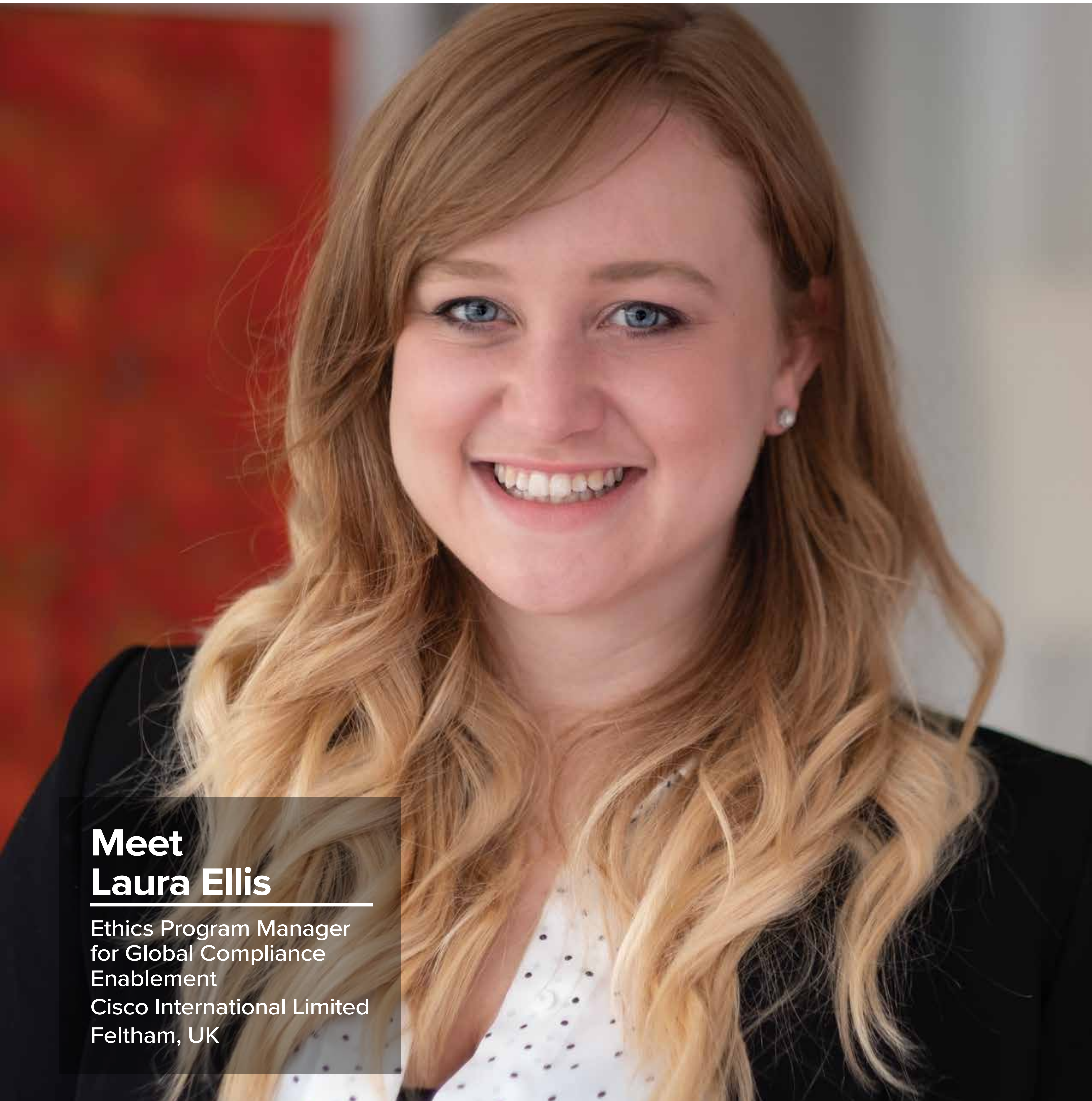
SCCE™
corporatecompliance.org

Compliance & Ethics PROFESSIONAL®

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

AUGUST 2018



Meet Laura Ellis

Ethics Program Manager for Global Compliance Enablement
Cisco International Limited
Feltham, UK

Board Audit Committee Compliance Conference

September 24–25, 2018 | Scottsdale, AZ | The Scott Resort & Spa

This Conference is designed for board members and members of an audit and/or compliance committee. Compliance officers and other senior organizational leaders are welcome to attend.

Buy one registration for $895 and get one for $595

Join us and learn:

- The latest on regulatory risk and compliance obligations
- How to fulfill your fiduciary obligations as a board member
- How to help improve your board performance

corporatecompliance.org/audit

Questions: jill.burke@corporatecompliance.org

SCCE™
Society of Corporate
Compliance and Ethics

by Gerry Zack, CCEP, CFE, CIA

How's your fourth-party due diligence?

Please feel free to contact me anytime to share your thoughts.
+1 612.357.1544 (Cell)   +1 952.567.6215 (Direct)
gerry.zack@corporatecompliance.org
@Gerry_Zack   /in/gerryzack

One of many fascinating aspects of the recent Panasonic Avionics Foreign Corrupt Practices Act case concerns the vetting of third parties. Bribes are often paid through third parties like vendors or other intermediaries. An important aspect of any anti-bribery compliance program is the performance of due diligence prior to working with third parties. A strong third-party due diligence process may detect shell companies or other signs of a suspicious vendor before the corrupt activity has a chance to take place.

Zack

Panasonic used the respected TRACE International to perform due diligence, and this due diligence cleared some sales agents but flagged others. Panasonic then chose to work with only the cleared sales agents. Exactly how it's supposed to work, right?

Where things broke down is that certain Panasonic employees arranged for an approved sales agent to use agents who did not pass as subagents. And that's the route that bribes took. Clearly, people violating internal controls can sink many otherwise well-designed systems. And I can only speculate what controls were in place to prevent this or what red flags existed that could have indicated that controls had been circumvented here.

But this also raises the question of the due diligence itself. If Agent A is cleared and Agent B is not, but Agent A subsequently engages corrupt Agent B, I guess Agent A isn't such a clean agent after all. Should Agent A have been cleared in the first place, given its corrupt intentions in using known corrupt subagents? What is an appropriate level of due diligence here—examining Agent A's practices for performing due diligence on its vendors? Should a company require that due diligence be performed on subcontractors to vendors—the equivalent of fourth-party due diligence?

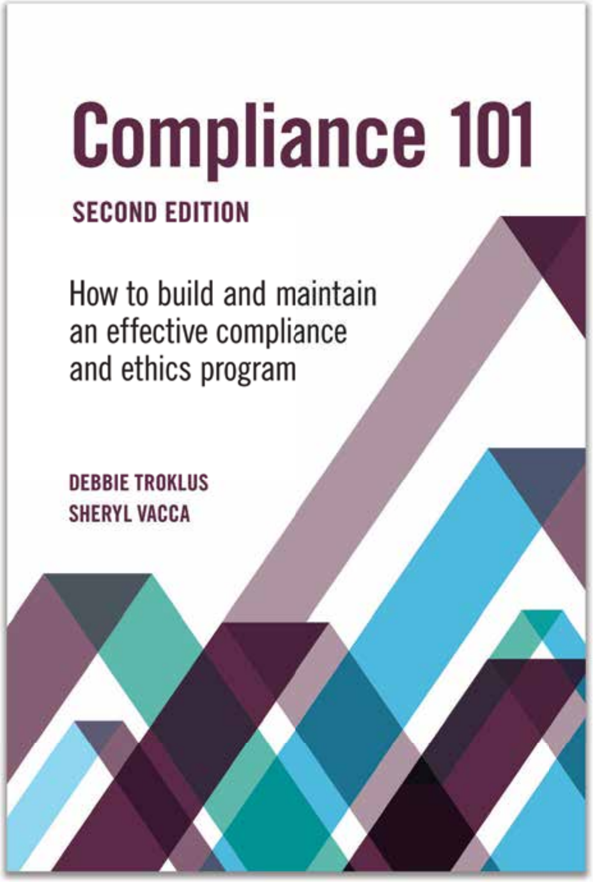
How many levels down should due diligence go? The answer, it appears, is the sometimes frustrating: It depends.

I hate the response, "Some things just can't be prevented," because I think it's wrong and it's the equivalent of throwing our hands up and surrendering. But how many levels down should due diligence go? The answer, it appears, is the sometimes frustrating: It depends. A risk-based approach to due diligence is critical—one that would in some cases conclude that going one level down is sufficient, while in other cases require digging several levels down, depending on a variety of relevant risk factors. Organizations that attempt the one-size-fits-all or checklist approach inevitably regret their decision. ✳

Compliance 101

SECOND EDITION

Revised with updated information and more guidance on best practices



Compliance 101

SECOND EDITION

How to build and maintain
an effective compliance
and ethics program

DEBBIE TROKLUS
SHERYL VACCA

As SCCE moves into its second decade of supporting the compliance and ethics profession, authors Debbie Troklus and Sheryl Vacca have updated this classic text with new insights and more tips on how to build an effective program that meets federal standards. More sample policy and procedure documents are included.

Compliance 101 provides the basic information you need to build and maintain an effective compliance and ethics program in your organization.

This book is ideal for compliance professionals new to the field, compliance committee members, compliance liaisons, board members, and others with compliance duties.

Contents

1 What is a Compliance Program?

2 The Seven Essential Elements

3 Organizational Steps

4 Tailoring Your Compliance Program

Appendices: Sample Program Materials

Glossary of Compliance Terms

For more information, and to purchase, visit:

corporatecompliance.org/Compliance101

by Roy Snell, CHC, CCEP-F

Singular Fact Syndrome

Please don't hesitate to call me about anything any time.
+1 612.709.6012 (Cell) • +1 952.933.8009 (Direct)
roy.snell@corporatecompliance.org
@RoySnellSCCE /in/roysnell

Basing opinions and decisions on "a fact" has become in vogue. What we need is a better understanding of the value of an independent and unbiased gathering of all relevant facts on which to base opinions and decisions. People who have a fact often admonish the person they are debating for not having a fact, and they claim the existence of one fact is enough. I call it Singular Fact Syndrome. Those with Singular Fact Syndrome indignantly and self-righteously hold their fact high in the air and say to people with an opposing view, "Don't come into this discussion without a fact. Look here, I have my fact. I am better than you, because I have my fact with me. You have not come prepared. You lose." (I may have exaggerated a bit there for dramatic effect.)

Snell

I have to give them an E for effort for recognizing the value of facts. However, is a fact better than nothing? It is a fact that many smokers do not die of cancer, but having that fact—and that fact alone—is useless and misleading. It's a sure sign that the individual has Singular Fact Syndrome. Sadly, those who have Singular Fact Syndrome are in really bad shape, because they think they have it all going on and they don't. My favorite Singular Fact Syndrome example was the person who told me they would not wear a seatbelt, because they saw a story once about someone who drowned when their car went into water when they had their seatbelt on. This was a well-to-do, mature, highly educated individual. Anyone can have Singular Fact Syndrome.

We have a lot of people who take a position and deliberately look for a fact that supports their position. They may have to plow through a lot of facts that work against their case, but those with Singular Fact Syndrome are able to ignore facts that do not help their case. It's a hideous disease.

If you want to be an effective, honest, and credible individual, you have to look at *all* the facts.

If you want to be an effective, honest, and credible individual, you have to look at *all* the facts associated with a particular point that you want to make. Many people do not have Singular Fact Syndrome. They see right through your singular fact argument. You look silly and possibly dishonest or manipulative to those who do not have Singular Fact Syndrome. We would all be better served if we were more conscious of when we do this and study effective, unbiased, comprehensive analysis and decision-making techniques. ✳

Contents

August 2018

FEATURES

18 **Meet Laura Ellis, CCEP-I**
an interview by Gerry Zack

24 **Meet Richard Walden**
by David D. Dodge
Richard Walden talks about ethics and leadership in the world of sports.

29 [CEU] **Anti-bribery/compliance pitfalls at the U.S. state level**
by Don McCorquodale and Susan Carr
An examination of compliance issues that affect state and local sales markets in the U.S.

36 [CEU] **ISO 37001 Certification: Understanding and navigating the process**
by Maurice L. Crescenzi, Jr.
An in-depth look at the specifics of ISO 37001 and the certification process.

46 **Making the most of the FCPA Corporate Enforcement Policy**
by Valerie Charles
Companies can seize on enticements offered by the Corporate Enforcement Policy as they seek to build an effective compliance program.

DEPARTMENTS

8 **News**

11 **SCCE news**

16 **People on the move**

70 **SCCE congratulates newly certified designees**

72 **SCCE welcomes new members**

75 **Takeaways**

76 **SCCE upcoming events**

COLUMNS

3 **Letter from the Incoming CEO**
by Gerry Zack

5 **Letter from the CEO**
by Roy Snell

23 **Empirically speaking**
by Billy Hughes and Dian Zhang

27 **Ethics ~~vs.~~ ~~or~~ AND compliance**
by Steven Priest

35 **Compliance, life, and everything else**
by Thomas R. Fox

45 **View from the front lines**
by Meric Craig Bloch

49 **Kaplan's Court**
by Jeffrey M. Kaplan

53 **The view from Nickel City**
by Jennifer L. Kennedy

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

74 **The last word**
by Joe Murphy

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

> “It is so important to look at the person in front of you as an individual and try not to overgeneralize.”
>
> *See page 20*

ARTICLES

50 **Establishing ethics compliance for the banking sector in Bosnia and Herzegovina**
by Mujo Vilašević
Bosnia and Herzegovina can serve as a case for how compliance in financial institutions can serve the community itself and help develop banks as a business in general.

54 **Compliance: Addressing the intensifying age of statutory regulations**
by Ken Chamberlain
Changes in the global business environment require a robust compliance infrastructure to ensure an organization’s interests are protected.

62 **Your settlement with the government requires an Independent Review Organization: Now what?**
by Bert F. Lacativo and Adam Lampert
What is an Independent Review Organization (IRO), what does it mean for your company, and how can you select the best candidates?

67 [CEU] **Five ways to reduce the likelihood of a third-party breach**
by Dov Goldman
Organizations large and small remain vulnerable to data breaches. How can you minimize your company’s risk?

Compliance & Ethics Professional® (CEP) (ISSN 1523-8466) is published by the Society of Corporate Compliance and Ethics (SCCE), 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. Subscriptions are free to members. Periodicals postage-paid at Minneapolis, MN 55435. Postmaster: Send address changes to *Compliance & Ethics Professional Magazine*, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. Copyright © 2018 Society of Corporate Compliance and Ethics. All rights reserved. Printed in the USA. Except where specifically encouraged, no part of this publication may be reproduced, in any form or by any means, without prior written consent from SCCE. For subscription information and advertising rates, call +1 952.933.4977 or 888.277.4977. Send press releases to SCCE CEP Press Releases, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. Opinions expressed are those of the writers and not of this publication or SCCE. Mention of products and services does not constitute endorsement. Neither SCCE nor CEP is engaged in rendering legal or other professional services. If such assistance is needed, readers should consult professional counsel or other professional advisors for specific legal or ethical questions.

STORY EDITOR/ADVERTISING
Margaret Martyr
+1 952.567.6225 or 888.277.4977
margaret.martyr@corporatecompliance.org

PROOFREADER
Patricia Mees, CCEP, CHC
+1 952.933.4977 or 888.277.4977
patricia.mees@corporatecompliance.org

COPY EDITOR
Bill Anholzer
+1 952.405.7939 or 888.277.4977
bill.anholzer@corporatecompliance.org

DESIGN & LAYOUT
Pete Swanson
+1 952.405.7903 or 888.277.4977
pete.swanson@corporatecompliance.org

FRONT COVER AND PAGE 18:
Photography by Helen Jones Photography @ helenjonesphotography.co.uk

Compliance & Ethics
PROFESSIONAL

EDITOR-IN-CHIEF

Joe Murphy, Esq., CCEP, CCEP-I
Senior Advisor, Compliance Strategists
jemurphy5730@gmail.com

EXECUTIVE EDITORS

Roy Snell, CHC, CCEP-F
CEO, Society of Corporate Compliance and Ethics
roy.snell@corporatecompliance.org

Gerard Zack, CFE, CPA, CIA, CCEP, CRMA
Incoming CEO, Society of Corporate Compliance and Ethics
gerry.zack@corporatecompliance.org

VOLUME 15, ISSUE 8

Survey: Misconduct drives away good employees

A recent survey of corporate employees shows the lasting damage of compliance violations in the workplace: the good employees are more likely to leave. An infographic about the survey by business consultant Gartner Inc. reports that 30% of its survey respondents have observed misconduct in the workplace in the past year. Of those who witnessed at least one compliance violation, 59% are actively looking for another job, compared with 27% of respondents who have not witnessed workplace misconduct. What's more, of respondents who report the misconduct, 62% are actively job searching, compared with 50% of those who observed misconduct but did not report it. For more information, see the infographic: https://gtnr.it/2tiUSM6.

Canada releases details of new cybersecurity strategy

The Canadian government announced in June that it is committing $155.2 million over five years to create a new Canadian Centre for Cyber Security. The new center will house all of the federal government's cyber expertise under one roof, led by a senior official from National Defence. In addition, the government has committed $116 million over five years to create a national cybercrime coordination unit, which is expected to be up and running by the fall. It will also launch a voluntary cyber certification program that will outline best practices to help businesses understand and respond to cyber threats. Federal officials have said they recognize that Canada has a shortage of high-tech workers, and they are working with universities and schools to encourage more young people to consider such careers; however, no funding has been set aside yet for specific initiatives. For more information, view the government press release: http://bit.ly/2Ij9DLg.

FTC announces hearings on Competition and Consumer Protection in the 21st Century

The U.S. Federal Trade Commission (FTC) and its new chairman, Joe Simons, will go on a cross-country listening tour this fall to help determine "whether broad-based changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection enforcement law, enforcement priorities, and policy." Fifteen or more hearings will seek to address topics, such as privacy and security abuses, the potential risks posed by big data, and the commission's tools to enforce antitrust laws for media, tech and telecom company mergers, and the development of new lines of business. The FTC is modeling the effort on its 1995 "Global Competition and Innovation Hearings." These hearings will begin in September and will continue into January 2019. Through August 20 the Commission will accept public comment on the topics to be covered. For more information, see the commission's announcement: http://bit.ly/2JUKW6M ✳

Read the latest news online ▶ corporatecompliance.org/news

Socialize!

Connect with us and your compliance colleagues on all of your favorite social media platforms.

Join the compliance conversation and help grow the compliance community.

corporatecompliance.org/ sccenet	facebook.com/ SCCE	twitter.com/ SCCE	bit.ly/LIGroupSCCE bit.ly/LinkedInSCCE	youtube.com/ compliancevideos
pinterest.com/ theSCCE	instagram.com/ theSCCE	corporatecompliance.org/ google	complianceandethics.org	complianceandethics.org/ category/podcasts

2018 International Basic Compliance & Ethics ACADEMIES

FROM THE SOCIETY OF CORPORATE COMPLIANCE & ETHICS®

24-27 SEPTEMBER
MADRID, SPAIN

The Society of Corporate Compliance and Ethics International Basic Compliance & Ethics Academies® provide three and a half days of classroom-style training in the fundamentals of compliance and ethics management. Learn everything from understanding risk, and setting policies, to training and investigations.

