JANUARY 2023

COMPLIANCE & ETHICS PROFESSIONAL

CEP MAGAZINE

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

MATT SILVERMAN, JD, LLM
GLOBAL TRADE DIRECTOR & SENIOR COUNSEL,
VIAVI SOLUTIONS, CHANDLER, ARIZONA, USA

COMPLIANCE AS A CATALYST (P8)

SCCE®

Aerospace, Defense & Government Contracting Compliance & Ethics Conference

February 21, 2023 • Virtual (CT)

Get up to speed on Aerospace, Defense & Government Contracting

Join us from the comfort of your home or office to learn how experienced professionals navigate day-to-day compliance issues amidst the internal standards and external regulations of this high stakes industry.

Topic highlights include:

- Federal Acquisition Regulation (FAR) compliance
- Employee reporting and speak up culture
- ERM/GRC strategies
- Artificial Intelligence
- Cyber security and CMMC
- Diversity, equity, and inclusion (DEI)

Register
corporatecompliance.org/2023aerodef

SCCE®
Society of Corporate Compliance and Ethics

Learning from the FBI

by Gerry Zack

I recently returned from the Corporate Compliance Professional Outreach Event — presented in late September by the Federal Bureau of Investigation (FBI) — a popular event SCCE & HCCA has sponsored with the FBI annually. I last wrote about the SCCE/FBI Corporate Compliance Outreach Event for *Compliance Today* magazine in 2019, shortly after that year's event and just before the pandemic, which resulted in the cancellation of the 2020 and 2021 outreach events.[1] The event is organized by the FBI's Office of Integrity & Compliance, which is responsible for the Bureau's compliance program.

The entire program was excellent and well-organized. But one of the key takeaways for me this year was how the FBI practices so much of what we suggest as "best practices" for compliance programs. There are many things the FBI does well, so I'll focus on just a few of them in this column.

First, the FBI identifies compliance risks at multiple levels below the enterprise level. This is an important element of the risk assessment process. Some compliance risks may be unique to a single business unit, while others can affect many units or the entire organization. Accurately capturing this information makes for a much more reliable assessment of the significance of risk and helps establish risk priorities.

The FBI's compliance program also relies heavily on collaboration with units that own the risks — as well as other units — for its success. The Office of Inspections and the Office of Internal Auditing are the two other legs of the three-office group that makes the compliance program work. The Office of Internal Auditing has established a robust data analytics program to monitor activities for signs of compliance problems.

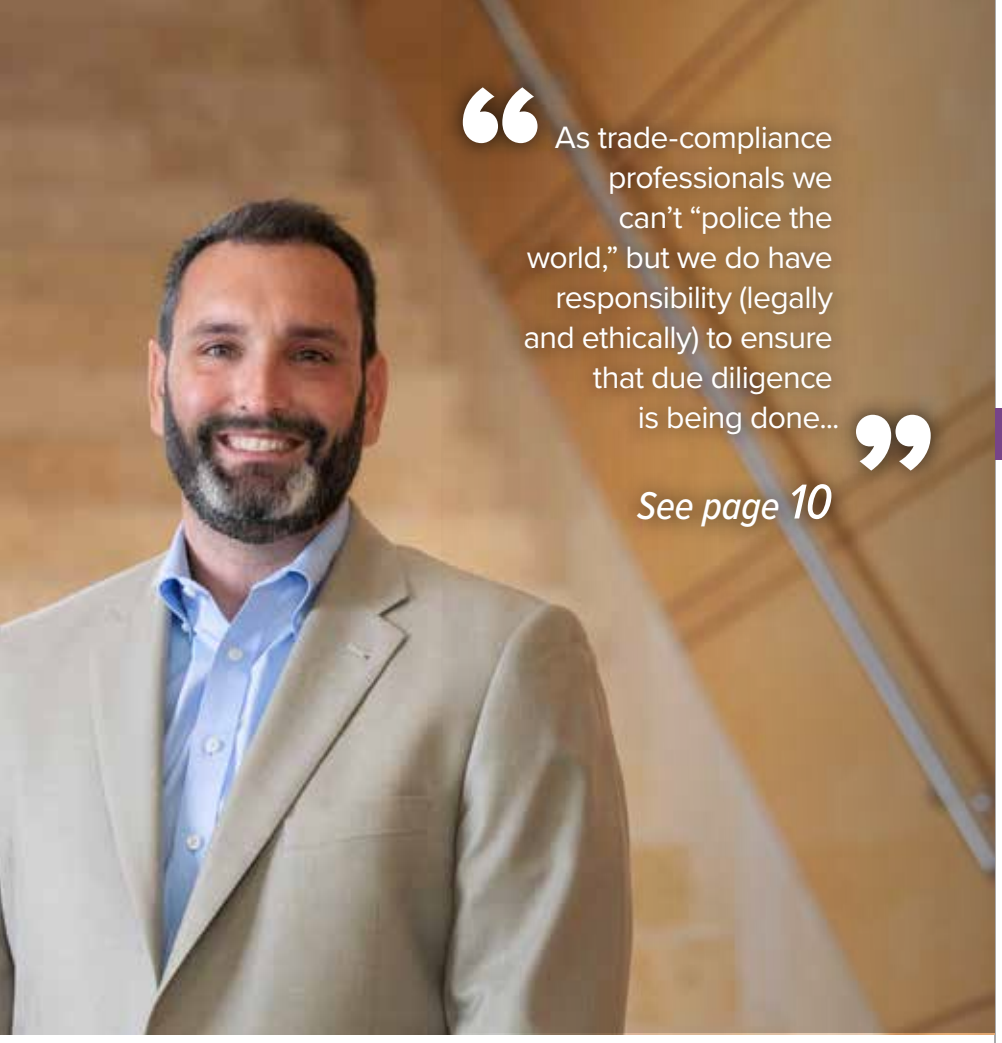
And a final characteristic of the compliance office that impressed me is the inclusion of two special agents in the office. This is done to provide perspective to the compliance team as it works with the various units within the FBI. Including people with hands-on experience in the business units has emerged as an excellent way for organizations to strengthen their compliance programs, and it was great to see the FBI embrace this practice.

The FBI continues to impress me as a stellar example of a government agency that acknowledges and fixes its weaknesses and continues to make improvements to its compliance program on an ongoing basis. Thank you for sharing your program and experience with us.

Gerry Zack
CCEP, CFE, CIA
(gerry.zack@corporatecompliance.org, twitter.com/gerry_zack, linkedin.com/in/gerryzack) is CEO of SCCE & HCCA in Eden Prairie, Minnesota, USA. Please feel free to contact Gerry anytime to share your thoughts: +1 612.357.1544 (cell), +1 952.567.6215 (direct).

Endnotes

1. Gerry Zack, "Observations from the FBI Compliance Academy," *Compliance Today* October 2019, https://compliancecosmos.org/observations-fbi-compliance-academy.



COMPLIANCE & ETHICS PROFESSIONAL

CEP MAGAZINE

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

January 2023

Columns

Features

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

VOLUME 20, ISSUE 1

Departments

Articles

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

Virtual Compliance & Ethics Essentials Workshop

Essential knowledge for your compliance career

Whether you're new to compliance or have been practicing for a while and need a refresher, attending an SCCE Compliance & Ethics Essentials Workshop is for you!

In this four-day virtual workshop, industry leaders will guide you through the core elements of a compliance program and get you caught up on the latest strategies and best practices for you to bring back to your organization.

Workshop topics include:

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

Upcoming 2023 Workshops

February 6–9 • CENTRAL TIME (CT)

May 15–18 • CENTRAL TIME (CT)

September 18–21 • CENTRAL TIME (CT)

October 16–19 • CENTRAL EUROPEAN TIME (CET)

December 4–7 • CENTRAL TIME (CT)

Learn more and register
corporatecompliance.org/essentials

SCCE
Society of Corporate Compliance and Ethics

SCCE association news

Essential learning for your growing career

corporatecompliance.org/essentials

If you're just starting out in your compliance career, it's important to lay a foundation with all the essentials. Understanding the core elements of a compliance and ethics program will help guide you to areas where your organization may need help, or topics that are of interest to you to explore. Just as a house can go in many ways once the foundation is laid, so can your career and your program—but it all starts with those essential building blocks.

It's not just first-time practitioners who need to understand the essentials, though. Home remodels, additions, and upgrades all require a look back at the foundation to make sure nothing has crumbled, shifted, or changed in terms of construction codes. The same is true in compliance. If you've been in compliance for a few years and feel the need to revisit the essentials, don't worry. It's not unusual. In fact, SCCE has found that often more than 40% of our workshop attendees have been in compliance for 5 or more years. In this ever-evolving industry, it makes sense to do a wellness check on your understanding of the basics from time to time.

Our essentials workshop is a four-day comprehensive look at the core elements of a compliance program and can fit the needs of those brand new to compliance as well as those looking for that refresher. Our instructors, experienced industry leaders, will guide you through the fundamentals and help you build, reconstruct, and/or re-examine your compliance foundation for years of success and confidence in your role.

Does your role fall into one of these categories?

- Compliance officer
- Internal auditor
- Data privacy officer
- Regulatory compliance specialist
- In-house or external compliance lawyer
- Compliance student
- Compliance analyst
- Compliance assistant
- Compliance specialist
- Compliance coordinator
- Compliance administrator

If yes, please join us in 2023 for one of our Compliance & Ethics Essentials Workshops and get ready to build a great career!

Learn more and register
corporatecompliance.org/essentials

SCCE COMPLIANCE 101

Explore the fundamentals of corporate compliance and ethics

Newly updated and in its third edition, *SCCE Compliance 101* is an overview of compliance programs and a compliance officer's role. Perfect for new practitioners, board members, or staff education, this book features guidance and insight on:

- Benefits and administration of a compliance program that follows the seven essential elements
- Government guidance and laws
- Risk assessment, monitoring, and auditing
- Program assessment and measuring effectiveness
- Sample compliance forms, templates, and plans

Now in its third edition!

SCCE Compliance 101 has been updated with new insights and tips on how to build an effective compliance program. It has all new chapters focusing on risk assessment, investigations, government oversight, and more, as well as new sample policies, forms, and further resources to explore.

About the authors

Authors Debbie Troklus and Sheryl Vacca have decades of compliance and risk management experience in both corporate and healthcare settings. Troklus and Vacca sit on SCCE® & HCCA®'s Board of Directors and serve as key faculty members at SCCE® & HCCA® Academies.

Learn more
corporatecompliance.org/compliance101

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 *scott.moe@corporatecompliance.org*

- **Forrest Deegan** is now the chief ethics and compliance officer for Victoria's Secret in Columbus, Ohio, USA.
- Noventiq has appointed **Gareth Tipton** as global chief compliance officer and vice president of legal, governance and compliance in London, England, United Kingdom.
- **Felipe Maldonado Garcia** is now the director of compliance programs at Salesforce in Miami, Florida, USA.

COMPLIANCE AS A CATALYST

Meet Matt Silverman

JD, LLM

Global Trade Director & Senior Counsel at VIAVI Solutions

an interview by Adam Turteltaub

Matt Silverman (matthew.silverman@viavisolutions.com) is Global Trade Director & Senior Counsel at VIAVI Solutions in Chandler, Arizona, USA.

Adam Turteltaub (adam.turteltaub@corporatecompliance.org) is Chief Engagement & Strategy Officer at SCCE & HCCA, based in Eden Prairie, Minnesota, USA.

AT: You have tremendous experience in trade compliance, which has gone in recent years from a very low-profile field to one that makes headlines on the news. What led you to it?

MS: I started out my legal career practicing in an area of law that I really didn't enjoy. My expectations in being a trial lawyer hadn't panned out how I had expected. So, I decided to make a big career change. I went back to school at Georgetown to study international trade law and during my time in Washington, DC, I also got great opportunities to work on trade law and policy in places like the U.S. Senate, U.S. Trade Representative, the World Bank, and in the global trade group at a major law firm. My experience in DC helped me focus my practice on trade law and to begin a broader career in compliance that is developing to this day.

AT: It's a complex area of compliance. For those who may be unfamiliar, can you give us an overview of the key risk areas?

MS: Trade compliance generally gets divided into four areas: export controls, customs, sanctions, and antiboycott compliance. Export controls are the laws and regulations that control the export of goods, technology, software, and services all over the world, depending on the type (or "classification") of the item and where it is being exported to. Customs work is a broad area but is focused on compliance in the import of goods — everything from tariff codes to supply-chain security to compliance with regulations concerning the import of hazardous goods. Sanctions always seem to get the most buzz in the news. This area of practice deals with restrictions on individual parties and countries (e.g., sanctions on Russia and Iran). Finally, antiboycott compliance (an often-overlooked area of trade compliance) is centered on the US antiboycott laws and the types of language that US companies can agree to regarding foreign boycotts — specifically, the Arab League boycott of Israel. The commonality among all these areas is that they are dependent in some ways on the day-to-day geopolitical environment, which makes the job of a trade-compliance professional both challenging and exciting!

AT: It's important to remember that this doesn't apply to just hard goods. Services and data can also be restricted. What are some typical areas to be on the lookout for that might be missed?

MS: That's right. A lot of what keeps me busy during the day (and keeps me up at night) is not necessarily related to what most people may think of as "traditional" exports. For example, managing the export of defense services or the export of US-controlled technology to a foreign national is a big part of trade compliance. The latter, referred to as a "deemed export" can be overlooked or misunderstood by global companies in that it's an area unique to US law (no other countries have the concept of deemed exports). Deemed-export controls restrict the transfer of technology to people based on their nationality, not their geographic location. Deemed exports pose specific complications for trade-compliance professionals and often require working with stakeholders in human resources and IT security to ensure compliance. Some of the biggest areas of concern are the relationships between deemed exports and data privacy, as well as antidiscrimination laws. The balancing act between trade compliance and these other areas require trade-compliance professionals to maintain a breadth of compliance knowledge.

The balancing act between trade compliance and … other areas require trade-compliance professionals to maintain a breadth of compliance knowledge.

AT: The whole area of dual-use technology that could be put to civilian or military purposes is a particularly tricky one. What systems should organizations have in place to ensure their products are being used for the intended purpose and not the prohibited one?

MS: It all starts with having comprehensive policies and procedures that relevant stakeholders within the business receive training on and understand.

This is true for almost any area of compliance, but it's of particular concern for trade compliance because the implications of noncompliance can be so severe. At the core of these policies and procedures are requirements for the business to *know your customer* (KYC). KYC training should be led by trade-compliance professionals to ensure the relevant stakeholders (sales, procurement, marketing, etc.) know who they are dealing with and selling to, as well as the "red flags" to be aware of. In addition, having an end-user program in place is a good way to ensure compliance as well as mitigate any potential liability that can result if an item does get into the hands of the wrong person. As trade-compliance professionals we can't "police the world," but we do have responsibility (legally and ethically) to ensure that due diligence is being done — which may often go above and beyond what is required by law.

AT: Sanctions have been growing in both scope and frequency over the last few years. We have seen them directed at nonstate actors, Iran, and most recently Russia. Many businesses have likely had to add or increase their export control efforts dramatically. What's the best way to start?

MS: It's key to understand your business (where your offices are, where and who you sell to, what classification of products you sell, etc.) and how that overlaps with new export controls and evolving sanctions. Sanctions on many countries are often incredibly complex, but if you don't understand the basics about your products, your supply chain, and your sales footprint, it's impossible to apply the rules. Having a good understanding of the risk appetite and "aggressiveness" of the business is critical in informing the trade-compliance professional's role. While we never sacrifice compliance for profits, trade compliance (just like most other compliance areas) can often find room for acceptable compromise to avoid overcompliance.

AT: One thing that can't be overlooked as part of an exports control program is antiboycott law, which prohibits supporting boycotts of US allies. In practice, it most often comes up as it relates to the Arab boycott of Israel. How big of an issue is that these days, or with improving relations between Israel and its neighbors, is it less of a concern?

