on the fact that the disclosure should be precise and hard to misinterpret. Accordingly, it is recommended to stay away from vague terms like "sp" (sponsored), "collab" (collaboration), or stand-alone terms like "thanks" or "ambassador."

The good news is that social media platforms are adjusting to disclosure requirements. They are helping influencers and brands to disclose their relationships via new features. Recently, Instagram developed a feature where the text "paid partnership with..." can appear in the influencer's stories. This caption is translated in the user's language preferences to ensure comprehension. Therefore, ask your marketing colleagues to keep a close eye on these developments and to inform you. This way it is possible to keep your contracts, training, and briefing documents up to date with the latest transparency requirements.

Let's not forget about basic advertising rules

Even though influencer marketing has its own regulatory environment, basic advertising laws also apply to online content. As an ethics and compliance manager in the pharmaceutical industry, I undoubtedly dedicate a considerable amount of time to this topic. One the most well-known controversial posts in my industry was back in 2015. Kim Kardashian posted about a prescription morning sickness pill without listing the side effects and safety information required by the U.S. Food and Drug Administration.[7] However, looking back, one might wonder how we can expect influencers to know specific laws for advertising.

The answer is not straightforward and missteps keep happening. For example, in April 2020, the manufacturer of detox tea, Teami LLC, agreed to

settle a lawsuit for $15.2 million (the amount of the total sales of the products) due to unsubstantiated claims and failure to disclose connections between influencers and the company.[8] At the same time, the 10 influencers involved in the campaign received letters from the Federal Trade Commission.[9] The Federal Trade Commission regulates numerous topics across sponsored content in the US. This example demonstrates that, in this situation, both traditional advertising and social media rules were breached.

To minimize risks, the most common and risk-averse practice includes a review of the post internally prior to it being released publicly. This can cause delays in the campaign and inhibit the real-time communication of social media but will help ensure compliance with regulations. While influencers might easily accept this review for the initial post, it might be very difficult to convince them on the same process for their replies in the comment section of their channels. Therefore, training the influencer on rules incumbent to your industry is highly recommended. In addition, monitoring posts and answers, in accordance with privacy laws, may help you mitigate the risks associated with your industry.

Are all the risks only regulatory?

Absolutely not! Influencer marketing can easily lead a company to a public relations nightmare. Enlisting influencers means attaching the company's name to the influencer and vice versa. While this might not have big impacts when using the image of a fictional character like Santa Claus or a tiger, these types of partnerships might look like the company endorses the values of the influencer. One can easily understand how this brand's association might lead to unfavorable marketing if the influencer does something publicly that reflects poorly on the brand — especially if the marketing campaign is running.

Compliance programs should therefore be able to prevent potential crises. This starts with the process of selecting and hiring influencers. We must collaborate with our marketing colleagues to establish a specific due diligence process. Questions should be different from the traditional due diligence process for vendors and might include:

- Do they have a history of not adequately disclosing relationships with brands?
- Do they disclose their remunerations publicly?
- Has the influencer posted offensive texts, images, or videos in the past (e.g., sexist, racist)?

These background checks might help your brand avoid hiring someone with a highly controversial online history. These will not protect you against future actions of your influencers but will give you a good picture of the person. In addition, contracts can include very strong morals clauses and the ability to exit quickly if necessary.

On top of these protective measures, training the teams to understand the reputational risks associated is fundamental. Best practices suggest having high-risk trainings for high-profile employees. This is because these high-profile employees can be viewed as brand ambassadors or influencers without understanding it. A recent example of this lack of awareness happened in March 2020, when the chief executive of Harrods in the UK appeared in a TikTok video on his daughter's account pretending to cough and struggle to breath due to COVID-19.[10] The bad press coming from this incident reflected poorly on Harrods' business.

It is imperative to define a way to monitor and listen to what is happening on social media with your influencers. Many platforms exist that screen for words in public posts and provide you with trends. This becomes essential to proactively identify a crisis. Finally, having an at-the-ready crisis management plan will ease the hardest situations.

Monitoring posts and answers, in accordance with privacy laws, may help you mitigate the risks associated with your industry.

Continue the dialogue with marketing

Influencer marketing can boost a company's message and increase sales. It is an exciting marketing technique that requires a level of compliance to be built into the program approval process. If this is overlooked, it can result in regulatory and reputational

damages, and also hurt the core values of your organization.

Although this article focused mostly on how to address risks within the ethics and compliance department, I urge you to secure a continuous dialogue with your marketing colleagues to understand the latest trends in their techniques. Staying close to your teams is crucial to continuously revisit your program and ensure your companies are well equipped to manage the associated risks.

Endnotes

1. Jill J. Avery and Ayelet Israeli, "Influencer Marketing," *Harvard Business School Technical Note*, 520-075, March 2020, https://hbs.me/326NMMY.
2. Alan Yu, "Should cities pay influencers to help stop the spread of COVID-19?" *WHYY*, June 19, 2020, https://bit.ly/2JwA13N.
3. Decree No. 2019-1530 of December 30, 2019 on the transparency of links of interest between companies producing or marketing health products for human use and the persons mentioned in 7 ° bis of I of article L. 1453- 1 of the public health code, https://bit.ly/324bfhW.
4. Advertising Standards Authority, *Influencers' guide to making clear that ads are ads*, February 2020, https://bit.ly/2HUvKX8.
5. Federal Trade Commission, *Disclosure 101 for Social Media Influencers*, November 2019, https://bit.ly/3mOPme6.
6. Pascal Wabintz, "Why surreptitious advertising is not off the table" *HORIZONT*, September 19, 2017, https://bit.ly/2I1D978.
7. Carolyn Y. Johnson, "The FDA just recalled Kim Kardashian's Instagram post," *The Washington Post*, August 11, 2015, https://wapo.st/36d9X5x.
8. Federal Trade Commission, "Tea Marketer Misled Consumers, Didn't Adequately Disclose Payments to Well-Known Influencers, FTC Alleges," news release, March 6, 2020, https://bit.ly/3ergf4T.
9. Federal Trade Commission, "Teami LLC: Warning Letters to Instagram Influencers to Prominently Disclose Paid Endorsements," letter, March 20, 2020, https://bit.ly/2TLT4sP.
10. Paul Thompson, "Harrods boss 'mocks coronavirus victims' as he coughs and says 'I'm gonna die!' in shocking TikTok video," Daily Mail, March 20, 2020, http://dailym.ai/35SBGIo.

Takeaways

- Using influencers on social media to promote a brand is an essential marketing technique.
- Influencer marketing poses regulatory and reputational risks.
- Main regulatory risks are related to intellectual property, data privacy, advertising, and disclosure.
- New regulations are emerging around this technique (e.g., public disclosure of payments).
- Dialogue with marketing colleagues is key to managing these risks along with suitable processes and trainings, adapted contracts, and crisis and exit strategies.

LEARN THE ESSENTIALS OF EFFECTIVE COMPLIANCE & ETHICS MANAGEMENT

BASIC COMPLIANCE & ETHICS ACADEMIES

CCEP EXAM OFFERED

Our Academies provide you with the continuing education units (CEUs) needed to sit for the optional CCEP certification exam offered on the last day.

ACADEMIES OFFERED IN 2021

June 21-24 • Amsterdam

August 2-5 • Seattle, WA

August 9-12 • New Orleans, LA

October 4-7 • Washington, DC

November 15-18 • Fort Lauderdale

Register
corporatecompliance.org/academies

SCCE
Society of Corporate Compliance and Ethics

YOUR ORGANIZATION HAS RECEIVED A DATA ACCESS REQUEST. WHAT NOW?

by Patrick O'Kane

Patrick O'Kane

(patrick.okane@fisglobal.com) is a London-based UK Lawyer (Barrister) and Data Protection Officer for a US Fortune 100 company.

There has been something of a tsunami of privacy regulation over the past few years, and this is set to accelerate. According to Gartner, 10% of the world's population in 2020 had a modern privacy law regulating the use of personal data, and it predicts that by 2023, 65% of the world's population will have a modern privacy law.[1]

Since 2018, we have had major privacy laws implemented: the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the US, and the General Data Protection Act in Brazil. A major new privacy law is expected in India — the Personal Data Protection Bill — in 2021.

These regulations have many features in common, including security requirements, large penalties and fines for breaches of the regulation, and privacy notice requirements. They also share an important common feature. They give individuals the right of access over their personal data. Under privacy regulations, an access request is usually a right for an individual to access and receive a copy of all of the personal data your company holds on them. This may include any record containing their name or information.

Knowledge is power

In the movie *My Cousin Vinny*, the inexperienced but streetwise defense lawyer Vinny Gambini is trying his first murder case against an experienced prosecutor. "I'd sure like to get a look at your files," he says to the prosecutor. Vinny is delighted with himself and feels he has been very skillful when the prosecutor immediately grants him access. Vinny, in his naivete, doesn't know that he had a legal right to access the files all along.

More and more individuals are learning about their own legal right to access their personal data, so it is becoming more prevalent on a global scale.

The challenges of the right of access

In the digital age, data are the new oil, and companies are keen to drill for as much as possible. Privacy regulations want to control the flow of that oil and ensure that privacy rights and freedoms are upheld.

Companies face many challenges in dealing with access requests because there are two competing interests at work. Regulation, in the form of GDPR, wants to limit personal data processing and to give individuals access to their personal data. Conversely, companies want to slice, dice, and commoditize as much personal data as they can with limited interference.

Companies hold all sorts of information about people, from marketing and human resources data to the most sensitive information relating to a client's conduct, finances, or health. Personal data can be held in myriad different forms across multiple locations.

Much of the personal data may be held off premises, including data held in the public cloud. Personal data are often held by a multiplicity of vendors and business partners. They come in various shapes and sizes, such as customer call recordings, security camera footage of individuals, purchase history, records of website activity, paper records, etc. Then there is the dreaded email. One United Kingdom access request made by an employee to their employer necessitated the review of 500,000 emails at a cost of $150,000.[2] The burden of dealing with these requests can cost companies up to $2 million a year.

There is also the problem of identity checks. The BBC News site reported a case where a University of Oxford researcher decided to conduct an experiment on access requests.[3] He contacted 83 companies pretending to be his fiancée. His fiancée had agreed to participate in the experiment and allowed him to see if he could obtain her data from various companies. Of the 83 companies he contacted, 24% supplied him the personal information of his fiancée.