Topics addressed at an academy include:

- Standards, policies, and procedures
- Compliance and ethics program administration
- Communications, education, and training
- Monitoring, auditing, and internal reporting systems
- Response and investigation, discipline and incentives
- Anti-Corruption and Bribery
- Trade Sanctions
- Risk assessment

corporatecompliance.org/academies

Questions: lizza.catalano@corporatecompliance.org

INTERNATIONAL ACADEMIES
OFFERED IN 2018-2019

RIO DE JANEIRO, BRAZIL
26–29 NOVEMBER, 2018

DUBAI, UAE
13–16 JANUARY, 2019

HONG KONG
11–14 FEBRUARY, 2019

10,900+
COMPLIANCE PROFESSIONALS
HOLD A COMPLIANCE CERTIFICATION BOARD (CCB)® CREDENTIAL

REGISTER EARLY TO RESERVE YOUR SPACE

ACADEMIES ARE LIMITED TO 75 PARTICIPANTS

SCCE™
Society of Corporate Compliance and Ethics

SCCE *conference news*

Compliance growth globally has been tremendous, and SCCE's International Academies are paving the way to creating strong global compliance teams. SCCE has been offering Compliance Academies for more than 10 years, and the faculty has heard issues, best practices, and discussions from more than 7,500 participants. The consistency and collaboration of the faculty provides attendees with the highest quality of education. The class sizes are limited to 75 participants to enhance the interaction and networking time, and allow you more opportunity to engage with faculty and build on your understanding of what is being taught in the academy. You can be confident that your global team is getting the same education whether they are attending the academy in Rio de Janeiro or our newest location, Hong Kong.

Upcoming International Academies:

- São Paulo, Brazil | 20–23 August 2018
- Madrid, Spain | 24–27 September 2018
- Rio de Janeiro, Brazil | 26–29 November 2018
- Dubai, UAE | 13–16 January 2019
- Hong Kong | 11–14 February 2019
- Amsterdam, Netherlands | 6–9 May 2019
- Singapore | July 2019

Learn more online at www.corporatecompliance.org/academies

Growth has been so great, we have added regional events around the globe, and we expect that growth to continue! Regional Conferences have quickly become a popular enhancement to our stateside members and participants, offering one-day conferences in more than a dozen cities throughout the United States. Now we are pleased to offer these local, one-day conferences in São Paulo, Sarajevo, Dubai, and Singapore. Be sure to check out the agendas for these additional global events online as well!

International events:

- São Paulo, Brazil | 24 August 2018
- Sarajevo, Bosnia, and Herzegovina | 4 October 2018
- Dubai, UAE | 17 January 2019
- Singapore | July 2019

Learn more online at www.corporatecompliance.org/regionals

Find the latest conference information online ▶ corporatecompliance.org/events

SCCE *website news*

Contact Tracey Page at +1 952.405.7936 or email her at tracey.page@corporatecompliance.org with any questions about SCCE's website.

Top pages last month

- Home Page
- About Membership
- Why Join?
- July Academy
- My Account

Number of website visits last month

149,954

Website facelift

You will notice some changes on the website in the next couple months. We are in the process of updating our sites to make them more user-friendly! As we grow as an association, our site must grow with us. Our new site will run faster with more activity and new features. We look forward to your feedback once the sites are live this fall.

SCCEnet – SCCE's social network

Members and nonmembers alike use SCCE.*net* as a way to communicate and get advice from other compliance professionals. But did you know you are also able to upload documents? There's a full library of resources and templates accessible to our compliance professionals.

Video of the Month

Corporate Culture

Nancy Turner discusses how you can encourage a good corporate culture. ✷
http://bit.ly/cep-votm-2018-08

SOCIALIZE!

Connect with us and your compliance colleagues on all of your favorite social media platforms. Join the compliance conversation and help grow the compliance community.

- corporatecompliance.org/sccenet
- facebook.com/scce
- twitter.com/SCCE
- bit.ly/LIGroupSCCE
bit.ly/LinkedInSCCE
- youtube.com/compliancevideos
- pinterest.com/theSCCE
- instagram.com/thescce
- corporatecompliance.org/google
- complianceandethics.org
- complianceandethics.org/category/podcasts

Find the latest SCCE website updates online ▶ corporatecompliance.org

SCCE *blog highlights*

Contact Doug Stupca at +1 952.567.6212 or email him at doug.stupca@corporatecompliance.org with any questions about SCCE's blog.

The DOJ Evaluation Guidance: A road map to compliance

***Sascha Matuszak** is a Reporter at SCCE & HCCA.*

It's been more than a year since the Fraud Section of the Department of Justice (DOJ) issued its Evaluation of Corporate Compliance Programs,[1] but it is helpful to revisit this document to be reminded of what the DOJ looks for in a compliance program and some of the questions they would ask during a criminal investigation. The document begins by explaining the thinking behind releasing this type of guidance. The decision to initiate a criminal investigation in a corporation is governed by the so-called Filip Factors[2] (Michael Volkov has a quick summary at https://bit.ly/2kWuunE), and those factors include the existence and effectiveness of the corporation's preexisting compliance program. See this passage from the Evaluation Guidance itself:

Matuszak

> Because a corporate compliance program must be evaluated in the specific context of a criminal investigation that triggers the application of the Filip Factors, the Fraud Section does not use any rigid formula to assess the effectiveness of corporate compliance programs.

Find the latest SCCEnet updates online ▶ corporatecompliance.org/sccenet

> We recognize that each company's risk profile and solutions to reduce its risks warrant particularized evaluation. Accordingly, we make an individualized determination in each case. There are, however, common questions that we may ask in making an individualized determination. This document provides some important topics and sample questions that the Fraud Section has frequently found relevant in evaluating a corporate compliance program.

The topics in question

The Evaluation Guidance contains 11 sample topics, each followed by several questions related to that topic. The list is not exhaustive, but it provides enough of a framework that a competent compliance officer could use this document as a road map toward creating an effective compliance program. Ricardo Pellafone outlined ways to implement this guidance for our blog last August.[3] Pellafone's method is to approach the Evaluation Guidance from a project planning point of view, and to think in terms of business processes instead of topics and questions, as the DOJ has laid it out. It's a very useful post and recommended reading.

For those who want to tackle the project on their own while using primary sources, here are the topics:

- Analysis and Remediation of Underlying Misconduct
- Senior and Middle Management
- Autonomy and Resources
- Policies and Procedures (Design and Accessibility; Operational Integration)
- Risk Assessment
- Training and Communications
- Confidential Reporting and Investigation
- Incentives and Disciplinary Measures
- Continuous Improvement, Periodic Testing and Review
- Third Party Management

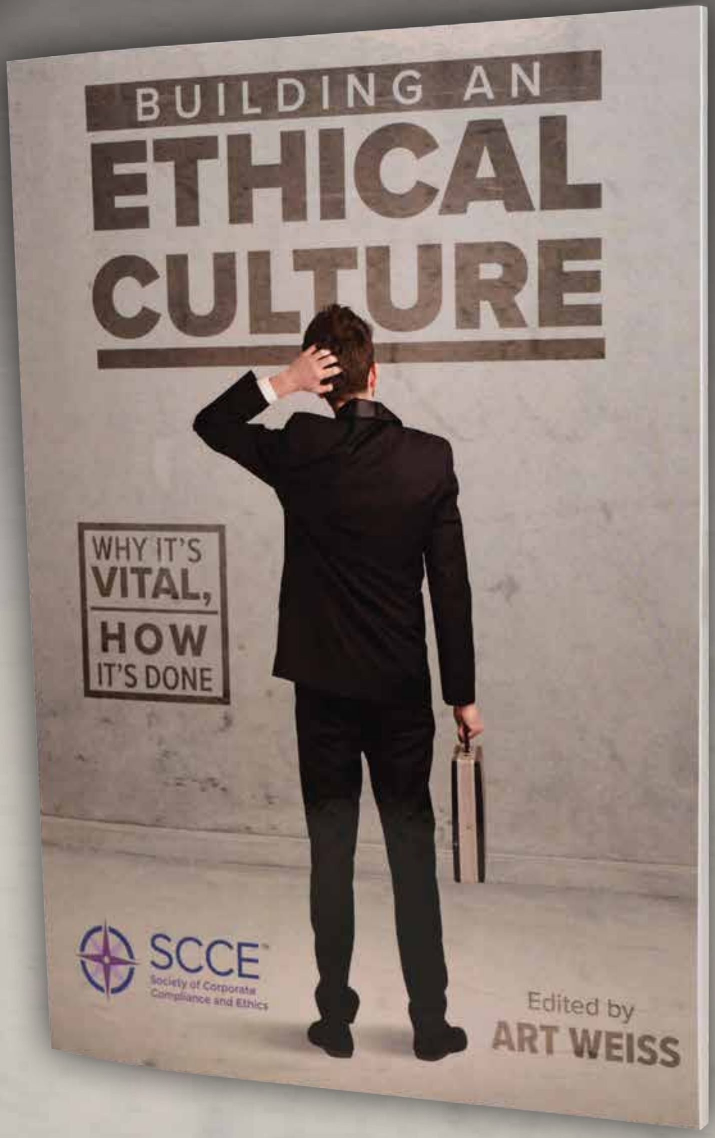
Mergers and acquisitions

Each topic is followed by the types of questions an investigator would ask in order to determine, among other things, what the company in question has done to assess risk, enable compliance officers, and adequately inform and train staff. Law firm Baker McKenzie put together an informative summary of the Evaluation Guidance, including commentary on the questions and topics.[4] They conclude that this type of guidance, which demonstrates the Fraud Section's growing expertise in the compliance field, is a welcome and helpful development:

> The prevailing message from the Evaluation Guidance, however, is that companies themselves must take ownership of their programs, adequately resource them, properly tailor and integrate them into their business, and regularly update and enhance them. The Fraud Section is becoming increasingly refined in its ability to evaluate compliance programs and test whether the programs are functioning as expected. We expect this trend to continue. ✳

[1] Available at https://bit.ly/2lEphmk.
[2] Available at https://bit.ly/29sQSSu.
[3] Richard Pellafone: "How to implement the DOJ's Evaluation of Corporate Compliance Programs" *The Compliance & Ethics Blog;* August 2, 2017. Available at https://bit.ly/2JiMebt.
[4] Baker McKenzie: "DOJ Issues New Compliance Program Evaluation Guidance" February 28, 2017. Available at https://bit.ly/2JxTK1d.

NEW



BUILDING AN ETHICAL CULTURE

AVAILABLE NOW!

corporatecompliance.org/books

With this book, you'll learn:

- What it means to have an ethical culture and why it's critical to your organization's survival
- How to build a solid foundation for a compliance and ethics program that thrives
- How to inspire, support, and reward ethical behavior
- Strategies and tactics to strengthen and reinforce values-based behavior and a commitment to integrity over time

Published by the Society of Corporate Compliance and Ethics (SCCE)

PEOPLE on the MOVE

- **Melanie Reker** has been promoted to Chief Compliance Officer North America at De Lage Landen Financial Services, Inc., in Wayne, Pennsylvania.
- In Dallas, Texas, Children's Health recently promoted **Javier Montemayor** to Chief Compliance Officer and Vice President of Accreditation and Regulatory Affairs.
- In New Delhi, India, Cranex Limited has hired **Prakash Kedia** as Company Secretary and Compliance officer.
- **Millie Richardson** of London-based Global Reach Partners has been named Chief Compliance & Risk Officer.
- NeoGenomics has hired **Stephanie Bywater** as its new Chief Compliance Officer in Fort Myers, Florida.
- Sequant Capital has hired **Erik Wilgenhof Plante** as its Chief Compliance Officer in London.
- Freddie Mac, based in McLean, Virginia, has announced **John Krenitsky** as its new Senior Vice President and Chief Compliance Officer.
- **Kiersten Boyce** joins the University of California–Riverside as the Associate Vice Chancellor and Chief Compliance Officer.

RECEIVED A PROMOTION?
Have a new hire in your department?

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

margaret.martyr@corporatecompliance.org

Become a Certified Compliance & Ethics Professional (CCEP)®

- Broaden your professional qualifications
- Increase your value to your employer
- Gain expertise in the fast-evolving Compliance field

There's never been a tougher or better time to be a part of the Compliance and Ethics profession. Budgets are tight, governments around the world are adding new regulations, public trust in business is low, and employees are tempted to cut corners.

As a Certified Compliance & Ethics Professional (CCEP)®, you'll be able to demonstrate your ability to meet the challenges of these times and have the knowledge you need to help move your program and your career forward.

Learn more about what it takes to earn the CCEP at
compliancecertification.org/ccep

Hear from your peers

Melanie Reker, *CAMS, CCEP*

Chief Compliance Officer North America
DLL Financial Services
Pennsylvania

1) Why did you decide to get certified?

I decided to become a Certified Compliance & Ethics Professional (CCEP)®, because it is renowned and respected in the field of Compliance. The certification provides a great overall framework for what a Compliance function in each company should look like. Content and level of sophistication can then be customized per your organization's risk profile. Since a lot of material and focus is on anti-money laundering (AML) these days, it is a great way to prepare your organization for the level of scrutiny to shift from AML to core compliance, and you can be ready at your pace.

2) How do you feel your certification has helped you?

The certification confirms that you are a serious Compliance professional. It allows team members, peers, superiors, etc., to rely on your expertise. At the same time, it allows you to reach out to your CCEP certified network, as well as the SCCE network, to stay abreast of what's happening in the Compliance field, so you can provide the right level of proficiency and assurance for your organization.

3) Would you recommend that your peers get certified?

Absolutely. It is an efficient and fun way to excel in your field, boost your confidence, and create an unparalleled network.

CCEP™

Laura Ellis, CCEP-I
Ethics Program Manager for Global Compliance Enablement
Cisco International Limited
Feltham, UK

an interview by Gerry Zack

Meet Laura Ellis

Laura Ellis (laellis@cisco.com) was interviewed in May 2018 by **Gerry Zack** (gerry.zack @ corporatecompliance.org), Incoming CEO of SCCE & HCCA, based in Minneapolis, MN.

GZ: Thanks for taking the time to be interviewed for *Compliance & Ethics Professional*. Tell us about your role as an Ethics Program Manager for Cisco.

LE: Currently my role is primarily looking after our Ethics Case Management tool and process. If you email, call, or contact the Cisco Ethics Office in any way, it comes to me. The team often calls me the "smiley" side of ethics and compliance, because if something comes to me, you are already doing the right thing by reporting or disclosing it. If someone else from our team meets you, it can be not so smiley. I love my job, because it's global and I get to work with many people in different areas of the business to help solve problems, provide advice, or take the next steps toward internal investigations.

GZ: Structurally, where does the Global Compliance Enablement function sit within Cisco, and how do you interact with other functions?

LE: Global Compliance Enablement is part of the Legal department at Cisco, and my manager reports directly to the general counsel/CCO, and we in turn report out to the Audit Committee of the board of directors. I think, structurally, it works well at Cisco—we have great relationships with the senior leadership, and our tone at the top is really strong when it comes to ethics and compliance. There is a conscious effort on our side to make sure that we are the "yes" team, hence the term "enablement" in our title.

We work closely with all other business functions as we try to instill the mentality that everyone at Cisco owns compliance; and when you're such a large company, it's hard to be everywhere at once without fostering great relationships.

GZ: You have a fascinating background. You've gone from a degree in philosophy to a position in ethics and compliance in just a few short years, with a few stops along the way. At what point did ethics and compliance become interesting to you, and were there any specific events that led to this?

LE: I feel so fortunate to have gotten to where I am in such a short space of time. The last five years have been a complete whirlwind. My interest in ethics started when I was studying philosophy at university. I'll be honest, I never in a million years thought that I could get a job related to the general term "ethics," but I was fortunate enough to have a degree that allowed me to take additional classes in different departments, and I found that the business school was doing a class entitled Business Ethics. It was an incredibly interesting class, where we learned a lot about corruption and business scandals such as Enron. However, the moment I knew that this job was for me was when we were asked a series of problem questions relating to business ethics. We were asked to stand at either side of the room depending on what you thought the outcome should be. Essentially the lecturer was trying to show that if you stood on one end of the room, you were putting profits over ethical behavior. Out of the series of questions, 90% of the time I was the only one standing on the "ethical" side of the room. I was completely shocked that these highly educated business students were willing to, hypothetically, put their bottom line above the wellbeing of their employees or even the law. I knew that it wasn't malicious or with any specific intentions; however, it highlighted to me how, in many cases, there is a lack of focus on protecting the integrity of your company or the people who work for you. It was then that I knew that I had to find out how to, metaphorically, stand on the other side of the room as a day job.

GZ: What has surprised you the most about the field of ethics so far?

LE: The biggest surprise for me was that this field, in many companies, derived from Legal. It seems foolish now, as I can completely understand the transition in a business to look from legal regulations to a focus on compliance overall and ethics. However when I joined this profession, it was a time when there was a great shift away from compliance as a regulatory field and more toward ethics, with emphasis on company culture. Now that I am one year into my part-time law degree, it is even clearer to me where this industry came from and how important it is to have both.

When I started this job, as a recent graduate, I had wide-eyed hopes to save everyone and teach the whole world how to be good. It took me a long time to step more into the middle of this balancing act and look toward the legal requirements and the risk tolerance in business decisions.

GZ: You co-presented a very well-received session on millennials in Frankfurt at the European Compliance & Ethics Institute. Every generation has its stereotypes, some deserved and some not. What generalizations about millennials in the workplace do you think are reasonably accurate and which are unfounded?

LE: A key part of the research I conducted in preparation for our presentation showed that many traits of millennials vastly differ depending on which country they are from, cultural backgrounds, and what experiences they have had. Therefore, it is so important to look at the person in front of you as an individual and try not to overgeneralize. That being said, there are of course some trends that appear, hence why we have such stereotypes to begin with.

If I may, I'd like to answer your question slightly differently; instead of saying which generalizations in the workplace are reasonably accurate or unfounded, I'd rather say which resonate with me or do not resonate with me. Personally, the stereotype that millennials in the workplace want to make an impact absolutely hits home. I understand that the negative side to that stereotype seems to be that we expect a promotion every six months. However, for me, I simply want to feel like a valued part of any team or organization, much like, I suspect, most others do too, regardless of their generation. That doesn't need to be reflected in my career progression; instead, I want to be able to see that the changes we are putting forward for the company are having an impact.

> It is so important to look at the person in front of you as an individual and try not to overgeneralize.

"Entitled" is the stereotype I hate the most. I understand where this may have come from because, unlike previously, the millennial generation will be worse off than our parents, and this then created an angry cohort of teenagers yelling, "But that's not fair." The millennial generation was born between 1980 and 1995, which means that today the youngest millennial is 23 years old. We are not teenagers stomping our feet anymore; we are, if we're lucky, working adults. I never received a medal for participation, and I never had my mum call in sick to work for me. I was, like so many others, taught that hard work, a bit of luck, and accepting opportunities was the only way to get to where you wanted to be.

Ultimately, when it comes to my generation, I believe that those who shout the loudest are the only ones heard, and I "blame" social media for this. There may have been teenagers who became obsessed with smashed avocado on toast in the '70s, but without Facebook, how would you know? The 5% of millennials who do feel entitled and are spending their money on pumpkin spice lattes make up the 95% who are happy to post about it. I believe that they are the exception, not the rule.