MS: It's still a concern as it applies to the Arab League boycott, and in some cases, outside the Arab League. US companies who deal with countries and companies in the Middle East must be aware of the language in documents like contracts, requests for quotes, and invoices that could pose boycott concerns. Training is key. Trade compliance may be responsible for providing guidance, but if the contracts, procurement, or sales teams don't know how to spot problematic language, having an antiboycott policy in place is meaningless.

AT: The sales and marketing team will need to be brought up to speed quickly. What have you found is the best way to train them? Do they need nuance or just enough to know when they should be calling you or your colleagues for help?

MS: Yes, some nuance is necessary, otherwise you'd have these teams calling the trade-compliance function every minute to have questions answered or seek approval for a potential opportunity or sale. Of course, you want them to err on the side of contacting trade compliance if they aren't sure about an issue, but you also want them to have enough knowledge to be able to make decisions autonomously, while being mindful of compliance concerns. In general, we want to encourage the business to reach out with questions while being proactive in the training and knowledge we provide.

AT: Where do companies typically make mistakes in their export control programs?

MS: The biggest mistakes are often the simplest to correct. Companies that don't have written and comprehensive policies and procedures in place are making a big mistake. Some companies operate under the impression that knowledge as to trade-compliance policies or processes can simply "live in people's heads." This approach is concerning for several reasons. First, when those people leave the company, who retains this knowledge? Second, informal or unwritten policies and procedures lead to inconsistency in their application. Our trade-compliance approach is to ensure we have up-to-date policies and procedures in place and that our business is regularly trained on them.

AT: You've done a lot of speaking in the past few years, not just on trade compliance but on a variety of other topics. What prompted this?

MS: The speaking was at first a natural progression from my

trade-compliance career; I had developed a good amount of practical knowledge in the field that I wanted to be able to share with others at industry events and conferences. The speaking I do now is sometimes related to trade and compliance topics, but I also speak on issues of leadership, employment engagement, and my experience in building and improving champions networks. Speaking has been a great outlet for me share my knowledge and insights with a larger community (not just trade compliance or compliance in general), as a lot of what I speak about has broad applicability across organizations and industries.

AT: While export controls is its own specialty field of compliance, it's not separate from compliance. What I mean is it's not like export controls people sit alone in a dark room during their work. You need to build awareness of the issues in the sales force and among management. You also must be accessible to answer questions and try to find solutions. How do you encourage that interaction and discourage the belief that you're only there to prevent sales from happening?

MS: There are multiple avenues to this approach to make sure the business is aware that while we are here to protect the company and remain compliant, it's not our *goal* in trade compliance to be a roadblock. One approach I prefer is to involve stakeholders early on and throughout the drafting and implementation of trade-compliance policies that may directly impact them. For example, if we draft a new policy on hiring foreign nationals, this policy is going to have an impact on functions like human resources and talent acquisition. We take an inclusive and collaborative approach with relevant stakeholders in the business: "How is this policy going to make your job difficult?" "How can we make it fit better with what you do and be feasible for you to follow and adhere to?" "What is confusing about the policy?" "What needs streamlining?" "What are we not considering that we should?" This approach can be utilized for almost any organizational function, as it encourages stakeholder interaction and involvement with compliance. In many ways, the trade-compliance function can serve as a *catalyst* to the business, by encouraging and assisting in the development of compliant solutions to otherwise restrictive laws and regulations.

AT: One way to increase outreach that I know you are a fan of are compliance champions, or ambassadors programs. You speak at and helped shape the SCCE "Leading an Effective Ethics & Compliance Ambassadors Program" virtual event. What led you to ambassador programs as a possible solution to compliance challenges?

MS: I saw how well they functioned at companies I had worked for, especially at large companies where people were spread out all over the world. When I joined my previous company, I was tasked with the goal of creating a trade-compliance champions network. I collaborated with leaders of that company's existing champions networks (ethics, IT security, and privacy) to develop *my* version of a network. I learned the difficulty in developing such networks is not just in recruiting champions or structuring the program, but in getting the commitment needed from management and the workforce. These are lessons and experiences I carry with me as I speak on this subject and continue to work on champions network development.

In many ways, the trade-compliance function can serve as a catalyst to the business, by encouraging and assisting in the development of compliant solutions to otherwise restrictive laws and regulations.

AT: Through the years, what have you found are the best ways to encourage people to serve as ambassadors?

MS: You want to recruit volunteers, not "volun-tolds." Serving as an ambassador shouldn't be a form of punishment to low-achieving or disinterested employees. It should be the mark of a productive and loyal employee to whom their colleagues look as someone they can approach for questions or concerns. A great way to find and recruit potential ambassadors is to write a compliance article and post it on an internal company board. See who responds in the comment

section. You can often find people in areas across the business who have an interest in compliance this way, and who may be willing to help serve as an ambassador.

AT: Other than having the right ambassadors, what do you find is best for encouraging employees to interact with them?

MS: First, employees have to be aware that a champions network exists! Champions networks need to be internally publicized, whether that's through branding, emails, newsletters, posters, or meeting announcements (or all the above) so the workforce knows who their champions are and the service they provide. Through all this publicity, the messaging needs to be clear: champions provide a service to help inform and protect employees, not to act as spies or report those they see acting noncompliant. Publicity and trust are key components of an effective champions network.

AT: Ambassador programs have exploded in popularity over the last few years. Looking to the future, how else do you see compliance evolving?

MS: I see champions networks becoming more popular and necessary, especially given the trend of remote work. Generally, employees working from home more and going into the office less have, in turn, resulted in less organic interaction and engagement with their colleagues. This leads to less awareness and engagement when it comes to compliance. Compliance champions networks of all sorts can help to fill in these gaps. More generally, a growing trend toward corporate social responsibility, including environmental, social, and governance initiatives, is going to require a broadening of compliance roles. As just one example, the trade-compliance function now needs to be more aware than ever of forced labor concerns in its company's supply chains, and be prepared to act accordingly. I see compliance professionals becoming less and less siloed in their future roles — trade compliance will be no exception.

AT: Thank you, Matt, for your insight!

CREATING EFFECTIVE COMPLIANCE TRAINING

FEBRUARY 15-16, 2023 | *VIRTUAL*

JUNE 21-22, 2023 | *VIRTUAL*

JULY 31 - AUGUST 1, 2023 | *IN-PERSON • ORLANDO, FL*

NOVEMBER 1-2, 2023 | *VIRTUAL*

Gain insights and strategies for developing and managing a successful compliance training program

Learn how to:

- Identify and understand your organization's training needs
- Develop engaging and effective training content
- Determine which educational model is best for your workforce
- Help managers build on-the-job compliance awareness

Register online
corporatecompliance.org/compliancetrainingworkshops

SCCE
Society of Corporate Compliance and Ethics

"GOAT" COMPLIANCE PROGRAMS

by Mark Jenkins

Mark Jenkins
CFE
(mjenkins@kreller.com) is the Director of Forensic Investigations with the Kreller Group in Dallas, Texas, USA.

I have always loved to compete in sports, even though I have been consistently mediocre. In contrast, I like to watch sports because I like watching the Greatest Of All Time — a.k.a. the "GOAT."

People will always debate about the GOAT in each sport. Tom Brady, with seven Super Bowl victories, is a great candidate for football. Serena Williams has won 23 major singles titles, dominating women's tennis for the last two decades. My personal all-time favorite is Earvin "Magic" Johnson, who won five NBA titles in basketball in the 1980s. Each checked many boxes: they had great technique and intangibles, worked to improve aspects of their craft in the off-season, and had solid overall game IQ. All have at least one thing in common: results. They won — a lot — at the highest levels of their respective sports.

What about the gold standard in anti-bribery/anti-corruption (ABAC) compliance programs? What makes a program the GOAT? Whatever the U.S. Department of Justice (DOJ) and Securities and Exchange Commission (SEC) demand of companies? The DOJ/SEC guidance in the last decade should be part of every compliance program because, as we will explore, it sets a standard. However, continuous monitoring — which includes regularly conducting third-party audits — is also necessary for GOAT status and, more importantly, to detect and prevent corrupt activity.

What are the regulatory demands?

The DOJ/SEC, for the last decade, has supplied several guidance documents, including *A Resource Guide to the U.S. Foreign Corrupt Practices Act* which details what it expects in corporations' ABAC compliance programs. They expect that a compliance program is well-designed, in good faith, and uses continuous monitoring. They also set forth the following statement:

> "Third, companies should undertake some form of ongoing monitoring of third-party relationships. Where appropriate, this may include updating due diligence periodically, exercising audit rights, providing periodic training, and requesting annual compliance certifications by the third party."[1]

Compliance officers might push back and claim, "Well, this is just guidance."

However, take this random selection of DOJ enforcement actions against 20 companies from the DOJ website in the last five years (2017–2022) — there is no statistical significance in my selection — and review specific points from indictments, information documents, and DOJ press releases (see Figure 1).[2]

Figure 1: 20 Enforcement actions

Description	No.	%
Failure to Disclose	20	100%
Third-Party Intermediary	17	85%
Companies Monitored	13	65%
Received Credit	8	40%
Disguised Payments	8	40%
FCPA Repeat Offenders	5	25%
Total Reviewed	**20**	

None of the 20 companies (I did not look at individuals charged) voluntarily disclosed their bribery issues. There could be many reasons the 20 did not: counsel may have recommended that they not reveal, the entity did not believe they would be discovered, the compliance program did not include continuous monitoring, or the compliance program did not catch the issue when it occurred. Regardless, not voluntarily disclosing the bribery issues appears to have cost the offenders in the penalty assessment phase.

Seventeen out of 20 (85%) enforcement actions involve bribes being funneled through a third-party intermediary (TPI). The DOJ assigned 13 entities (65%) a monitor, meaning the DOJ had no confidence that the entity's compliance program was adequately equipped going forward. An entity being assigned a monitor is equivalent to the "death penalty" in NCAA sports. The company must pay the monitor to micro-analyze the development or enhancement of the compliance program over several years. Monitors are usually legal or consulting firms with substantial billable rates.

Five of the randomly chosen companies were repeat offenders. At least three had three or more offenses.

Based on this back-of-the-envelope analysis, TPIs often participate in corrupt activity and, overall, inadequately designed compliance programs by the offenders are evidenced. DOJ shows no signs of slowing down — nor are the trends deviating from assigning costly monitorships. Compliance officers should take heed to ensure their program's integrity and focus on the highest risks.

Risk scoring TPIs

Despite the above findings on third-party involvement in corruption, companies realistically need to conduct a cost/benefit analysis, as most organizations need help to afford to conduct due diligence and/or TPI audits on every vendor.

Before deciding if a TPI should be audited, a risk-scoring exercise is warranted. Entities can go through varying levels of sophistication as part of risk scoring. If a company does not risk score its TPIs wisely, costs will not be distributed to the greatest areas of concern. Risk factors and questions to consider can include:

- The geographic location of the TPI and where it conducts business determine prominent levels of corruption in those countries.
- Identifying TPIs with contact points with foreign government officials and where those contact points are in the transactions (e.g., customs, taxes, licenses, permits such as building a facility, and visas).
- The revenue generated through the TPI.
- The role of the TPI. Is the intermediary a commercial agent, broker-dealer, distributor, professional services provider, or selling products directly to the company?

- History with the TPI. Has the company conducted business with the TPI in the past, and if not, how was the TPI introduced to the company? Did a foreign government recommend the TPI? Did the TPI approach the company?
- The reaction by the TPI to a due diligence investigation conducted on the TPI and its owners. Was there pushback when requesting financial or ownership information? Was the due diligence questionnaire filled out completely?
- The results of the due diligence investigation, were there red flags and, if so, what was the nature of the risk concern(s)?[3]

Choosing TPIs

Based on risk scoring, a prioritized list of high-risk vendors should be developed, and audits conducted on the highest-risk TPIs. If red flags were found in the due diligence and the company decides to continue doing business with the TPI, then the company should audit the TPI as soon as possible before going forward.

Audit steps and techniques

Audit team

Before an audit begins, assemble a qualified team. The team should consist of experienced investigators and forensic accountants familiar with obtaining and analyzing large accounting and financial datasets. If the team members are external to the company, the company's internal auditors or compliance professionals should be part of the team since they should understand the company's business operations. Also, it is important to use the local country's resources to familiarize themselves with the local customs, language, regulations, and business processes. You may think that sounds like a lot of people for an audit. Typically, you can find practitioners with many of these skill sets; therefore, fewer people will be needed.

Audit objective

The goal of the audit should be discussed and solidified. Generally, audit goals should be identifying areas of risk in (a) the entity's compliance programs, (b) transactions, and (c) the key owners/employees (tone at the top).

To meet these objectives, discussions with key employees should be conducted to determine their level of understanding concerning ABAC compliance, internal controls, and their attitudes towards both.

Sample document request

Although each TPI's audits are unique, a typical document request (covering at least two years and the most current year) should include several resources (see Figure 2).

Employee interviews

Discussions with TPI key employees/owners will be needed; therefore, use experienced interviewers who understand this is not a deposition nor a forensic interrogation/elicitation interview. Professionals leading the discussion should never be heavy-handed; however, it is critical to maintain "professional skepticism" and probe further if answers do not appear to be fruitful. Professional skepticism means not accepting answers to questions or the documents provided at face value without investigating further. For instance, if TPI representatives say they conduct third-party due diligence investigations on high-risk vendors, you should request and review those reports.

Below is an example of where professional skepticism was warranted, from a case study conducted by Kreller:

> On behalf of a lender, Kreller conducted due diligence on a borrower. Based on interviews with the borrower, it seemed appropriate to review underlying documents. There were significant findings that the third party (of the

Figure 2: Document request examples

Financial Statements

a. Balance Sheets
b. Income Statements
c. Statement of Cash Flows
d. Notes to Financial Statements*
e. Audit Opinion Letter (if audited)

**extremely important!*

Accounting/Banking Information

a. Chart of Accounts
b. Bank Statements
c. Trial Balances
d. Company Tax Returns

Policies & Procedures

a. ABAC policies & procedures
b. Code of conduct
c. Internal control policies

Historical Information

a. Country Corruption Issues
b. TPI Red Flags from Due Diligence Reports

borrower) had historical fraud issues. In reading the contract (between the borrower and TPI) and payment information, the borrower hired the TPI despite the due diligence red flags and paid the TPI hundreds of thousands of dollars annually to obtain licenses from government entities in a highly corrupt country. Since the lender decided to "dig deeper" and show professional skepticism, the lender was able to make informed decisions. Based on the above and other findings and information, the lender decided to discontinue funding.

Transactional testing

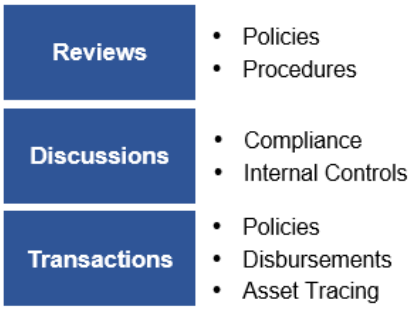
Typically, the audit will start with a review of the policies, procedures, and financial information. The interviews will guide where the focus of the transactions should be. Depending on the services provided by the TPI and its interactions with government officials, tracing the payments made to the TPI from the company and then the TPI to third parties may be a main area of focus. Identifying charts of account descriptions used in bribery payments (or historical frauds specific to the company) should be reviewed, and transactions analyzed. In the 20 companies evaluated in the earlier section, the following terms (and abbreviations) used to pay bribes were found: commissions, commission payments (CP), remuneration, incentive payments (IP), advances, consultant payments, engineering fees, and advance payments (AP). There are many others to review, such as entertainment, gifts, miscellaneous, meals, etc.[4]

If these or similar terms are found, review support for these transactions.

Here are the three steps in the audit process (also summarized in Figure 3):

1. Reviewing what the company says it does (i.e., policies and procedures used to implement and enforce those policies).
2. Talking to employees to understand what the employees say they actually do in accordance with those policies.
3. Testing whether what the company and employees stated (and documented) is consistent and demonstrated within actual transactions.