How does my company deal with access requests?

The rules on access requests under GDPR and CCPA have high expectations. They expect that you can find all the data on a particular person within a strict time limit (one month under GDPR and 45 days under CCPA).

There are three steps you can take to ensure access requests are dealt with properly within your company.

1. **Stay on top of records management**: Records management is too often ignored within companies. Companies must ensure that records and data are subject to deletion time limits. Otherwise obsolete data can accumulate and cause risks and liability to companies, particularly if the data are the subject of a security breach. Put strict time limits in place around the retention of data within your company and enforce those time limits vigorously.
2. **Put a written procedure in place**: This is an instruction manual on how your company will deal with access requests. The procedure for dealing with access requests should include:
   - Details on how individuals can make an access request.
   - How the person's identity is verified before granting the request.
   - How the company should search for the data.
   - How the data are reviewed before they are sent out.
   - How the data are sent out securely.
   - How staff are trained on access requests.

In the digital age, data are the new oil, and companies are keen to drill for as much as possible.

3. **Train, train, train**: Many of your staff will interact with individuals and customers. Would each of those staff members know what to do if a customer said to them, "I want a copy of my data," or, "I want to access all my data"? They should know because that customer has just made an access request, and the clock is now ticking. All staff should have some general knowledge of access

requests, and this could be included in your general privacy training module. Some departments will require more detailed knowledge of access requests as they relate to their department. For example, human resources will need to be trained on handling employee access requests. Information technology may need to be trained on finding and accessing data across many different systems.

Stay ahead of the privacy law tsunami

Dealing with access requests is a big part of privacy compliance. And with the deluge of privacy regulations expected over the next three years, companies must act now to ensure they have the appropriate systems and controls in place to deal with these requests.

Would each of those staff members know what to do if a customer said to them, "I want a copy of my data," or, "I want to access all my data"?

About the author

Patrick O'Kane has helped lead a major GDPR implementation project across a group of more than 100 businesses and previously led the privacy team at a large group of insurance companies in London. He is the author of *A Practical Guide to Managing GDPR Subject Access Requests* and *GDPR – Fix it Fast: Apply GDPR to Your Company in Ten Simple Steps*, is certified in European Union and US privacy regulations, and was made a Fellow of Information Privacy by the International Association of Privacy Professionals in 2020.

Endnotes

1. Laurence Goasduff, "Gartner Says By 2023, 65% of the World's Population Will Have Its Personal Data Covered Under Modern Privacy Regulations," news release, Gartner, September 14, 2020, https://gtnr.it/3escH2x.
2. Deer v University of Oxford [2017] EWCA Civ 121.
3. Leo Kelion, "Black Hat: GDPR privacy law exploited to reveal personal data," BBC News, August 8, 2019, https://bbc.in/3l2R7E6.

Takeaways

- Ten percent of the world's population is currently covered by a modern privacy law, and the number is predicted to increase to 65% by 2023.
- Companies are collecting more data. There are rights under new and upcoming privacy regulations for individuals to access and obtain a copy of their data.
- In order to manage access requests, companies must ensure they are deleting old data from their systems regularly.
- It is important to put proper procedures in place to ensure your company can find, redact, and transfer data to the individual.
- Your staff must be trained to be able to recognize, escalate, and deal with access requests from customers and staff.

SCCE MEMBER BENEFIT

4 complimentary member exclusive web conferences a year

Valued at $99 each, a $396 savings! If you are unable to join us live, we will provide the recording for download later.

UPCOMING DATES

FEBRUARY 3

Register now
corporatecompliance.org/webconferences

OTHER MEMBER BENEFITS & RESOURCES

CONFERENCE DISCOUNTS

Members receive exclusive savings on all SCCE in-person, virtual, and web conferences.

corporatecompliance.org/events

COSMOS™

Navigate the Compliance Universe

Our online content platform provides SCCE members free access to *Compliance & Ethics Professional (CEP)* magazine with powerful search and links to relevant resources. And a growing collection of subscription-based compliance books and newsletters.

compliancecosmos.org

PUBLICATIONS DISCOUNTS

SCCE offers a wide variety of educational resources, available in digital and print formats. Enjoy your member-only discount on books, manuals, and newsletters.

corporatecompliance.org/store

CERTIFICATION

SCCE members save on Compliance Certification Board (CCB)® exams. Options include: Certified Compliance & Ethics Professional (CCEP)®, Certified Compliance & Ethics Professional–International (CCEP-I)®, and Certified Compliance & Ethics Professional–Fellowship (CCEP-F)®.

corporatecompliance.org/certification

COVID-19 RESOURCES

SCCE has developed a variety of complimentary COVID-19 resources to stay informed, manage risk, and maintain the effectiveness of your compliance and ethics program.

corporatecompliance.org/covid19

SCCE®
Society of Corporate Compliance and Ethics

NEW DATA REVEAL THE GROWTH OF COMPLIANCE IN LATIN AMERICA

by Alejandra Montenegro Almonte and James Tillen

Alejandra Montenegro Almonte

James Tillen

Alejandra Montenegro Almonte *(aalmonte@milchev.com) is Vice Chair of Miller & Chevalier's International Department in Washington, DC.*

James Tillen *(jtillen@milchev.com) is the Chair of the International Department at Miller & Chevalier.*

A perennial challenge for chief compliance officers (CCOs) is assessing corruption risk in their companies' countries of operation. Many CCOs turn to Transparency International's Corruption Perception Index (CPI), which annually ranks countries based on the perceived levels of corruption in their public sector generally. Companies use CPI scores to determine what amount of due diligence to conduct on a third party, what locations to audit, what employees to train, and whether to enter into a new market. Yet a CPI score does not tell the whole story for a particular country, and overreliance on the CPI can lead companies to miss specific risks or focus too many resources on low-risk areas.

With this challenge in mind, our firm, in partnership with several law firms across Latin America, began conducting a corruption survey of the countries in the region every four years to provide CCOs with more detailed corruption data to help organizations assess and address particularized risks within each jurisdiction. The 2020 survey[1] yielded important information about the changing corruption landscape in the region that CCOs will find useful in making risk-based decisions related to the region. It additionally assessed anti-corruption compliance practices, which can help CCOs benchmark their programs and determine where compliance concepts are accepted and where more efforts may be required to implement effective compliance components.

Ranking government corruption

Understanding the corruption risks of the countries in which businesses operate is the starting point to an effective anti-corruption compliance program, so the survey asked the respondents to evaluate corruption in countries within the region. Consistent with CPI results, respondents viewed corruption as a significant obstacle in multiple countries, including Venezuela, Nicaragua, Honduras, and Ecuador. The majority of respondents viewed corruption as an insignificant obstacle in Uruguay, Chile, and the United States. It should be noted that while conducting the survey, the continued instability in Venezuela made it difficult to obtain reliable data from respondents in the country. While respondents from other countries numbered in the dozens and Venezuelan

respondents actively participated in our prior surveys, only eight people in total from Venezuela responded in 2020. Because of these low numbers, we were unable to include the results for Venezuela in assessing responses to most of the questions. Notably, respondents in other countries overwhelmingly ranked Venezuela as the most corrupt country surveyed in the region.

Respondents also evaluated corruption in nine specific areas of government within their countries: executive branch, legislative branch, judicial branch, customs, prosecution service or investigators, police, municipal/local authorities, political parties, and state-owned companies. These questions were designed to help CCOs better understand whether corruption risk varies within a country's government and, if so, where that risk is most heightened. This breakdown of corruption risk by government areas can be leveraged by CCOs to help guide risk assessments of their own operations. For example:

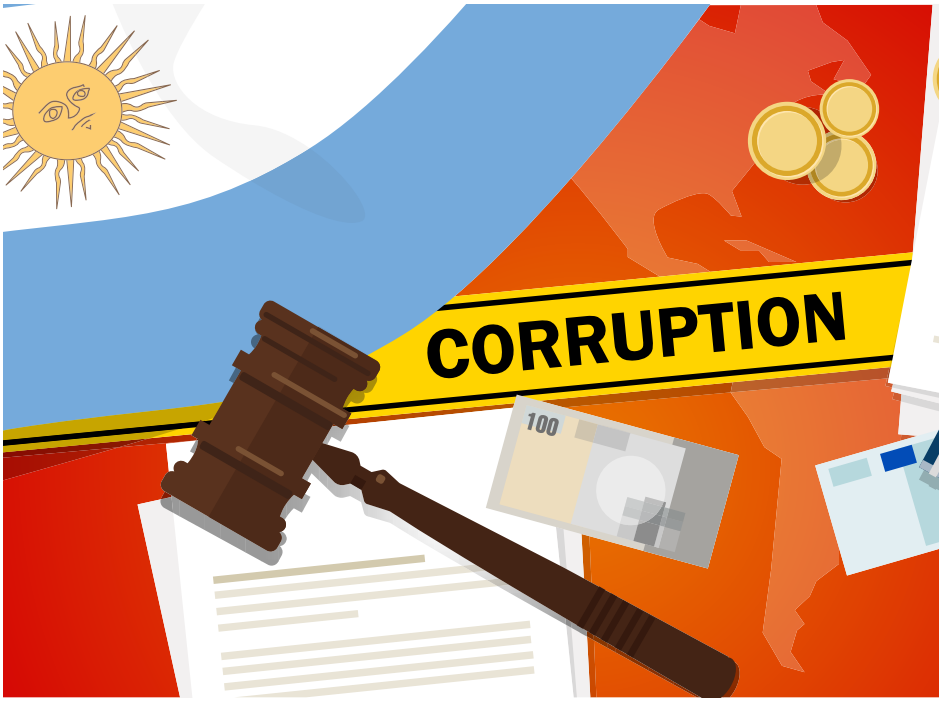
- Companies importing into multiple countries in the region will be interested in knowing the percentages of respondents who viewed **customs authorities** in particular countries as "significantly corrupt." Colombia (82%), Argentina (76%), and Nicaragua (75%) achieved the highest percentages, and Chile (22%) and the United States (25%) received the lowest percentages of the countries evaluated. CCOs may also be interested in understanding where their risk profile may have shifted in the last four years. Although in 2020 Argentina and Chile are at different ends of the corruption risk spectrum, when compared to the 2016 results, it's apparent that these countries were heading in different directions: Argentina's risk profile improved from 91% to 76%, while Chile's risk profile increased from 8% to 22%.
- Companies contracting with **state-owned companies** in Ecuador (81% respondents viewed them as significantly corrupt) and Colombia (77%) should be more concerned about the corruption risk associated with those relationships than companies contracting with state-owned companies in the United States (25%), Chile (32%), and Costa Rica (37%).
- Companies facing litigation or criminal actions in the region can evaluate risks in dealing with **prosecution services or investigators** — viewed as most corrupt in Mexico (77%) and Bolivia (74%) — and **the judiciary** — viewed as most corrupt in Nicaragua (94%) and El Salvador (86%).
- Finally, companies that interact often with local **police** in the course of their operations would benefit from understanding that respondents viewed the police in the following countries as significantly corrupt: Mexico (88%), Peru (85%), and Bolivia (85%).