GZ: You did a lot of research in preparing for your presentation. Did any of the results of your research surprise you? Were there things you weren't consciously aware of regarding millennials?

LE: I wasn't really consciously aware of anything on this topic when I started. I went into this research with a completely open mind. It was actually the 2017 SCCE European Conference in Prague that ignited my interest for this subject. I attended an interesting presentation on millennials in the workplace and was fortunate enough to sit next to another millennial. We had never spoken before, and she turned to me and said, "I'm sorry, but do you know anyone like the people they are describing?" We looked around the room, and many people were nodding in agreement with the speaker, agreeing that all millennials were in fact entitled and lazy. So I thought, if I didn't know any and I certainly did not resonate with the stereotypes being discussed, I had to find out who these people were and work out if my new friend and I were the exception or the rule.

I think the piece of research that most surprised me was the differences across cultures. There's a fantastic article in the *Guardian* that looks at what millennials are called in different countries and how that name has been shaped by different trends. For example, in the USA, they should be called "Generation Debt," due to the eye-wateringly high student debts. In the UK, we are called "Generation Rent," because very few young people can afford to get on the housing ladder. My favorite, however, is in China, where they are named *Ken Lao Zu*. The one child policy introduced in 1979 has left the millennials in China with an unbalanced population of 33 million more males than females and without siblings. *Ken Lao Zu* translates as, "the generation that eats the old," happy to parasitically live off their doting parents.

GZ: You mentioned the impact of culture on millennials. Which do you think has a greater impact on how an individual makes ethics-related decisions in the workplace—their age (shaped by interacting mostly with people of similar ages) or the geographic region (shaped by economic, cultural, and other events unique to that region)?

LE: I think historically it has always been geographic region and the norms of your culture in your country. It is fair to say that bribery, for example, is viewed differently in places like India versus somewhere like the USA. However, I do think that that is changing. Social media and the internet has played such a huge part in the transmission of information and broadening individual perspectives. I am always so pleased to see a business ethics-related scandal make the headlines. Not because this is a good thing to happen, but because I am so proud to live in a time when the general public is actually interested in holding businesses accountable for unethical behavior. Hence, the more that business corruption and unethical scandals are posted in the media, the more individuals across the world will open their eyes to a different way to do business.

GZ: So, what does all of this mean? How should ethics and compliance professionals consider generational differences in carrying out their duties?

LE: I think it means that the world of business ethics is changing, and it is our job to keep up. Some of the highest-rated shows on Netflix are about corruption and business scandals. Unethical businesses are making headlines. And whilst it can still be argued that many people won't choose not to buy from Starbucks due to a scandal, research shows that they may think twice before choosing to work there.

Apathy is no longer an excuse to ignore addressing culture in your company. For potential new hires, it is common practice to Google the company before even completing the application form. For your current employees, the newer generations want to be proud to work for you and want to feel as if the company is making a positive impact. So I believe that it is our responsibility, as compliance and ethics professionals, to step up to the plate. Not only by demonstrating the great corporate social responsibility of your company, but that there are people within the organization who care about organizational justice and doing what is right. I've always been proud to tell people what I do for a living and even prouder when someone within Cisco reaches out to us because they know that their company will help to do the right thing.

GZ: Another of your attributes that is representative of a trend we see is that you entered the field of ethics and compliance at an early stage of your career, unlike many members of the profession who came before you, who spent many years in other roles before transitioning to ethics or compliance. What advice do you have for other people just graduating or very early in their careers who are considering entering the compliance and ethics profession?

LE: I truly believe that now is the best time to join this profession. Compliance and ethics is no longer a requirement that people roll their eyes at; it is hot and new and flashy, and there is actually a wealth of material to prove what can happen if you do not have an effective program. My advice would be that connections are key. I would not be anywhere near where I am today if I hadn't put the laptop/phone screen down and braved face-to-face networking. I always found talking about myself incredibly uncomfortable, but being able to talk to other people in Cisco about the importance of my role, or at conferences regarding any of my successes or shortcomings, has been invaluable. There is a wealth of knowledge out there if you know how to tap into it.

GZ: Laura, thanks much for sharing your experiences with our readers. ✳

Don't forget to earn your CCB CEUs for this issue

Complete the *Compliance & Ethics Professional CEU* quiz for the articles below from this issue:

- **Anti-bribery/compliance pitfalls at the U.S. state level**
  by Don McCorquodale and Susan Carr (page 29)
- **ISO 37001 Certification: Understanding and navigating the process**
  by Maurice L. Crescenzi, Jr. (page 36)
- **Five ways to reduce the likelihood of a third-party breach?**
  by Dov Goldman (page 67)

To complete the quiz:

Visit **corporatecompliance.org/quiz**, log in with your username and password, select a quiz, and answer the questions. The online quiz is self-scoring and you will see your results immediately.

You may also fax or mail the completed quiz to CCB:

FAX: +1 952.988.0146

MAIL: Compliance Certification Board
6500 Barrie Road, Suite 250
Minneapolis, MN 55435, United States

Questions? Call CCB at +1 952.933.4977 or 888.277.4977

To receive 1.0 non-live Compliance Certification Board (CCB) CEU for the quiz, at least three questions must be answered correctly. Only the first attempt at each quiz will be accepted. *Compliance & Ethics Professional* quizzes are valid for 12 months, beginning on the first day of the month of issue. Quizzes received after the expiration date indicated on the quiz will not be accepted.

by Billy Hughes and Dian Zhang

How Compliance should adapt to the Digital Age

Billy Hughes *(william.hughes@gartner.com) is an Executive Advisor, and* ***Dian Zhang*** *(dian.zhang@gartner.com) is an Analyst at Gartner in Arlington, VA.*

Digitization—the process of applying digital technology to conduct an activity that had previously been done through analog means—permeates almost all aspects of business and is fundamentally reshaping how it operates. As such, discussions about driving business performance with analytics and artificial intelligence, among others, are on the rise.

Hughes

Zhang

Seeing these opportunities, business leaders are making big bets on digitization. According to a 2017 Gartner survey[1] of senior executives, 83% expressed digital business goals for their organization to achieve, and 69% already had specific digital initiatives underway. Moreover, 77% of CEOs indicated a high level of concern over risks associated with digitization.

This means your Compliance teams will need to match the business step-for-step by digitizing assurance activities and controls that are too manual and experimenting with technology to get new insight into key risks.

Build Compliance processes into digital workflows

As more corporate functions perform their work digitally, teams must integrate compliance processes into the digital workflows the rest of the business follows.

To start, make online training courses and key policies mobile-friendly. Likewise, add dropdown options in your web forms to help employees report misconduct or ask Compliance questions. Also consider embedding the preapproval process for gifts and entertainment in the existing platform where employees submit expenses.

Such steps allow employees to meet Compliance requirements, without sacrificing speed and efficiency. As employees move to capture new opportunities, Compliance can keep the pace by embracing digital capabilities.

Adopt new technologies to provide proactive assurance

At Gartner, we've seen some Compliance teams pilot programs that use algorithms to evaluate third-party due diligence questionnaires and conduct vendor screenings against sanctions lists. Other teams are working on projects to mine large datasets of text-based information (think claims for insurance companies) to identify patterns and root causes.

Turning ideas like these into reality requires collaboration across functions. Whether it's through an enterprise-wide Information Governance Committee, a GDPR working group, or a new agenda item for the Compliance Committee, more conversations about the risks and opportunities of digitization need to happen. Compliance teams that plunge headfirst into these conversations will have a chance to shape how data is used and protected, while those that shy away will be forced to react as their business partners act first and ask (compliance) questions later. ⁕

[1] Gartner, "Gartner Survey Shows 42 Percent of CEOs Have Begun Digital Business Transformation," press release, April 24, 2017. https://gtnr.it/2trgK8Y

an interview by David D. Dodge

Meet Richard Walden

Richard Walden (athleterep@aol.com), an attorney and partner in the law firm of Burris, Schoenberg & Walden, LLP, was interviewed in February 2018 by David D. Dodge (david@sprtsoc.com), CEO, Sports Officiating Consulting, LLC in Carlsbad, California.

DD: What led you to collaborate with others in writing the book, *Sport, Ethics and Leadership*?

RW: Two things. First, I attend many sports events (in some years nearly 200) and also participate in recreational sports. I see many examples of poor sportsmanship and coarse behavior by fans and participants, and often wonder why people act that way and why other fans, athletes, and management don't do more to curb that bad behavior. So the questions of what is an "ethical" fan or athlete and what can good leadership do to foster "ethical" behavior are on my mind when I am at sporting events.

Walden

Secondly, I've taught sports law at the University of San Francisco master's program in sports management since about 2001. In teaching that course, I realized that we'd often touch on the philosophical and ethical components of issues, not just the legal. I spoke with the dean about creating a sports ethics course. While preparing the proposal for that course, I recalled actual things I'd seen at events over the years to use as examples for the course. I also began looking for a suitable textbook and did not find one to my liking, so I mentioned to the dean that perhaps one byproduct of the course would be that I'd write my own textbook.

At some point, I realized that I did not have time to pursue the course or the book any further and shelved the project. A year or two later, the dean was talking to another sports lawyer and professor (Ron Katz), who mentioned that he was interested in writing a book on sports ethics. The dean remembered my interest in the subject and put us in touch.

Ron and I got together and decided to see if we could get a book deal. Ron had a much broader vision for the book than my original one, so the scope of the book quickly expanded. As it expanded, we realized that it was becoming a bigger undertaking and that there were topics that would be better addressed by other experts. So we recruited a sports philosopher, Jack Bowen; a leadership expert, Don Polden; and an expert on amateur and intercollegiate athletics, Jeff Mitchell. We then came up with an outline of chapters, which we divvied up based on our areas of interest and experience. The collaborative part of this was seamless.

DD: Why is ethical leadership so important in the microcosm of sport?

RW: I don't have any social science data to rely on, just my opinions, but I think that sports are so important in our society and so prevalent that they end up shaping behavior and norms. Kids emulate the batting stances of their baseball idols and the basketball moves of their favorite NBA stars; they imitate the way they wear uniforms, even the trash-talking and other behaviors exhibited by athletes they look up to. People take many social and behavioral cues from the sports world. So I think that sports have a profound influence on non-sports behavior.

I also think that the more we are invested in sports, the more we need ethical leadership. The use of performance-enhancing drugs, other forms of cheating by athletes or officials, the response of teams and leagues to things like violence on and off the playing field, and player injuries like football concussions are all things that can erode our trust and enjoyment of sports if not thoughtfully dealt with.

DD: In light of the recent sexual abuse scandals at USA Gymnastics and at Michigan State University, what is the risk of focusing preventive programs solely on sexual abuse rather than all areas of risk?

RW: That is a great question. In the past I think we've seen scandals addressed individually and on an ad hoc basis with little or no thought to how that scandal fits against the sports culture backdrop in which it arose or how to have a cohesive policy to promote ethical behavior across the board. If fans get drunk and rowdy, stop selling alcohol after the seventh inning. If an athlete bullies another, punish him or her. If a fan or player files a suit, settle it. But rarely is thought given to a broader risk management policy and how the school or team or league leaders can do just that: lead. I think that much of Roger Goodell's problems since he took over the National Football League (NFL) stem from this sort of myopic, "plug each hole in the dam as they pop up" approach.

> Rarely is thought given to a broader risk management policy and how the school or team or league leaders can...lead.

I think that the gymnastics scandal will likely follow the same pattern and will not, other than perhaps with a few visionaries and outliers, result in a more comprehensive approach to risk management.

DD: Although compliance, ethics, and integrity programs are common in other businesses and industries, why have sports leaders been slow to adopt such programs?

RW: I honestly don't know. I think that part of the answer may be that even today sports are still often viewed less as businesses or industries and more as pastimes, activities, and pleasures. Obviously, this has changed over the last few decades as the business side of sports has taken a higher profile, but there is still a sentiment that sports are different. I think the fact that sports often involve behavior that is inappropriate in other industries, such as physical contact, means that sports does not fit the "typical" compliance model. Sports, at least professional sports, are dependent upon competition, whereas in other industries, competition is the enemy, which may also be a factor. Finally, sports historically have been more or less self-regulated, which has likely slowed the process.

DD: From your book, "most failures in sport organizations are caused by failures in leadership..." What can be done to aid sports leaders in advancing their leadership capabilities?

RW: The book does a good job of discussing the different kinds of leadership and leadership styles. In doing so, it is apparent that one size does not fit all, and some styles do not work for some people. However, there are still certain characteristics or qualities that all good leaders possess, such as integrity, vision, and the ability to communicate. Certainly, litigation and the threat of litigation are increasingly driving leaders in the sport industries to get out ahead of issues rather than simply reacting.

Recently, Major League Baseball (MLB) extended the safety netting at its ballparks even though, for the most part, teams have been immune from fan suits for injuries from foul balls. The National Hockey League (NHL), learning from the NFL concussion-related suits and claims, has instituted its own concussion protocol. MLB has issued no-hazing guidelines for its teams. Although these sorts of policies and steps are not entirely divorced from the threat of litigation, they are more forward-looking than remedial.

DD: In your book, you talk about the humanity of sport and the moral concept of sportsmanship. Can you expand on that for our readers?

RW: The concept of sportsmanship embraces more than simply not cheating and following the strict letter of the rules. It includes the "unwritten rules" of each sport, such as hockey's informal code of conduct, which states that in a fight, one does not continue to punch an opponent after he has fallen to the ice. A perfect example relates to MLB's rule changes to increase the pace of games. Traditionally, if an umpire is struck by a pitch or a foul ball, the catcher will go out to the mound to allow the umpire a moment to regroup. This sort of mound visit based on unwritten rules of sportsmanship may become a thing of the past, since new rules limit the number of mound visits. In golf, for example, players are trusted to self-report rules infractions. There are countless such examples in sports. Because the culture of sports goes far beyond the written rules, sports are a perfect setting for discussions about humanity, integrity, and behavior. As Alan Greenspan once said, "Rules cannot substitute for character."

DD: Thank you for your time, Richard. ✳

ethikos
THE JOURNAL OF PRACTICAL BUSINESS ETHICS
JULY/AUGUST 2018
Vol. 32 | No. 4
EXAMINING BUSINESS ETHICS SINCE 1987
Before you change corporate culture, define it
page 1
The dangerous duality of sexual harassment investigations and ethical risk mitigation
page 5
SCCE

by Steven Priest

Why employees don't speak up

Steve Priest (steve@integrityII.com) is President of Integrity Insight International. www.integrityII.com

The two main reasons employees don't speak up are the belief that management won't do anything about their concerns, and that raising issues will result in negative consequences (see my columns in the June and April issues of *Compliance & Ethics Professional* magazine). In more than 1,000 focus groups in 40 countries, I have also frequently heard other reasons. Though not as significant, these should still be on your radar:

- **"They won't listen to me."** This is closely associated with employee engagement questions that ask employees whether their opinions are valued.
- **"They already know."** Some employees believe management is like the Wizard of Oz, at least insofar as misconduct is concerned. Encouraging employees to report issues, even if they think management might already know about them, is one way to address this.
- **"I don't know all the facts."** Although this is almost always true, some employees use it as an excuse not to bring up problems. Make sure employees know conducting investigations is not their responsibility!
- **"My manager says 'Don't bring me a problem without a solution.'"** This well-meaning managerial mantra stifles employee openness.
- **"It's not my job."** These employees feel that the scope of their jobs is narrower than it is. Traditional "ethics is everybody's job" messages are the standard prescription, but I doubt that much will move employees with this constricted view of self.

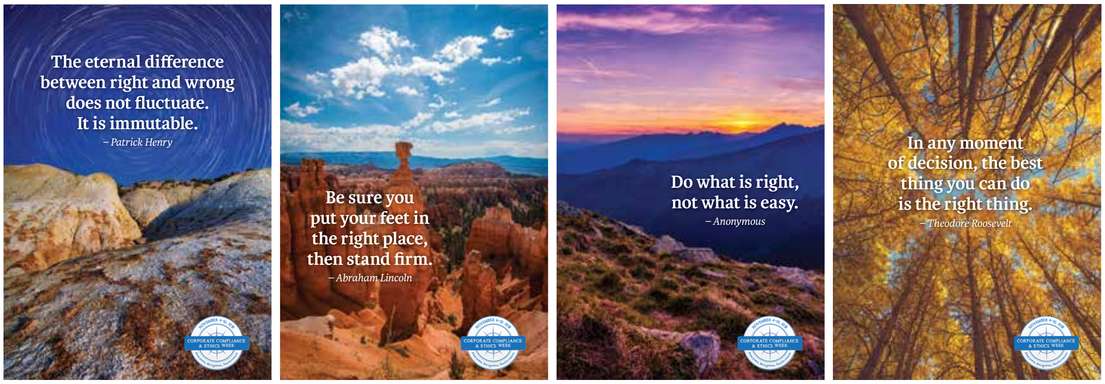
Priest

- **"I have a shy personality."** Yes, I hear this. Computer-based alternative reporting channels will help, but it's hard to change somebody's personality!
- **"It's not done in my country."** This is a common rationale in parts of Europe, Asia, and Latin America. Unfortunately, it is true. We have seen movement by having local country management emphasize a "listen and learn" mind-set that goes beyond compliance. The emphasis has to be on improving the business across the board.
- **"I don't know where to go."** This is probably the easiest one to address. Make sure employees know about alternative reporting channels in addition to the management chain they are familiar with. Communicate how these processes work to safeguard the identity of the reporter and to pave the way for fair, professional investigations.

Underlying all these concerns is the desire for procedural justice for all. In my next column, I will describe reasons why employees raise concerns and how your organization can use them as a foundation for procedural justice. ✳

Corporate Compliance & Ethics Week

November 4–10, 2018 ✶ PLAN TO CELEBRATE!


The eternal difference between right and wrong does not fluctuate. It is immutable.
– Patrick Henry
Be sure you put your feet in the right place, then stand firm.
– Abraham Lincoln
Do what is right, not what is easy.
– Anonymous
In any moment of decision, the best thing you can do is the right thing.
– Theodore Roosevelt

Inspirational Poster Pack

20" x 28" each. Four colorful, glossy posters showcasing different ethics messages. Perforated strip along bottom allows easy removal of 2018 Corporate Compliance & Ethics Week logo after the week is over.

$30.00 per pack (min. order 1 pack)

8-in-1 Multi-tool with LED

Four Phillips head and four flathead magnetic steel alloy screwdrivers of varying sizes fold out of the handle. Includes a powerful flashlight with 6 LEDs. Requires 3 AAA batteries. 4.75" x 1.75".

$8.50 ea. (min. order 10)

Corporate Compliance & Ethics Week
AWARENESS, RECOGNITION, REINFORCEMENT

Highlighter

Yellow and pink, dual-end liquid highlighter.

$1.25 ea. (min. order 25)

Retractable Badge Holder

Blue with Corporate Compliance & Ethics Week logo imprint, 3.25" x 1.25" x 0.63".

$1.50 ea. (min. order 25)

Silicone Awareness Bracelet

Show your Corporate Compliance & Ethics Week pride. Printed with the theme: Awareness, Recognition, Reinforcement.