Figure 3: Three steps of the audit process



Final thoughts

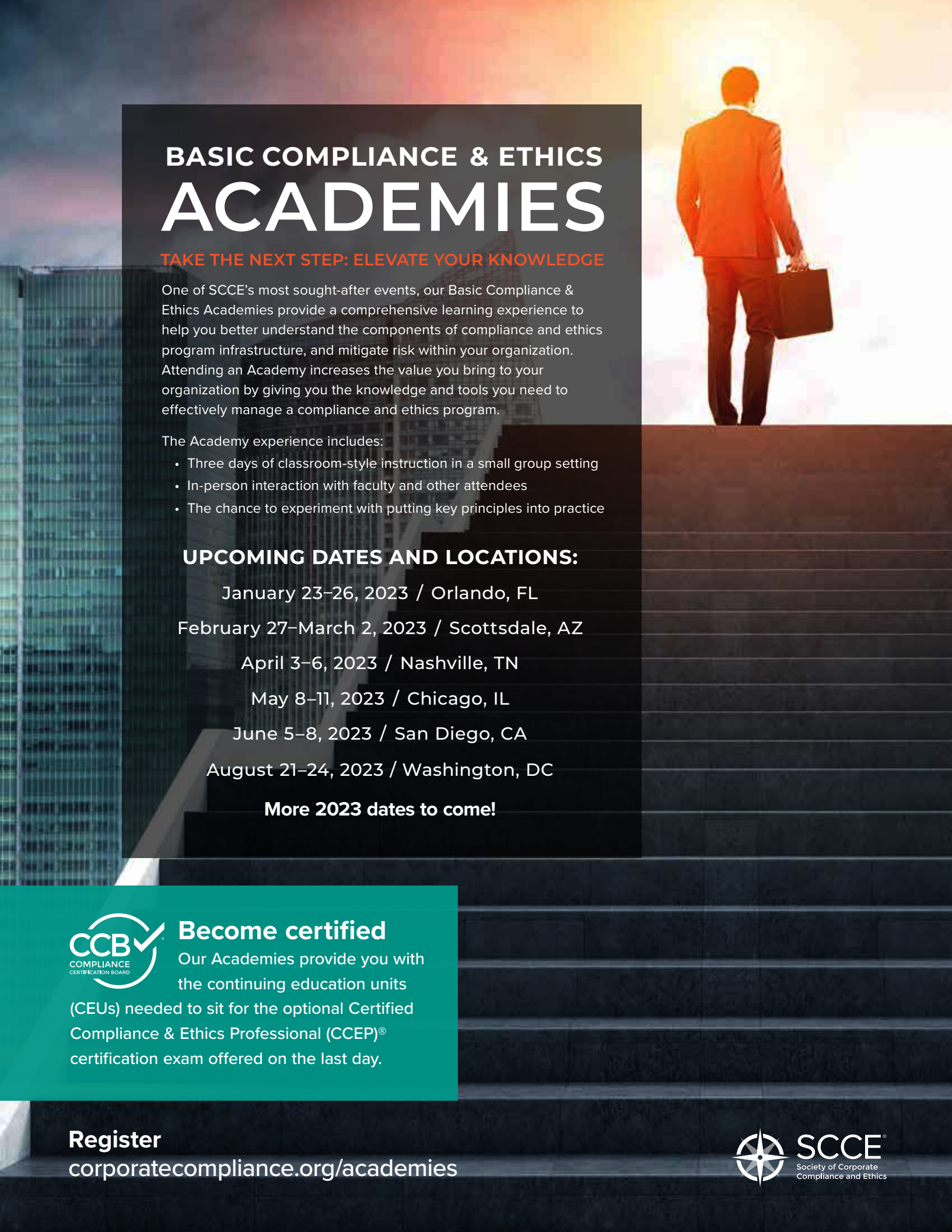
It is essential to integrate your findings and update your compliance program based on results of the risk assessments, internal investigations, and TPI audits (much like the sports GOATs who continually enhance their skills off-season). The ABAC compliance program must become smarter and evolve as new information is incorporated and potential risks uncovered. The regulatory agencies will not tolerate "dusty" ABAC programs created and left on the shelf.

Endnotes

1. U.S. Department of Justice, Criminal Division, and U.S. Securities and Exchange Commission, Enforcement Division, *A Resource Guide to the U.S. Foreign Corrupt Practices Act*, second edition, updated July 2020, 62, https://www.justice.gov/criminal-fraud/file/1292051/download.
2. U.S. Department of Justice, Criminal Division, "Enforcement Actions," website, database, last updated February 14, 2022, https://www.justice.gov/criminal-fraud/enforcement-actions.
3. Jaclyn Jaeger, "Best practices in preventing a third-party data breach," *Compliance Week*, January 7, 2019, https://www.complianceweek.com/third-party-risk/best-practices-in-preventing-a-third-party-data-breach/24704.article.
4. U.S. Department of Justice, Criminal Division, "Enforcement Actions."

Takeaways

- Compliance programs should incorporate Department of Justice guidance.
- It is essential to audit high-risk third-party intermediaries (TPIs).
- Integrate the results of your audits into your policies.
- Transaction testing should confirm policies and discussions.
- A TPI audit should accurately assess risk and be conducted with professional skepticism.



BASIC COMPLIANCE & ETHICS ACADEMIES

TAKE THE NEXT STEP: ELEVATE YOUR KNOWLEDGE

One of SCCE's most sought-after events, our Basic Compliance & Ethics Academies provide a comprehensive learning experience to help you better understand the components of compliance and ethics program infrastructure, and mitigate risk within your organization. Attending an Academy increases the value you bring to your organization by giving you the knowledge and tools you need to effectively manage a compliance and ethics program.

The Academy experience includes:

- Three days of classroom-style instruction in a small group setting
- In-person interaction with faculty and other attendees
- The chance to experiment with putting key principles into practice

UPCOMING DATES AND LOCATIONS:

January 23–26, 2023 / Orlando, FL

February 27–March 2, 2023 / Scottsdale, AZ

April 3–6, 2023 / Nashville, TN

May 8–11, 2023 / Chicago, IL

June 5–8, 2023 / San Diego, CA

August 21–24, 2023 / Washington, DC

More 2023 dates to come!

CCB COMPLIANCE CERTIFICATION BOARD

Become certified

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

Register
corporatecompliance.org/academies

SCCE® Society of Corporate Compliance and Ethics

"Big Data," big regulations, and big ethics

by Robert Bond

Data knows no jurisdictional boundaries, nor restrictions on international data transfers, so it seems odd that in 2023 we are still debating regulations that seek to control transfers of personal data.

We should have reached a point where the need to respect personal information, keep data secure, and enable trust becomes not only a focus for regulators and an expectation for citizens but also a compliance and ethical duty for governments and businesses.

For thousands of years, governments and other authorities have collected information on citizens in various ways. Statistical information about people has been valuable for managing economies and humanitarian needs. More recently, however, technological advances have meant personal data can be collected, obtained, analyzed, used, transferred, and shared in myriad ways — some good and some bad.

We have certainly reached a point in time where personal information has a tradeable value; yet trading such data comes with moral and ethical obligations as well as legal and regulatory requirements.

As consumers become more educated about how their personal information is collected and shared and how the appropriate use of such data can provide valuable outcomes, consumers also expect legal and ethical standards to be adhered to. Where rights in personal data are abused and where such personal data is used for purposes for which consumers have no reasonable expectation, then consumers will exercise their rights — both legal and moral — to gain satisfaction and compensation for failure by governments and businesses to respect privacy, secure data, and enable trust.

The use of new technologies such as smart devices, the Internet of Things, and artificial intelligence, coupled with the economic and humanitarian uses of "Big Data" analytics, means that there must be a balance between the acquisition of personal data and the rights of citizens.

A balance must be struck between the needs of governments to access personal data, the economic drivers for businesses to process and share personal data, and the rights and expectations of citizens in controlling their personal information.

Governments need to implement laws and regulations that appropriately manage the data ecosystem, be accountable for their own use and misuse of personal data, and encourage education and communication to businesses and citizens as to the duties and standards attached to economic and ethical use of personal data. CEP

Robert Bond

(rtjbond@icloud.com) is a compliance and ethics professional at Bond & Bond Ltd based in the United Kingdom.

BEGINNER'S GUIDE TO SOC 2, PART 2

by Wesley Van Zyl

Wesley Van Zyl

(wesley@scytale.ai) is a Compliance Success Manager for Scytale in Johannesburg, Gauteng, South Africa.

In Part 1, we discussed the first phase an organization is advised to undergo to have a successful audit and attain SOC 2 compliance, including the first three steps of the audit-readiness process.[1] As a reminder, there are many stages and responsibilities in a SOC 2 process, but they can generally be broken down into the following six key steps:

1. Consider finding a SOC 2 consultant or partner
2. Identify your scope
3. Perform the gap analysis
4. Gather evidence for each control
5. Perform the audit
6. Review the SOC 2 report

In Part 2, we continue to dive in with the next half of the SOC 2 compliance process, covering steps 4–6.

Gathering evidence for each control

By now, you should have:

1. Defined your scope and know what Trust Service Criteria to include.
2. Selected a Type 1 or Type 2 audit and decided on the audit period if a Type 2 review is being performed.
3. Completed the gap analysis and addressed the gaps by implementing all the relevant controls to address the SOC 2 criteria for the in-scope Trust Service Criteria.

Now, the evidence-gathering period in the SOC 2 project can be defined as the period before the auditor arrives to do the actual audit review. For example: if the audit period is established to be January 1 to June 30, this means the auditor will arrive towards the end of June or the beginning of July to perform

the audit. This gives the team six months to gather the evidence before the auditor arrives. All controls that have been scoped for the SOC 2 audit need proof to show that the controls are (1) designed and implemented and (2) operating effectively. If a Type 1 audit is being performed, then the evidence is only needed for the first point. If a Type 2 audit is being performed, then evidence will be required for both points.

Obtaining evidence regarding the design and implementation of controls

Design and implementation of the controls are normally tested together. It is important that the evidence clearly shows the auditors that the controls management is in place and implemented as management says they are. Management cannot say they have antivirus software installed on all end users' laptops, and then on the first laptop that is checked, the auditors find the software is not installed. Failing a control on design and implementation is a much more significant deficiency than failing a control on an operating effectiveness level — which is discussed below.

Obtaining evidence regarding the operating effectiveness of controls

As mentioned above, when providing a Type 2 report, the auditor will test those controls that the auditor has determined are necessary to achieve the criteria stated in the service organization's description of its system. The auditor will also assess the operating effectiveness of those controls throughout the period, which must be at least three months and at most 12 months.

When testing for operating effectiveness, the auditor needs to select a sample throughout the period and obtain evidence for the sample to ensure the control was operating effectively throughout the testing period. Using the antivirus example, the auditor will not only ask for one user's laptop but select a sample of laptops.

Evidence provided for the sample selected can range from screenshots to emails to physical documentation. In essence, the evidence provided needs to clearly indicate that the control is being performed as designed over a period of time. In a day and age where almost all the evidence will be electronic, it is important the pieces of evidence have a date stamp. Evidence that does not have a date stamp can provide difficulties for the auditor in determining the evidence's validity.

Evidence obtained in prior audits about the satisfactory operation of controls in previous periods does not provide a basis for a reduction in testing — even if it is supplemented with evidence obtained during the current period. This means the evidence provided needs to be from the current review period.

Perform the audit

Currently, a SOC 2 audit process uses the "trust but verify" approach by external auditing teams. The theory behind this approach is that the company needs to provide evidence to match what they are saying about their controls and security posture, and this evidence needs to be tested by the auditors. This approach allows the auditing team to stay independent of pulling the evidence. Before issuing the report, this is the final phase, and all evidence about the controls scoped for the SOC 2 project must be ready. Unsatisfactory evidence or evidence that cannot be provided will be noted as a finding in the SOC 2 report by the auditor. Depending on the severity and number of the results, SOC 2 compliance might not be obtained.

Auditing firms and auditors differ, but they all follow a similar process in performing the SOC 2 audit.

Failing a control on design and implementation is a much more significant deficiency than failing a control on an operating effectiveness level.

Pre-audit phase: Sampling

The auditors will request the control list before commencing the audit. From the control list, they will determine which controls a sample selection will be needed if a Type 2 audit is being performed. The auditor will send the samples to management to gather the required evidence before the auditor arrives. The most common lists of information from which auditors select their samples are:

- List of all changes
- List of new employees
- List of terminated employees

- List of board meeting minutes
- List of management minutes
- List of endpoints

Background of the company
On the first day of the audit, management will need to give some background of the company, what product or service offerings are part of the SOC 2 scope, and other information that may offer context to the auditors. This is normally a "get to know" each other phase between the auditor, management, and consultant.

Control and evidence review
This phase is the most significant. This is where the auditor will review the control design, implementation, and operating effectiveness (if a Type 2 audit was requested). This includes the review of the samples selected by the auditor before commencing the audit. The auditor will start from the top and review the evidence for each control from the control list. Some controls will need more explanation than others, which is why it is important to be able to explain the process supporting the evidence that was prepared.

Queries and feedback
At this point, the auditor is documenting their working papers, based on the evidence provided for each control and concluding on each of the controls. Any queries or outstanding items are communicated to management and resolved in this audit phase. The auditors will also offer feedback on any open items where more information is needed or on the status of the SOC 2 audit.

System description analysis
The system description is usually given to the auditors before the start of the audit; however, this is only a preference and not a requirement. The system description needs to be ready and provided to the auditors before the SOC 2 report can be prepared.

Reporting
Once all queries have been resolved and the auditor has received all the evidence and the system description, the auditor will start preparing the SOC 2 report.

Review the SOC 2 report

Once the audit has concluded, you should be notified by the auditing team that the audit review has ended, and the SOC 2 report should be finalized within two to four weeks. This phase of the SOC 2 process requires little involvement from management and is mainly covered by the auditor.

A SOC 2 report has four sections and one optional section. This report is a combined effort between management, the auditor, and the consultant; however, the auditor is responsible for developing the report and signing it off before issuing it to the organization.

The five sections in the SOC 2 report

- **Section 1 – Management's assertion letter:** A summary of what services the organization offers and what its components are. There is a standard template for this letter.
- **Section 2 – Independent service auditor report:** Prepared by the auditor in which they give their opinion on the audit performed. A summary of the results of the SOC 2 audit.
- **Section 3 – System description:** The organization provides a detailed system description that includes background on the organization, explains the control environment, and offers a list of controls that will address the SOC 2 criteria.
- **Section 4 - Applicable Trust Service Principles, criteria, related controls, tests of controls, and results of tests:** This section delivers the details of the auditor's work that was performed and, significantly, the results of each control that was tested and whether there were any exceptions or deviations.
- **Section 5 – Other information provided by the organization:** This section is optional. Any information the organization wants to include in the report can be provided in this section and is typically discussed with the auditor at the end of the audit.

The auditor will share a draft report with management so that they can review it and provide comments on anything that requires further clarification or something that management may not agree with. This is normally resolved in a closeout meeting with the auditors. If exceptions or deviations were found in a particular department by the auditing team, it would be best to have that department's manager sit in and discuss potential shortcomings that were found. This will provide a line of communication between the organization's management team, the auditors, and the department manager where the exception or the deviation is found. Once all queries have been resolved, the auditors will issue the final SOC 2 report to management.

Conclusion

After a successful SOC 2 review, annual maintenance of the SOC 2 compliance process is necessary to continue the process effectively and remain compliant. This will involve the following factors:

- Impact of organizational changes on the control environment
- New legislation and compliance requirements
- Changes in business and risks
- Contractual adjustments
- Changing requirements from user organizations (your clients)
- Recommendations from the auditor

The SOC 2 report is not just a tool for meeting requirements; it is usually the single best description of the information security of your supporting processes, controls, and procedures. CEP

Endnotes

1. Wesley Van Zyl, "Beginner's guide to SOC 2, Part 1," *CEP Magazine*, December 2022.

Takeaways

- Design and implementation of the controls are usually tested together.
- All controls that have been scoped for the SOC 2 audit need evidence to show that the controls are (1) designed and implemented and (2) operating effectively.
- A SOC 2 audit process uses the "trust but verify" approach by external auditing teams.
- The auditor is responsible for developing the report and signing it off before issuing it to the organization.
- The SOC 2 report is not just a tool for meeting requirements; it is generally the single best description of the information security of your supporting processes, controls, and procedures.