These specific data points have become more relevant to CCOs in light of the recent U.S. Department of Justice (DOJ) update to its *Evaluation of Corporate Compliance Programs* guidance,[2] in which it stresses that companies should conduct risk assessments that help identify particularized corruption risks.

Compliance is making headway — but still lags for some

Data on compliance programs were collected on a country-by-country basis and also by company type — namely public vs. private companies and multinational vs. regional companies — making the data more useful for organizations benchmarking against companies with similar operational footprints and corporate structures. While respondents from multinational and publicly traded companies continue to lead the path in compliance, a growing number of regional and private companies have made meaningful strides in their own compliance programs in the last four years. For instance, both multinationals and local/regional companies have shown an upward trend in the following key categories: full-time compliance personnel (38% of local/regional companies and 77% of multinationals); anti-corruption assessments and audits (46% of local/regional companies and 71% of multinationals); third-party due diligence policies (49% of local/regional companies and 81% of

Notably, respondents in other countries overwhelmingly ranked Venezuela as the most corrupt country surveyed in the region.



multinationals); and monitoring of third parties (31% of local/regional companies and 54% of multinationals). These data points indicate that compliance is becoming increasingly embedded in the fabric of Latin American businesses and should encourage CCOs to continue their pursuit to strengthen their own company's programs.

As indicated above, the survey additionally asked respondents questions regarding the specific steps their companies take to reduce corruption, including which elements of a compliance program their companies have implemented (e.g., anti-corruption training and policies; procedures for gifts, travel, and entertainment for government officials; mergers and acquisitions due diligence; anonymous reporting mechanisms; full-time compliance personnel; and monitoring of third parties). Overall, the data indicate that while an increased number of companies in the region have embraced a wide range of anti-corruption compliance program elements, several countries continue to lag behind, creating a divergence in compliance program maturity between "Most Developed" and "Least Developed," with only two countries (Guatemala and Honduras) in the "Developing" category (Figure 1). Understanding the maturity of compliance programs in specific countries may help CCOs benchmark their own programs against country-specific practices and expectations.

** Moved up since the 2016 survey. Due to the small number of total responses received from Venezuela, the country was excluded from this ranking.*

This benchmarking is particularly important for CCOs operating in Latin American countries that have adopted anti-corruption laws with compliance program expectations, such as Argentina, Brazil, Chile, Colombia, Costa Rica, Mexico, and Peru. Respondents from these countries report the most developed compliance programs in the region, exceeding the regional average in every category included in the survey. In addition to benchmarking, it is important for CCOs to understand the compliance requirements in the laws and how they compare to other standards that may be applicable to their companies, such as expectations of the DOJ and Securities and Exchange Commission found in the *Resource Guide to the U.S. Foreign Corrupt Practices Act, Second Edition*.[3]

Understanding the compliance landscape in specific countries and by type of company may also help CCOs anticipate challenges in the application of their programs, such as identifying third parties and joint venture partners that may be more or less likely to understand and accept due diligence requirements and compliance expectations in contract terms. Similarly, CCOs may be able to anticipate which acquisition targets are more likely to have existing compliance programs that are addressing risks. Lastly, by using these data, CCOs may be able to identify which subsidiaries may be more accepting of training, hotlines, and other program components and, conversely, where more effort will be required to embed such elements.

Armed with more knowledge

Corruption challenges in Latin America are diverse and ever-changing, posing many challenges to CCOs administering compliance programs in the region. The data set from the 2020 Latin America Corruption Survey has provided a starting point for CCOs to identify risk regionally and within countries. With this information, CCOs may be able to more effectively

benchmark and anticipate issues when implementing their compliance program.

About the authors

Alejandra Montenegro Almonte's practice focuses on internal corporate compliance, internal investigations, and government enforcement actions across a variety of business-critical areas, including anti-corruption, internal controls, and other ethics and compliance violations.

James Tillen's practice focuses on the U.S. Foreign Corrupt Practices Act and other international compliance issues.

Endnotes

1. Miller & Chevalier, *2020 Latin America Corruption Survey*, accessed November 9, 2020, https://bit.ly/36iPigf.
2. U.S. Dep't of Justice, Criminal Div., *Evaluation of Corporate Compliance Programs* (Updated June 2020), http://bit.ly/2Z2Dp8R.
3. U.S. Dep't of Justice and the Enforcement Div. of the U.S. Securities and Exchange Comm'n, *A Resource Guide to the U.S. Foreign Corrupt Practices Act, Second Edition*, July 2020, https://bit.ly/2FBw5g7.

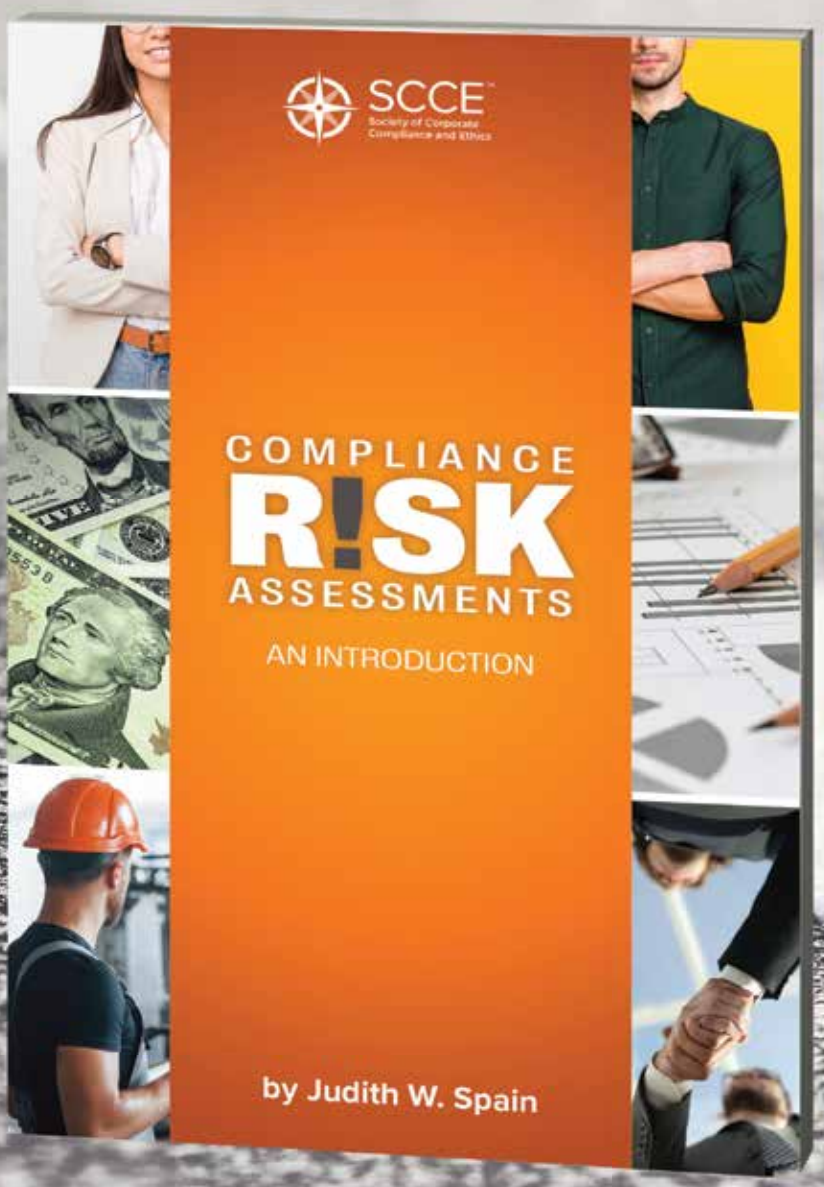
Takeaways

- New data from a survey of corruption perceptions in Latin America can assist chief compliance officers in tailoring their compliance programs to address risk and compliance expectations.
- Results show which government areas, from customs (highest risk in Colombia) to the police (Mexico), present the greatest risk.
- Insight into anti-corruption compliance programs in Latin America is providing useful benchmarking data for chief compliance officers..
- Several countries have mature compliance environments (e.g., Argentina and Brazil), whereas others lag significantly behind US standards (e.g., Bolivia and El Salvador).
- Local anti-corruption laws with compliance standards have led to improved compliance programs in several countries (including Costa Rica, Chile, and Peru).

Your guide to defining, assessing, and addressing risk

This book walks you through the compliance risk assessment process step by step.

Learn how to build a robust process, avoid common pitfalls, and work towards continuous improvement.



Learn more
corporatecompliance.org/risk-intro

SCCE
Society of Corporate Compliance and Ethics

What if they hate me?

by Kristy Grant-Hart

"They hate me. I'm sure they hate me. Or they will hate me," said my client. She'd been relocated to Eastern Europe, where the company had just finished a massive investigation resulting in the firing of two regional leaders. She was parachuted in to keep an eye on things and to try to revamp the culture. The investigation had been long and slow, exhausting everyone, including her. She worried that even with a new manager, the remaining leaders would harbor resentment. What was she to do? And more importantly, what are you to do when you perceive robust distrust and anger in pockets of your organization?