$0.50 ea. (min. order 50)

Sanitizer Spray

Clear .17 oz lightly scented hand sanitizer with Corporate Compliance & Ethics Week logo. Meets FDA requirements. Travel size: 3.25".

$2.00 ea. (min. order 25)

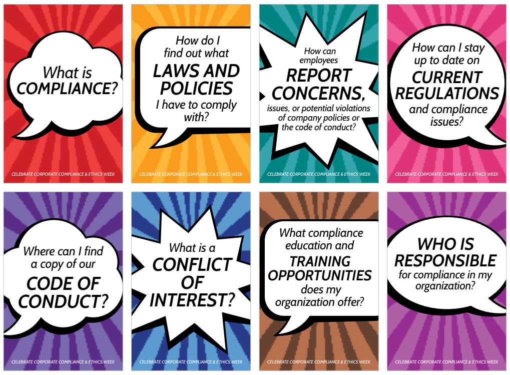

What is COMPLIANCE?
How do I find out what LAWS AND POLICIES I have to comply with?
How can employees REPORT CONCERNS, issues, or potential violations of company policies or the code of conduct?
How can I stay up to date on CURRENT REGULATIONS and compliance issues?
Where can I find a copy of our CODE OF CONDUCT?
What is a CONFLICT OF INTEREST?
What compliance education and TRAINING OPPORTUNITIES does my organization offer?
WHO IS RESPONSIBLE for compliance in my organization?

Table Tents (8-pack)

Pre-cut, 4"×6" two-sided cardstock tents with 8 questions to get your employees thinking about compliance.

$5.00/8-pack (min. order 5)

5-in-1 Lint Brush

Includes lint brush, shoehorn, mirror, comb, and sewing kit. Convenient desk and travel size.v 4.25" x 1.5".

$4.00 ea. (min. order 10)

Padfolio with sticky notes and flags

Three sticky notes in various colors and shapes, and five neon sticky flags. 3.25" x 5.25".

$3.25 ea. (min. order 10)

Stylus Pen and Phone Stand

Black-ink pen features a stylus at the top with a pen cap that bends over to create a phone stand.

$1.50 ea. (min. order 25)

ORDER DEADLINE: October 5, 2018

corporatecompliance.org/CCandEWeek

NOVEMBER 4–10, 2018
CORPORATE COMPLIANCE & ETHICS WEEK
Awareness, Recognition, Reinforcement

by Don McCorquodale and Susan Carr

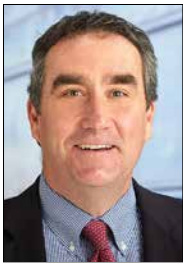
Anti-bribery/compliance pitfalls at the U.S. state level

- The United States state and local government sales market is very large.
- The state and local sales markets permit easy access to decision makers.
- Significant compliance issues must be addressed when selling directly to state and local government employees and leaders.
- A compliance strategy must be incorporated into corporate sales planning.
- Failure to address compliance issues can lead to severe penalties and public scrutiny.

__Don McCorquodale__ (don.mccorquodale@sas.com) is Legal Counsel and Director of State Government Relations, and __Susan Carr__ (susan.carr@sas.com) is Senior Principle Compliance Counsel, at SAS Institute Inc. in Cary, North Carolina.

As compliance and legal professionals, we are asked to help business leaders determine specific and potential risks when entering a new market, developing a new product or solution, or partnering with others in the market. In these evaluations, there is much emphasis on compliance with anti-bribery laws, such as the United States' Foreign Corrupt Practices Act (FCPA) and the United Kingdom's Anti-Bribery Act, as well as country-specific anti-bribery laws. In recent history, we have seen a lot of research, training, and effort put into spreading the word about various compliance issues involving global trade and bribery, data protection, and export/import concerns in those cross-border transactions. This effort is important, because transparency and an even playing field will help ensure a thriving global economy.

It is equally important, however, to remember the United States' domestic laws, which are designed to prevent domestic bribery and increase transparency when businesses engage with state or local governments. Rather than providing broad-brush guidance to "not engage in bribery," these laws provide specific rules that must be followed in government procurement or government engagement. These rules (1) outline the activities that require individuals to publicly register as lobbyists and report their activities (Lobby Laws); (2) limit the types of payments that can be made to third parties in government procurement (Contingent Fee Bans); (3) limit the types of expenditures vendors and those acting on their behalf can make to government employees (Gift Rules); and (4) provide limits on transitions from public to private sector, and sometimes from private to public sector (Revolving Door/Conflicts of Interest). Failure to comply with these rules can subject your company and its employees to adverse media attention, debarment from government contracting or bidding on a contract at issue, contract cancellation, and significant criminal or civil fines and penalties.


McCorquodale

Carr

The rules apply to practically all businesses selling and marketing into United States federal, state, and local governments. Although the laws have the common foundation to prevent bribery and foster transparency in government procurement, they are different in each jurisdiction, and businesses selling to governments at all levels in the U.S. would be wise to implement a domestic anti-bribery compliance program that is equally as robust as their global anti-bribery compliance program.

Market

The United States government sales market has several common attributes among the federal, the 50 states, and more than 89,000 local governments. These common attributes include: each governmental entity generally has a need for technology, goods, and services; and each entity has some level of autonomy to make purchasing/implementation decisions from the more geographically senior government body (i.e., federal government for states and state government for locals).

Likewise, these entities are also quite diverse in reference to social priorities, historical implications, economic factors, and current economic conditions. Because of this diversity, one set of marketing and sales strategies will not fit well across the state and local geographies.

Many companies have targeted the United States government marketplace for sales because of the size of the cumulative marketplace. Many people know that the federal budget is massive. However, many are surprised to discover that state and local government spend is nearly equal to the federal spend. The total federal budget is approximately $3.8 trillion per year, with approximately $450 billion awarded in new prime contracts each year.[1] The National Contract Management Association (NCMA) expects total state and local government expenditures to be a very similar number of $3.5 trillion dollars in 2018.

> Many are surprised to discover that state and local government spend is nearly equal to the federal spend.

One can also compare individual US states to various global national economies. The gross domestic product for the three largest US states are: California, $169 billion; New York, $101 billion; and Texas, $82 billion. California's economy is the eighth largest in the world, just ahead of Russia.[2]

In addition to being a large marketplace, state and local governments are particularly attractive to sales professionals because of comparatively easy access to decision makers. For example, it is not out of the ordinary for a company representative to call on a state governor, her/his staff, or an agency head to discuss/pitch a product. These senior state and local leaders in turn have much more autonomy and influence on the final contract decisions.

Pitfall areas: Compliance perspective

The large revenue potential and easy access to decision makers make the state and local government sales pool particularly attractive, and the company sales team will want to jump in quickly and wade in as deeply as possible. However, the sales teams may not be aware of risks and restrictions associated with selling in the state and local government marketplace. It is true that companies and their sales teams have much easier access to decision makers at the state level compared to the federal or international levels. However, with this ease of access comes risk of undue influence or ethics violations. A recent 50-state study conducted by the Center for Public Integrity gave only three states a grade higher than a D+ for integrity in the state public sector.[3]

Companies would be wise to provide a life raft in the form of compliance training, oversight, and auditing incorporated into the sales process, before sales professionals engage directly with government employees.

Whether your sales team is already in the pool or considering jumping in, here are a few compliance items that must be considered and addressed along with associated risks.

Lobbying

Individuals who engage in certain interactions with government officials and employees may be required to register or report under applicable lobbying laws.[4] The historical definition of lobbying has expanded greatly in the local and state government marketplace over the past ten years because of various pressure points such as government investigations, media attention, and public outcry for more transparency. The definition of lobbying in many state jurisdictions is much broader than many people would imagine. The general lobbying definition is "an attempt to *influence a decision*." In many jurisdictions, an attempt to influence a decision can include a conversation with a senior state official about a company's product. Because of the broad definition, a sales person's efforts at the state level could easily cross the lobbying threshold, which could impose specific obligations and restrictions for the sales person and the company. At the local government level, large municipalities—such as New York City, Los Angeles, Chicago, and Boston—have implemented lobbying guidelines similar to state restrictions that should be considered before proceeding with direct sales.

Note that most state and local enforcement agencies have the authority to impose civil fines for failure to register. For example, the city of Chicago imposed a $90,000 fine in 2017 on a large internet company whose executive sent an email to the mayor referencing a city ordinance that affected the company. It was determined that the email was considered lobbying, and a violation occurred.

Selling product or solution to senior agency staff, elected officials, or elected officials' staff

During the past several years, there has been a noticeable increase in sales interactions and marketing events in state and local government capitals across the United States. In fact, many companies now employ sales teams based in the capitals, with the specific goal of engaging with these senior government officials. If your company is targeting senior agency or elected officials as part of the sales strategy, it would be important to develop specific training, monitoring, and audit systems for these employees and those who support the sales efforts. As you develop the training, monitoring, and audit process, you should review the various statutory requirements that are generally enforced by either the state ethics office, secretary of state office, or the attorney general. If your budget allows, it is a good practice to establish a relationship with outside counsel that is familiar with multistate issues.

Once a sales person or other company employee crosses the lobbying threshold definition, the sales person—and likely the company—will have very specific registration and reporting requirements that will follow them throughout the year and likely into the next year. These requirements vary widely throughout the states—from minimal reporting to very detailed and as frequent as every two weeks. In addition, civil and criminal penalties may apply if a deadline is not met or a form is intentionally not completed correctly.[5] Here is an example of an affirmation that a sales person or compliance person may need to make in Massachusetts:

> *Under the **pains and penalties of perjury**, I certify that I am (Name) of (Company) and that the disclosure report I am submitting is complete and accurate for the period indicated. I further understand that any violation of the lobbying laws is **punishable by civil and/or criminal penalties.***

Gifts

Simply providing a pen or a book outlining the need for your product to a government employee could cause issues for you or the recipient. Many jurisdictions provide very specific definitions of gifts and impose limits on the amounts vendors or lobbyists can spend for the benefit of a government employee.[6] Your sales team should be aware of these rules and should comply fully. Some jurisdictions may permit a small gift, such as a reasonable meal, but others prohibit even a cup of coffee or bottled water.

Unfortunately, there is no standard guidance that works for all jurisdictions. If you do not want to invest the time and energy to research the various rules and guide your sales team as questions arise, the best option is to train your sales team to avoid giving any gift to any state employee.

Although many of the gift restrictions are imposed on the government employee, many states also impose these same gift restrictions on the company and/or company employee. In 2012, a New York utility was fined $1.2 million for violating the state prohibition of giving gifts to state workers.

Some jurisdictions may permit a small gift, such as a reasonable meal, but others prohibit even a cup of coffee or bottled water.

Revolving door

Hiring a former government employee can help companies better understand government opportunities and provide greater access to decision makers, but it can also create issues under laws restricting movement between the public and private sector. Government employees have unique knowledge about government needs, agency or government operations, familiarity with the decision makers, and an understanding of issues the agency may be facing. Historically, the media and the public have shown interest, and at times outrage, when a government employee leaves government and applies their unique knowledge and contacts to financially enrich themselves. To protect governments from misuse of power, many state and local governments implemented specific rules a government employee—and in many cases, the new employer— must follow when transitioning to the private sector, so called "revolving" door laws.[7] These restrictions could also affect how your company bids on a contract if an agency employee is being considered or simply expressed an interest in a job. Many sales teams ask their HR counterparts to recruit government employees. If your company plans to hire a current government employee, it is very important that you have a solid process in place to ensure you and the candidate are complying with the revolving door rules. This process should include: (1) training for the HR recruiter and sales management, and (2) an audit mechanism to make sure pre- and post-employment restrictions are followed.

Compliance leadership is needed

State and local government sales are further complicated by the political undertones that underlie government operations. If, for example, a contract is championed by one administration, the purchase objective/decision may not be supported by the new administration. The new administration may look for superficial ways to terminate the agreement, including violation of lobbying or procurement rules. By following the domestic anti-bribery laws that seek to ensure open, transparent, and honest government procurement, you can protect your company, employees, and customers from a shifting political climate.

If your company has not previously addressed the risks of domestic anti-bribery law compliance, I encourage you to take the lead to understand the risks and chart a path forward to help guide your sales and sales support teams who are targeting state and local opportunities. Compliance can be a valuable partner to Sales as they navigate the United States government marketplace. If you will be creating a domestic anti-corruption program, be prepared for some pushback, or outright dismissal, from your sales colleagues. Be confident in your role and know that your guidance will position your company and colleagues as trusted partners in the government sales space.

One of the most important factors in being a successful salesperson and vendor in the government space is transparency and acting in an ethical manner. Many of the government employees and senior officials appreciate vendors that respect the rules and help them avoid tripping over the ethics and compliance line. ✳

Acknowledgement: *The authors wish to acknowledge SAS Institute's Brian Zuercher, Vice President and General Counsel—Ethics and Compliance, for his input on the article's content and leadership on these important compliance issues.*

1. Bloomberg Government: Annual Review of Government Contracting: 2015 edition. Available at https://bit.ly/2LpPNcs
2. *Idem.*
3. *Washington Post*: How Ethical is Your State Government? November 9, 2015. Available at https://wapo.st/2tBMk2X
4. National Conference of State Legislators: How States Define Lobbying and Lobbyists: November 6, 2017. Available at http://bit.ly/2KgZBbE
5. National Conference of State Legislators: Ethics: Criminal Penalties for Public Corruption/Violations of State Ethics Laws, April 2007 Available on Illinois General Assembly Website at http://bit.ly/2KpxR4U
6. National Conference of State Legislators: Legislators Gift Restrictions Overview, November 7, 2017. Available at http://bit.ly/2Kl5vIQ
7. National Conference of State Legislators: Revolving Door Prohibition, December 15, 2017. Available at http://bit.ly/2MV41Dv

CALL FOR AUTHORS

SCCE
corporatecompliance.org
Compliance & Ethics PROFESSIONAL
A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS
JUNE 2018
Meet Thomas Topolski, CCEP-I
Executive Vice President, Turner & Townsend
see page 18

Share your expertise

Compliance & Ethics Professional is published monthly by the Society of Corporate Compliance and Ethics (SCCE). For professionals in the field, SCCE is the ultimate source of compliance and ethics information, providing the most current views on the corporate regulatory environment, internal controls, and overall conduct of business. National and global experts write informative articles, share their knowledge, and provide professional support so that readers can make informed legal and cultural corporate decisions.

To do this, we need your help

We welcome all who wish to propose corporate compliance topics and write articles.

CERTIFICATION is a great means for revealing an individual's story of professional growth! *Compliance & Ethics Professional* wants to hear from anyone with a **CCEP**, **CCEP-I**, or **CCEP-F** certification who is willing to contribute an article on the benefits and professional growth derived from certification. The articles submitted should detail what certification has meant to the individual and his/her organization.

EARN CEUs

The CCB awards 2 CEUs to authors of articles published in *Compliance & Ethics Professional.*

If you are interested in submitting an article for publication in *Compliance & Ethics Professional*, email **margaret.martyr@corporatecompliance.org**.

Please note the following upcoming deadlines for article submissions:

- September 1
- October 1
- November 1
- December 1

Topics to consider include:

- Anticipated enforcement trends
- Developments in compliance and ethics and program-related suggestions for risk mitigation
- Fraud, anti-bribery, and anti-corruption
- Securities and corporate governance
- Labor and employment law
- Anti-money laundering
- Government contracting
- Global competition
- Intellectual property
- Records management and business ethics
- Best practices
- Information on new laws, regulations, and rules affecting international compliance and ethics governance

by Thomas R. Fox

The DAG on the culture of compliance

Thomas R. Fox *(tfox@tfoxlaw.com) is the Compliance Evangelist.*
www.fcpacompliancereport.com *@tfoxlaw*

Fox

It is not often the Deputy Attorney General discusses the importance of corporate culture, yet Rod Rosenstein did so at a conference I attended in May, where he stated, "Ethical, law-abiding companies can better attract investors and partners. People want to do business with companies that they perceive as honest and reliable." Moreover, a culture of compliance "mitigates risk, making companies more valuable and less likely to encounter unanticipated costs that may result from protracted investigations and penalties."

Most interestingly, Rosenstein went on to add, "Compliance should not be treated as separate and distinct from other business goals. A culture of compliance must be fully integrated into corporate culture. Employees should be trained and encouraged to think about compliance issues in making business decisions." Finally, he noted, "In a company with an adequate and effective compliance program, the legal, compliance, and audit departments are not the only repositories of professionals monitoring and evaluating what the business side does."

These remarks by Rosenstein are significant for every compliance practitioner and corporate compliance program. They clearly portend that the Department of Justice (DOJ) will begin to evaluate corporate culture as a part of their assessment of a company under a Foreign Corrupt Practices Act (FCPA) investigation. It also ties into a key second component of Rosenstein's remarks, which was two basic questions the DOJ will consider when assessing corporate culture in the context of an FCPA investigation.

First, "What was the state of the compliance program at the time of the improper conduct?" Second, "What is the current state of the compliance function, after remediation to address any lessons learned?" It all begins with a root cause analysis, and the next inquiry is to consider what steps did a company take and are they (or were they) effective?

Rosenstein neatly tied together how a culture of compliance drives to not only protect a company by preventing illegal conduct from occurring, but if employees go off and engage in conduct that violates the FCPA, if you do not have a robust compliance program with a detect prong, you will not find out about the misconduct. This will not only remove your opportunity to self-disclose and begin with the presumption of a declination, but it will also allow the misconduct to continue, making your illegal conduct greater and your final penalty costlier. ✳

by Maurice L. Crescenzi, Jr.

ISO 37001 Certification: Understanding and navigating the process

» The International Organization for Standardization (ISO) is a non-governmental organization that facilitates the international unification of industrial standards and management systems.

» Registrars or "certifying bodies" issue ISO certifications, and leading practices suggest it is best to obtain ISO certifications from accredited registrars.

» ISO 37001 establishes a standardized management system for managing the risk of bribery and corruption in both the public and private sectors.

» Although ISO 37001 has been received positively in the international ethics and compliance community, there is an accompanying sentiment that it does not introduce anything fundamentally new.

» How quickly and widely ISO 37001 will be adopted in the public and private sectors remains to be seen.

Maurice Crescenzi *(mcrescenzi@aol.com) is Managing Director, Ethics and Compliance Practice Leader at Grant Thornton LLP in New York, NY.*

The International Organization for Standardization (ISO) is a non-governmental organization based in Geneva, Switzerland. ISO was formed in 1947 as a result of the merger of two previously separate standards-setting organizations, the International Federation of the National Standardizing Associations and the United Nations Standards Coordinating Committee. ISO's charge is to "facilitate the international coordination and unification of industrial standards."[1,2] In pursuing its mission, ISO works closely with more than 700 international, regional, and national organizations across approximately 162 countries to establish business standards. ISO's list of partners includes the World Trade Organization (WTO), World Standards Cooperation (WSC), and the United Nations (UN).[3]

Crescenzi

To date, ISO has published more than 21,000 international standards that apply across a range of industries and organizational functional areas. These standards help organizations improve operational efficiency and effectiveness. They also promote good management practices. Generally, ISO standards are neither industry- nor product-specific.