Let's stay connected!

Follow SCCE on social media:

- Keep up with industry trends
- Stay up to date on compliance news
- Learn about upcoming conferences and events

Find us on:

Connect with us
corporatecompliance.org/socialnetworks

SCCE
Society of Corporate Compliance and Ethics

Taxes and ESG

by Gerry Zack

Minimizing a corporation's taxes through legitimate tax planning is perfectly legal, whereas tax evasion is a compliance issue. Somewhere in between is a plethora of other tax issues, making tax transparency an important environmental, social, and governance (ESG) consideration for organizations.

On the surface, corporate taxes may not appear to be an ESG issue. But look more closely and it becomes apparent that taxes can impact all three elements of ESG. Environmental issues can trigger taxes or tax credits based on the company's activities. Social issues can have similar effects with taxes, such as those associated with health or credits for social investments. And governance may have the most direct connection with taxes, since this is the category under which transparency is measured and through which disclosures — both required and voluntary — are made in financial reports, websites, and other channels. Additionally, paying taxes is increasingly viewed as one way companies can demonstrate their commitment to supporting society through government-funded programs.

Increasingly, stakeholders want to know what taxes are being paid and why, which taxes are being avoided and how, and where all this fits with the values of the company and stakeholders. For example, did the company avoid or significantly reduce its income taxes by earning credit for responding to an environmental or social investment incentive? Or did it do so by establishing shell companies in tax havens to shelter income from taxation in countries in which most of its operations are carried out?

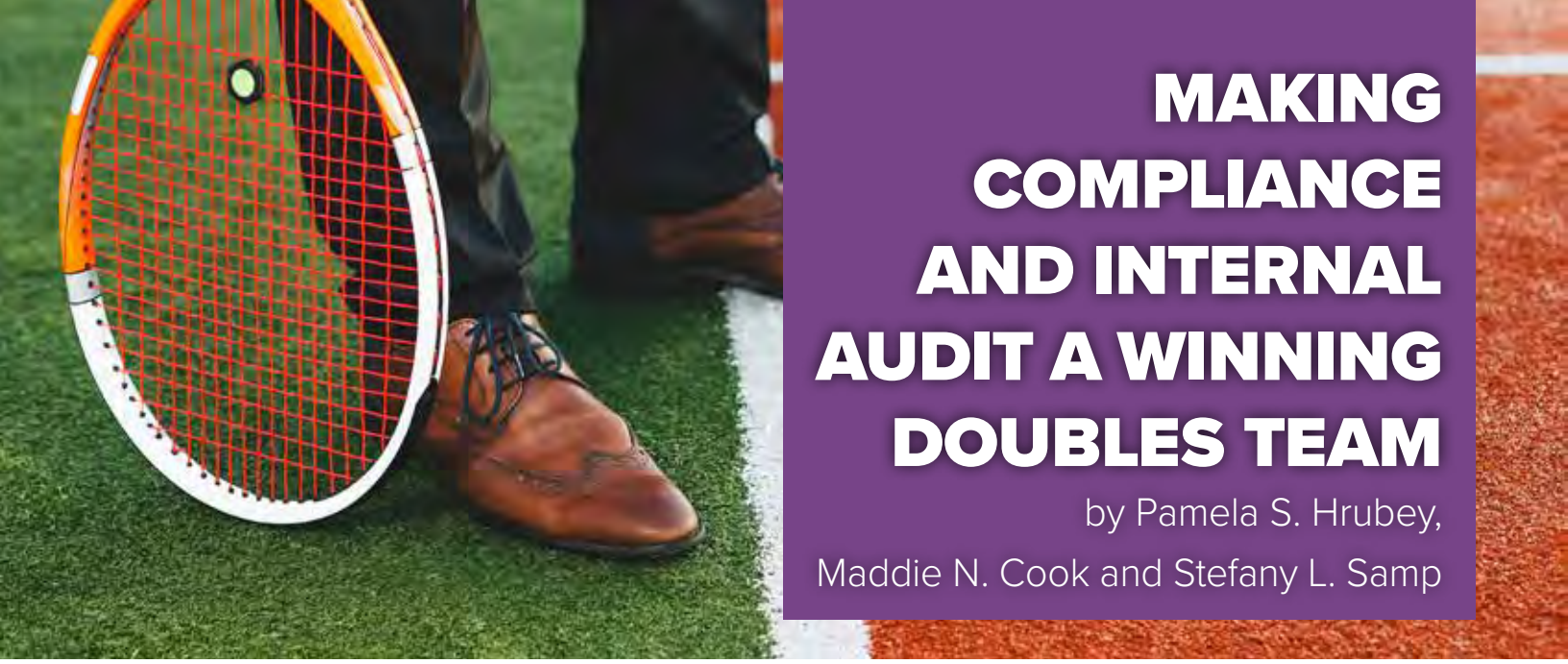
If this is something you haven't given much thought to, you're in luck. There's a lot of guidance out there on this issue. The Organisation for Economic Co-operation and Development has done much work on curbing tax avoidance, and the United Nations Principles for Responsible Investment (PRI) has published some useful guidance on the issue.[1] Additionally, there are standards, such as GRI 207 from the Global Reporting Initiative[2] and its Sustainability Reporting Standards.[3]

Key among the significant disclosures to be made in this area are information about the organization's tax strategy and how this strategy relates to both the business and the sustainable development strategies of the company. That can be uncomfortable if there is no connection.

Gerry Zack
CCEP, CFE, CIA
(gerry.zack@corporatecompliance.org, twitter.com/gerry_zack, linkedin.com/in/gerryzack) is CEO of SCCE & HCCA in Eden Prairie, Minnesota, USA. Please feel free to contact Gerry anytime to share your thoughts: +1 612.357.1544 (cell), +1 952.567.6215 (direct).

Endnotes

1. Principles for Responsible Investment, "What is tax fairness and what does it mean for investors?" discussion paper, December 6, 2021, https://www.unpri.org/download?ac=15325; Principles for Responsible Investment, "Evaluating and engaging on corporate tax transparency: An investor guide," May 2018, https://www.unpri.org/download?ac=4668.
2. Global Reporting Initiative, "GRI 207: Tax 2019," last accessed November 14, 2022, https://www.globalreporting.org/standards/media/2482/gri-207-tax-2019.pdf.
3. Global Reporting Initiative, "GRI Standards in English," website, last accessed November 14, 2022, https://www.globalreporting.org/how-to-use-the-gri-standards/gri-standards-english-language.



MAKING COMPLIANCE AND INTERNAL AUDIT A WINNING DOUBLES TEAM

by Pamela S. Hrubey, Maddie N. Cook and Stefany L. Samp

Pam S. Hrubey, DrPH, CCEP, CIPP/US, FIP
(pam.hrubey@crowe.com) is a principal in consulting at Crowe.

Maddie N. Cook, CPA
(maddie.cook@crowe.com) is in consulting at Crowe.

Stefany L. Samp, CCEP, CPA
(stefany.samp@crowe.com) is in consulting at Crowe.

In many organizations, the second and third lines of defense struggle to work as a team — either unintentionally or under the false notion that independence standards require complete separation. In these situations, compliance and internal audit can be like a doubles tennis team trying to return shots without communicating before or during the game. This would be a disaster on the tennis court, with players going for the same shots or missing others completely. The same is true in business. Without close collaboration, risks and opportunities either will be overmanaged or will slip through the cracks between the lines of defense. It is possible, however, for companies to shore up communication and coordination between compliance and internal audit, so they play as an effective doubles team.

If an organization is less mature or in initial high-growth stages and going public, it might not yet have dedicated compliance and internal audit teams, or it might have the dreaded "department of one." In these situations, sharing knowledge between limited resources is even more crucial. They also can advocate for each other as they ask for the necessary resources.

Collaboration tips

Build regular touchpoints between teams. Chief compliance officers (CCOs) and chief audit executives (CAEs) gain value from having regular touchpoints as leaders. CCOs have regular contact with teams through training, issues raised, and partnering with the business to integrate compliance into daily processes. CCOs can share themes they see with CAEs to help inform scheduled internal audits or drive a focused internal audit in an area of concern. CCOs and CAEs often have teams or employees that they want to keep a closer eye on because of complaints, investigations, expense audits, and so on. Discussing those "problem children" can give both compliance and internal audit teams information they need to dig deeper or include specific activities in ongoing monitoring or sample selections. Remember that both teams can maintain their independence while collaborating.

Deputize each other's teams to support your mission. Compliance should deputize internal audit to advocate for key compliance priorities such as data privacy, anticorruption, and environmental, social, and governance (ESG) issues. Internal audit has many contact points with the business where it might observe risks or opportunities in compliance areas it is not

specifically auditing. Empower internal audit to bring those potential issues to the compliance team's attention so issues can be investigated and compliance programs can be updated as needed.

Internal audits should deputize compliance to identify potential issues that might affect audits. When the compliance team feels empowered to share issues, internal audits can design and perform more risk-based audits.

By deputizing each team to keep its eyes and ears open for the other, each team gains support without any additional cost to the business and can more quickly and thoroughly address risks.

Collaborate on risk assessments. Both compliance and internal audit might be conducted enterprise-wide and/or targeted risk assessments during the year. It benefits both teams to coordinate timing and avoid duplicating work. Whenever possible, stakeholders going through risk-assessment interviews or surveys appreciate having a coordinated discussion instead of several. Risks can be inadvertently miscommunicated when stakeholders hear the same question worded differently, or they can get confused about who is responsible for doing what and in which situation. When assessments still are done separately, they are most successful when the compliance and internal audit teams share results. Having results from all completed assessments provides better inputs for internal audit plan preparation and compliance program management strategies.

Share risk rankings. Management will be able to digest results of risk assessments and audits more easily if, no matter who prepares them, the results are presented in one voice. Regardless of whether it's an enterprise risk assessment, a compliance assessment, or an internal audit, ideally, risk rankings used for likelihood, significance, and velocity will be the same for all reports — especially when those reports are presented to the most senior stakeholders, including boards of directors. Finance and other teams should not be forgotten, as they might use risk rankings for fraud or Sarbanes-Oxley Act assessments. Using shared risk rankings keeps individual subject-matter experts from assuming their area of expertise is the highest risk, lets the actual highest risks rise to management review, and helps the company prioritize corrective action plans.

Aligning on rankings can be challenging, but companies with a wide range of compliance and internal audit teams have successfully done so. For first assessments, compliance and internal audit often can work together to develop simple tables that outline criteria and a shared heat map format. For more mature teams and large, global organizations, the legal team might need to help develop a more detailed framework, including examples of scenarios and how they would be ranked using the shared rankings.

Collaborate on data analytics. In general, compliance and internal audit teams have made strides in the past several years toward implementing ongoing monitoring programs using data analytics. In some companies, these analytics have been developed but are overlapping or missing risks because of assumptions that another team is reviewing a particular risk. In some cases, both teams are spending inordinate amounts of time reviewing false positives — including on the same transactions — because both compliance and internal audit built similar analytics. Sharing analytics programs and discussing false positives can improve both teams' time spent.

Hold joint training sessions. Compliance and internal audit face constantly changing regulations and increasing scopes of work. When evolving topics affect both teams, consider joint training. For example, both teams might be scrambling to get up to speed on ESG reporting requirements and what they mean for the company's systems and processes in the near term. Bringing in specialists to train both teams together allows each team to understand the impact on all lines of defense.

Management will be able to digest results of risk assessments and audits more easily if, no matter who prepares them, the results are presented in one voice.

For the win

Playing doubles in tennis means the entire court is

covered even though each player takes fewer steps. This concept transfers to risk assessment because sharing risk assessment results allows both compliance and internal audit to provide strong support for the company overall without duplicating their efforts, which makes everyone involved winners.

Takeaways

- Collaboration between internal audit and compliance can take place while retaining necessary independence.
- Deputize the other team. Covering the entire surface of the court (or company) is easier when teams collaborate to watch for emerging or existing risks.
- Compliance and internal audit should present risk assessment results to management in one voice, using the same risk rankings to make reporting comparable.
- Collaboration gets easier with practice. Practice collaborating by establishing regular touchpoints between compliance and internal audit.
- Internal audit and compliance teams should work together to learn about changes inside and outside of the organization. Share knowledge and improve skills collaboratively.

Implementing a useful annual work plan

by Ahmed Salim

As we kick off the new year, it is important to ensure your annual work plan has been approved by your compliance committee and other necessary stakeholders and has been socialized organizationally for buy-in. More importantly, your work plan should have been implemented based on your identification of risk during your annual risk assessment.

What is an annual work plan?

Work plans are the foundation of a compliance program, as they provide a roadmap of what the program will focus on in the upcoming year. Work plans should be designed around your specific program, and projects should be created to address gaps and weaknesses identified during the risk-assessment process.

Tools for presenting a work plan

There are several project-management tools that can be useful to help document and visualize your program's work plan. It is vital that a program aligns on the best method to communicate the department's work plan that will allow stakeholders outside compliance visibility into the programs in an easy and digestible format. Utilizing online platforms like Canva or Microsoft Excel spreadsheets can also serve as a useful tool to communicate your work plan.

How to ensure work plan success

Reporting on the status of the work plan at your compliance committee and board meetings is essential, as it apprises leaders of the work you are doing and shines a spotlight on important initiatives the program has implemented in the year. To ensure completion of your work plan, it is critical there are routine check-ins and well-defined milestones and goals to assist with the successful completion of your work plan throughout the year.

Regardless of how you present the work plan, what stakeholders are involved, or where the information comes from, it is imperative an annual work plan be created to drive the success of your program while working on risks identified during the risk-assessment process.

Ahmed Salim

(ahmed.salim@irhythmtech.com) is Director of Ethics and Compliance Services at iRhythm Technologies in San Francisco, California, USA.

HOW TO CREATE AN EFFECTIVE DATA PROTECTION TRAINING PROGRAM

by Simon Blanchard

Simon Blanchard

(simon@dpnetwork.org.uk, linkedin.com/in/simonblanchard/) is a Partner at Data Protection Network Associates, based in the United Kingdom.

In any organization, big or small, our people are our greatest asset. From a compliance perspective, we might sometimes be tempted to think of our people as a risk. After all, a high proportion of data breaches and violations of data laws occur when employees make mistakes.

Many of these mistakes could be prevented with improvements to the training provided. Train people well and they'll become your eyes and ears on the ground. An effective training program will equip people with the necessary knowledge and skills to switch a potential risk into a real advantage.

Data protection laws, like the European Union and United Kingdom General Data Protection Regulation (GDPR) and California Consumer Privacy Act, require organizations to provide adequate training and awareness activity for employees who handle personal data. I'd argue that we should go beyond "adequate" and tailor our training programs to help our people understand how these laws apply to their specific roles, whatever they are.

Research on training provided

The Data Protection Network's Privacy Pulse Report of data protection and privacy professionals found that the message about the need for data protection training had landed.[1] Eighty percent of responders said their businesses had delivered data protection training within the last 12 months.

But is the quality and relevance of this training good enough for people to really get to grips with the data they use in their day-to-day roles? Is it sufficient to enable them to recognize weaknesses and change their behaviors?

The survey revealed that while some organizations provide training

tailored to specific business areas or job roles, these were in the minority. The lion's share of training was delivered through generic online courses.

Why should we adopt tailored training?

Data protection law is complex and nuanced. This complexity grows when you're handling the data of people from different jurisdictions around the world. A vanilla "one-size-fits-all" generic training solution can only take you so far. This may be suitable for some, but more is needed for those who use personal data regularly in their roles.

People from various business areas need varying levels of data knowledge to do their jobs. Some business areas will have their own distinct data challenges. How data protection law applies practically to different roles will vary enormously. Marketing teams need a distinct skill set for operations, as do people in human resources (HR) or customer service teams.

What does "good" look like?