You're here to do a job

While mistrust and resentment may exist, it doesn't matter whether everyone likes you. You're in the organization to do a job, and that job is to drive compliance with the law and the creation of an ethical culture. In the face of indignation, remember that your mission is critical. Separate yourself as a person from yourself as a compliance officer. The true you is separate from your job.

Trust takes time

It would be nice if trust could be built or rebuilt in a day, but the truth is, a million little microactions need to take place to build the bonds of positive goodwill. Try not to be frustrated with the pace; instead, focus on the little wins along the way. A smile from someone in the office can be counted as a success.

Start over

At the first leadership meeting my client attended, she acknowledged the challenges that the investigation had caused, then reminded everyone that she had been brought in to help the business succeed. It was a new day with new management, and she was there to start over with them. When feelings have been hurt, whether through an investigation, disciplinary action, or the firing of a colleague, acknowledge the pain, then turn the page.

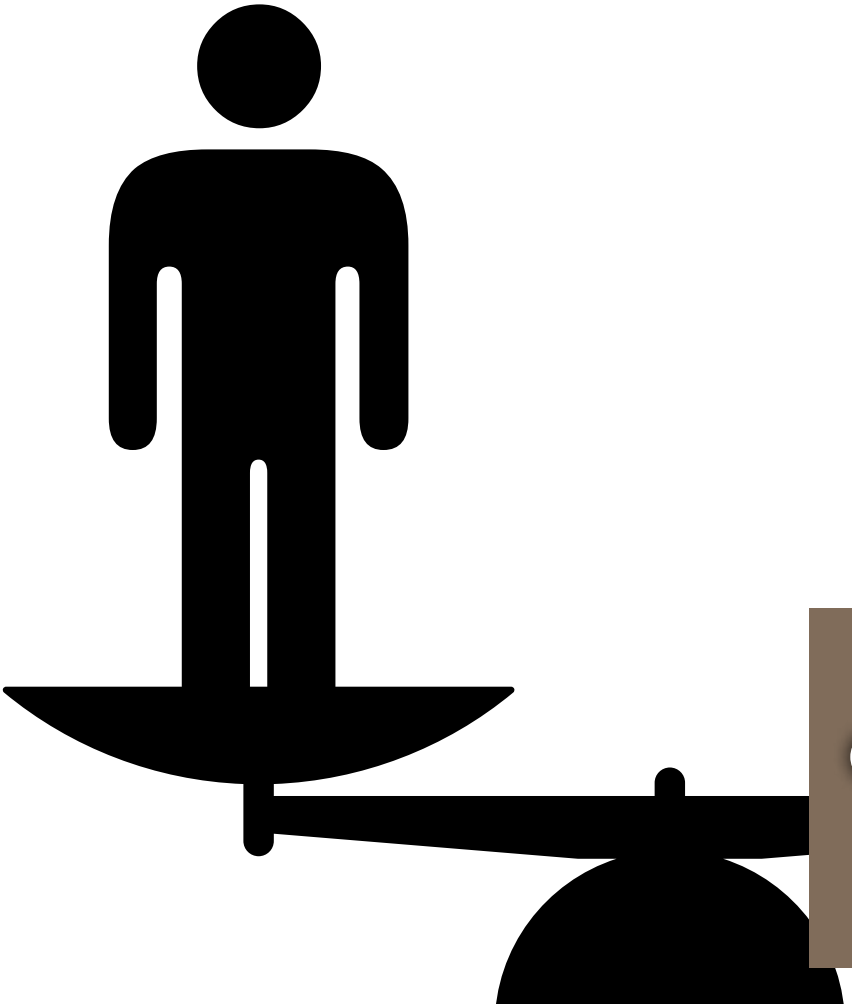
Find allies

While some people may dislike you, there will always be someone who believes in compliance and ethics. Cling tightly to those who share your mission. Give trust before receiving it, and you'll be much more likely to build trust in return.

Kristy Grant-Hart

(kristygh@sparkcompliance.com) is the Managing Director of Spark Compliance Consulting in London, and author of the book, How to be a Wildly Effective Compliance Officer.

ComplianceKristy.com
@KristyGrantHart
bit.ly/li-KristyGrantHart



ENSURING ORGANIZATIONAL JUSTICE FOR ALL

by Emeka N. Nwankpah

Emeka N. Nwankpah
JD, MBA, CCEP
(emeka.nwankpah@gmail.com) is the former Chief Integrity & Compliance Officer for Tenneco's Clean Air and Powertrain Divisions, and is Principal, Integrity & Compliance Consultant for Connected Compliance LLC in the Metro Detroit area of Michigan, USA.

/in/emeka-nwankpah-jd-mba-ccep

Ralph Waldo Emerson said that "A foolish consistency is the hobgoblin of little minds."[1] While this is generally true, achieving organizational justice, through focusing on fairness and well-reasoned consistency when determining and administering discipline, is a coveted sign of sophistication and effectiveness in the world of ethics and compliance.

So what is organizational justice?

Organizational justice is the process by which an organization investigates and addresses employee misconduct, and the way an organization manages employee perceptions about and expectations around that process. To be clear, there are aspects of investigations and how the organization addresses employee misconduct that need to remain "behind the veil" for privacy and employment law reasons. However, there are many aspects of the same that can and should be shared with employees, some of which are highlighted below. This transparency helps manage employee expectations and reduces the inherent concerns and consternation employees have related to investigations. This in turn helps employees feel more comfortable about coming forward and participating in investigations. It is difficult to trust the process if you have little, if any, visibility into that process.

There are three aspects of organizational justice, and they all center around a notion of intentional fairness: fair process, fair treatment, and fair discipline.

Fair process

Fair process deals with how the company investigates misconduct (i.e., how an organization views the complaint, the accuser, and

the accused). All complaints (or portions thereof) should be treated as potentially credible unless they clearly are not. All accusers should be treated with respect and repeatedly encouraged to provide information. All those accused of misconduct should be a presumed innocent until proven otherwise. There should be a commitment to follow the evidence and not to try to fit the facts into a preconceived conclusion. There should be an intentional balancing of the employee's legal rights with the company's reputation, ongoing business interests, and stated company values. Lastly, the process should be based on an established investigation protocol that is used clearly and consistently.

Fair treatment

Fair treatment deals with how those directly involved in the investigation will be treated — specifically, the maintaining of confidentiality and anonymity (where requested). This involves sharing information on a strict "need to know" basis and, when in doubt, not sharing it. Fair treatment also means treating everyone involved (the accuser, the accused, and witnesses) with respect and guarding their reputations. Those involved should be interviewed, not interrogated; the interviewers should be courteous but thorough; and the interviewees should be told that their cooperation and candor are required and expected. Lastly, a "no retaliation" warning should be given to all involved.

Fair discipline

Fair discipline deals with providing management with enough information to determine the appropriate level of discipline once misconduct is verified. This involves sharing key verified facts about the investigation, information about how similar cases were handled in the past and an appropriate range of discipline levels. In other words, the goal is to ensure the determined discipline is consistent with the organization's core values and with disciplines for similar misconduct in the past.

Organizations without justice encourage misconduct

So far, we have covered the "what" and "how" of organizational justice. Now for the why. It's quite simple — everyone wants to be treated fairly. So the worst thing an organization can do in this context is to have a double standard of handing out heavy punishment to less favored employees and/or giving light or no punishment to favored employees for similar misconduct. Doing this undermines the credibility of the organization's leadership. More than this, it can actually encourage more misconduct, because if there is no consistent discipline, employees may conclude that there are no actual rules. And if there are no "real" rules, employees will get the message that they can get away with almost anything if they kiss up to the right people. And believe me, many employees will try.

Fairness pays huge dividends

Organizational justice is a critical component to maintain a healthy company culture. It reinforces the rule of law within the organization and helps manage expectations. It provides stability by establishing clear rules; a fair process to investigate misconduct; fair treatment for those involved; and fair, consistent, and appropriate discipline. That fairness and consistency will go a long way to show employees that they are valued and respected. But while this all may seem logical, *it takes work*. Why? Because we are all human, and many times, there is pressure to be more lenient on favored employees and more severe on difficult employees. But consistent fairness pays huge dividends — especially if the company is ever involved in a labor and employment lawsuit or governmental enforcement action.

The process should be based on an established investigation protocol that is used clearly and consistently.

So companies have a clear choice: Either do the work necessary to ensure organizational justice (and reap its short- and long-term benefits) or investigate and/or address employee misconduct based on the feeling of the day, which will inevitably result in double standards. Phrased differently, a double standard is the most likely result when companies do not seek organizational justice with intention, perseverance, and consistency. And unlike the foolish consistency that Emerson criticized, organizational justice

demonstrates a sophistication that enhances a company's culture and the effectiveness of its ethics and compliance program.

Endnotes

1. Ralph Waldo Emerson, "Self-Reliance," *Essays*, 1841, https://bit.ly/3eI12g6.

Takeaways

- Maintaining organizational justice is an important way to cultivate a healthy ethical culture and an effective ethics and compliance program.
- Organizational justice occurs when organizations consistently investigate and address employee misconduct in a way that ensures a fair process, fair treatment, and fair discipline.
- Managing employees' expectations and promoting an appropriate level of transparency helps reduce the inherent concerns employees have related to investigations.
- Organizational justice ensures misconduct is addressed based on principles of equity, not based on how the organization feels about the accused party.
- Organizations that do not seek organizational justice with intention and consistency will create a double standard, knowingly or not.

VIRTUAL CONFERENCE

Applying the COSO ERM Framework to Compliance Risk Management

January 21, 2021

SCCE & HCCA partnered with Committee of Sponsoring Organizations of the Treadway Commission (COSO) to create a guidance on the application of COSO's Enterprise Risk Management framework to the management of compliance risk. Published in November 2020, the guidance is based on current practices and expectations for effective compliance and ethics programs.

To assist in understanding and applying the guidance found in the publication, SCCE & HCCA has developed a one-day virtual conference.

Register online
corporatecompliance.org/2021coso

SCCE®
Society of Corporate Compliance and Ethics

IS YOUR COMPANY'S JOB APPLICANT-TRACKING SYSTEM MAKING COMPLIANT INQUIRIES?

by MaryEllen O'Neill

MaryEllen O'Neill
JD, CCEP
(meocos@hotmail.com) is a consultant based in Washington, DC, with 20 years of compliance experience.