Perhaps the most well-known ISO standards relate to quality and environmental management systems; however, ISO has also published standards that help organizations improve in other areas, such as social responsibility, sustainability, and enterprise risk management—standards that reflect the cross-industry, global imperative of achieving long-term organizational growth, and at the same time minimizing negative environmental and social impacts.[4]

Not all ISO standards carry the same weight or effect, however. In some instances, ISO standards simply set forth guidance, good practices, and advice. In other instances, ISO standards set forth actual *requirements*. Organizations may strive to be formally certified with regard to the latter category of requirements-based standards. ISO 37001 is considered a requirements-based standard—with regard to which organizations may strive for certification.

ISO 37001: Anti-bribery management systems

In October 2016, after a three-year drafting process, ISO published standard 37001, which sets forth a comprehensive framework for designing, implementing, and maintaining anti-bribery and anti-corruption programs.[5] The drafting effort was led by lawyer Neill Stansbury, who served as the secretariat and chairperson for the drafting committee—ISO Technical Committee ISO/TC 309. Supporting this effort were approximately 37 participating countries, 22 observing countries, and 8 liaison organizations.[6, 7] ISO 37001 applies to public, private, and non-governmental organizations equally. ISO 37001 is voluntary.

ISO developed and published this standard because bribery and corruption is a widespread, global issue affecting both the public and private sectors. One of the most destructive and complex problems of our time, and a trillion dollar crisis by all accounts, ISO links bribery and corruption to social, moral, economic, and political concerns—as well as to poor organizational governance and unfair competition in the global marketplace.[8]

ISO acknowledges that governments around the world have made progress combatting bribery and corruption through various laws, guiding frameworks, conventions, and regulatory agency guidance and enforcement; however, ISO maintains that public and private organizations must also play a critical role in battling corruption. Organizations can help pursue this objective by proactively developing anti-bribery and anti-corruption programs and extending them to the third parties with which they do business.[9] ISO 37001 is intended to help organizations do just that.

In some instances, ISO standards simply set forth guidance, good practices, and advice. In other instances, ISO standards set forth actual *requirements*.

ISO 37001 sets out a framework for an organization's anti-bribery and anti-corruption program. Notwithstanding the structure of the table of contents, the ISO 37001 program framework—when distilled to its essence—is composed of the following ten elements: (1) culture, (2) governance and oversight, (3) risk assessments and due diligence, (4) policies and procedures, (5) training and communications, (6) speaking up (whistleblowing), (7) investigations and case management, (8) auditing and monitoring, (9) third-party risk management, and (10) continuous improvement. Each element is composed of detailed guidance and requirements. ISO 37001 also expects organizations to document all aspects of its program sufficiently.

Despite the generally positive splash that ISO 37001 has made on the international ethics and compliance scene, there is an accompanying sense that ISO 37001 does not introduce anything fundamentally new. In fact, some ethics and compliance professionals view the release of ISO 37001 as a "complete yawner," because the standard reflects a program framework previously established in numerous other leading-practices sources.[10]

For example, ISO 37001 resembles closely the framework set forth in an elder-sibling standard, ISO 19600—Standard on Compliance Management Systems (2014). ISO 19600 establishes a framework for a compliance program management system that can be applied across a host of compliance risk areas, including anti-bribery and anti-corruption, antitrust and competition law, anti-money laundering, and so on. Some ethics and compliance professionals, therefore, question the need for ISO 37001, since much of its essence had been previously covered in ISO 19600.

Moreover, the anti-bribery and anti-corruption compliance program framework set forth in ISO 37001 reflects—albeit in an ISO management-system format and in an ISO writing style—many of the same underlying requirements, expectations, and guidance set forth in key legislation (e.g., U.S. Foreign Corrupt Practices Act [FCPA], UK Bribery Act), guiding frameworks (e.g., U.S. Federal Sentencing Guidelines, OECD), agency guidance (e.g., Department of Justice and Securities and Exchange Commission Guidance, UK Ministry of Justice Bribery Act 2010 Guidance), and program-design requirements set forth in many deferred prosecution agreements related to FCPA violations.

However, although a common programmatic structure recurs across many of these guiding frameworks, it is equally true that the level of guidance and technical prescription set forth in ISO 37001 goes beyond other forms of guidance in many respects.

The standard reflects a program framework previously established in numerous other leading-practices sources.

For instance, although the U.S. Federal Sentencing Guidelines generally call for organizations to "periodically assess the risk of criminal conduct and…take appropriate steps to design, implement, or modify [the program] to reduce the risk of criminal conduct identified through this process," ISO 37001 drills into this programmatic element with greater specificity and prescription, requiring organizations to: (1) undertake regular bribery risk assessments; (2) identify, analyze, assess, and prioritize bribery risks; (3) evaluate the maturity of the related controls intended to mitigate bribery risks; (4) review the risk assessment process on a regular basis; and (5) document the risk assessment process.[11] ISO 37001 also provides approximately two pages of guidance as to designing and implementing the risk assessment process.

In addition, although the "risk assessment" section of ISO 37001 is technically limited to Section 4.5, it can be said that ISO 37001 addresses additional risk assessment-related requirements in other sections, too (e.g., Section 4.1, Understanding the Organization and its Context; Section 4.2, Understanding the Needs and Expectations of Interested Parties; Section 4.3, Determining the Scope of the Management System; Section 4.4, Management System Processes). The risk assessment example is just one comparative example between one particular guiding framework (i.e., the U.S. Federal Sentencing Guidelines) and ISO 37001. There are many other examples, too—across other programmatic elements (e.g., communications and training) and other guiding frameworks and agency guidance.

Regardless of whether ISO 37001 introduces anything fundamentally new, it is important to remember that ISO 37001 is an internationally agreed-upon standard that can apply equally to public and private organizations around the world. Some of the more well-known anti-bribery and anti-corruption laws and pieces of guidance, whose releases predated the issuance of ISO 37001, are limited to certain geographies and jurisdictions. ISO 37001, on the other hand, is truly global. More than 50 countries supported the drafting effort.

Moreover, ISO 37001 is auditable, which means that an independent body can certify that an organization's anti-bribery and anti-corruption compliance program meets the minimum requirements and expectations set forth in ISO 37001.[12] These are important distinctions between the myriad legacy anti-bribery and anti-corruption frameworks and pieces of guidance—and ISO 37001.

Accreditation and certification

Although ISO develops standards, it does not—itself—certify organizations with regard to its standards. The ISO certification process is administered by external certification bodies (CBs) or "registrars." These CBs and registrars commission onsite audits of the organization's program to determine whether the program satisfies the requirements of the ISO standard in question. Certifications are typically good for three years, with the first year involving the initial certification review, and the subsequent two years involving annual surveillance reviews. In all instances, CBs and registrars may only base their audit and review work on the scope of the standard in question. They may not audit or review aspects of the organization that are outside of the scope of the ISO standard under consideration.

CBs and registrars are sometimes (but not always) accredited by bodies that sit one level above the CB or registrar. These bodies are known as regional accreditation agencies. For example, in the United States, the ANSI-ASQ National Accreditation Board (ANAB) accredits CBs and registrars that, in turn, certify organizations with regard to their ISO-based programs. This hierarchy is intentional, positioning accreditation one level higher than certification. This one-over-one model is analogous to higher education, where students receive a degree or certification from a university that, itself, has been accredited by a higher accreditation body.[13]

From an organizational perspective, it is recommended—although not required—that organizations strive to obtain ISO certification from certifying bodies and registrars that are accredited by accreditation agencies, since this is thought to give more weight and credibility to the certification. In the United States, ANAB appears to be positioned to accredit CBs and registrars with regard to ISO 37001, which ANAB considers a "base standard program." However, as of the date of this writing (February 2018), it does not appear as though any accredited CBs or registrars have been established in the United States regarding ISO 37001.[14]

Scope and cost of certification

Generally speaking, ISO certifications attained at the parent company or headquarters level of an organization are only valid for that organizational entity. Headquarters-level certifications typically do not extend to other parts of the organization, such as subsidiaries, business units, or country markets, unless those aspects of the organization were included in the scope of the review performed by the CB or registrar. In most instances, each organizational entity must apply for its own certification. At times, however, a "group certification" can be issued at the headquarters level and applied to other aspects of the organization, if the initial review or audit is scoped that way in the first place, and if the fees take this extended scope into consideration.[15]

The cost of striving for ISO certification can vary. The cost depends on a number of factors that include: (1) the pricing models and fee ranges of the CBs and registrars; (2) the organizational, functional, and geographic scope of the certification; and (3) the number of organizational entities striving for certification.[16]

Costs associated with ISO 37001 certification may also be contingent on whether it is the first, second, or third attempt to achieve certification. Organizations often seek a second or third attempt when the CB or registrar identifies major non-conformities (i.e., significant gaps in the program) and minor non-conformities (i.e., minor gaps). The pricing related to second or third attempts can also vary depending on the remediation window allowed.

> Costs associated with ISO 37001 certification may also be contingent on whether it is the first, second, or third attempt to achieve certification.

Early adopters: Public sector

Since its release, several countries and local governments have adopted ISO 37001 as their official anti-corruption standard. These countries and governments include Singapore, Peru, Philippines, Malaysia, and the Chinese province of Shenzhen. It also appears that certain European countries are in the process of adopting ISO 37001.

In the public sector, "adoption" can mean various things. In some cases, a country will "adopt" ISO 37001 and create an accreditation system for the CBs or registrars who will, in turn, perform independent ISO 37001 certifications. For instance, the United Kingdom is in the process of developing an accreditation model of its own, but it has yet to be completed.

Other countries will "adopt" ISO 37001 such that their national standards bodies embrace the standard and encourage organizations to comply with it locally. For instance, Singapore recently adopted ISO 37001 and announced its own version of the standard: Singapore Standard (SS) ISO 37001. Singapore has also created an agency under its Ministry of Trade and Industry, which will provide training, consulting, and financial support for organizations interested in obtaining certification.[17] The same sort of activity is underway in Malaysia and China.[18]

The Malaysia Department of Standards and the Anti-Corruption Commission (MACC), together, implemented a country-specific version of ISO 37001 known as the Malaysian Standard 37001. The MACC intends to strive for ISO 37001 certification to further strengthen its efforts to combat corruption. In China, the Shenzhen Institute of Standards and Technology (SIST) has adopted ISO 37001 and intends to provide ISO 37001 certification and guidance. The SIST continues to work across China to generate support for adopting ISO 37001.[19]

The third meaning of ISO 37001 "adoption" in the public sector refers to when a federal, state, or local government itself strives for certification. Research indicates that the Quebec cities of Granby and Brossard will strive for ISO 37001 certification in 2018.

Early adopters: Private sector

Since the release of ISO 37001 in 2016, several organizations have achieved ISO 37001 certification. These organizations include Terna Group and ENI SpA (Italy), Robert Bosch Middle East (UAE), Alstom (France), CPA Global (Jersey, UK), and Ekvita (Azerbaijan). In addition, research suggests that, as of February 2018, about a dozen organizations have achieved certification in Malaysia. In the United States, several companies, such as Walmart and Microsoft, have publicly announced their intention to strive for certification once accredited CBs and registrars are established in the United States.

Benefits of ISO 37001 certification

Many benefits are associated with designing, implementing, and maintaining an anti-bribery and anti-corruption program in line with ISO 37001. Although some of these benefits relate to concepts like competitive advantage or board-level assurance, it is important to highlight the most important benefit: An effectively designed anti-bribery and anti-corruption program reduces the risk of bribery and corruption. This is good for business. It is good for employees, stakeholders, and communities. And it is good for the free markets. There are other benefits too.

First, ISO 37001 certification may help to assure the governing authorities and executive teams of organizations that sound, efficient, and effectively designed anti-bribery and anti-corruption controls and processes are in place and operating as intended. This helps the governing authorities of organizations satisfy their obligation to be knowledgeable about the content and operation of the compliance programs in place within their organizations.

Second, designing and implementing an anti-bribery and anti-corruption program in line with ISO 37001 will help to provide a defense, if there is ever a breach, regulatory inquiry, enforcement action, or investigation. ISO 37001 provides a comprehensive, end-to-end framework for managing the risk of bribery and corruption, and it also requires establishing and maintaining extensive documentation, both of which will help evidence a well-designed program.

Third, ISO 37001 is, at its core, a management system. Over time, management systems have helped organizations run smoothly, efficiently, and effectively. Such systems help organizations manage interrelated aspects of their operations in order to achieve their strategic objectives. ISO 37001 helps organizations organize, streamline, and optimize their anti-bribery and anti-corruption risk-management efforts — rather than attempting to manage the risk of bribery and corruption in a disintegrated, siloed, or fragmented manner.

Fourth, compliance is a journey in any organization. Even the most established organizations with mature and highly optimized compliance programs can benefit from incorporating additive aspects of ISO 37001 into their programs, thereby taking their programs to the next level. New, younger, or rapidly growing organizations can benefit from ISO 37001 too, because the program framework can help manage risk in a resourceful, effective manner. This can be valuable if or when the young organization strives to raise capital or undertake an initial public offering.

Fifth, it is no secret that more than 75% of enforcement actions related to bribery and corruption involve the misconduct of third parties.[20] Over the years, some US-based global organizations have struggled to develop and implement anti-bribery and anti-corruption programs and controls with regard to the third parties with which they do business, in part because such efforts are often seen as US-centric exercises and FCPA-focused. ISO 37001 establishes a common, global approach to managing bribery and corruption risk, regardless of where organizations are headquartered and where their third parties are conducting business.

Sixth, research suggests that, over time, organizations may begin to require ISO 37001 certification as a condition of doing business. Therefore, organizations, contractors, suppliers, and consultants that are not ISO 37001 certified will be at a competitive disadvantage. Similarly, the public sector may soon require organizations that bid on government contract work to be ISO 37001 certified. Uncertified organizations will be at a competitive disadvantage when it comes to government work.

ISO 37001 establishes a common, global approach to managing bribery and corruption risk, regardless of where organizations are headquartered.

Seventh, even when ISO 37001 is not a tender requirement, organizations that are ISO 37001 certified will be able to demonstrate to the procuring organization that they have designed an anti-bribery and anti-corruption compliance program in line with internationally recognized standards—and that they have had the program independently certified. This may help give the certified organization a competitive advantage over the uncertified organizations that are competing with it for business.

Lastly, organizations that achieve ISO 37001 certification will shine brightly in the ethics and compliance community and elsewhere. ISO 37001 certified organizations will be able to attract and retain top talent across the organization, especially the ethics and compliance function. Accomplished, dynamic, and forward-looking professionals are drawn to organizations that demonstrate a genuine commitment to organizational values, long-term sustainable growth strategies, and robust and meaningful risk-management practices.

Certification readiness

Striving for ISO 37001 certification—as with striving for any ISO certification—is a substantial undertaking. It involves a significant level of time, resources, and documentation. Some organizations move through the certification process efficiently and successfully, because they are prepared for the certification process. Other organizations experience challenges and findings of nonconformities, which will require remediation and perhaps a second or third attempt at certification.

Given the level of effort associated with striving for certification, some organizations elect to undertake an ISO 37001 readiness assessment exercise. This helps organizations evaluate the current state of their anti-bribery and anti-corruption program against the framework, expectations, and guidance set forth in ISO 37001. A readiness assessment helps organizations understand what they are doing well and where there may be opportunities for enhancement. Readiness assessments also help organizations pull together the documentation that will eventually be needed for the certification process.

Even organizations that do not aspire to ISO 37001 certification undertake a readiness assessment simply because it is a healthy and worthwhile exercise. They conduct readiness assessments because it establishes a baseline against which to enhance the program at a strategic and tactical level moving forward, and because it helps them satisfy the expectation that their programs be evaluated periodically, an expectation set forth in other guiding frameworks (e.g., U.S. Federal Sentencing Guidelines.).

Conclusion

ISO 37001 establishes a management system and compliance program framework for managing the risk of bribery and corruption in both the public and private sector. ISO issued this standard to help combat global corruption—a trillion-dollar problem. Although ISO developed the standard, it does not issue certifications. The ISO certification process is administered by CBs or registrars, which are sometimes accredited by higher organizations called regional accreditation agencies.

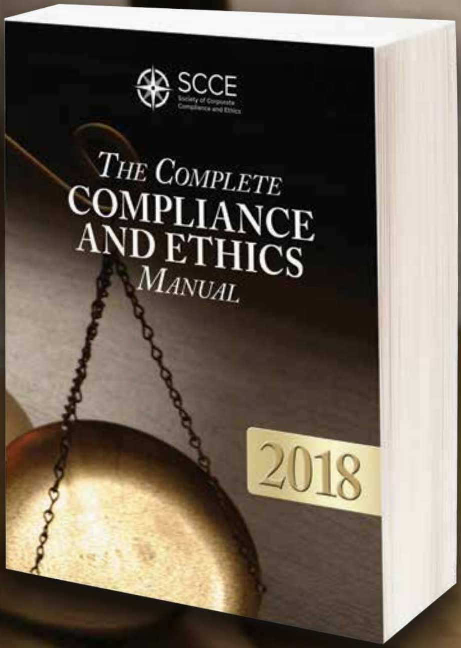
Although it is debatable whether ISO 37001 introduces anything fundamentally new, ISO 37001—by its very existence—will help to bring greater consistency to the manner in which anti-bribery and anti-corruption compliance programs are designed, implemented, and audited around the world. ISO 37001 certification will also help organizations organize a defense if faced with a breach, inquiry, investigation, or enforcement action.

As of February 2018, several governments have adopted this new standard, and several organizations have become certified. Because more than 50 countries supported the development of ISO 37001, it is likely that additional countries will adopt the standard. It is also likely that other organizations will strive for ISO 37001 certification, once additional CBs and registrars become accredited.

While ISO 37001 continues to gain traction around the world, many organizations remain in a wait-and-see mode, while weighing the cost-benefit of striving for ISO 37001 certification. In the meantime, some organizations will elect to undertake an ISO 37001 readiness assessment, which will allow them to gain a deeper understanding of the current state of their anti-bribery and anti-corruption programs, if they eventually decide to go for certification—or even if they do not. ✳

The opinions in this article are the author's and do not necessarily represent the position of any institution.