A great way to start is to collaborate with key business functions or teams to get under the skin of what they do with data and identify which areas of the data protection law are most relevant to their roles. Here are a few examples:

- **Marketing teams** often need to understand core data protection principles, the conditions for legitimate interests and consent. They need to know about the right to object, the use of cookies, and how to compliantly approach profiling for marketing purposes. They must fully appreciate how data protection law interplays with legislation covering electronic marketing.
- **HR teams** have a completely different set of priorities for how they compliantly handle people's data. They need to understand how data laws apply to the range of data tasks they carry out for employment purposes and for recruitment, such as diversity, onboarding, conducting appraisals and personal development plans, handling health and sickness data, employee communications, and so on.
- **Procurement teams** need to understand the difference between controllers, processors, and joint controllers. They must recognize what good supplier due diligence for data protection looks like.
- **Customer service teams** need to have the proper knowledge to handle privacy-related queries from members of the public.

Consider the audience and judge what style of training delivery would work best. There are many options: a straightforward presentation, a specific online module, or a workshop-style session where participants don't just come to listen but actively take part in group work. A workshop should get them to think hard about how the data protection principles and other aspects of law apply to their roles.

Wherever possible, include relevant examples, case studies, regulatory fines, and exercises to illustrate what good and bad practices look like.

Successful training will embed core messages and encourage people to make positive changes or at least be more diligent about their data handling and sharing of personal data.

Go the extra mile to help them manage personal data securely, responsibly, and ethically.

Successful training will embed core messages and encourage people to make positive changes or at least be more diligent about their data handling and sharing of personal data.

Getting the balance right

Clearly, bespoke training for everyone — especially in a big organization — could become too time-consuming and costly. It often works best to take a balanced and pragmatic approach when deciding which business areas or job roles would benefit most from tailored training.

It can pay to focus on the areas which have the greatest exposure to personal data risks. Target the training to influence and mitigate those risks.

Where do the biggest risks lie within your business? Is it marketing, sales, supplier management, or privacy rights requests? Not everyone needs to understand the intricacies of carrying out a risk assessment,

such as a Data Protection Impact Assessment (DPIA). But are the people you want to conduct DPIAs equipped with the skills to do them effectively? Which roles or teams need to understand the complexity of international transfers?

If you are receiving growing volumes of subject access requests, the people responsible for handling them will need in-depth training on the nuances entailed.

The focus will naturally depend on the dynamics of the specific organization: the sectors it operates in, whose data is handled, the sensitivity of the data, and the activities undertaken.

Remember inductions and refreshers

Most businesses include an element of data protection training as part of their new starter induction program. Certainly, regulators would expect data protection training to be done swiftly before new employees are let loose to handle personal data.

Making sure people have appropriate knowledge and skills is one of the best ways to reduce the risk of a data breach or other violations of data protection law.

Along with an ongoing program to raise awareness, regular refresher training is vital. It's an opportunity to remind people of the core principles and considerations they need to keep top of mind.

It's easy to let this lapse, but as we've seen from regulatory action, authorities often question what staff training was in place. Training can help you meet your GDPR accountability requirements.

Final thoughts

Making sure people have appropriate knowledge and skills is one of the best ways to reduce the risk of a data breach or other violations of data protection law.

In our experience, businesses gain huge benefits and peace of mind from taking the time to pass on specialist knowledge to others.

Just like any successful communication, it's far more effective when you put your audience front and center and tailor the message to meet their needs.

Endnotes

1. Data Protection Network, *Privacy Pulse Report 2022*, January 4, 2022, https://dpnetwork.org.uk/wp-content/uploads/2022/01/DPN-Privacy-Pulse-Report_2022.pdf.

Takeaways

- Our people are our greatest asset. It pays to invest the time and train them well. With the proper knowledge, they can prevent a minor problem from turning into a big one.
- Certain teams across the business will benefit hugely from bespoke data protection training tailored to meet the needs of their day-to-day roles.
- We recommend that you focus your learning and development efforts on the teams with the greatest exposure to data risk.
- Adapt the content and style of delivery depending on your audience. Whatever the format, try to make it engaging!
- Don't forget induction training for new employees and regular refreshers.

Compliance as a profit center

by Nick Gallo and Giovanni Gallo

There's a movement afoot to transform the perception of compliance and ethics from a cost center to a source of strategic value. The ethics experts who recognize and adapt to this opportunity are building amazing careers and powerful programs that improve their teams' perception and effectively serve the good of their missions and all employees.

Below are four ways to broaden your perspective of your division to live out and communicate the true value we provide.

Make the return on investment case

Strategic leaders know how to put their objectives in terms other people care about, and money is one of the most common languages. You don't provide value just by avoiding fines! Never submit a budget request without highlighting the positive ways improving an ethical culture will influence employees and the specific objectives currently top of mind for executives.

Set the vision

Profit centers are not focused just on getting the program through another cycle but building to something greater that supports the whole company's mission. Give the team you manage and the people you report to the context of how your next actions fit into your medium-term plan and how the things your team is doing will help them achieve the vision they have for their own role.

Test and iterate

Innovation is not reserved for high-tech or creative types. You should demonstrate effectiveness on a small scale or a subset of your program review area and improve or expand the approach based on the results. "Still doing fine" or "nothing terrible" does not garner attention, respect, or budget.

Lead in all directions

Important functions have a noticeable impact on other important divisions in the company, regardless of whether they have formal authority. As compliance and ethics become more empowered, we must all be ready to ask for help, collaborate, and provide specific value to the division leaders around us. Find out what they care about and what they would be willing to help with and build from there. Nobody thinks their IT department is irrelevant to their job today, even though many would have said that 30 years ago.

From improving employee communication and software platforms to environmental, social, and governance, and the search for a solution to the Great Resignation, senior leadership is finally hungry for solutions we've spent our careers preparing to deliver. If you are already doing great on these fronts, start leveraging those into more rousing discussions. If you (like many of us) are stuck in old structures or patterns of thinking, 2023 is your chance to be the change you want to see in the world of compliance.

Nick Gallo

(ngallo@ethico.com) is co-CEO of Ethico and a lifelong student of healthy workplace cultures, based in Charlotte, North Carolina, USA.

Giovanni Gallo

(ggallo@ethico.com) is co-CEO of Ethico and a lifelong student of healthy workplace cultures, based in Charlotte, North Carolina, USA.

2022 COMPLIANCE & ETHICS INSTITUTE

That's a wrap! CEI 2022

SCCE's 21st Annual Compliance & Ethics Institute (CEI) was an amazing testament to the strength of our compliance community. Between our in-person experience and the virtual attendees, we had more than 1,000 committed compliance professionals together building connections, sharing ideas, and dedicating themselves to effective compliance and ethics programs across the globe. In many ways, the "new normal" has quickly evolved into just "normal", with more participation options to fit individual needs and budgets, a better understanding of how the remote workforce impacts our industry, a greater appreciation for the personal connections that are made when we do have the opportunity to gather in person, and a willingness to meet people where they are and engage through a variety of mediums.

This year's CEI had a tremendous selection of educational sessions, including a new track on Environmental, Social, and Governance (ESG). SCCE has long been committed to diving into emerging topics, and I was pleased with the reception our ESG content received. If you missed those sessions (or any others) due to the sheer volume of options, we're pleased to once again offer participants access to recordings of all the sessions for 60 days after the conference so you can gain additional insights.

There is no way to cover all the positive moments and interactions in this brief recap, but I would be remiss not to highlight the presentation of our 2022 SCCE Compliance & Ethics Award to COSO (Committee of Sponsoring Organizations of the Treadway Commission) Chairman Paul Sobel. It is always a great honor for me to bring compliance champions to light.

Thanks to all who helped make CEI 2022 such a great experience. I hope to see everyone in Chicago, IL in 2023 for the 22nd Annual Compliance & Ethics Institute!

Gerry Zack
CEO of SCCE & HCCA

Attendee voices:

Adam Balfour (He/Him) • 2nd
Vice President and General Counsel for Corporate Compliance and Vice President...
1w •

Compliance Learning

Like many others, I learned a lot from this week's **Society of Corporate Compliance and Ethics (SCCE)** CEI in **#Phoenix**. I picked up a number of new ideas from the different sessions I attended, and also learned just as much from the conversations I had with other attendees during the coffee breaks, walking around the vendor exhibits, over meals and other random interactions during the few days there. Learning can take place during formal training (such as classroom or online training), but we can also learn so much through less formal ways including conversations, coaching and mentoring.

When organizations - especially leaders, managers and supervisors - regularly have conversations with employees about ethics and integrity, we can really enhance the opportunities for employees to ask questions, see different perspectives and to learn in a less formal environment. If we only focus on helping employees learn about ethics and compliance in traditional class room settings, then we are (according to the Center for Creative Leadership's 70-20-10 model) missing out on 90% of how adults learn. There are so many different things organizations can do to help employees learn - share stories of when other people have spoken up (especially personal stories by leaders), connect strategic projects to organizational values and help employees get more comfortable with understanding whether leaders are truly committed to the organization's compliance program.

Sabrina Faleiro Marinho, CCEP - I (She/Her) • 2nd
Global Sr. Legal Manager Ethics & Compliance/ Labor & Employment at Wildlife ...
1w •

It was awesome to take part in the 21st Annual Compliance & Ethics Institute. I am so grateful to have met a lot of inspiring people from around the globe, reconnected with amazing compliance colleagues from Brazil, engaged in meaningful discussions and attended such enriching and insightful sessions.
Society of Corporate Compliance and Ethics (SCCE) congrats for the incredible conference.
Excited to put all these ideas into practice and continue to enhance **Wildlife Studios** Integrity program.
See you in Chicago next year!

Ling-Ling Nie • 2nd
Executive Leader • Legal Strategist • Advisor • Innovation • Technology • Transfor...
1w •

This year's **Society of Corporate Compliance and Ethics (SCCE)** conference was the best one yet! And this is my favorite photo! What a treat to team up again with the fabulous **Junna Ro** and **Kim Yapchai** to chat about the benefits and exciting opportunities that come from moving across industries and roles to experience true fulfillment and wellness in your professional and personal lives.
#compliance #esg #ethics #versatility

RETROSPECTIVE

This year's CEI included a robust online platform for attendees to participate in sessions and connect with their peers.

Volunteer Project

SCCE partnered with No Child Hungry to help pack hygiene kits and be a bright light in someone's life. All kits packed were distributed to MANA House, a facility that houses homeless veterans in Phoenix, AZ.

WOMEN IN LEADERSHIP? TRUST ME, "SHE'S NOT READY"

by Solomon Carter

Solomon Carter

(solomoncarter2000@gmail.com) is Chief of Staff and leads the Physicians Group Practices, Patient Financial Services, Office of Professional Development at Emory Healthcare in Atlanta, Georgia, USA. He also serves as a consultant specializing in diversity, equity, and inclusion; policy; human resources; change management; and compliance.

Over the years, I have had the pleasure to sit on interview panels for myriad roles both inside and outside the leadership space. I sit for my own organizations and as an external guest panelist. Particularly with new remote video capabilities — unlike before, where everything was in person — technology has allowed me to meaningfully participate in interview panels across the nation. In some, I am a consultant for the purposes of offering an interview panel's evaluation; in others, I am there to provide an unbiased and uninfluenceable perspective on a candidate's interview performance.

I participate on panels pertaining to a countless list of disciplines — some of which I may only possess general knowledge — but it doesn't matter. Why? Because the characteristics to thrive in leadership are the same everywhere, from a finance vice president or operations manager to a compliance chief or a director of widgets in a factory. Judgement, courage, communication, accountability, and integrity look the same everywhere if you know what to look for. "If these three things happened, would you report your boss and why?" are salient questions that transcend industry.

Why have a guest panelist?

Guest panelists can be very important because, often, workplace dynamics can hinder the work a panel tries to do. For example, if an interviewer is the boss of four other panelists, it will not be a diverse panel. Even if they are a rainbow coalition of every demographic known to man and have an eye for diversity, equity, and inclusion, the panel will be unduly influenced because if they all report to one person on the panel, they will

ultimately be more inclined to agree with what they say.

This circles back to why having an outside set of eyes on your interview panels is good. It's also a great learning opportunity for your firm to see how someone not from your business culture uses their critical thinking skills and analysis to come to conclusions and advance their arguments.

Additionally, it's refreshing to have a panelist who doesn't particularly care "who is who" on the panel and doesn't have any allegiances other than what they objectively observed in the interview. A guest panelist probably won't have an opinion on one person or the other because they don't work there. They don't have to deal with management downstream like the rest of the panel, worry about a business request being slowed down, or other overt or microaggressions that may surface if they don't agree with a key influencer.

If you're not using external panelists for your interviews, you might be missing out on some really good intel that could propel your program higher with better interview panel experiences, more astute panelists, more quality selections, and a better atmosphere of fairness — all of which enhance performance and insulates you from risk. It's something to consider.

She's not ready

In my travels, I have seen a litany of behaviors that speak to workplace culture, societal influences, trends, tendencies, and idiosyncrasies that speak to the full range of how an interview panel could be administered for better or for worse. It's particularly educational and fascinating. But of all the organizational commonalities — whether it's high excellence, utter incompetence, or everything in between — one common denominator above all in interview settings is when evaluating women, particularly for leadership or promotion. A panelist far too frequently says, "She's not ready." Name a race, color, creed, ethnicity, religion, or title, and then continue down the line — that excuse transcends every cultural difference you can imagine.

Men, in particular, are notorious for giving that answer when asked why a woman should not be provided a promotion or opportunity. It is the most common linguistic commonality I have come across, and nothing else comes close. To make matters worse, many people who have been part of powerful systems and structures that allow that kind of abstract answer to go unmolested almost always agree with that kind of unmerited answer. Everyone sits there, nods their heads in agreement, and parrots what a panelist uttered without anyone requiring them to articulate exactly why "she's not ready." It is commonplace, and it is horrible. And it is particularly difficult to see women fail to advocate for candidates who, in many ways, represent their employee experience the most.

The next time you hear someone say, "She's just not ready," I recommend you have the professional bearing, courage, integrity, empathy, compassion, and decency to say, "What exactly do you mean by that? Could you please explain it in detail? But before you do, *is she ready to learn*? Because if she is, and I believe that she is, then she should be afforded the opportunity the organization is presenting." And then sit there with your head held high.

After receiving promotions, women usually don't have the same structures and support systems men receive along with the opportunity to grow within their new roles.

Give women the support they need

To that end, after receiving promotions, women usually don't have the same structures and support systems men receive along with the opportunity to grow within their new roles. Repeatedly, due to unattainable expectations, implicit bias, and arbitrary performance standards, women are required to know every single element of a position *before* receiving an advancement opportunity, which is inherently unfair. It also places an abstract requirement on women that is discriminatory in nature because most of the time, not even the panelists who agree that "she's not ready" can name every single accountability that the candidate would have to know to succeed. They certainly wouldn't have had a chance to learn them in an hour-long interview, nor could they know all her knowledge,

skills, and abilities to properly assess her suitability for the role based on the abstract standard of "being ready" during the allotted interview period. Because what does that even mean? Without a detailed accounting of what they do and do not know — which they undoubtedly could not have ascertained through targeted questions most often not designed to reveal that specific determination — it is usually a nonsensical, unreasonable, and uniquely arbitrary standard to reject women in lieu of advancing a clear and cohesive intellectual reason why she should be denied an opportunity. But because there's no expectation for a panelist to offer that kind of professional explanation for the rejection of a candidate, it's never done.

I have also observed that when a woman who's been in a role for several years "isn't ready," the people who have the nerve to say so are the very ones who should have been centrally charged with getting her "ready" in the first place. But there's no accountability for them despite being the leaders of the "unready" candidate. I've used the Socratic method of questioning to help panelists understand that that kind of answer is a greater condemnation of the leaders of the interviewee than anyone else. The ability to digest that revelation varies from place to place. It's fascinating.

Lastly, many times, when our female colleagues finally receive an advancement opportunity and require greater support, the very people who came into the organization fully supported from the time they applied and who have been sliding into home plate since their new employee orientation are the very same people who are the first ones to say, "See, I told you that she wasn't ready," when doing the so-called evaluating. It's shameful, hypocritical, and goes against every form of ethical expectation we should uphold.