One of the first impressions a job applicant and potential new employee has of your company is your online job applicant-tracking system (ATS), so when was the last time you or someone on your team reviewed your company's ATS for compliance with current employment and other laws? I have been surprised by the number of systems that directly or indirectly request information prohibited by either federal or state law — and often both. And these are not small operations that lack the knowledge or manpower (but who would nonetheless be liable); they are substantial companies with large legal and compliance departments. Pre-employment inquiries should be solely geared to an applicant's job capability. When using an ATS to screen applicants, the overriding question should be: What do I need to know prior to the interview about a candidate's ability to do the job? These are just some of the most common issues I have seen with ATSs in use.

Revealing an applicant's age

The US Age Discrimination in Employment Act (ADEA)[1] of 1967 is a very robust, well-developed, and frequently invoked age-discrimination law. The ADEA protects workers and *potential* workers from age-based discrimination in terms of hiring, firing, and other conditions of employment. In addition to the federal ADEA, individual states have their own laws protecting workers from discrimination based on age.

Despite the robustness of the law, I have discovered systems that require applicants to put in birthdates; without providing a year, the applicant cannot proceed. Although an applicant can lie, they should not be put in this position. In addition, a question that is always asked at the end of the application process is

whether you have answered the questions truthfully, followed with a warning that failure to tell the truth can be grounds for revocation of a job offer and/or termination.

Where some systems directly ask for an applicant's age, some systems ask questions designed to subtly (or not so subtly) determine this information, such as requiring a candidate to put in the year they graduated from college. There should be little doubt how a court faced with whether such a question could be used for discriminatory purposes would rule. Some states, such as New York, for example, have specifically found that asking a candidate about years of school attendance and/or dates of graduation are illegal because the questions are subtle methods of asking a candidate's age. Some systems ask the question but do not make an answer to this question mandatory. Unsophisticated applicants may provide the information nonetheless, and once they do, the company has information to potentially discriminate against an applicant based on age. It would fall to the company to prove age bias was not the reason they did not hire the applicant.

Asking about the applicant's political affiliation

Perhaps the most surprising question I've discovered in an ATS portal is a question asking about political leanings by companies with no political affiliation, so what does the answer to this question have to do with an applicant's ability to do the job? Inquiring about political affiliation raises the applicant's concern that their answer could be used for discriminatory purposes and raises doubts about the inclusiveness of the company's work environment.

There are currently no federal laws prohibiting this question, but some state laws, such as New York's Labor Law § 201-d,[2] prohibit employers from discriminating against employees because of their legal political or recreational activities when conducted outside the workplace and outside working hours, without using employer equipment or other property. California and the District of Columbia have similar laws.

Requesting social media account links

A frequent question I've found asks applicants to provide links to their social media accounts, including LinkedIn, Facebook, Instagram, and "other." Some of the systems suggest an applicant connect to the company via their social media accounts. Although LinkedIn is geared toward employment, other social media accounts are not, and searching them may reveal personal information that could arguably then be used by a company to discriminate against applicants.

Because of the personal information people often share on their nonprofessional social media profiles, a company may directly or inadvertently come across information on an applicant's personal social media account that could be considered "protected." For example, an applicant's social media profile can reveal age, race, sexual orientation, gender identity, national origin, religion, a disability, and other protected characteristics that may not be revealed in a résumé. A company may be liable in an anti-discrimination case if an applicant can demonstrate their job candidacy was adversely affected by the prospective employer's social media search, when the search results included information about the applicant's protected class. For example, an applicant sued a company when he was not hired for a position for which he was very qualified. A subsequent investigation revealed that during the hiring process, a hiring committee member found the applicant's personal website referencing religious topics. The court in that case found that there was a genuine factual issue about whether religion was a motivating factor in the company's failure to hire the plaintiff.

Some states, such as New York, for example, have specifically found that asking a candidate about years of school attendance and/or dates of graduation are illegal.

Many states have laws in place that protect applicant and employee online privacy by explicitly prohibiting employers from asking for access to social media profiles and/or the disclosure of the usernames, passwords, and other login information that allow access to or observation of personal social media accounts. Some states, such as California, Virginia, and Oregon,

have specific employee/employer social media laws in place, while others have laws related to general internet privacy.

Asking for an applicant's Social Security number

I've often discovered ATS requirements for applicants to provide their Social Security number (SSN). The notes included with the requirement provide something along the lines of "We use your SSN to identify your records and for background checks and other requests for information about you from employers, schools, banks, and others who know you, to the extent allowed by law." But none of this happens until after an applicant becomes an employee, at which point, an employer needs an employee SSN for tax forms. There is no reason an employer needs an applicant's SSN number before this person receives a job offer, and in fact, using an applicant's SSN before a job offer is prohibited in some jurisdictions, such as in the District of Columbia.

I've also seen the request for an applicant SSN justified "for security purposes." However, there is no security reason to require an applicant's SSN before a job is offered, and further, collecting it at this point creates new risks for a company. Any company or third-party system can be hacked, so an ATS with SSNs, names, addresses, phone numbers, etc. can be a rich source for identity thieves. An applicant's SSN is not directly related to the applicant's ability to perform a specific job, and their information is often viewed by numerous individuals — none of whom have a need to know this information nor have access to it.

New laws, such as the California Consumer Privacy Act (CCPA),[3] can apply to employment records in some situations, putting additional burdens on companies that have such confidential applicant information. The fines are steep — $7,500 per record. On October 11, 2019, California Governor Gavin Newsom approved a moratorium on employers' compliance with CCPA[4] as long as employers are collecting the data of its employees and job applicants solely for purposes relating to employment. Pursuant to the terms of the amendment, the moratorium ended January 1, 2021, and employers are still obliged to inform people (including employees and job applicants) of the categories of personal information they collect — and the purposes for its use — at or before the point of collection.

If you must have a number to track applicant files, ask the applicant to pick a number, use the last four digits of the applicant's phone number, or have the system generate a number. If it is solely required for tracking, there are many options for a number other than asking for an applicant's SSN.

Asking for an international applicant's information — in violation of GDPR

Although this article focuses on US laws, there are international laws that affect the information that companies can request of applicants. The European Union's General Data Protection Regulation (GDPR) is one of these laws. It applies to companies that process data of EU residents and exists to protect the kind of personal data that applicants provide and can be identified through, such as their names, physical addresses, or phone numbers found on most résumés and in applicant-tracking systems. GDPR requires companies to collect data only for "specified, explicit and legitimate purposes."[5] This means, for example, that a company can source candidate data as long as it collects *job-related information only* and the company intends to contact sourced candidates within 30 days.

To be in compliance with GDPR, companies should collect only the data needed to assess an applicant's ability to perform job functions, such as education type and level, work history, work skills, etc., along with contact details. Companies should not, however, process data that have no bearing on an applicant's ability to perform a job, such as cultural information, during the recruiting process. If a company needs to process this type of data (e.g., disability, cultural, genetic, or other information often gathered for the equal employment opportunity survey), GDPR requires a company to ask for an applicant's consent. The company must ask for consent in a clear and intelligible way and provide candidates with clear instructions on how to withdraw their consent should they wish to do so.

Beyond limiting the type of information sought from a job applicant, GDPR also provides important rights to applicants. For example, applicants have the right to ask a company to delete and stop processing their personal data, which is known as the right to be forgotten. Companies must be able to locate every place where it maintains applicant information and delete it within one month after receiving the request.

In addition to the right to be forgotten, applicants have the right to ask what data of theirs are being maintained by the company. Applicants can request that a company make corrections to any inaccuracies. Companies must grant both requests within one month and provide applicants with a free electronic copy of their own personal data upon request.

What should you do?

Here are the steps you can take to ensure your organization's ATS is asking the right questions:

1. Identify all the locations in which your company has offices and where it's hiring employees. (Note: They may not be the same, so all locations are important.)
2. Determine the restrictions, prohibitions, and requirements of the applicable local, federal, and international laws.
3. Check your ATS to determine its compliance with applicable laws and what needs to be updated.
4. If your company has outsourced its applicant tracking, don't forget to check the vendor's systems and ensure there are appropriate provisions in the vendor contract, especially as it pertains to compliance, liability, and indemnification.
5. Make sure you or someone on your team is part of any conversation about updating the system.
6. Review your ATS on a yearly basis to make sure any changes in laws or regulations have been appropriately incorporated into the system.
7. Make sure the individuals who work with and/or oversee the ATS have appropriate training on applicable legal prohibitions.
8. If the ATS requires that an applicant choose an option from a drop-down menu to answer a question, make sure all possible options are included. Not having all the choices and not providing an opportunity to write in a correct response does not present an image of inclusiveness.

Companies should not, however, process data that have no bearing on an applicant's ability to perform a job.

Revisit your company's ATS

Applicant-tracking systems have morphed from simply collecting basic information to determining an applicant's job capability to

collecting all sorts of information that may be needed during the entirety of an applicant's employment. However, a review of many of these systems indicates that rarely do companies determine whether collecting the information required by their system at this stage of the hiring process is appropriate or legal.

Endnotes

1. 29 U.S.C. §§ 621–634.
2. Discrimination against the engagement in certain activities, N.Y. Consol. Laws, Lab. § 201-d.
3. California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199 (West 2018), http://bit.ly/2sAsI2P.
4. An act to amend Sections 1798.130 and 1798.145 of the Civil Code, relating to consumer privacy, Cal. Assemb. B. 25 (October 14, 2019).
5. Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. L119/35.

Takeaways

- If your company's applicant-tracking system (ATS) asks illegal questions or questions that imply exclusivity, you will lose qualified candidates and could face legal action.
- The ATS should be reviewed by legal and compliance to ensure it is in compliance.
- Those who have access to the ATS should have regular training on the confidentiality and security of its information, and on inappropriate application questions.
- Determine whether the ATS needs to be in compliance with international laws as well as federal and state laws.
- Include a review of the ATS in your annual compliance plan to reflect evolving laws and regulations, any new company locations and acquisitions, etc.