[1] ISO Quality Services Ltd. website available at http://bit.ly/2N1j7aO.
[2] Neill Stansbury: "International Anti-bribery Standard ISO 37001" Transparency International UK. November 2, 2016. Available at https://bit.ly/2JetvgW
[3] *Idem*.
[4] ISO 2600—Social Responsibility; ISO 20121—Event Sustainability Management Systems; ISO 3100—Risk Management—A practical guide for SMEs.
[5] See ISO 37001 (2016). Available at http://bit.ly/2lwYS8d
[6] *Ibid* Ref #2
[7] Diana Trevley: "Certifying Your Anti-bribery Program with ISO 37001: What's In It For Me?" Society of Corporate Compliance and Ethics, January 23, 2017. Available at https://bit.ly/2xR23kf.
[8] ISO 37001, Introduction (2016)
[9] *Idem*
[10] Mike Koehler: "ISO 37001 Is a Complete Yawner" FCPA Professor; October 24, 2016. Available at https://bit.ly/2sJjUDG
[11] *United States Sentencing Commission, Guidelines Manual*, §(8)(B)(2)(1)(c); and ISO 37001 § 4.5.1 through ISO 37001 § 4.5.4
[12] Russ Berland and Michelle Shapiro: "International Standards Organization Issues Certification Standard for Anti-bribery Compliance Systems," Lexology; November 1, 2016. Available at https://bit.ly/2sL0BtT
[13] Cynthia D. Woodley: "Who Accredits the Accreditor?" *Professional Testing Blog*; April 20, 2017. Available at https://bit.ly/2JBGwk5
[14] Center for Responsible Enterprise and Trade: "ISO 37001: A Year in Review" November 15, 2017. Available at https://bit.ly/2M9mPOS
[15] Discussion with ISO representative on 28 September 2017
[16] Spark Consulting "ISO 37001: Your Questions Answered." Available at http://bit.ly/2lx6tUn
[17] *Ibid*, Ref #15
[18] *Idem*
[19] *Idem*
[20] OECD: Foreign Bribery Report: An Analysis of the Crime of Bribery and Foreign Public Officials. OECD Publishing, 2014. Available at http://bit.ly/2lj1bLS


SCCE
Society of Corporate Compliance and Ethics
The Complete
COMPLIANCE
AND ETHICS
Manual
2018

by Meric Craig Bloch, CCEP-F, CFE, PCI, LPI

Be smart in an interview, but don’t outsmart yourself

***Meric Craig Bloch** (mbloch@shrinenet.org) is Corporate Director, Investigations for Shriners Hospitals for Children. He has conducted over 400 workplace investigations of fraud and serious workplace misconduct, and is an author and a frequent public speaker on the workplace investigations process.* @fraudinvestig8r

The goal of any investigation is to learn the true facts of the matter. In most compliance investigations, the information on which you rely will come from interviews. And the success of each interview depends on the quality of the information you receive.

Bloch

But what does the interviewee gain from speaking to you? Perhaps the person who makes the report to you benefits. For everyone else, the best thing that can happen to them is…nothing at all. Simply a thank you for their time, and off they go.

Your success as an interviewer depends on your training and experience, of course. But it also depends on your flexibility as a questioner. So adjust your style to harmonize with the traits and moods of the witness. Flexibility serves you well.

There are many errors that you can make while adding your personal touches. Some of the more common are:

- **Showing personal prejudice** or allowing prejudice to influence how you conduct the interview. This destroys your objectivity and credibility.
- **Bluffing, misleading, or lying** destroys your credibility and encourages similar behavior from the witness.
- **Hurrying encourages mistakes and omissions** and leads you to evaluate improperly the veracity of the information provided.
- **Making assumptions, drawing unconfirmed inferences, or jumping to conclusions** may result in important information not being requested or allow false or unverifiable information to be introduced into the investigation.
- **Making promises you can’t keep** destroys your credibility and may cause the witness to react negatively to other investigators in the future.
- **Looking down at or degrading the witness** or showing a contemptuous attitude may anger the witness and encourage unnecessary emotional barriers.
- **Placing too much value on minor inconsistencies** allows you to get “hung up” on minor or irrelevant issues.
- **Anger results in your surrendering control to the witness,** serves as a relief to the witness, and is a distraction from the information-gathering process.
- **Underestimating the mental abilities of the witness**, especially by talking down to them, antagonizes the witness and invites them to trip you up.

A smart investigator has no use for these tactics. A professional knows they serve no productive purpose. So be smart in the interview. Just don’t outsmart yourself. ✳

by Valerie Charles

Making the most of the FCPA Corporate Enforcement Policy

» The Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy encourages organizations to voluntarily disclose FCPA violations.

» Companies need to cooperate with the Justice Department if investigations occur and remediate the cause of the violation.

» There are five key capabilities of an effective compliance program.

» Compliance officers must determine the company's level of willingness to embrace the Enforcement Policy.

» Data analysis can help compliance officers understand the costs and benefits of working with the FCPA Enforcement Policy.

***Valerie Charles** (vcharles@ganintegrity.com) is the Chief Strategy Officer for GAN Integrity in New York City.*

Charles

In November 2017, the U.S. Justice Department released the latest evolution of the Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy. Companies are being encouraged to disclose FCPA violations voluntarily, cooperate with investigations, and remediate weaknesses by building effective compliance programs. Those three pillars of FCPA enforcement are still central today. The Corporate Enforcement Policy simply emphasizes them so much that, ideally, corporations will see no other useful course of action except to embrace all three.

Let's look at how corporate compliance professionals can seize on the enticements offered in the Enforcement Policy as they seek to build an effective compliance program.

What the policy entails

Launched in 2016, the FCPA Pilot Program was the precursor to the FCPA Corporate Enforcement Policy. The pilot program offered companies that violated the FCPA steep discounts in monetary penalties if they met three criteria:

- Voluntarily disclose the violation
- Cooperate fully with the Justice Department in ensuing investigations
- Remediate the policy or internal control weaknesses that led to the violation in the first place

With the Enforcement Policy, the Justice Department is rewarding good behavior. If an FCPA violator meets all three criteria, the Justice Department's presumption will be not to prosecute at all—no monetary penalties, no compliance monitor, no deferred-prosecution agreement. Instead, the company secures a full declination to prosecute, which the Justice Department will announce publicly. That approach reflects the enforcement philosophy of the Trump administration: that individuals commit crimes rather than corporations, and whole organizations should not suffer for the misdeeds of a few.

This doesn't mean organizations get off scot-free. Ideally, the company must still conduct a thorough investigation and remediate any compliance program weaknesses. Neither action comes cheap.

The Justice Department is also more strictly punishing bad behavior. For example, if the violation includes "aggravating circumstances," criminal charges and monetary penalties remain likely. Aggravating circumstances can include senior executives involved in the misconduct, significant profits gained from violations, or pervasive misconduct within the company.

If companies don't disclose violations, but then do cooperate and remediate weaknesses after the Justice Department begins its own investigation, the company will be eligible for a 25% reduction in fines based on the U.S. Sentencing Guidelines.

If a company wants to avoid the assignment of a compliance monitor, then according to the Enforcement Policy, it must have an effective compliance program in place by the time the FCPA investigation is resolved. If the company already has a compliance program in place, any weaknesses identified as part of the investigation must be remediated.

Five compliance program priorities

The priorities for an effective compliance program can be boiled down to five key capabilities.

Make risk assessments contextual

Where and how the company operates should inform how these assessments are done. For example, if the company relies heavily on third parties in emerging markets, it should know which parties are most at risk for corruption. Or, if the company has decentralized approvals for spending, it should know which executives handle transactions in high-risk markets.

Make the connection between risks and policies, procedures, and controls

If the company identifies third parties as a significant risk, how is due diligence performed? If spending approvals are decentralized, how do the company's payment systems allow a comprehensive review by senior executives, audit personnel, or others?

Compliance programs should put steps in place to reduce the risks identified above.

Cooperate fully

What does the Enforcement Policy mean by "cooperation"? It means turning over all facts related to a violation, including attributing those facts to specific sources whenever possible. So, the company needs strong policies for litigation holds, e-discovery, and data preservation. Even if the investigation itself is done by auditor or outside counsel, the compliance program must foster an environment that supports strong investigation ability.

Communicate a strong compliance culture

From clear language in the Code of Conduct, to executive communications stressing ethical behavior, to stern discipline for employees or third parties who engage in corruption anyway—these are all aspects of a culture of compliance. Foremost, a strong culture of compliance leads to what the FCPA Enforcement Policy wants above all: self-disclosure of FCPA violations.

Find and fix weaknesses

According to the Enforcement Policy, companies are required to demonstrate a thoughtful root cause analysis of why misconduct happened and, where necessary, remediate those weaknesses. So an effective compliance program (possibly working with Internal Audit, outside counsel, or other advisers) must have a "diagnostic capability" that can lead to new policies, procedures, or controls as warranted.

Action items for compliance professionals

Implementation of the above capabilities will differ from one organization to the next. The chief compliance officer's (CCO) role at the moment is to assess the company's ability and appetite to embrace the FCPA Enforcement Policy—and from there, develop a road map of how the company can embrace the Enforcement Policy to the fullest extent, given the risks and resources the company has.

It's also important for compliance professionals to determine the company's level of willingness to embrace the Enforcement Policy. That is, how eager will the company be to disclose an FCPA offense voluntarily?

Data analysis can help with this task. For instance, given the company's past transgressions (if any), or the volume of transactions that might lead to FCPA violations, what potential penalties would the company face for nondisclosure? With sufficient analytics, a company can understand the costs and benefits of working with the FCPA Enforcement Policy or avoiding disclosure and hoping for the best.

The time is now

The U.S. Justice Department is on a mission to woo companies that are unsure about how to handle FCPA violations. The FCPA Corporate Enforcement Policy is designed to reassure companies that they will be rewarded, not punished, for admitting misconduct and working to prevent it in the future. To align with these Enforcement Policy goals, an effective compliance program is critical—and the time is now. Compliance professionals will put their companies on better footing with the Justice Department by taking this opportunity to assess the effectiveness of their programs.

by Jeffrey M. Kaplan

Conflict of interest risk assessment: Part 2

***Jeffrey M. Kaplan** (jkaplan@kaplanwalker.com) is a Partner with Kaplan & Walker LLP in Princeton, NJ.*

My prior column teed up the topic of conflict of interest (COI) risk assessment by identifying risk assessment needs that many organizations have, whether they know it or not.[1] In this column, I offer some tips on how to develop and implement an assessment process that meets those needs. This discussion—like that in the prior column—draws from prior posts in the *Conflict of Interest Blog* (www.conflictofinterestblog.com), of which I am editor.

Kaplan

One framework for assessing COI-related risks is to identify and analyze the "reasons" and "capacities" for conflicts on the part of all relevant individuals and entities—employees, various third parties, and the organization itself. "Motivations" are reasons to engage in wrongdoing purposefully. An employee having a personal economic interest in an entity that does business with your organization is the most obvious form of COI motivation. But less tangible personal interests can create motivations too, such as reputation or political affiliations, both of which can lead to COI-related involvement with suppliers and other third parties.

The other broad category of reasons—"misunderstandings"—refers mainly to COI-related expectations that may truly not be understood (e.g., third-party standards). But this factor also encompasses standards that are known but underappreciated, as COI rules might be in certain cultures or industries.

"Capacities," in this context, means a party's ability to engage in harmful behavior. In some industries (e.g., financial services), such capacities for harmful conflicts-based conduct are widespread. More broadly, a key consideration for this aspect of risk assessment is the extent to which an individual exercises discretion over matters that could involve COIs. Most obviously in this category are individuals in management or procurement positions. But there are also many other, less obvious functions that could have COI risk-creating capacities, including that of agents.

Of course, a COI risk tends to be highest for individuals or functions where both "reasons" and "capacities" are significant, and in such instances, companies should consider deploying a full range of conflict-of-interest mitigation measures (e.g., targeted training and communications, auditing and monitoring, defined accountabilities, and other controls). The same is true with regard to COI risks for which only one of these dimensions is significant, but the potential impact of a COI is high. ✳

[1] Jeff Kaplan: "Conflict of interest risk assessments, Part 1" *Compliance & Ethics Professional*, June 2018;15(6):53.

by Mujo Vilašević

Establishing ethics compliance for the banking sector in Bosnia and Herzegovina

» Transitional and integration processes toward the European Union give specific challenges to each transitional country.

» The banking sector has had its development in Bosnia and Herzegovina and has reached the point where it has higher standards of regulation than the country itself.

» The Compliance function has been introduced formally in the banking sector via new regulatory framework.

» Ethics compliance is a completely new approach and challenge in Bosnia and Herzegovina, which will help the path of development for the banking sector in general.

» Institutional support by state bodies will be *conditio sine qua non* for establishing ethics compliance.

***Mujo Vilašević** (mujo.vilasevic@sparkasse.ba) is a Regulatory Compliance Associate at Sparkasse Bank dd BiH in Sarajevo, Bosnia.*
in /in/mujovilasevic

Vilašević

Transitional countries face the full package of challenges in regulatory framework, especially the banking and financial sector in general. Post-crisis period—after 2007, 2008, and 2009—financial stress brought us many new rules for financial stability, which represent a new road of protection for all institutions in case of similar financial disturbances. Furthermore, countries in transition—and those that deal with the European Union (EU) and NATO—have to face additional steps in order to provide a stable economy, a stable market, financial security, and law enforcement. Due to its specific legal and social situation, Bosnia and Herzegovina (BiH) can serve as a case of how just one segment—compliance in financial institutions—can find its way in order to serve to the community itself and to help develop banks as a business in general. That is the aim of this article.

Regulatory framework

The new regulatory framework in the banking sector of BiH—established by the Federal Banking Act[1] and the Banking Act of Republic of Srpska[2], along with bylaws adopted by banking regulators and banking agencies—has formalized the Compliance function more than ever before.

Banking acts in BiH have identically defined the Compliance function as a control function in banks together with the Risk Management function and the Internal Audit function. Legal prerogatives of this function are:

- Following the compliance of the bank's business with the Banking Act, bylaws of the agency, and other regulations and standards of cautious banking, anti-money laundering, and counterterrorist financing procedures, as well other acts which define the banking business;

- Identifying oversights and risk assessments as a consequence of non-compliance with legal acts and other regulations, such as the risk of supervision measures and sanctions from the regulator and other bodies, financial losses, and reputational risk;
- Advising the management board and other responsible individuals on the application of relevant regulations, standards, and rules, including information on actualities in these areas; and
- Assessment of the effects that the bank's business will have due to changes of relevant regulations.

These prerogatives are similarly defined in Croatia and the Republic of Srbija.[3]

So, within its legal definition, Compliance in the banking sector of BiH is established as regulatory compliance. However, some different light is given by the bylaws, in which, for both entities, it is defined that employees of the Compliance function, as well as others, have to "know the rules of the profession, good business practices and business ethics." This regulation tells us that compliance prerogatives should not be limited to regulatory compliance, but should include business ethics and good business practices.

How do regulatory compliance and business ethics connect in the banking sector in BiH?

If we overlook periods of development of the economy in general, and within the banking sector as well in BiH, we can conclude that there are specific periods:

- **Postwar period and restorations in privatization** (i.e., conversion of state into private ownership after the breach of the socialist economy). This is the period in which foreign financial institutions came into the BiH market and invested their capital. This is where the first frames of today's financial market of BiH were constituted.
- **Millennial transition period** from the end of the '90s and the beginning of the 2000s. We had a powerful expansion of the banking sector thanks to the satisfying investment conditions in Bosnia's new market.
- **The global financial crisis period** within and after 2007 and 2008. Within this period, there was significant capital consolidation of small banks.
- **Post-crisis period after 2010**. During this period, European standards were implemented in the financial sector, with the aim to prevent similar financial effects.

It is important to remember that for all these periods, complex political and social situations in BiH have been constant. But, step by step, the banking sector has advanced and has established itself on a higher level, mostly by complying with European standards of business. This was inevitable and mandatory. This compliance is part of the overall package integrating the European status quo within BiH as a country, such as within business practices of local subsidiaries of banks with headquarters in the EU that keep the majority of their banking sector in BiH. The EU transition is currently the most important social, legal, and economic transition of BiH.

Another trend that is coming for businesses within these channels is that modern business has yet another, inevitable measure: competition in personality, as it is named by Lynn Sharp Paine.[4] We now have come to be aware that the profit of the company becomes dependent on its role in society and on its internal relations that the company sets up. This is where we find the link with business ethics, adjusted to the needs and possibilities of the banking sector. This represents an important pillar for the banking "competition in personality." This approach has a long-term profit for the banks: growth in reputation and company stability.

What does business ethics mean in the banking sector?

A lot of water has crossed under the bridge since it became well known that every company has to bring something new and something special to make a profit. Our specialty is ethics,[5] and it is necessary to show users and partners that a company has an ethics function. Today, it is no longer enough to have sponsorship in a community or to donate to affected members of the community. The ethical approach and business ethics in the banking sector ask for additional engagement, both internal and external ethical behavior as part of a bank's business strategy. This approach is significantly related to a company's integrity. Business ethics and integrity are jointly connected, and therefore they should be considered as such in the banking sector as well. This approach often considers hard choices and unpopular decisions of management, but its purpose is directed at the welfare of the company and the community in general. How is this applicable? Regulations have, in a small measure, given prerogative to compliance officers to proceed in this business segment.

Ethical business should be implemented both internally and externally, in areas such as:

- Selection of candidates for middle and high management
- Ethics and business codes
- Precise rules of ethical behavior in the company
- An ethics committee or similar mechanism that would be able to consider and sanction conduct that is not in accordance with the ethical standards of the company
- Selection of business partners
- Clear, precise, and consistent rules for sponsorships and donations that would reflect the integrity of the company

These examples are only the beginning, and they need to be set out as rules—even regulatory demands—in the banking sector of BiH, and they could easily apply in every transition country.

Compliance officers should be in charge of ethics processes in the above-mentioned areas and be compliant with rules that are established for ethical business.

Of course, such implementation does not mean a "good cop/bad cop" situation. Compliance should be addressed in the wider picture of the company and always bear in mind the possibilities and restrictions that are set by regulations. After all, such an approach is defined by the Basel Committee on Banking Supervision recommendations[6] for compliance in financial institutions. It always depends on the circumstances and possibilities of the institution.

Instead of a conclusion...

The process of implementing the European standards will be difficult, long, and filled with hard choices. Compliance officials are established, and they serve to ease this process. Business ethics is yet another challenge the banking sector in BiH will have to face. It remains to be seen how and when government institutions will provide their support to private companies, without which this process is not possible. ✳

The opinions in this article are the author's and do not necessarily represent the position of any institution.

1. Official Gazette of Federation of BiH no. 27/17.
2. Official Gazette of Republic of Sprska, no. 3/16.
3. Decision on internal control systems in Croatia, Official Paper no. 1/15.
4. Lynn S. Paid: *Value Shift: Why Companies Must Merge Social and Financial Imperatives to Achieve Superior Performance*, McGraw-Hill Education; August 22, 2002.
5. Ana Aleksić: "Business Ethics: Element of successful business" *ResearchGate*; January 2007. Available at https://bit.ly/2kzSZXB.

6 Available athttp://bit.ly/2lxr5M5

by Jennifer L. Kennedy, BA

Fraud – a thing that keeps me up at night

Jennifer Kennedy *(jenniferkennedy@barberinstitute.org) is Administrator, Governance, Risk Management & Compliance at Barber National Institute in Erie, PA.* *bit.ly/li-JenniferKennedy*

"What keeps you up at night?" I get asked this question a lot. Mostly from board members. It can be a strange question to answer, and the focus may change on any given day, but a constant on the "keeping me up at night" playlist is fraud—fraudulent billing to be exact.

Kennedy

This is not because fraud is pervasive in my industry. It's mostly because of the penalties and damage caused. And because as a compliance leader, I feel it's my duty to prevent, detect, and correct these issues. My feeling is that if something is missed and a BIG investigation takes place, the compliance team has failed.

Recently *Disability Scoop*, a web source for developmental disability news, published an article from the *Anchorage Daily News* about the investigation into an Alaska nonprofit over allegations of fraudulent billing.[1] In this case, the Alaska Medicaid program contended that the provider billed for services not provided, billed for overlapping services with the same provider, and failed to repay money owed to the program as identified in internal audits performed by the provider. The investigation, which began in 2016, resulted in a settlement agreement in which the provider agreed to pay $2.3 million and entered into a 5-year corporate integrity agreement.