In the spirit of basic compliance, it is incumbent upon us as leaders to ensure our interview panels are not causing us to operate outside of our risk tolerance, which is what the moving goalposts of abstract language, unclear terminology, and arbitrary expectations do. Denying equity, inclusion, and the liberty of advancement to all our colleagues is anathema to creating a fair, just, and ethical culture for all. Aside from lacking humanity, it is also a bona fide compliance, ethics, and risk issue.

In closing, I encourage everyone to challenge their interview panel norms. When you hear someone give a poorly supported argument as to why "She's not ready," have the courage and decency to ask, "Is she ready to learn? Because if she is, then let's grant her the opportunity!" Help dismantle the structures in place that limit our female colleagues, disenfranchise them, and dehumanize them in a way that should violate every policy, ethos, standard of ethics, and value statement of the organizations we otherwise proudly serve. Everyone should feel compelled to hold interview panels accountable and speak up for what is right.

Because trust me when I tell you: nine times out of 10, she's ready!

Takeaways

- Consider having external guests (who are, in theory, neutral) participate in and evaluate your interview panels.
- Don't be fooled by "diverse" interview panels where influential leaders are accompanied by the people who report to them because that's far from fair and diverse.
- Through training, accountability and discipline, written standards, and culture-shaping opportunities, aggressively dismantle the moving goalposts of abstract language, unclear terminology, and arbitrary interview expectations that disenfranchise our colleagues and expose us to risk.
- Ensure everyone understands that the way interview panels are administered and how opportunities are given represents serious compliance, ethics, and risk consideration.
- Challenge the argument of "She's not ready," and ask, "Are they ready to learn?"

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

Sign up by 24 January and save on registration!

11TH ANNUAL SCCE ECEI EUROPEAN COMPLIANCE & ETHICS INSTITUTE

20–22 MARCH 2023 • AMSTERDAM

We can't wait to welcome you to Amsterdam

Join us in March 2023 for compliance learning and networking at the European Compliance & Ethics Institute (ECEI). This in-person event will provide insight into unique European compliance challenges and solutions, as well as the chance to engage with compliance & ethics colleagues from Europe and around the world.

Enhance your knowledge, your network, and your credentials

- Learn from top compliance experts
- Build your professional network
- Earn live Compliance Certification Board (CCB)® continuing education units (CEUs)
- Sit for the optional CCEP-I® exam

What past attendees are saying

"The advanced sessions were organised in a pragmatic and practical way to ensure challenges from everyday work were addressed."

"The ECEI consistently offers high-quality, cost-effective, engaging content over a range of relevant E&C topics."

Learn more
corporatecompliance.org/2023ECEI

SCCE® Society of Corporate Compliance and Ethics

Better board communication

by Teri Quimby

There are two types of compliance officers: those who *say* they add value by checking the boxes and those who *do* add value to the long-term governance journey. Which one are you?

A board of directors has fiduciary duties to its company, including compliance oversight. Board members are looking for information that not only drives decision-making but also assures accountability to internal and external stakeholders. Through better communication and documentation of good governance, a compliance officer can add value by assisting a board in meeting its fiduciary duties. In doing so, the board maintains a positive view of the compliance function. On the other hand, compliance officers who simply offer a "check the box" approach are merely providing noise without any substance to back it up.

The new certification announced by the U.S. Department of Justice, which requires CEOs and chief compliance officers to certify the "reasonable design" of programs to prevent corruption, easily extends to all compliance areas.[1] Also noteworthy is the Federal Trade Commission's unanimous vote to hold the alcohol marketplace company Drizly, as well as its CEO, accountable for a data breach involving 2.5 million customers. Of particular interest in this proposed agreement are the enforcement terms that extend to the CEO personally — and follow him to *future* positions with other companies.[2] With these new and evolving government policies, coupled with continued enforcement actions, a bright spotlight is shining on the importance of personal and professional compliance accountability for the C-suite and board. With the high cost of poor communication, regular and targeted compliance discussions at board meetings and documentation of good governance practices are in everyone's best interest and are critical in the current regulatory environment.

What value do I bring to the board?[3] Compliance officers should be asking themselves this question regularly. The answer to this question, and the type of compliance leader you are, may determine whether you have a seat at the table. Don't just try to find a seat by checking the boxes and going through the motions, but rather, be proactive by creating critical compliance conversations with board members — you may find that they pull up a chair at the table for you.

Teri Quimby
JD, LLM
(teri@teriquimby.com, linkedin.com/in/teriquimby) is the president of Quimby Consulting in Michigan, USA. She has served on and worked with numerous boards and commissions.

Endnotes

1. Mark A. Rush and Nadia K. Brooks, "What the C-Suite and Board Should Know About the New CCO Certification Requirement from the DOJ," *National Law Review* Vol. XII, No. 179 (June 28, 2022), https://www.natlawreview.com/article/what-c-suite-and-board-should-know-about-new-cco-certification-requirement-doj.
2. Federal Trade Commission, "FTC Takes Action Against Drizly and its CEO James Cory Rellas for Security Failures that Exposed Data of 2.5 Million Consumers," news release, October 24, 2022, https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million.
3. Teri Quimby and Adam Turteltaub, "Meet Teri Quimby: Communication is a priority," *CEP Magazine*, October 2022, https://compliancecosmos.org/meet-teri-quimby-communication-priority.

DATA AND COMPLIANCE: A GUIDE TO BEING AN INFORMATION HERDER, PART 1

by Randolph Kahn and Jay Cohen

Randolph Kahn, Esq.

(rkahn@kahnconsultinginc.com) is Founder & President of Kahn Consulting in Highland Park, Illinois, USA.

Jay Cohen

(jcohen@ghclaw.com) is Of Counsel to the law firm of Giordano Halleran & Cielsa and a Senior Advisor at Compliance Systems Legal Group in Wilton, Connecticut, USA.

A recent headline encapsulates the problem big business has with data and compliance: "Large Wall Street firms agreed to pay $1.8 billion in fines over failures to keep electronic records such as text messages between employees on personal mobile phones."[1]

Isn't it strange how little some companies care about one of their most valuable assets? A shipping company knows where every shipping container is located 24/7. A financial institution documents the existence and ownership of every asset in its control. A restaurant chain micromanages its inventory so it has the freshest product for customers with minimal waste and maximal profits. But every business today is also an information business; most big companies spend significant portions of their budget on IT to make their business efficient, competitive, and responsive to their markets and customers. The commodity of information is so valuable that it is sold and traded and has transformed businesses. And yet, most executives have little to no clue about all the information assets their companies have or how they are being created and used. And that is a compliance failure waiting to happen and a strategic advantage squandered.

The ever-evolving information legal environment

With each passing year, more jurisdictions regulate information in more ways, and that doesn't appear to be slowing down. As the information universe expands, so do the laws and regulations that seek to regulate it. It is not just the European Union (EU) and its privacy laws; United States jurisdictions are becoming more prescriptive in how the various states and the federal government expect information to be managed. Increasingly, laws and regulations dictate what your company can and cannot do with information, how long to keep it, how it needs to be secured, and how it must be managed. So, companies are well-served to stay on top of relevant laws and regulations as they evolve and grow.

One such example may make the point. Recently, the U.S. Department of Justice (DOJ) issued a revised memorandum to guide federal prosecutors in evaluating corporate compliance programs.[2] This guidance includes a discussion of the need for corporations to bolster their information management

practices relating to new communication technologies and the use of personal devices for work purposes. According to the DOJ, "all corporations with robust compliance programs should have effective policies governing the use of personal devices and third-party messaging platforms for corporate communications, should provide clear training to employees about such policies, and should enforce such policies when violations are identified." So, companies are well served to revisit their policies, practices, retention directives, and training.

Becoming an information herder, not a hoarder

So, what makes an information herder and not a hoarder? It's about right-sizing your information footprint — promoting business and compliance in the process — by knowing what information assets you have, keeping them in conformity with records-retention policies and requirements, and then purging outdated content in the ordinary course of business.

This two-part article is a guide to unearthing information-related issues with compliance, legal, or privacy implications and then developing a plan to better take control of information assets to be more competitive and harvest the economic value of information, while mitigating risk and promoting compliance. Part 1 will describe the various information-related legal and compliance issues, and Part 2 will provide a road map to fix them. In this way, you can help your organization become an information herder, effectively managing your information, rather than an information hoarder, just keeping it all forever.

Information management is a C-suite responsibility

Over time, information has become a clear differentiator. Businesses that use and exploit information properly are rewarded with efficiencies and profitability. Companies that fail to get their information act together wither or sputter. Companies that treat information as overhead and an expense required to run internal operations need to learn how to use that same information as an asset. Legislators and regulators increasingly see information and its management as the responsibility of the senior leaders at a public company. For example, cybersecurity disclosure rules proposed by the U.S. Securities and Exchange Commission (SEC) in March 2022 would require, among other things, that each public company disclose information about its board's oversight of cybersecurity risks and its management's role and expertise in assessing and managing cybersecurity risks and implementing relevant policies and procedures.[3] The rules would further mandate annual reporting about the cybersecurity expertise on the board.

And for some companies, information is the strategic asset that gives their business meaning and value. In such cases, executives understand that protecting, managing, and harvesting information is existential. For example, Airbnb (one of numerous examples) connects consumers and owners of private homes — which is all about information. In essence, the company is nothing more than information and technology.

Today, the mishandling of company information — such as experiencing information security or privacy failure — will mostly likely implicate and impact management like never before. Exposure of company data may be viewed as tantamount to mismanaging company assets, which can negatively impact careers and stock valuations; it may result in penalties imposed by regulators or courts. But perhaps most notably, customers and employees alike expect "their" information to be securely and privately retained; when it gets exposed, the court of public opinion may be the most painful reminder that information matters.

Companies that treat information as overhead and an expense required to run internal operations need to learn how to use that same information as an asset.

Theft of information and intellectual property

General Keith Alexander, who served as director of the National Security Agency, chief of the Central Security Service, and commander of the United States Cyber Command, once said, "The loss of industrial information and intellectual property through cyber espionage constitutes the 'greatest transfer of wealth in history.'"

And in recent years, the problem of countries, companies,

and individuals misappropriating company information and trade secrets of US companies has only become bigger and more expensive to address. Economic espionage is a major drain on competitive advantage, unique intellectual property (IP), and market share. Not only are US companies directly hurt by the theft of their IP, but they may end up competing against their own technology advanced by the IP thief. Protecting this treasure trove of information requires knowing what data exists, where it exists, who has access to it, and how it is protected.

Growth of information

Information volumes have been growing every year for many decades, and that growth will likely continue unabated. Much of this information is "unstructured" — that is, outside organized databases — and thus difficult to find and organize. Information tends to be ill-managed or not managed at all. Also, companies very often comingle important with unimportant information. That makes environments like the shared drive the perfect target of hackers because employees store all kinds of information there, including data that may have substantial value to the company, like intellectual property, or to its customers, like personal information.

Still suffering from pack rat-itis

Most businesses and their employees keep too much information, and some keep everything. There are various reasons for this reality, which we will explore in Part 2. Suffice it to say, employees usually think all their information is essential, may be of some future value or are afraid to purge content to run afoul of a legal obligation. And at the company level, IT professionals have fallaciously convinced themselves that storage is cheap. When keeping everything is a mode of "management," the law of diminishing returns applies. To the extent that information is somewhere but can't be easily accessed, it is a bad use of company resources. But perhaps more importantly for legal and compliance professionals, that scenario is the worst of all possible worlds. If litigation strikes, it is clear that information is somewhere, but it can't be readily accessed.

The new and ever-expanding universe of information

Companies are challenged not just by the volume of information but also by new technologies, business models, and ways of communicating with employees and customers. There are applications that embed collaboration and communication tools that promote work performance, but these may be less effective at managing the informational output as a company record when necessary. New and more efficient business models put company information in the "care, custody, or control" of third parties, which will be discussed later.

Work from home

Workforces have been gravitating away from the office work setting for the past couple of decades. But COVID-19 was another major game changer for companies and information, though many didn't fully appreciate what was happening to their data gems. As employees were forced to work remotely, they were using technologies to connect and collaborate and store more company information in the cloud and on various home devices with a range of setups and vulnerabilities. We have learned that this reality gives cyber thieves and hackers opportunities to exploit the resulting chinks in the information-security armor. And it creates the obvious issue of how companies will protect, access, and manage information outside their physical control.

Bring your own device, another iteration

The business world has been dealing with employees wanting to use their own phones and computers for work. This has had several iterations, but now it is accepted that companies allow employees to use their own devices for work. The pandemic made this a necessary evil. It makes economic sense for companies to keep employees happier by permitting them to use their own devices, but company information may be comingled on personal devices. The company will need to ensure it has all its information and that its employees protect and follow company rules. Indeed, recent SEC and Financial Industry Regulatory Authority fines totaling over a billion dollars made clear that companies knew their employees were using personal devices and applications to conduct business and had insufficient policies and practices to regulate its use in conformity to law.[4] These fines were imposed despite the absence of any demonstrated harm to individuals but simply because the firms' compliance programs failed to keep up with and cover their employees' information-management practices.

All companies — not just the broker-dealers and investment

advisors sanctioned in these cases — have legal obligations to retain and, at times, produce business-related communications. They would do well to heed the admonition of SEC Chair Gensler when announcing these enforcement actions, "As technology changes, it's even more important that [companies] appropriately conduct their communications about business matters within only official channels, and they must maintain and preserve those communications" as required by law.[5]

Cloud and the explosion of information-storage locations

Most companies are in a new information reality, where more and more information is located in more and more locations that the company may or may not control or own and even may have limited access to. And therein lies part of the problem. Say, for example, the company hires a third-party retirement-plan administrator that manages the information about employee plan participants somewhere in the cloud. Where the information is located, who "owns" it, and under what circumstances the employee or company can access it are all more complicated questions than they used to be. But companies are reluctant to ignore that new reality. More is not merrier when it comes to the proliferation of storage locations. The complexity of understanding where information resides is becoming more challenging with certain types of data, such as smart-device data. Does the data reside on the sensor or device, and does it get transmitted to the manufacturing of the sensor or device? Understanding how data flows and moves is essential in today's world.

To cut costs and have "infinite" scalability, most big companies have moved their data to one of several types of cloud providers or have outside business processes that are not their competency. So, companies like Microsoft, Google, Amazon, or other big cloud-storage providers have more and more of your company's information, and companies are storing less on premises with their own technology.

Third-party providers and contracts

Like the cloud-storage providers, companies are "outsourcing" more company functions to a whole host of companies that provide services and often function through a technology platform owned or controlled by a third-party provider or a contract or provider of theirs. It could be a customer service or human resources company providing human capital management software, or a factor agent providing cash or financing in return for accounts receivable. The critical point is that some third-party company is acting on behalf of another company with storage, control, and/or use of the company's data. Who "owns," retains, manages (and deletes, when requested in some circumstances) that data is rather complex but needs to be addressed.

Likewise, there increasingly are all kinds of relationships that have emerged in the last couple of decades that give some third-party access to other companies' information (usually with consent). Again: who gets to see, use, and manage company information when the company is no longer the holder or controller of that information is a complex question that must get addressed. Additionally, often the wrong company employee is negotiating third-party cloud contracts without sufficient input from other essential stakeholders like legal, compliance, privacy, etc.

Where the information is located, who "owns" it, and under what circumstances the employee or company can access it are all more complicated questions than they used to be.

Artificial intelligence

Most big companies harness artificial intelligence (AI) daily to answer complex business questions, predict customer needs, respond to customer inquiries, unearth trends, etc. And, of course, AI is dependent on information — usually lots of it. So, employees working on AI projects will want as much information as the company can retain. That, of course, flies in the face of how lawyers, privacy professionals, storage managers, compliance, and records managers want information to be managed. For them, less information for shorter periods is usually the right answer.

Compounding the complexity of AI data is the reality that not

only are volumes a challenge, but when working in the AI space, data is used to unearth answers which may create new and more data. The secondary use of information, as well as what regulations govern it and what privacy consents allow, is a complex problem to understand.