A VIRTUAL CONFERENCE

9th Annual SCCE ECEI

European Compliance & Ethics Institute

15–17 March 2021

Join your compliance and ethics peers at the 2021 virtual European Compliance & Ethics Institute (ECEI) to learn about the challenges facing the European and global compliance & ethics community. This is the place to find out about the latest solutions to your challenges, hear strategies to mitigate risk, and improve your organization's compliance program.

ECEI's educational sessions will provide you with the opportunity to earn live Compliance Certification Board (CCB)® continuing education units (CEUs) from the convenience of your home or office.

The 2021 agenda includes a range of trending topics including:

- Anti-Corruption
- Pandemic Learnings
- Crisis Management
- Data Protection
- Implementing Global Trade Compliance
- Investigations
- Risk Management
- **The latest from the UK SFO and US DOJ**

Register before 2 February for a discounted rate.

Register today:
corporatecompliance.org/2021ECEI

SCCE
Society of Corporate Compliance and Ethics

ENHANCE YOUR CAREER

Gain credibility, show dedication to excellence.

- Expand your job skills
- Demonstrate compliance knowledge
- Invest in your profession
- Show your dedication to excellence

Follow these 5 steps to certification:

1. Gain Work Experience
2. Earn & Submit CEUs
3. Apply to Take Exam
4. Schedule Your Exam
5. Take Exam

> "The certification tests you on broad yet fundamental Compliance & Ethics topics that will give you the requisite knowledge to perform at a high level regardless of industry."

Learn more
corporatecompliance.org/certification

BECOME CERTIFIED

Become a compliance resource for your company.

Ways to earn continuing education units:

ATTEND

- Events hosted by SCCE & HCCA
- Events hosted by other organizations
- University courses related to compliance
- Live or recorded web conferences

STUDY

- Take magazine quizzes in *CEP* or *Compliance Today* Magazine
- Complete book quizzes in SCCE & HCCA publications
- Read approved articles in our premium newsletters
- Complete approved self-study activities

CONTRIBUTE

- Present a topic at an SCCE or HCCA event, or outside events
- Present a web conference
- Teach a university course
- Publish an article in *CEP*, *Compliance Today*, or outside publications related to compliance
- Publish a guest post on SCCE & HCCA's blog

CCEP®
CERTIFIED COMPLIANCE & ETHICS PROFESSIONAL

CCEP-I®
CERTIFIED COMPLIANCE & ETHICS PROFESSIONAL-INTERNATIONAL

CCB COMPLIANCE CERTIFICATION BOARD

Oh no, compliance is siloed from legal!

by Joe Murphy

Joe Murphy
CCEP
(jemurphy5730@gmail.com) is a Senior Advisor at Compliance Strategists, SCCE's Director of Public Policy, and Editor-in-Chief of CEP Magazine.

We still hear this question: Should compliance & ethics (C&E) be part of legal or siloed/divorced/separated? What may follow is a list of "horribles" of this gulf and the reasons why the two should, therefore, be combined.

But this is a false dichotomy. C&E is a multidisciplinary field. It is not law, but it is also not human resources, security, audit, or any other one field. It does, however, need to work with each of those fields. Being a lawyer is a qualification for providing legal advice but not for most of the core elements of compliance work.

Why would compliance need to come under legal? I have not heard general counsels saying human resources needs to report to them, nor the internal audit department. Yet these parties have important control functions. Here is the point: In order for different organizations to work together, it is unnecessary for one to report to the other.

If the general counsel is a self-confident professional, there will be no problem with this. Counsel knows the lawyer's role is to provide legal advice and assistance. Legal wouldn't claim that the sales department needs to come under their control — just that there needs to be ongoing communications and a cooperative relationship.

C&E performs a very important function for legal. Compliance helps get the advice — the message — out to the company's people. It also helps ensure these people are going to legal when legal issues come up. It does this through methods that are not the lawyers' province: effective management steps.

Legal and C&E should not be siloed, but they should be working closely together. For example, the legal department might designate one lawyer who is the C&E liaison. This person could participate in working groups related to the compliance program and might review investigation reports and monitor what comes through the helpline. When legal issues come up, this lawyer would ensure the right lawyer is involved.

We should not accept a false dichotomy. The "report to me" argument does not exist for human resources, or audit, or security, or information technology. They all need to work with legal and have cooperative relationships. The same is true for C&E. Close, but not controlled.

Takeaways

January 2021

COMPLIANCE & ETHICS PROFESSIONAL
CEP MAGAZINE

Tear out this page and keep for reference, or share with a colleague. Visit www.corporatecompliance.org for more information.

Returning to business travel: Mitigating risk for your employees

Michael F. Savicki (page 16)

» Governments have responded to COVID-19 with various restrictions designed to stop the spread. These requirements continue to evolve.
» Considering the increase of air travelers passing through security checkpoints, companies should develop the end-to-end business travel experience for their travelers.
» Organizations' travel policies need to be regularly reviewed and updated to protect both the well-being of employees and their own corporate reputations.
» A documented internal approval process should be in place prior to booking and provide employees with up-to-date travel requirements, including border closures and quarantine measures.
» Employers should be mindful of their duty of care obligations and require travelers to book using the company's tools and policies for oversight purposes.

Protecting corporate data in the work-from-home era

Melody Haase (page 20)

» Security practices must be shared, embraced, and followed by all.
» If it is in practice at your organization, stop to consider if Bring Your Own Device is still the right option.
» Aim for continuous improvement in your information technology department.
» Be prepared with logging, backups, and insurance.
» Choose the solutions that are right for your organization.

Rethink your policy management system to strengthen your compliance program

J. Veronica Xu (page 26)

» Policies are a triangular framework that consists of three elements: (1) a policy management and review process, (2) a policy library and database system, and (3) policy training.
» Policy management plays a fundamental role in structuring a company's business practices and ethical framework, so it is essential to the company's long-term success.
» Policy management requires continuous attention, cross-functional collaboration, and a sustainable approach that focuses on departmental contribution, buy-in, and teamwork.
» Making policies easily accessible to employees is one of the effective ways to promote compliance.
» Establishing policies and maintaining them are the first two steps leading to a lasting and effective policy program; training on policies is also crucial.

Balancing effective compliance policies against the ubiquity of ephemeral messaging

Daniel J. Polatsek (page 32) **CEU**

» Communication between compliance personnel and management should be established to assess the utility and risk of the use of ephemeral messaging and personal mobile devices.
» Internally memorialize the business justification for using ephemeral messaging and personal mobile devices within the context of the risks.
» In-person and webinar training on the permissible and prohibited uses of ephemeral messaging and personal mobile devices for company business should be considered.
» Compliance departments should partner with information technology to understand the capabilities of its own record retention and ability to suspend ephemeral messaging for an investigation.
» Companies should have an express privacy policy mandating employees' consent to the company's monitoring and collection of ephemeral messages and company communications on personal devices.

Engage with your marketing team to avoid influencer marketing risks

Caroline Franco (page 38)

» Using influencers on social media to promote a brand is an essential marketing technique.
» Influencer marketing poses regulatory and reputational risks.
» Main regulatory risks are related to intellectual property, data privacy, advertising, and disclosure.
» New regulations are emerging around this technique (e.g., public disclosure of payments).
» Dialogue with marketing colleagues is key to managing these risks along with suitable processes and trainings, adapted contracts, and crisis and exit strategies.

Your organization has received a data access request. What now?

Patrick O'Kane (page 44) **CEU**

» Ten percent of the world's population is currently covered by a modern privacy law, and the number is predicted to increase to 65% by 2023.
» Companies are collecting more data. There are rights under new and upcoming privacy regulations for individuals to access and obtain a copy of their data.
» In order to manage access requests, companies must ensure they are deleting old data from their systems regularly.
» It is important to put proper procedures in place to ensure your company can find, redact, and transfer data to the individual.
» Your staff must be trained to be able to recognize, escalate, and deal with access requests from customers and staff.

New data reveal the growth of compliance in Latin America

Alejandra Montenegro Almonte and James Tillen (page 48)

» New data from a survey of corruption perceptions in Latin America can assist chief compliance officers in tailoring their compliance programs to address risk and compliance expectations.
» Results show which government areas, from customs (highest risk in Colombia) to the police (Mexico), present the greatest risk.
» Insight into anti-corruption compliance programs in Latin America is providing useful benchmarking data for chief compliance officers..
» Several countries have mature compliance environments (e.g., Argentina and Brazil), whereas others lag significantly behind US standards (e.g., Bolivia and El Salvador).
» Local anti-corruption laws with compliance standards have led to improved compliance programs in several countries (including Costa Rica, Chile, and Peru).

Ensuring organizational justice for all

Emeka N. Nwankpah (page 54)

» Maintaining organizational justice is an important way to cultivate a healthy ethical culture and an effective ethics and compliance program.
» Organizational justice occurs when organizations consistently investigate and address employee misconduct in a way that ensures a fair process, fair treatment, and fair discipline.
» Managing employees' expectations and promoting an appropriate level of transparency helps reduce the inherent concerns employees have related to investigations.
» Organizational justice ensures misconduct is addressed based on principles of equity, not based on how the organization feels about the accused party.
» Organizations that do not seek organizational justice with intention and consistency will create a double standard, knowingly or not.

Is your company's job applicant-tracking system making compliant inquiries?

MaryEllen O'Neill (page 58) **CEU**

» If your company's applicant-tracking system (ATS) asks illegal questions or questions that imply exclusivity, you will lose qualified candidates and could face legal action.
» The ATS should be reviewed by legal and compliance to ensure it is in compliance.
» Those who have access to the ATS should have regular training on the confidentiality and security of its information, and on inappropriate application questions.
» Determine whether the ATS needs to be in compliance with international laws as well as federal and state laws.
» Include a review of the ATS in your annual compliance plan to reflect evolving laws and regulations, any new company locations and acquisitions, etc.