That this happened at all is a massive failure. A failure of the board, agency leadership, and especially those charged with compliance duties. This was an agency that was performing internal audits. They had identified issues, including billing errors, and failed to report and reimburse the state.

A constant on the "keeping me up at night" playlist is fraud — fraudulent billing to be exact.

As a compliance professional in a similar industry, these are the stories of nightmares. As the person charged with identifying and mitigating these types of issues, I strive every day to ensure that the job is being done.

As compliance professionals, we need to stay the course, do the hard work, deliver the bad news (if there is any), and hold our organizations accountable. If we don't, we could end up front page news. ✳

[1] Annie Zak: "Arc Chapter To Pay Nearly $2.3 Million Over Medicaid Billing" *Anchorage Daily News*; May 1, 2018. Available at https://bit.ly/2xSc5BM.

by Ken Chamberlain

Compliance: Addressing the intensifying age of statutory regulations

- We've said goodbye to the old and have entered a new world of Compliance.
- The emphasis is now on an ever-changing regulatory framework for business.
- The tide of regulatory enforcement is accelerating.
- Effective risk and compliance infrastructures are absolutes.
- Make compliance, risk assurance, and whistleblowing solutions workable.

__Ken Chamberlain__ (ken.chamberlain@csi-group.org) is Managing Director at CSI Group in Moscow, Russia.

Today we face incredible changes in the global business environment and a revolution in digital technologies. It has never been more critical to deliver robust compliance infrastructures, to ensure that your organization's most precious assets and information are protected against theft or misuse, and to make sure the integrity of the people you do business with is legitimate. The threats are also not limited to external parties, but equally from within, as the volume, frequency, and potency of such incidents gain momentum.

Effective risk and compliance management requires going beyond the letter of the law. In today's business world and an ever-demanding commercial environment, we face a countless number of dynamic regulations, which often results in the "business world" having uncertainty about how to apply the necessary regulatory conditions in their specific business environment. The uncertainty of when to choose between the letter of the law versus the spirit of the law can create an untold number of headaches to achieve "absolute" compliance. This could ultimately lead businesses and regulators to differing conclusions on how to implement these laws.

Chamberlain

Leaders face unparalleled challenges

Since the turn of the millennium, we have witnessed a series of events that had global impacts: formerly stable economies (e.g., Italy, Greece, Spain) requiring international bail-outs; the 2008–2009 global financial recession; and the ever-increasing number of terrorist attacks, which resulted in the introduction of new laws and regulations, heightened enforcements, and ever-increasing financial penalties. Unprecedented cases of reputational damage and loss of shareholder value now appear with high regularity in the media: WorldCom, Enron, Lehman Brothers, and Bernard L. Madoff Investment Securities, to name but a few. Additionally, when the trusted custodians of endorsing business performance (e.g., Arthur Andersen) become embroiled in scandal, it does beg the question, "Who audits the auditors?" Although trust must never be considered a control, in the words of the late Ronald Reagan, "Trust… but verify."

Consequently, business leaders now face unparalleled challenges in ensuring their organizations can implement the necessary compliance controls that these new times present and expect.

Business leaders must confirm that their organizations:

- Have a clear understanding of their risk tolerance;
- Perform systematic risk assessments on all their operational activities, both internal and external;
- Liaise transparently and honestly with all regulators;
- Regularly communicate and provide training to all employees to reinforce their accountability for ensuring compliant practices;
- Develop and maintain a culture of integrity;
- Ensure ethics and compliance are embedded components of their business strategies and operational management;
- Have the appropriate financial and operational control mechanisms in place to ensure actual or attempted wrongdoing can be rapidly identified;
- Really know who their business is actually doing business with;
- Make sure employees' remuneration packages are aligned to compliant behavior;
- Meet with, and communicate with, the chief compliance officer; and
- Identify the points of compromise speedily and effectively mitigate the risk of recurrence.

Organizations will find themselves exposed from a regulatory and enforcement point of view if they cannot show processes and procedures around these metrics.

In parallel, we have also seen extraordinary demands on businesses for increased revenues. This scenario—especially when aligned and supported by improper bookkeeping—results in the pressure to declare and falsely report exponential bottom-line income, with numerous organizations stating assets strongly exceeding their intrinsic value. Collapse was perhaps inevitable, bringing down companies and individuals, and shattering reputations. Some successes were too great to actually believe. Widespread redundancies; corporate insolvencies; collapsing property values following commonly witnessed mortgage frauds; stock price crashes; and banks folding, leaving customer financially exposed, led to rampant acrimony, ultimately resulting in regulators having to take enforceable countermeasures.

So many far-reaching laws, to highlight but a few, have been introduced: from capital adequacy to anti-money laundering, to counterterrorism financing, to data protection, to anti-bribery and corruption, to consumer protection. Each significantly impacts the immediate and future regulatory landscape. Add into the mix cultural differences, differing regional business values, and respective interpretations on how to implement policies in practical ways, and we're right back to the confusion between applying the letter of the law versus the spirit of the law. All this brought a determined focus by regulators to build compliance programs and increase the culpability of executives and employees to prevent misconduct.

One may even legitimately ask, "Can I ever be totally globally compliant?" The truth is, probably not!

Achieving the three lines of defense (i.e., operational management, effective risk management and Compliance functions, and independent Internal Audit) requires effort, resources, and commitment supported by not just the tone at the top (as words and actions can sometimes be polar opposites) but by proving necessary financial investment and a zero tolerance policy toward offenders and violations.

Organizations must never adopt a "too proud to ask" culture. Where any uncertainty exists, external experts should be considered and employed to independently assess the existing frameworks and infrastructure and provide objective guidance to achieving necessary success.

> One may even legitimately ask, "Can I ever be totally globally compliant?" The truth is, probably not!

What does the future require?

There is a prerequisite that all businesses demonstrate that they assign not only suitably qualified personnel, but that they also allocate the necessary financial support to deliver governance, effective programs, and control environments to support identification, management, and mitigation of risks. Businesses must ensure embedded integrity within their organizations, to the point where employees enact these requirements almost subconsciously. The tentacles of enforcement are not just internal to the business, but extend to all interactions with suppliers, agents, contractors, partners, etc.

Although exponential regulatory punishments are being actively applied and enforced, on the opposite side of the same coin, specific regulatory guidance to deliver necessary corporate governance is less than desirable. Businesses can feel somewhat abandoned in building such an infrastructure, supported only by very limited guidelines. Such guidelines do tend to emphasize the consequences of non-compliance but fail to provide practical support on the journey to achievement.

The evolution of whistleblowing and the ability to report any suspicions anonymously—without fear of reprisal or retaliation in any form (e.g., ostracism, exclusion, or simply giving the cold shoulder) —is not only gaining momentum but witnessing exponential management and regulatory support. Sadly, however, it remains a fact that not all jurisdictions, cultures, and business leaders support such initiatives. Add to that an open belief that "our organization is fireproof" and a blatant refusal to accept that a business has exposures, and businesses are inevitably led to disaster.

My own experience has confirmed strong correlations between incidents of not only policy violations, but also white-collar crime, usually as a result of poorly maintained or supported—or the complete lack of—an embedded, practical, and workable whistleblowing hotline.

One of the foundations of success is providing appropriate training to all employees on the necessity of total compliance and their ability to raise questions, seek guidance, and receive performance feedback. Key components of successful training are:

- Keep it simple and role specific (i.e., don't apply a one-size-fits-all approach).
- Build a series of sessions, as opposed to lengthy marathon, to maintain interest and ensure information is absorbed.
- Blend training with examinations to ensure thorough understanding and execution. Ideally, an examination should not immediately follow the training session, but come one or two weeks later, ensuring information retention.
- Apply a blend of both classroom and online training.
- Never adopt a one-off approach. For example, training is required immediately post-hire, following a role change or promotion, after regulatory or internal policy changes, or immediately after any merger or acquisition.
- Maintain an effective tracking program: TTT (Train, Track, and Test). It is imperative that formal attendance, the specific subject trained, and the date training was provided is recorded.
- Make it stimulating and applicable to the organization and operating environment.
- Provide real-life (sanitized) examples that the audience can relate to—get their attention.
- Send a message that your organization employs robust control monitoring mechanisms.
- Make clear the personal impacts for wrongdoing and the importance placed on compliance.

This should be supported with employee compliance support mechanisms:

- Provide a dedicated compliance training portal on the business website.
- Give portal access to all appropriate policies, procedures, codes of conduct, etc.
- Introduce a compliance support line for compliance inquiries.
- Activate a compliance (whistleblowing) hotline for actual or suspected incident escalation.
- Consider the introduction of departmental "compliance champions"—individuals who are specialized on necessary compliance requirements in their area(s) of expertise.
- Introduce compliance quizzes with nominal value prizes.
- Organize themed compliance days/weeks.

Organizations' responsibilities

It is critical that any compliance program reports directly to the board, who in turn commit their oversight to promote a culture and mind-set, ensure support is visible, continue development, and deliver justice to wrongdoers. The board, in turn, must demonstrate their uncompromising compliance position in practical and observable ways by being the "voice of compliance."

The compliance program must be designed to enable and support informed decisions and must be an integral component of the business's infrastructure. It should be supported, be adaptable to the dynamic operational landscape, and be a prerequisite for any business in both its strategy and operations.

Compliance programs must address the following core principles to effectively prevent, detect, and respond to any alerts, suspicions, or proven incidents of misconduct—endemic or opportunistic. Key elements of such a program should be specific to the business's environment.

Change oversight

Robust change management processes will ensure changes that may have compliance impacts are reviewed. Compliance testing should be performed and confirmed prior to any changes being made and going live in the operational theatre. Failure to do so may result in alternate non-compliance and high-risk processes being unwittingly adopted.

Deliver what is required
Maintain an inventory of regulatory compliance requirements relevant for each compliance program in each operational area of the organization. Generalizing simply will not work, because the requirements for HR or health and safety have little correlation to, say, data protection or anti-money laundering. Employ your legal counsel as a liaison officer to the Compliance function, to keep abreast of changes or amendments to existing regulations or the introduction of new regulations, and to communicate these well in advance, enabling a dedicated team to prepare in advance for the changes.

Proactive process development to ensure compliance
Identify and appraise all compliance risks, making the appraisal not insular to each department, but assessing any multiple or interconnected responsibilities. The decision-making process quite often spans multiple operational departments. Quantify and deploy a numeric risk score (ranking) not only from a financial impact, but additionally from operational impacts (e.g., financial investment, resources), reputation, and brand preservation. Set objectives and targets for delivery, implementation, and ownership based on the top priorities. Now it becomes possible to define a schedule of initiatives, assign responsibilities, and agree to the timeframe for completion. It is also critical to have representatives from all affected departments integral to this process.

Risk assurance and compliance in every theatre of operations
The organization must establish systematic checking and inspections in all departments to evaluate compliance with regulations, and company policies and procedures. Audit's performance must be focused on the risks, capable of measurements and reporting, with emphasis placed on managers taking responsibility for compliance. If breaches are identified, additional investigation to the root cause must be completed, and if premeditated or deliberate wrongdoing is identified, the matter should be escalated for consideration of appropriate disciplinary actions.

> If breaches are identified, additional investigation to the root cause must be completed.

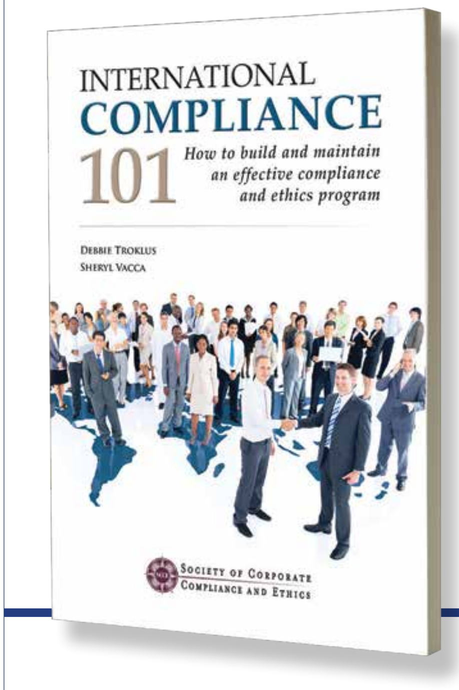
Appropriate and achievable mitigation plans
Identify, record, and categorize all non-compliance issues, irrespective of their potential impact, both from an operational and regulatory perspective. Implement an appropriate corrective or preventive action plan based on the criticality of the findings. Adhere to strict timely completion, with supporting documentation of all corrective or preventive actions, including delivery of any updated polices and relevant communication and compliance training provided.

To summarize:

- Give systematic and rigorous compliance risk assessments to identify key existing and emerging risks.
- Assign owners to regulatory risk areas and ask them to partner with the Compliance team.
- Change implementation supported by grounded proof of concept.
- Provide clear and unambiguous policies and procedures, including escalation procedures of actual or suspected incidents.
- Ensure adequate due diligence of employees, suppliers, partners, and clients.
- Offer effective and role-specific communication, training, and tracking.
- Provide appropriate and unfettered data access and analytical support.
- Lead effective and management-supported investigations and mitigation.
- Ensure competent, transparent, and unbiased fact-based internal and external reporting.

Conclusion

Organizations that take the lead in this new era will not just achieve compliance success, but will also create an environment of trust with their employees, customers, regulators, and shareholders that is based on sound ethical principles and behaviors, while also increasing shareholder confidence, improving business reputation, and strengthening the corporate identity and brand. ✳


INTERNATIONAL
COMPLIANCE
101
How to build and maintain an effective compliance and ethics program
Debbie Troklus
Sheryl Vacca
Society of Corporate Compliance and Ethics

2019 INTERNATIONAL BASIC COMPLIANCE & ETHICS ACADEMY

13-16 January | Dubai, UAE

10,900+ Compliance Professionals

hold a Compliance Certification Board (CCB)® credential

Learn the essentials of managing compliance & ethics programs

CLE

APPROVED

COMPLIANCE TRAINING AND CERTIFICATION (OPTIONAL)

Budgets are tight, governments around the world are looking to add new regulations, public trust in business is low, and employees are tempted to cut corners. Demonstrate your ability to meet the challenges of these times and have the knowledge you need to help move your program and your career forward by joining more than 10,900 people around the world who have already earned a Compliance Certification Board (CCB)® designation. CCEP-I® certification is not tied to the laws of one country, but reflects the knowledge needs of compliance professionals globally. It draws upon international frameworks for effective compliance programs.

To learn more about what it takes to earn the CCEP-I® designation and demonstrate your expertise, visit compliancecertification.org.

Register Early to Reserve Your Space

ACADEMIES LIMITED TO 75 PARTICIPANTS

corporatecompliance.org/academies

Questions? lizza.catalano@corporatecompliance.org

SCCE™
Society of Corporate Compliance and Ethics

by Kristy Grant-Hart

The four Bs that determine whether you should take the job

Kristy Grant-Hart *(KristyGH@SparkCompliance.com) is the Managing Director of Spark Compliance Consulting in London, and author of the book,* How to be a Wildly Effective Compliance Officer. *ComplianceKristy.com* *@KristyGrantHart* *bit.ly/li-KristyGrantHart*

Grant-Hart

Congratulations! After an interview (or six!), you've finally been offered that new job. Or perhaps you're testing the waters—updating your LinkedIn profile and telling your network that for the right gig, you might be available. But how do you know whether the job you're considering is worth taking? Here are the four Bs that can help you determine that.

Budget

A Compliance department cannot operate without a proper budget. One of my friends describes her program as being put together with "bubble gum and duct tape." That is not a tenable situation, and the inability to afford travel, training programs, and enough staff to make the program work means one of two things: Either the company isn't really dedicated to compliance, or its financial situation isn't good enough. Either way, skip a job in a company without a decent compliance budget.

Boss

Who is the boss of the Compliance program? If you answered, "an independent chief compliance officer who reports to the board and CEO," congratulations! If you answered, "the general counsel," or "the head of Audit," proceed with caution. These functions aren't always aligned with compliance goals, and having compliance filtered to the board by another party can undermine the program's effectiveness.

Behest

The Merriam-Webster dictionary defines "behest" as "an urgent prompting." Behest is closely aligned with mandate. Have the CEO, board, and other members of the C-suite made it abundantly clear that Compliance has authority to do what it needs to do, and the business must do what is asked of them? If so, great! If not, this may be a black hole job. Without mandate, you're basically asking the business to do you a favor and comply, which is not a situation you want to be in.

Baseline culture

Before accepting a new role, look at the baseline culture of the company. Does the company showcase its values? When you visit, how does the place feel? Tired? Grumpy? Invigorated? Although you may be in charge of changing culture, that instruction can take a long time to complete. Look at the baseline culture *now* and decide whether you want to take on the challenge.

It's always difficult to know whether to take a new job. But if the four Bs line up successfully, you're best off taking the opportunity. ✳

by Bert F. Lacativo, CPA, CFE, CFF, and Adam Lampert

Your settlement with the government requires an Independent Review Organization: Now what?

- » Begin searching for and interviewing Independent Review Organization (IRO) candidates as soon as it becomes apparent that the settlement agreement will require one.
- » Choose your IRO carefully to ensure that it has the credentials, experience, and independence necessary to accomplish the tasks outlined in the settlement agreement.
- » Begin preparing the information that the IRO will need to perform its assigned tasks so that it can be completed within the normal 60-day reporting timeframe.
- » Ensure that claims and compliance process maps, policies, and procedures are prepared, because the IRO will likely be required to review them as part of their work.
- » Be prepared to respond quickly to questions and requests from the IRO, and agree on a timeframe to review its findings and respond, if necessary.

__Bert F. Lacativo__ (blacativo@glassratner.com) is a former FBI Special Agent and a Senior Managing Director and National Head of Investigations for GlassRatner in Dallas, TX. He is currently leading an IRO engagement. __Adam Lampert__ (alampert@glassratner.com) is an associate for GlassRatner in Dallas, TX.

The Health and Human Services Office of Inspector General (OIG) has accused your company of improprieties, and after careful negotiation by your counsel, there is an agreement to settle under the auspices of a Corporate Integrity Agreement (CIA). Now that your company has entered into a CIA, it can get back to business as usual, right? Not so fast. As part of the CIA, the OIG has required that the company engage (at its expense) an Independent Review Organization (IRO). Let's explore what an IRO is and what this might mean for your company.

IRO history

According to the OIG publication, "Protecting Public Health and Human Services Programs: A 30-Year Retrospective," the first CIAs were signed in 1994. CIAs were originally constructed around the core elements of the Federal Sentencing Guidelines as follows:

- Implementation of compliance measures
- Appointment of a compliance officer
- Developing compliance-specific policies and procedures
- Developing and delivering compliance-related training programs

Lacativo

Lampert

- Developing and implementing compliance-related reporting mechanisms

The first CIAs did not include the requirement for a company to engage an IRO, and it is not clear when the first CIAs contained that requirement. Nevertheless, the concept of an IRO emerged due to an ever-increasing number of settlements calling for oversight to ensure that the settling company did not violate the auspices of their CIA. The OIG found that this stretched their resources, causing the OIG to create an alternative means to monitor each company who entered into a CIA. The IRO concept was born with the IRO acting on behalf of the OIG to ensure that the settling company adhered to the CIA settlement terms.