In October 2022, the White House issued guidelines to safeguard personal data in any AI systems and algorithms from misuse in hiring, lending, and other business decisions.[6] Among the five principles in this bill of rights, "to guide the design, use, and deployment of automated systems" is Data Privacy, providing that, "You should be protected from abusive data practices via built-in protections and you should have agency over how data about you is used."

Biometric data

Companies increasingly use various biometric data to run their business more effectively and efficiently. Tapping into customer biometric data is part of so many businesses today, including healthcare, medical device, manufacturing, energy transmission, and so many others. That data is arguably owned by an individual who may have given the company access and the right to use the data. And then, there is the question of where the data is stored. Increasingly, biometric data may be stored on a third-party device or server, which the company may not "control."

Internet of Things

The Internet of Things (IoT) is a way in which information is created, collected, and very often sent automatically from one device to another — with or without the device owner's knowledge. For example, say an electric company has installed a smart thermostat that learns family behavior and self-manages the temperature setting for the house without human intervention. Normally there is some ongoing communication between the thermostat, the energy company, and perhaps a third party who made the thermostat or aggregates data for the electric company. But in any event, IoT is a world of connected devices that transmit data through the internet without human intervention. Data grows, but companies don't usually see, touch, or manage it. However, they may still be responsible for it.

Blockchain

Even if you don't think your company is using blockchain, various financial service companies with whom you do business may be. Cryptocurrencies will come and go, but blockchain is here to stay. According to technology-analysis firm Gartner, "Blockchain is a type of distributed ledger in which value-exchange transactions (in bitcoin or other token) are sequentially grouped into blocks. Each block is chained to the previous block and permanently recorded across a peer-to-peer network, using cryptographic trust and assurance mechanisms."[7]

Unlike a traditional clearinghouse, a blockchain implementation does not depend on just one entity to maintain the ledger of transactions. Blockchain relies on many independent third parties — miners — who compete to both verify each transaction and be the first to solve a math problem in exchange for payment. Each miner is responsible for maintaining an independent, often public memorialization of the transaction on the ledger of the chain ("block") of transactions. These miners do not exist in more traditional transactions with banks. Transactions are executed within the blockchain environment and thereafter are aggregated in blocks, which are retained forever and are constantly revalidated with new transactions memorialized in new blocks. The point is that company transactions may be memorialized on a third-party computer without the company's ability to control such transactions or dictate how

long the information related to the transaction is retained.

Digitization

Most large companies are experiencing an acceleration of digitization. That process helps build better business processes through strategic use of technologies. That is significant because it allows companies to reevaluate what they are doing and why. Companies often apply digitization to better-existing business processes without considering compliance needs. In other words, addressing issues such as privacy and security in a project's planning and design phases means it will not need to be retrofitted downstream.

Conclusion

What is clear is that information-related issues for lawyers and compliance professionals are becoming increasingly varied and complex. And those issues are not going away, while new ones appear to pop up regularly. It is no wonder, then, that 79% of lawyers surveyed by Wolters Kluwer for its 2022 Future Ready Lawyer Report said that "coping with the increased volume and complexity of information" is one of the three trends that will have the most impact on the legal profession over the next three years.[8]

Part 2 of the article will demystify many of these issues, provide a roadmap to mitigate risk and exposure, and help your company become not only faster, better, and cheaper but more legally compliant. Gurbir S. Grewal, the director of the SEC's Enforcement Division, made clear the imperative to act now because "a proactive compliance approach" to this new world of information management requires that companies "not wait for an enforcement action to put in place appropriate policies and procedures . . . and anticipate these emerging challenges."[9] To put the task another way, as reinforced by Commissioner Kristin Johnson of the U.S. Commodities Futures Trading Commission on that same matter, "Internal compliance programs must adopt internal controls consistent with this new landscape."[10] CEP

Endnotes

1. Agence France-Presse, "Large Wall Street firms fined $1.8 bn in US over lax recordkeeping," *MSN*, September 27, 2022, https://www.msn.com/en-ae/money/companies/large-wall-street-firms-fined-1-8-bn-in-us-over-lax-recordkeeping/ar-AA12jIT7.
2. U.S. Department of Justice, Office of the Deputy Attorney General, "Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group," memorandum, September 15, 2022, https://www.justice.gov/opa/speech/file/1535301/download.
3. U.S. Securities and Exchange Commission, "SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," news release, March 9, 2022, https://www.sec.gov/news/press-release/2022-39.
4. Agence France-Presse, "Large Wall Street firms fined $1.8 bn."
5. U.S. Securities and Exchange Commission, "SEC Charges 16 Wall Street Firms with Widespread Recordkeeping Failures," news release, September 22, 2022, https://www.sec.gov/news/press-release/2022-174.
6. The White House, Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People*, [white paper], October 2022, https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.
7. The DPO Academy, "The Blockchain GDPR Puzzle: An Expert Weighs In," December 6, 2018, https://www.dpoacademy.gr/l/the-blockchain-gdpr-puzzle-an-expert-weighs-in.
8. Wolters Kluwer, *The Wolters Kluwer Future Ready Lawyer*, 2022 survey report, last accessed November 10, 2022, https://images.go.wolterskluwerlr.com/Web/WoltersKluwerLRSUS/%7B60c69227-1c9c-45a1-818f-b7cc4863f1f9%7D_LR_white_paper_2022_09-01_FINAL_single.pdf.
9. U.S. Securities and Exchange Commission, Director of Enforcement Gurbir S. Grewal, "Speech at PLI Broker/Dealer Regulation and Enforcement 2021," (Speech, Washington, DC, October 6, 2021), https://www.sec.gov/news/speech/grewal-pli-broker-dealer-regulation-and-enforcement-100621.
10. U.S. Commodity Futures Trading Commission, Commissioner Kristin N. Johnson, "Statement of Commissioner Kristin N. Johnson Regarding CFTC Orders for $700 Million Penalty Against Bank-Affiliated Entities for Offline Communications," September 27, 2022, https://www.cftc.gov/PressRoom/SpeechesTestimony/johnsonstatement092722.

Takeaways

- Companies often do not understand the nature, creation, use, and retention of their information assets, and this is a compliance failure waiting to happen.
- More jurisdictions are regulating information assets in increasingly intrusive ways, so companies must revisit their policies, practices, retention policies, and training.
- The explosive growth in information — much of it unstructured — taxes the ability of organizations to find, organize, protect, and address the risks with these assets.
- Companies are challenged not just by the volume of information but also by new technologies, business models, and ways of communicating internally and externally.
- In-house counsel and compliance professionals must help demystify information management for the C-suite, applying proactive compliance approaches to turn information hoarders into herders.

SCCE SALARY SURVEY REVEALS A BRIGHT COMPENSATION PICTURE

by Adam Turteltaub

Adam Turteltaub

(adam.turteltaub@corporatecompliance.org, linkedin.com/in/adamturteltaub) is Chief Engagement & Strategy Officer, Society of Corporate Compliance and Ethics and Health Care Compliance Association, in Eden Prairie, Minnesota, USA.

The Society of Corporate Compliance and Ethics (SCCE) first surveyed compensation for compliance professionals back in 2013. The survey was last conducted in 2019, and with the pandemic-related changes to the job market, the association was eager to provide updated information for the compliance profession.

In June 2022, an email invitation was sent out to approximately 50,000 individuals on the association's mailing list requesting their participation. The responses were tabulated by an external research company to ensure both accuracy and confidentiality of the data.

A copy of the report can be found on the SCCE website.[1] Members of SCCE can also access an interactive version in which they can run custom data queries.

Findings

Compensation has increased across the board for compliance professionals at all levels. Chief compliance officers (CCOs) responsible for 76% or more of their organization's legal risk saw an average income of $224,461, up 17% from 2019 (see Figure 1). The greatest rise was seen for those managing 26%-50% of risk. These individuals saw a 31% increase.

Looking at staff, compensation for directors averaged $180,213, up 6.5% (see Figure 2). Managers were up 21% and assistant/specialists saw an average increase of 11%.

Compensation levels did vary considerably, though, based on where an individual works, both in terms of geography and type of corporation. CCOs in the West North Central region, for example, saw average compensation of $325,610, while those in the Mountain region saw just $190,596.

Figure 1: Average total compensation by percentage of company's legal and regulatory risk areas CCOs involved in

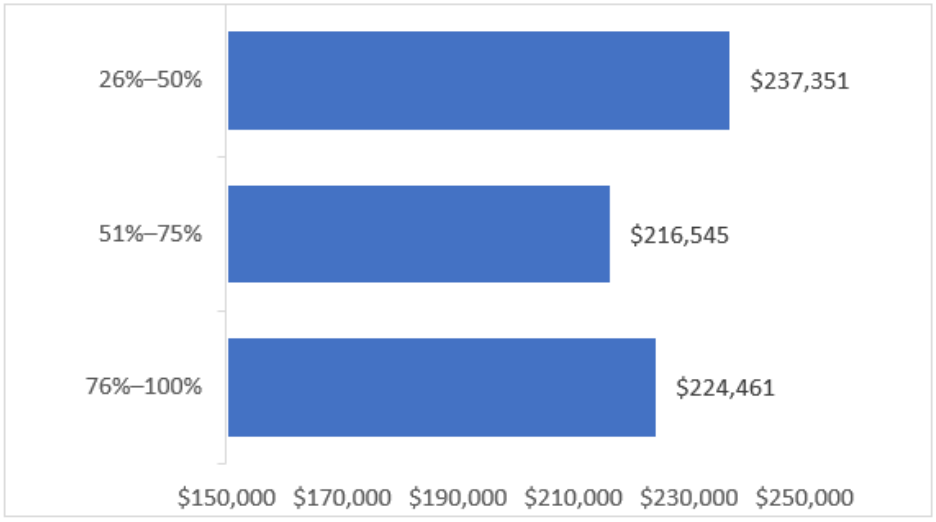
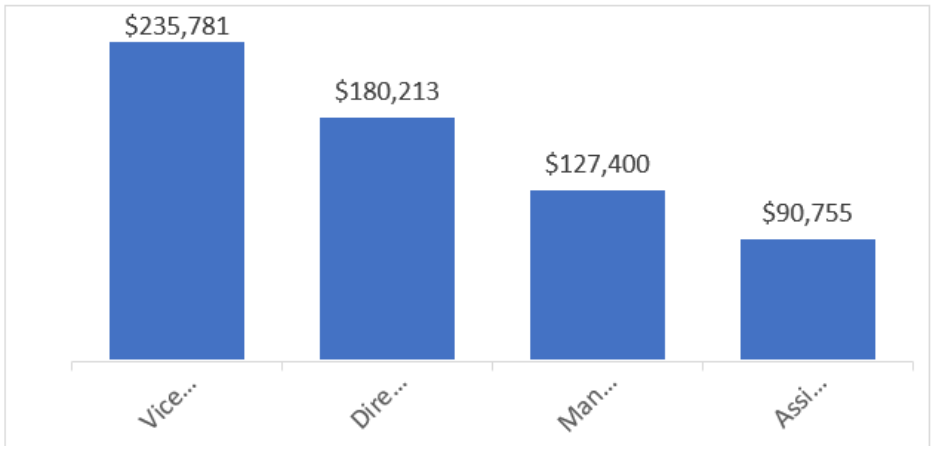
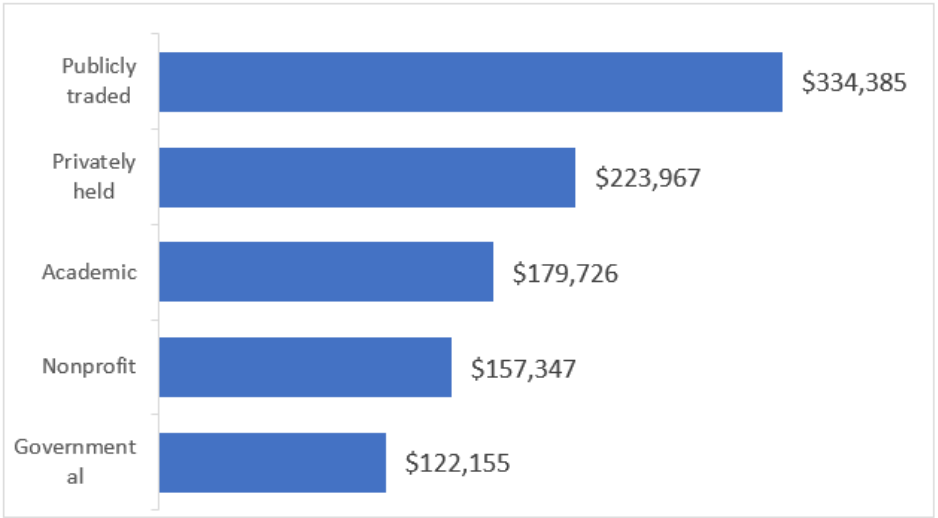


Figure 2: Average total compensation by title/level



Note: Vice presidents were a small sample size.

Figure 3: Average total compensation by type of organization



Of even greater difference was compensation based on whether the organization was for profit or not. CCOs at publicly traded organizations enjoyed average total compensation of $334,385 compared to just $157,345 at nonprofits, and $122,155 at governmental institutions (see Figure 3).

At the staff level, the differences were also stark with a director at a publicly traded organization earning almost twice as much as one at an academic institution (see Table 1 on page 50).

Certification correlated strongly with higher compensation. Individuals possessing a Compliance Certification Board designation generally earned far more than those who did not (see Table 2 on page 50).

To see more of the data, be sure to visit the SCCE website at *www.corporatecompliance.org/publications/surveys/2022-scce-salary-survey*.

Endnotes

1. Society of Corporate Compliance and Ethics, "2022 SCCE Salary Survey," updated October 17, 2022, https://www.corporatecompliance.org/publications/surveys/2022-scce-salary-survey.

Table 1: Average total compensation by type of organization

Type of Organization	Director	Manager	Assistant/Specialist
Nonprofit	$158,199	$110,093	$89,786
Privately Held	$157,083	$123,103	$83,403
Publicly Traded	$218,742	$140,713	$100,320
Governmental	*	$116,845	$81,322
Academic	$110,811	$91,700	$86,464

** Insufficient data*

Table 2: Correlation between certification and compensation

Certification	CCO	Director	Manager	Asst/Specialist
CCEP	$262,550	$188,739	$135,475	$111,708
CCEP-I	$210,682	$220,500	$93,082	$87,500
None	$189,645	$173,556	$109,362	$81,592

Regional Compliance & Ethics Conferences

General and specialty education for every level

These one-day events explore a diverse spectrum of topical compliance issues with educational sessions led by experienced compliance and ethics professionals. Events are either in-person or virtual, depending on location. Attendees will have the opportunity to earn live Compliance Certification Board (CCB)® continuing education units (CEUs).

Get the latest best practices, strategies, and updates in:

- Regulatory requirements
- Compliance enforcement
- Risk management
- Maintaining an effective compliance program

Upcoming Events

Each Regional conference features unique sessions and topics—no two events are the same!

February 10, 2023
California & Arizona | Virtual

February 23, 2023
Alaska | Virtual

March 3, 2023
New York & Boston | Virtual

April 28, 2023
Tampa, FL | In-person

May 19, 2023
Minneapolis, MN | In-person

June 16, 2023
Chicago, IL | In-person

August 11, 2023
Nashville & Atlanta | Virtual

September 22, 2023
Washington, DC | Virtual

October 27, 2023
Dallas, TX | In-Person

November 10, 2023
Seattle, WA | Virtual

Learn more and register
corporatecompliance.org/regionals

SCCE®
Society of Corporate Compliance and Ethics

TAKE YOUR CAREER

WHY BECOME CERTIFIED?

Enhance your credibility

Certification validates your compliance knowledge of current trends and regulations within the profession.

Increase your competitive edge

Certification sets you apart in the eyes of current and future employers, demonstrating your higher-level expertise.

Show your commitment to the profession

Compliance Certification Board (CCB)® certification affirms your dedication to the field of compliance, your position, and your organization.