SCCE upcoming events

JANUARY

January 8
Regional Compliance & Ethics Conference
ASIA • VIRTUAL

January 11–14
Compliance & Ethics Essentials Workshop
VIRTUAL

January 21
Applying the COSO ERM Framework to Compliance Risk Management
VIRTUAL

January 22
Regional Compliance & Ethics Conference
SOUTHERN CALIFORNIA • VIRTUAL

January 25
Challenges of Implementing a Risk-Based Third-Party Due Diligence Program
WEB CONFERENCE

January 28–29
Essentials of Compliance Investigations Conference
SINGAPORE • VIRTUAL

FEBRUARY

February 3
Six Principles for Great Compliance Training: Engage Your Audience, Make Your Message Stick, Increase Your Impact
WEB CONFERENCE

February 4
Regional Compliance & Ethics Conference
SOUTH AMERICA • VIRTUAL

February 5
Six Principles for Great Compliance Training: Engage Your Audience, Make Your Message Stick, Increase Your Impact
VIRTUAL

February 11
Regional Compliance & Ethics Conference
MIDDLE EAST & AFRICA • VIRTUAL

February 23
Corporate Compliance Enforcement Conference
VIRTUAL

February 26
Regional Compliance & Ethics Conference
ALASKA • VIRTUAL

2021

Applying the COSO ERM Framework to Compliance Risk Management
January 21 • VIRTUAL

Essentials of Compliance Investigations Conference
January 28–29 • Singapore – VIRTUAL
April 12–13 • VIRTUAL

Corporate Compliance Enforcement Conference
February 23 • VIRTUAL

European Compliance & Ethics Institute
March 15–17 • Europe – VIRTUAL

Higher Education Compliance Conference
June 13–16 • Anahiem, CA

Compliance & Ethics Essentials Workshop
January 11–14 • VIRTUAL
March 1–4 • VIRTUAL

Regional Compliance & Ethics Conferences
January 8 • Asia – VIRTUAL
January 22 • Southern California – VIRTUAL
February 4 • South America – VIRTUAL
February 11 • Middle East & Africa – VIRTUAL
February 26 • Alaska – VIRTUAL
March 5 • Minneapolis – VIRTUAL
March 26 • Boston – VIRTUAL
April 8 • Asia – VIRTUAL
April 23 • Tampa – VIRTUAL
May 7 • Richmond – VIRTUAL
May 14 • San Francisco – VIRTUAL

Event dates are subject to change.
Please visit **corporatecompliance.org/events** for event details.

SCCE Society of Corporate Compliance and Ethics

2020 *CEP* INDEX

Anti-corruption/anti-bribery

- Fight corruption and fraud with data and technology. July, *P. Chanda*
- Recent DOJ compliance policy makes the case for proactive monitoring. October, *E.R. Feldman*
- The everyday, sacred fight against global corruption. October, *K.H. Al-Nur*
- When the government comes knocking: Trends in FCPA enforcement actions. October, *S. Skeldon*
- Mitigating fraud risk in a COVID-19 world. December, *P. Greenspan*

Antitrust/competition

- Big antitrust implications for Big Tech. January, *B. Goncher*
- Effective risk assessments in the evolving antitrust compliance landscape. December, *P.D. Bernstein* and *A.C. Finch*

Board engagement, training, reporting

- Insights from the Delaware courts on board oversight of compliance programs. February, *R. Walker*
- Best friends forever: Nurturing the compliance/board relationship. March, *J. Ruff* and *E.M. Hunt*
- Be heard! Getting the top to deliver your message. September, *A. Barnard-Bahn*

Codes of conduct

- Preventing a 'code red' with an effective supplier code of conduct. March, *S. Hager* and *C. Mattoon*
- The journey to a new code of conduct. August, *W.J. Holzhauer*

Compliance and ethics, general

- Does your organization suffer from compliance prejudice? January, *I. Yeku*
- Foreign compliance risk, Part 1: Politics of business with China. February, *D.J. McCampbell*
- The challenges of building a compliance culture in multinational companies. February, *C. Eray*
- Don't be caught conducting 'desktop due diligence.' March, *I. Yeku*
- The financial compliance risks of business with China. March, *D.J. McCampbell*
- Compliance and legal: Different but aligned. April, *D. King* and *D. Waiters*
- Doing business with China: Managing your company's compliance risks. April, *D.J. McCampbell*
- Storytelling: The best tool you've never used. April, *L.B. Lentini Walker* and *S. Tschida*
- Compliance challenges in the cannabis business. May, *S.C. Kabange*
- Maximizing your compliance and ethics network. May, *E. Brotten* and *J. Drewiske*
- Compliance professionals make natural leaders. June, *J.M. Penrod*
- These five easy writing tips will boost your impact on compliance. July, *A. Yeung*
- Transparency keeps compliance and ethics trending. September, *S. Freidlin*
- The importance of humanizing compliance during a global crisis. October, *N. Gupta*
- Ethics and compliance is the immune system for your organization. November, *J. Suk*
- Be hard on your work, never yourself. December, *V. Eksi*
- Can non-law graduates qualify for compliance positions? Of course! December, *V. Zhou*

Compliance and ethics program management

- Get the $ for your budget. February, *M. Ramírez Chimal*
- Developing a data analytics-enabled compliance program for the real world. April, *M. Reeder* and *J. Kim*
- Data analytics: Data in motion tends to stay in motion. May, *M. Reeder* and *J. Kim*
- Evaluating your program according to the DOJ's Filip Factors. May, *D. Coney*
- Have you adapted last year's guidance to your program yet? May, *E. Simon*
- The importance of a comprehensive, risk-based approach to compliance. May, *M. Vilasevic*
- A look at the French Anticorruption Agency's updated compliance officer guidelines. June, *M. Lancri*
- Digitally automate your compliance scheme. June, *J. Kiyohara*
- Beyond risk mitigation: Implementing effective compliance programs for today's workplace. July, *G. Gallo*
- Compliance and governance in high-tech and agile delivery environments. November, *E. Brotten*
- Using organizational alliances to meet compliance objectives. December, *T. Umukoro*

Conflicts of interest

- 'Management by objectives': An impediment to corporate compliance. November, *I. Yeku*

Employee education/training
- Teaching your staff to be accountable. February, *S. Carter*
- Mentoring in compliance: Building and sustaining critical relationships. March, *L.B. Lentini Walker* and *D. Ayala*
- Compliance champions can help you drive a stronger compliance culture. May, *D. Milne*
- 'Championing' your compliance program. November, *M. Silverman*
- Compliance ambassadors wanted! November, *M. Ramírez Chimal*
- Upgrade your employee survey for more accurate results. December, *T. McAlister*

Ethics, ethical culture
- Unconscious bias and psychological safety: How they affect compliance. March, *M.B. Hood*
- Build trust with self-reflection and effective communication. April, *J.A. Thinnes*
- 'Making the numbers': How compliance can boost ethical sales behavior. September, *K. Kluvo*
- Looking to transform corporate culture? Start with core values. October, *J. Seeber*
- Food for thought: The social-ecological business ethics model in action. December, *D. Brady*

Higher education
- A schema for compliant, decisive curricular changes in higher education. March, *L. Kavlie*

Investigations and auditing
- Investigating high-profile individuals: Not as easy as we think. January, *M. Rueda*
- When your process doesn't match your procedures. January, *A. Holloman*
- The role of data analytics in regulatory inquiries. March, *S. Neuman* and *J. Dennis*
- The GDPR is not a shield against internal investigations. April, *K. von Reden-Lütcken*
- Conduct a legal premortem to identify and mitigate risk before a crisis. August, *J. Aronie*
- Who's responsible here? Getting it right when misconduct allegations arise. November, *B. Naples*

Interviews
- Meet Raj S. Kuppusamy: Raising the global ethical bar. January
- Meet Pedro Ruske Freitas: The evolution of Brazilian compliance. February
- Meet Diana B. Henriques: What if your gut is wrong? March
- Meet Lisa Kuca, CCEP: Crisis is a marathon, not a sprint. April
- Meet Seiichi Hara: Growing compliance in a context-dependent society. May
- Meet Barry Mano: 'One breath of scandal freezes much honorable sweat.' June
- Meet Blair Marks: The best defense is training. July
- Meet Thomas Meiers: Volkswagen's commitment to change. August
- Meet Peter C. Anderson: Righting the compliance ship. September
- Meet Bob Borntrager: Compliance in the public sector. October
- Meet Cansu Eray: Multicultural teams lead to success. November
- Meet Justin Ross: Delivering compliance globally. December

Measuring effectiveness
- Perfecting the recipe for your ethical culture assessment 'sauce.' October, *S.D. McGinnis* and *J.A. Gustafson*
- Five factors for discovering your compliance team's effectiveness. November, *A. Barnard-Bahn*

Mergers and acquisitions
- Dodging US employment law violations during international mergers and acquisitions. July, *T. Stromberg* and *J. Garcia*
- Gaining a seat at the M&A table. July, *K.T. Ingram*
- Organize your data today for smooth and lucrative mergers tomorrow. September, *V. Sunak*
- Sharpen M&A with compliance and ethics due diligence. September, *R. Rohr*

Modern slavery and human trafficking
- Private sector heroes: Fighting modern slavery through compliance. February, *M. Friedman*
- California's new human trafficking legislation requires higher employee training standards. June, *M. Friedman*
- Effective due diligence considers human rights risk. November, *L. Mooney*

Policy development/ implementation
- On giving and receiving: What does your hospitality policy say? July, *V. Pillai*

Privacy and data protection
- Budgeting considerations for continuous monitoring of data privacy and security. January, *A.T. Jackson*
- Privacy compliance challenges in 2020 and beyond. January, *M. Crespo* and *G. Beloto*
- The draft CCPA regulations reviewed: Key takeaways. February, *J. Terry*
- Use the human-centered approach for smarter security

and compliance teams. March, *S. Durbin*
- A new decade in data privacy: Complying with the CCPA. April, *C. Fleischmann* and *E. Hintz*
- Privacy: No longer a check-the-box function. April, *D. Solo* and *B. Sweeney*
- Learning to slow down in the Internet of Things era. May, *M. Lanterman*
- Three big tips to help keep your company GDPR compliant. May, *P. O'Kane*
- Big data: What's the big deal? June, *D. Hockley*
- Two years of GDPR: The security breach lessons we've learned. July, *J. Armstrong*
- Blockchain and the GDPR: Can the conflicts be resolved? August, *M. Brown*
- Is your cyber insurance enough? August, *E. Kron*
- The CCPA and when privacy law overlooks internal compliance functions. August, *S.L. Pardau*
- If you can't protect data, don't collect data. September, *D. Gonsowski*
- The 'data era' is revealing gaps in financial compliance technology. September, *Y. Hazan*
- Building an IT compliance center of excellence. October, *A.M. Bag*
- Compliance in a work-from-home environment. October, *R. Bond*
- Shifting to the ethical mindset when making data decisions. October, *P.S. Hrubey* and *C.M. Moschell*
- Consistency and transparency: Getting connected products to reflect organizational values. December, *B. McNeil*

Records management
- Blockchain: Moving target or trusted tech trend? August, *S. Dworak* and *T. Quimby*

Risk assessment/management
- Make risk management part of your remuneration plan. July, *E. Tsintzas*
- Mitigate more risks with a change management program. August, *H. Powell*
- Prioritize sanctions risk in your compliance program. August, *I. Yeku*
- Risk management starts with the employees. August, *P.H. Zietsman*
- Make compliance risk assessment your program's foundation. September, *M. Tuchow*

Third-party risks
- Third-party due diligence red flags: Now what? January, *M. Cutler*
- The tough Corporate Sanctions Act is on Germany's horizon. June, *M. Reischl* and *C. Skoupil*
- What legal teams should know about CCPA supplier readiness. June, *D. Goldman*
- Collaboratively building effective third-party risk management processes. December, *V. Pickens*

Trade, international
- What the evolving sanctions landscape means for your transnational organization. June, *I. Yeku*

Whistleblowing
- International whistleblowing legislation and America's False Claims Act. January, *M.S. Raspanti* and *M.S. Auten*
- Creating and leading a whistleblowing program: What to consider. February, *I. Yeku*
- Weaponizing whistleblowing. February, *S. Young*
- A practical guide for navigating the EU's whistleblower protection directive. April, *J. Arbery* and *L. Van Houten*
- An introduction to Brazil's new whistleblower protection law. June, *A.P. Barcellos*
- The overtaxed investigator: When whistleblower reports aren't properly prioritized. July, *M. Cutler*

Columns
Letter from the CEO, *G. Zack*
- Where are your program's boundaries? January
- Train them, then train them (and us) some more. February
- Oh, nobody worries about that provision. March
- The changing face of the profession. April
- So, who really owns compliance? May
- Lessons learned from an empty office. June
- Another argument for analytics. July
- A new appetite for risk? August
- But will it be enforced? September
- Weeding through due diligence. October
- The politics of ethics. November
- Turning the page on 2020 for SCCE. December

Conversations on culture, *S. Priest*
- This should make you squirm, but it probably won't. February
- A great message from Phil Rudolph, retired chief legal officer. April
- The egg is cracked open. June
- A pandemic is not your biggest risk. August
- Does the truth matter? October
- Farewell column. December

Empirically speaking, *B.K. Lee* and *D. Zhang*
- Responding to a new (and rising) social consciousness. February

- Getting started with ESG reporting: Choosing what to disclose. April
- How compliance can help respond to macro crises. June
- Balancing privacy, ethics, and safety during COVID-19. August
- Meeting DOJ's 2020 guidance on effective reporting and investigations. October
- Maximize compliance's impact by choosing applicability over accessibility. December

EU compliance and regulation, *R. Bond*
- Developing a global approach to data protection compliance. January
- Transfers of personal data from the EU in 2020. March
- Is it wise to keep personal data for longer than necessary? May
- Data protection and information security with remote work. July
- When is direct marketing 'fair' in the EU? September
- Prevent that dam(n) breach! November

How to be a wildly effective compliance officer, *K. Grant-Hart*
- Are you guilty of chronic over- and underestimating? January
- When uncertainty strikes, strike back. February
- What you can and can't change. March
- The critical question you're not asking. April
- Are you relevant? May
- Ouch! Stop all the friction. June
- Keep the pendulum from swinging too far. July
- The ultimate mastery. August
- On the crucial skill of managing expectations. September
- Forget what you learned in school. October
- Getting to the next 'yes.' November
- Anticipating and overcoming objections. December

Kaplan's court, *J. Kaplan*
- Risk assessment: The general and the specific. February
- Key elements of an investigations manual. April
- Beyond the attorney-client privilege. June
- Insider trading compliance programs. August
- Effective discipline according to the DOJ. October
- Culture assessments: The short course. December

The view from Nickel City, *J. Kennedy*
- New year, new you? February
- Internal audit: Friend or foe? April
- Compliance during crisis. June
- When is documentation too much? October
- Compliance in the age of cost containment. December

Byrne on governance, *E. Salmon Byrne*
- Willingness to report, faith in senior leadership are key to ethical culture. February
- Diversity comes to the boardroom-finally. May
- Evolving oversight: Trends with boards of directors. November

The other side of the story, *S.J. Kim*
- Progress has been made in Brazil, but questions remain. September
- Progress has been made in Brazil, but questions remain, cont'd. November

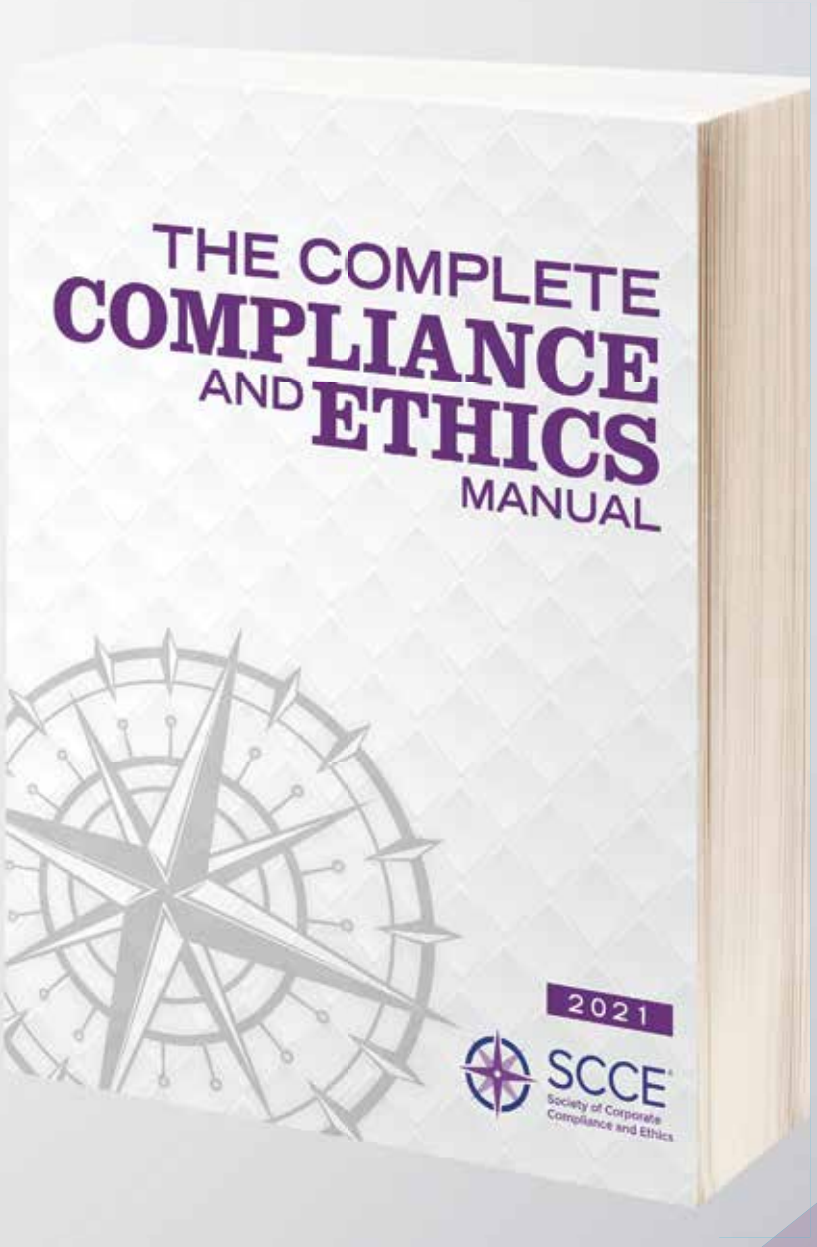
A view from abroad, *S. March*
- Strategic planning. January
- Nordic noir. March
- Airbus and the web of corruption. May
- Are boards missing the ethics boat? July
- Lessons from the time of COVID. September
- Under pressure. November

The last word, *J. Murphy*
- Do sociopaths matter for our compliance programs? January
- Hard work eats buzzwords for lunch! February
- Roy Snell. March
- Saying 'thanks'! A secret compliance tool that actually works. April
- Ready for the dog and pony show? May
- Training and communication. June
- In the field. July
- Learning from actual cases. August
- Reporting to the board: Is materiality the standard? September
- Live training is clearly the best way (or is it?) October
- Where are the cases? November
- To the one with a hammer, everything looks like a nail. December

Driven, *W. Johnson*
- Competition: Road to victory or collision course for disaster? January
- The 'pit stop' approach: Strategically improving efficiency and achieving goals. March
- Leadership in crisis management. May
- Crisis management: The aftermath. July
- Learn more about professional skills at the 2020 CEI. September
- Our last dance. November

One trusted source

Get the most up-to-date compliance and ethics information from one trusted source. *The Complete Compliance and Ethics Manual* has the information you need to build and maintain a successful compliance and ethics program.



New content in the 2021 manual includes the following topics:

- Root Cause Analysis
- Data Privacy Risk Management
- Does GDPR Apply to My Organization?
- California Consumer Privacy Act
- Establishing E&C Programs for Government Agencies
- Fake IDs and Confirming Identity

Upgraded content in 20 areas including:

- Employee Discipline and Compliance
- Independent Investigations Overseen by the Audit Committee
- Antitrust Law Risks
- Environmental Law Risks
- False Claims Act Risks

Available online now and in print mid-January.

AVAILABLE IN THREE FORMATS

Softcover print book

One-year online subscription

Money-saving bundle

Learn more
corporatecompliance.org/ccem

SCCE
Society of Corporate Compliance and Ethics

Fill your open positions with SCCE's Job Board

The SCCE Job Board is designed to connect organizations with job seekers in the compliance and ethics field.

Reach professionals from across the globe with varying levels of experience.

Get started
corporatecompliance.org/job-board/post-job

SCCE
Society of Corporate Compliance and Ethics