FIVE STEPS TO CERTIFICATION

1. Gain work experience
2. Earn and submit CEUs
3. Apply to take the exam
4. Schedule your exam
5. Take the exam

Applying for certification – The application process is easy! Once you have the necessary work experience and CEUs, go to corporatecompliance.org/apply-exam and fill out the online application form.

Learn more and get started

corporatecompliance.org/certification

TO THE NEXT LEVEL

CHOOSING YOUR TESTING OPTION

CCB offers a variety of testing options for your convenience:

- Electronic testing at a PSI Testing Center
- A paper and pencil exam at an SCCE conference (per availability)
- A remote proctored exam*: take your test from the comfort and safety of home!

**Offered for all CCB basic certifications, these exams can be scheduled (depending on availability) as soon as two business days after receiving PSI's confirmation, or weeks ahead to accommodate your schedule. Get the details at corporatecompliance.org/exam-info.*

ALREADY CERTIFIED?

Stay on top of your renewal requirements! – For our comprehensive list of CEU activity options, visit corporatecompliance.org/how-to-earn-ceus

Live vs. non-live credits – At least 20 of the 40 CEUs required for certification renewal must come from live education. Live CEUs are earned from education presented in real-time with the ability to interact with Q & A. Non-live CEUs are earned when an educational event is not interactive, such as a recorded webinar, authoring an article, self-study, etc.

Need more time to earn CEUs? – As a CCB certification holder, you have a one-month grace period beyond your renewal date to earn and submit CEUs. If additional time is needed beyond the grace period, you may file an extension for up to two additional months to complete the renewal requirements.

CCEP™ CERTIFIED COMPLIANCE & ETHICS PROFESSIONAL

CCEP-I™ CERTIFIED COMPLIANCE & ETHICS PROFESSIONAL-INTERNATIONAL

CCB® COMPLIANCE CERTIFICATION BOARD

Share your insight

When you write an article for *Compliance & Ethics Professional*® *(CEP)* Magazine, you demonstrate a commitment to the industry, gain visibility for your organization and program, and help your fellow practitioners meet compliance challenges with confidence and success.

Whether your experience is in enforcement, regulations, organizational culture and training, compliance essentials, or another area of compliance and ethics, your expertise has a place in *CEP*!

Share your insight with more than 7,000 compliance and ethics professionals by submitting an article to *CEP*. Whether you are new to writing or an experienced author—we'll assist you through the publication process.

Learn more
corporatecompliance.org/write-cep

SCCE®
Society of Corporate Compliance and Ethics

Takeaways

January 2023

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.

"GOAT" compliance programs

Mark Jenkins (page 14)

- Compliance programs should incorporate Department of Justice guidance.
- It is essential to audit high-risk third-party intermediaries (TPIs).
- Integrate the results of your audits into your policies.
- Transaction testing should confirm policies and discussions.
- A TPI audit should accurately assess risk and be conducted with professional skepticism.

Beginner's guide to SOC 2, Part 2

Wesley Van Zyl (page 20) **CEU**

- Design and implementation of the controls are usually tested together.
- All controls that have been scoped for the SOC 2 audit need evidence to show that the controls are (1) designed and implemented and (2) operating effectively.
- A SOC 2 audit process uses the "trust but verify" approach by external auditing teams.
- The auditor is responsible for developing the report and signing it off before issuing it to the organization.
- The SOC 2 report is not just a tool for meeting requirements; it is generally the single best description of the information security of your supporting processes, controls, and procedures.

Making compliance and internal audit a winning doubles team

Pamela S. Hrubey, Maddie N. Cook, and Stefany L. Samp (page 26)

- Collaboration between internal audit and compliance can take place while retaining necessary independence.
- Deputize the other team. Covering the entire surface of the court (or company) is easier when teams collaborate to watch for emerging or existing risks.
- Compliance and internal audit should present risk assessment results to management in one voice, using the same risk rankings to make reporting comparable.
- Collaboration gets easier with practice. Practice collaborating by establishing regular touchpoints between compliance and internal audit.
- Internal audit and compliance teams should work together to learn about changes inside and outside of the organization. Share knowledge and improve skills collaboratively.

How to create an effective data protection training program

Simon Blanchard (page 30) **CEU**

- Our people are our greatest asset. It pays to invest the time and train them well. With the proper knowledge, they can prevent a minor problem from turning into a big one.
- Certain teams across the business will benefit hugely from bespoke data protection training tailored to meet the needs of their day-to-day roles.
- We recommend that you focus your learning and development efforts on the teams with the greatest exposure to data risk.
- Adapt the content and style of delivery depending on your audience. Whatever the format, try to make it engaging!
- Don't forget induction training for new employees and regular refreshers.

Women in leadership? Trust me, "She's not ready"

Solomon Carter (page 36)

- Consider having external guests (who are, in theory, neutral) participate in and evaluate your interview panels.
- Don't be fooled by "diverse" interview panels where influential leaders are accompanied by the people who report to them because that's far from fair and diverse.
- Through training, accountability and discipline, written standards, and culture-shaping opportunities, aggressively dismantle the moving goalposts of abstract language, unclear terminology, and arbitrary interview expectations that disenfranchise our colleagues and expose us to risk.
- Ensure everyone understands that the way interview panels are administered and how opportunities are given represents serious compliance, ethics, and risk consideration.
- Challenge the argument of "She's not ready," and ask, "Are they ready to learn?"

Data and compliance: A guide to being an information herder, Part 1

Randolph Kahn and Jay Cohen (page 42) **CEU**

- Companies often do not understand the nature, creation, use, and retention of their information assets, and this is a compliance failure waiting to happen.
- More jurisdictions are regulating information assets in increasingly intrusive ways, so companies must revisit their policies, practices, retention policies, and training.
- The explosive growth in information—much of it unstructured—taxes the ability of organizations to find, organize, protect, and address the risks with these assets.
- Companies are challenged not just by the volume of information but also by new technologies, business models, and ways of communicating internally and externally.
- In-house counsel and compliance professionals must help demystify information management for the C-suite, applying proactive compliance approaches to turn information hoarders into herders.

SCCE upcoming events

JANUARY

January 18
FCPA Enforcement Update: Lessons Learned for Best Practices
WEBINAR

January 19
Sports, Compliance, and Ethics Conference
VIRTUAL

January 23–26
Basic Compliance & Ethics Academy
ORLANDO, FL • IN-PERSON

January 31
Great Expectations: CEO and CCO Certifications of Ethics & Compliance Program Effectiveness
WEBINAR

FEBRUARY

February 6–9
Compliance & Ethics Essentials Workshop
VIRTUAL

February 8
Bootstrapping Ethics
WEBINAR

February 10
Regional Compliance & Ethics Conference
CALIFORNIA & ARIZONA • VIRTUAL

February 15–16
Creating Effective Compliance Training
VIRTUAL

February 21
Aerospace, Defense & Government Contracting Compliance & Ethics Conference
VIRTUAL

February 22–23
Compliance Risk Assessment and Management
VIRTUAL

February 23
Regional Compliance & Ethics Conference
ALASKA • VIRTUAL

Feb 27–Mar 2
Basic Compliance & Ethics Academy
SCOTTSDALE, AZ • IN-PERSON

2023 We continue to add events and dates to our schedule. Please check the website for details.

Sports, Compliance, and Ethics Conference
January 19 · VIRTUAL (CT)

Aerospace, Defense & Government Contracting Compliance & Ethics Conference
February 21 · VIRTUAL (CT)

11th Annual European Compliance & Ethics Institute
March 20–22 · Amsterdam, Netherlands · IN-PERSON

Encouraging, Managing, and Integrating Employee Reporting
May 4 · VIRTUAL (CT)

Nonprofit Sector Compliance Conference
May 23 · VIRTUAL (CT)

Higher Education Compliance Conference
June 11–13 · Phoenix, AZ · IN-PERSON

ESG and Compliance Conference
June 28 · VIRTUAL (CT)
November 30 · VIRTUAL (CT)

Compliance in Smaller Organizations
July 20 · VIRTUAL (CT)

Compliance, Ethics, and Organizational Culture
August 3 · VIRTUAL (CT)

Auditing & Monitoring Conference
September 7 · VIRTUAL (CT)

22nd Annual Compliance & Ethics Institute
October 2–5 · Chicago, IL · IN-PERSON

Compliance & Ethics Essentials Workshop
February 6–9 · VIRTUAL (CT)
May 15–18 · VIRTUAL (CT)
September 18–21 · VIRTUAL (CT)
October 16–19 · VIRTUAL (Central Euro. Time)
December 4–7 · VIRTUAL (CT)

Creating Effective Compliance Training
February 15–16 · VIRTUAL (CT)
June 21–22 · VIRTUAL (CT)
July 31–August 1 · Orlando, FL · IN-PERSON
November 1–2 · VIRTUAL (CT)

Compliance Risk Assessment and Management
February 22–23 · VIRTUAL (Central Euro. Time)
April 20–21 · Anaheim, CA · IN-PERSON
June 26–27 · VIRTUAL (CT)
September 27–28 · VIRTUAL (CT)
December 12–13 · VIRTUAL (CT)

Fundamentals of Compliance Investigations
April 13–14 · VIRTUAL (CT)
June 1–2 · VIRTUAL (Singapore Time)
September 7–8 · VIRTUAL (Central Euro. Time)
November 28–29 · VIRTUAL (CT)

Basic Compliance & Ethics Academies
January 23–26 · Orlando, FL · IN-PERSON
February 27–March 2 · Scottsdale, AZ · IN-PERSON
April 3–6 · Nashville, TN · IN-PERSON
May 8–11 · Chicago, IL · IN-PERSON
June 5–8 · San Diego, CA · IN-PERSON
August 21–24 · Washington, DC · IN-PERSON

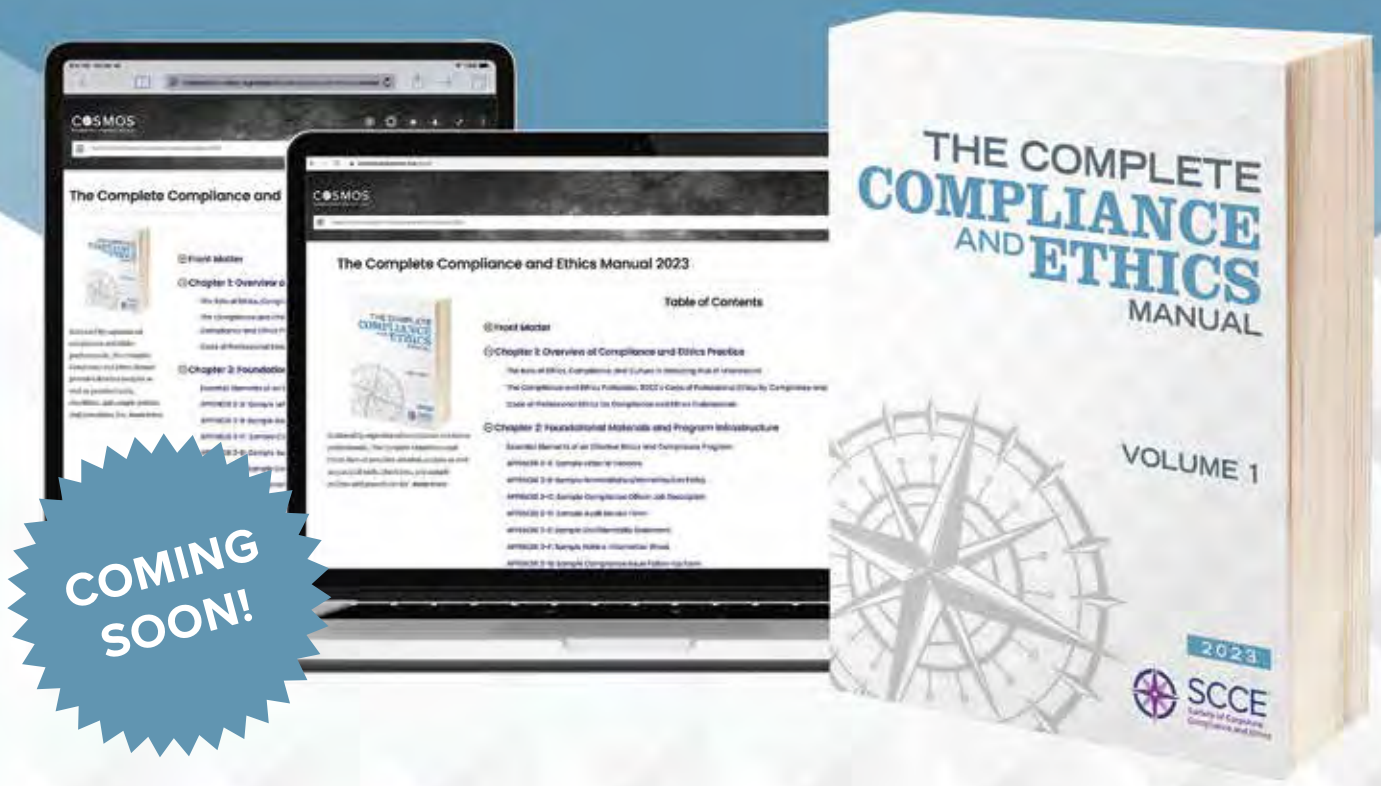
Regional Compliance & Ethics Conferences
February 10 · California & Arizona · VIRTUAL
February 23 · Alaska · VIRTUAL
March 3 · New York & Boston · VIRTUAL
April 28 · Tampa, FL · IN-PERSON
May 19 · Minneapolis, MN · IN-PERSON
June 16 · Chicago, IL · IN-PERSON
August 11 · Nashville & Atlanta · VIRTUAL
September 22 · Washington, DC · VIRTUAL
October 27 · Dallas, TX · IN-PERSON
November 10 · Seattle, WA · VIRTUAL

Webinars
Stay up-to-date on current issues in regulatory compliance, enforcement, plan development, and other areas of interest to compliance professionals and earn Compliance Certification Board (CCB)® CEUs without travel. Visit corporatecompliance.org/webinars to see our latest offerings.

Event dates are subject to change.
Visit **corporatecompliance.org/events** to learn more.

SCCE® Society of Corporate Compliance and Ethics

Your 24/7 compliance resource, updated for 2023—now spanning two volumes!



As your go-to guide for compliance, *The Complete Compliance and Ethics Manual* is now updated with new and revised content to ensure you have the most-current information to build and maintain a successful compliance and ethics program. This two-volume set is a must-have for compliance and ethics professionals across all industries.

New content, including 6 new articles:

- U.S. Antiboycott Laws: Understanding the Impact and Ensuring Compliance
- ESG, Cyber, and Privacy: Bridging the Divide
- EU Whistleblower Directive
- And more

Updated information in existing articles, including:

- Creating an Organizational Investigations Program and Conducting Effective Workplace Investigations
- Anti-Money Laundering Compliance Programs for Financial Institutions and Other Businesses
- Government Agencies: Effective Compliance and Ethics Programs Are Necessary for Public Trust
- And more

PURCHASING OPTIONS

One-year online subscription

Two-volume set of softcover print books

Money-saving print + digital bundle

Learn more

corporatecompliance.org/ccem

SCCE
Society of Corporate Compliance and Ethics

Compliance Risk Assessment and Management

February 22–23, 2023 | Virtual (Central European Time)

April 20-21, 2023 | Anaheim, CA ***IN-PERSON***

June 26–27, 2023 | Virtual (CT)

September 27–28, 2023 | Virtual (CT)

December 12–13, 2023 | Virtual (CT)

Get guidance and insights from experienced compliance professionals on how to conduct more effective risk assessments.

Key topics

- Risk assessment: introduction, definitions, and objectives
- Identification of compliance risks
- Assessing the severity of compliance risks
- Risk appetite and tolerance
- Effectiveness of internal controls
- Design and implementation of risk response/remediation plans
- Completing the compliance risk management cycle
- Integration with organizational risk management

Attendees can earn live Compliance Certification Board (CCB)® continuing education units (CEUs) for participating.

Register
corporatecompliance.org/cram

SCCE® Society of Corporate Compliance and Ethics

HCCA® Health Care Compliance Association