IRO qualifications

The selection of the IRO is left up to the settling company. It is advisable for a company to begin identifying and interviewing IRO candidates as it negotiates its CIA and becomes aware that one will be required. This is important, because the CIA will likely allow for a 90-day timeframe after the CIA is executed to engage an IRO without incurring agreed-upon daily monetary penalties as stipulated in the CIA. Although the company has responsibility for selecting the IRO, within 30 days of selection, the OIG has the opportunity to block the selection based upon the IRO's qualifications (or lack thereof) or the belief that the IRO cannot carry out the duties as outlined in the CIA (more on those duties later).

Typically, an IRO must possess the technical capability to conduct the required review (usually a detailed claims analysis), must demonstrate their independence (as defined by Government Auditing Standards issued by the Government Accountability Office), and should have a history of being an IRO or performing in a similar function. Once the company selects an IRO, an engagement letter that details the IRO's activities, responsibilities, and fees should be executed. Additionally, the IRO should sign a business associate agreement, which details the IRO's responsibilities regarding protection of personally identifiable information (PII) and other information protected under the Health Insurance Portability Accountability Act (HIPAA).

What does an IRO do?

The IRO's duties are specified in the CIA and are usually detailed in appendices to the formal agreement. Typically, the IRO is required to:

- Obtain a basic understanding of the company's business;
- Select a sample of claims submitted to and paid by a federally funded program (i.e., Medicare, Medicaid, Champus, CHIP). The size of the sample and whether it is to be selected randomly or based on a statistical formula is detailed in the CIA;
- Review the selected sample of submitted and paid claims, in accordance with applicable federal and state healthcare program rules and reimbursement guidelines, to determine whether the items and services furnished were medically necessary and appropriately documented and whether the claim was correctly coded, submitted, and reimbursed. If the IRO determines through its review that an overpayment has occurred, the IRO will be required to review the system(s) and process(es) that generated the paid claim and identify any problems or weaknesses that may have resulted in the identified overpayments;
- Provide its observations and recommendations on suggested improvements to the system(s) and the process(es) that generated the paid claim in its report; and
- Perform—depending on the language contained in the CIA—an extrapolation

to calculate an overpayment amount for the entire population if an overpayment is identified during the review of the claims sample selected.

The IRO will also prepare a claims review report that typically provides the following information.

Claims review methodology

- A description of the population subject to the claims review;
- A statement of the objective intended to be achieved by the claims review;
- A description of the process used to identify paid claims in the population and the specific documentation relied upon when performing the claims review (e.g., medical records, physician orders, CMS program memoranda, Medicare carrier, or intermediary manual or bulletins);
- A narrative description of how the claims review was conducted and what was evaluated; and
- A description of any supplemental materials the IRO relied on that were not contained in the claims files.

Statistical sampling documentation

- A copy of the printout of the random numbers generated by the statistical sampling software used by the IRO; and
- A description of the statistical sampling software used by the IRO (e.g., RAT-STATS, Excel).

Claims review findings

- A description of the company's billing and coding systems, including the identification by position description of the personnel involved in coding and billing;
- A description of the company's controls in place to ensure that all items and services billed to federal healthcare programs are medically necessary and appropriately documented;
- An explanation of the IRO's findings and supporting rationale regarding the claims review, including reasons for errors, patterns, etc. and the results of the claims review samples;
- Total number and percentage of instances in which the IRO determined that the coding of the paid claims submitted by the company differed from what should have been the correct coding and in which such difference resulted in an overpayment to the company;
- Total number and percentage of instances in which the IRO determined that a paid claim was not appropriately documented and in which such documentation errors resulted in an overpayment to the company;
- Total number and percentage of instances in which the IRO determined that a paid claim was for items or services that were not medically necessary and resulted in an overpayment to the company;
- Total dollar amount of all overpayments in the claims review samples;
- Total dollar amount of paid claims included in the claims review samples;

The IRO's report is typically required to include any recommendations for improvements to the company's billing and coding system.

- Error rate in the claims review samples (the error rate is calculated by dividing the overpayment in the claims review samples by the total dollar amount associated with the paid claims in the claims review samples); and
- An extrapolation to determine the estimate of the actual overpayment in the population at the mean point estimate or other statistical method as called for in the CIA.

A spreadsheet of the claims review results should be created that includes the following information for each paid claim: Federal health care program billed, beneficiary name and health insurance claim number, date of service, code submitted (e.g., DRG, CPT code), code reimbursed, allowed amount reimbursed by payor, correct code (as determined by the IRO), correct allowed amount (as determined by the IRO), and the dollar difference between allowed amount reimbursed by payor and the correct allowed amount.

The IRO's report is typically required to include any recommendations for improvements to the company's billing and coding system or to the company's controls for ensuring that all items and services billed to any federal healthcare program are medically necessary and appropriately documented.

The IRO's report would also include the names and credentials of the individuals who: (1) designed the statistical sampling procedures and the review methodology used for the claims review; and (2) performed the claims review.

Upon conclusion of the IRO's work and submission of its report, the IRO may be required to meet with representatives from the OIG to review the report and findings. This requirement is normally detailed in the CIA, and the obligation to cooperate with the OIG's requests should be clearly stated in the engagement letter between the company and the IRO.

How does the IRO interact with the company?

The IRO will request a meeting with the company to begin the process of identifying and selecting claims for their review. Company attendees at the meeting would likely include the company general counsel, chief compliance officer, and head of Information Technology. During that meeting the following should be discussed:

- **Who the primary contact point will be** for the IRO at the company;
- **Claims identification process**, including a description of how the claims are processed and housed, and any software programs used by the company to adjudicate and/or process and submit claims;
- **Description of compliance-related activities** undertaken by the company in connection with claims processing, submission, and handling of overpayments identified as part of the compliance function;
- **Process and timing** for the company to make the claims population available to the IRO for claims selection;
- **Process for the IRO to provide the claims selection to the company** so that the appropriate claim files and documentation can be provided to the IRO through a secure site to address requirements under HIPAA;
- **Timing and process** for the company to provide the selected claims and supporting documentation to the IRO. This is particularly important because most CIAs require the company to file a report that includes the IRO's findings within 60 days of their required reporting period. Particular care should be taken to understand what specific software, if any, may be necessary to allow the IRO to read the

supporting documentation. For example, certain "readers" may be required to view radiographs.

- **Process to discuss and address issues identified by the IRO** during its claims review to include any overpayments identified and potential for extrapolation of those overpayments to the entire population as called for in the CIA.

Can the IRO be removed/terminated?

The short answer is yes; however, there are requirements that must be followed.

If the company terminates its IRO or if the IRO withdraws from the engagement during the term of the CIA, the company is required to submit a notice explaining: (1) the reasons for termination of the IRO or (2) the IRO's reasons for its withdrawal to the OIG, normally no later than 30 days after termination or withdrawal. Additionally, within a given timeframe (typically 60 days) of termination or withdrawal of the IRO, the company will be required to identify a new IRO and provide the OIG with the proposed IRO's credentials for approval. If the OIG does not object within 30 days of submission of the information regarding the proposed IRO, the company may proceed to engage the new IRO in accordance with the terms of the CIA.

In the event the OIG has reason to believe that the IRO does not possess the requisite qualifications as described in the CIA, is not independent and objective, or has failed to carry out its responsibilities as described in the CIA, the OIG can notify the company in writing regarding the OIG's basis for determining that the IRO has not met the requirements of the CIA.

The company will be given a timeframe (usually 30 days) from the date of the OIG's written notice to provide information regarding the IRO's qualifications, independence, or performance of its responsibilities in order to resolve the concerns identified by the OIG. If, following the OIG's review of information provided by the company regarding the IRO, the OIG determines that the IRO has not met the requirements as described in the CIA, the OIG will notify the company in writing that the company will be required to engage a new IRO in accordance with the terms of the CIA. The company will be given a timeframe to engage a new IRO, which is typically within 60 days of its receipt of the OIG's written notice. As previously stated, agreed-upon monetary penalties may be incurred if a new IRO is not engaged within the timeframe stated in the CIA. The final determination as to whether or not to require the company to engage a new IRO is normally made at the sole discretion of the OIG.

Conclusion

Because selection of an IRO is a time-consuming process, care should be taken to identify and engage an IRO with the requisite qualifications and experience to avoid the headache of having to identify and engage a new one. Additionally, since most CIAs are for a five-year term, the IRO and company will "have to live with each other" for that time period. To avoid disagreements that could lead to IRO resignation or removal, we recommend that the company and the IRO meet after the conclusion of the initial review (and subsequent reviews) to discuss any issues encountered during the review process. This interaction will go a long way to ensure that subsequent reviews go smoothly. ✳

The views expressed in this article are the authors' and do not necessarily represent the views of GlassRatner.

by Dov Goldman

Five ways to reduce the likelihood of a third-party breach

- Create an inventory of all third parties and identify which of them have access to your data to reduce the risk of a data breach.
- Use a SaaS solution to centralize third-party documentation and workflows to help reduce risk.
- Designate responsibility and accountability to the board of directors/senior leadership to alleviate risk.
- Collaborate across job functions and form a third-party risk management committee to regularly review/update standard risk management processes.
- Ultimately, information security is more about managing risk and building customer trust than building widgets.

Dov Goldman *(dov.goldman@opus.com) is Vice President, Innovation & Alliances for Opus in New York City.*

Some of the largest organizations in the world remain vulnerable to data breaches. Recent widely reported, large-scale data attacks include household names like Best Buy, Sears, Yahoo!, Domino's, Uber, and of course, Equifax. The Identity Theft Resource Center[1] shared that the number of data breaches reported by US organizations reached an all-time high last year. We need a new perspective on risk management protocols—and we need it fast.

Goldman

How to reduce risk

Companies do not realize the vulnerabilities that come from their third-party relationships. A recent survey done by Soha Systems notes that 63% of all data breaches can be attributed to a third party. Consider the Uber data breach. The original exposure occurred through a third-party coding site used by Uber engineers.

A recent report from Ponemon and Opus, "Data Risk in the Third-Party Ecosystem," found these breaches on the rise. More than half (56%) of respondents experienced a third-party data breach, a 7% increase from last year. In the pharmaceutical and healthcare industries, the increase was even sharper: 61%.[2]

Companies do not have an adequate read on third parties throughout their organizations, which puts the companies at risk. Mistakes can be costly. A 2017 Cost of Data Breach Study found US companies spent an average of $7.35 million per breach in fines, remediation costs, and customer loss.[3]

Here are five tips[4] to reduce the likelihood of a third-party data breach.

1. **Manage all third parties based on their risk**
   Prioritize third parties with access to your data, whether it's non-public information about customers or your company's intellectual property; learn whether these third parties share this data with

others. Creating an inventory of all third parties can reduce risk by as much as 19%. Identify which firms have access to sensitive information and manage them in accordance with risk they expose your company to.

2. **Centralize documentation and workflows**
   Reduce risk by 15% to 20% by using a software as a service (SaaS) solution to centralize third-party documentation and workflows and facilitate visibility into, and evaluation of, the security practices of all third parties.
3. **Designate ownership**
   Assign accountability for your company's third-party risk management program from the board of directors and senior leadership to the third-party relationship manager. This can help alleviate risk by 10% to 14%.
4. **Create standards for success**
   Standards save money and drive efficiency. Collaborate across job functions and form a third-party risk management committee to regularly review and update standard risk management processes and controls to reduce risk by up to 15%.
5. **Monitor risks continuously**
   Consistent risk management program oversight can help reduce risks by up to 18%. Review and update vendor management policies regularly as well as conduct audits and assessments to ensure the security and privacy practices of third parties address new and emerging threats.

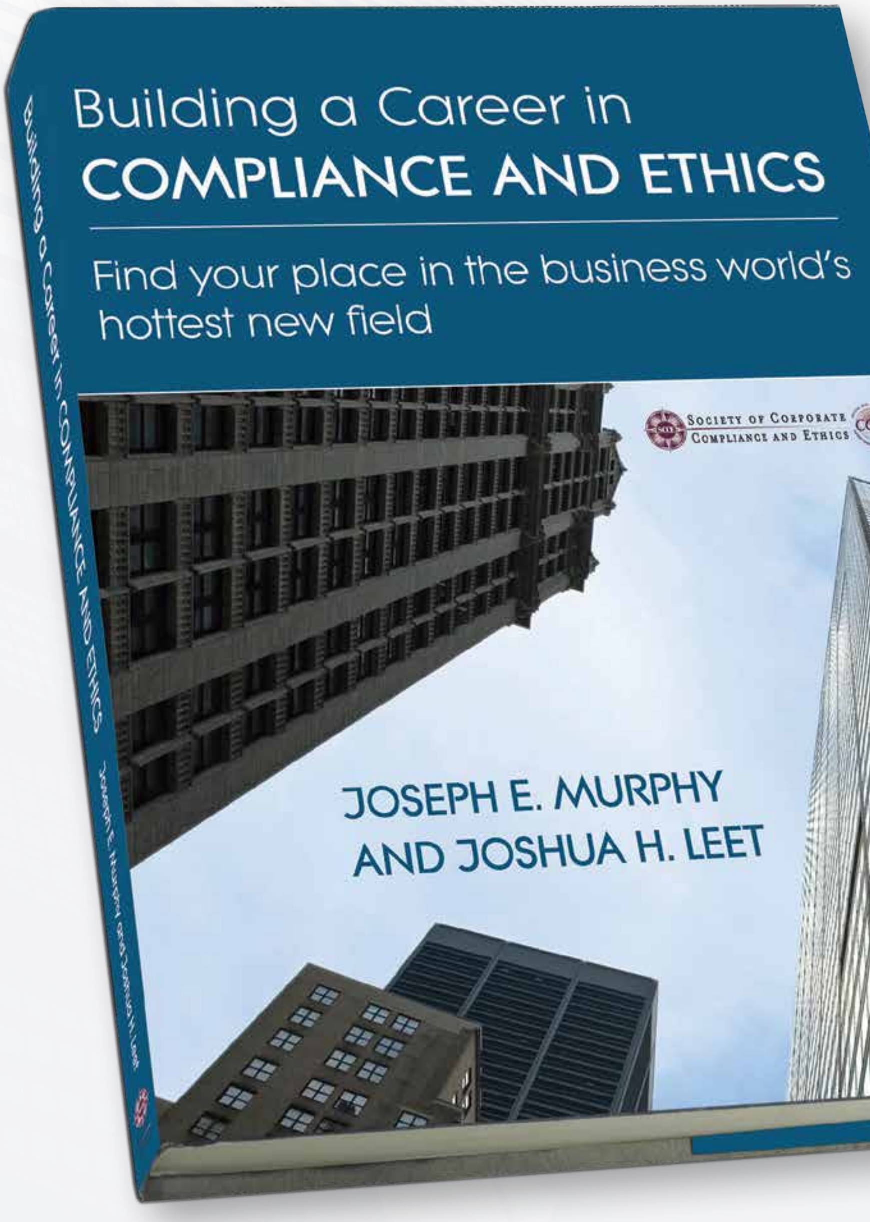
The influence of leadership

Although there are many factors that can contribute to a system infiltration, employing these tactics can help prevent companies from experiencing a debilitating third-party data breach. There needs to be buy-in from the executive level for companies to keep their information and customers protected. A recent Forrester research report, "Build a High-Performance, Customer-Obsessed Security Organization," stated that information security is about managing risk and building customer trust—not widgets.[5]

Technology plays a significant role in helping companies remain secure, but leadership must implement a sound risk management framework that evolves with changing business models, maintain a strong relationship with their customers, and ensure they are transparent in their security processes. ✳

1. Identity Theft Resource Center: "2017 Annual Data Breach Year-End Review." Available at https://bit.ly/2s3TGM9
2. Available at https://bit.ly/2kf0mDv
3. Available at https://ibm.co/2Bir60B
4. *Ibid*, Ref #2
5. Christopher McClean: "Build A High-Performance, Customer-Obsessed Security Organization" *Forrester*; July 13, 2017. Available at https://bit.ly/2IDqgiT.

SCCE
Compliance & Ethics PROFESSIONAL
The Red Flag Group
The Red Flag Group raises the bar with support from the Academies
see page 18


Building a Career in
COMPLIANCE AND ETHICS
Find your place in the business world's hottest new field
Society of Corporate Compliance and Ethics
JOSEPH E. MURPHY AND JOSHUA H. LEET
Building a Career in COMPLIANCE AND ETHICS
Joseph E. Murphy and Joshua H. Leet

Congratulations

Newly certified designees!

CCEP™

CERTIFIED COMPLIANCE &
ETHICS PROFESSIONAL

Achieving certification required a diligent effort by these individuals. Certified Compliance & Ethics Professional (CCEP)® certification denotes a professional with sufficient knowledge of relevant regulations and expertise in compliance processes to assist corporate industries in understanding and addressing legal obligations. Certified individuals promote organizational integrity through the development and operation of effective compliance programs.

- Lisa K. Akin
- Thomas Angelillo
- Gerald J. Borne
- Jill R. Conte
- Jaime Jue
- Susan Leiter
- Marie R. Martinez
- Suely R. Mello
- Ogechi C. Muotoh
- Joseph Murray
- Paula Payne
- Brianna C. Rice
- Allison Watts
- Maureen Yencha

CCEP-I™

CERTIFIED COMPLIANCE & ETHICS
PROFESSIONAL-INTERNATIONAL

The individual who earns the Certified Compliance & Ethics Professional - International (CCEP-I)® certification is a professional with knowledge of relevant international compliance regulations and has expertise in compliance processes sufficient to assist corporate industries in understanding and addressing legal obligations, and promoting organizational integrity through the operations of an effective compliance program.

- Agatha R. Asemota
- Chao Ru Joanna Chow
- Giovanna C. Crotti
- Luciano de Melo
- Juliana Ferraz Breno
- Ken Mack
- Joseph Murray
- Maria M. Vassallo

The Compliance Certification Board (CCB)® offers opportunities to take the CCEP and CCEP-I certification exams. Please contact us at ccb@compliancecertification.org, call +1 952.933.4977 or 888.277.4977, or visit compliancecertification.org.

CCB™
COMPLIANCE
CERTIFICATION BOARD

Become Certified

A few letters after your name can make a big difference.

Why do people add JD, MBA, or CPA after their name?
They know those initials add credibility.

Become a Certified Compliance and Ethics Professional (CCEP)®, a Certified Compliance & Ethics Professional-International (CCEP-I)® or a Certified Compliance & Ethics Professional-Fellow (CCEP-F)®.

Set the bar for your compliance team and demonstrate your skill in the compliance profession, increase your value in the workplace and to future employers, and showcase your compliance knowledge and experience.

Applying to become certified is easy.

To learn what it takes to earn the CCEP, CCEP-I, or CCEP-F designation, visit **compliancecertification.org**.

CCEP™
CERTIFIED COMPLIANCE & ETHICS PROFESSIONAL

CCEP-I™
CERTIFIED COMPLIANCE & ETHICS PROFESSIONAL-INTERNATIONAL

CCEP-F™
CERTIFIED COMPLIANCE & ETHICS PROFESSIONAL FELLOW

CCB™
COMPLIANCE CERTIFICATION BOARD

SCCE *welcomes* NEW MEMBERS

ALABAMA
- Khalilah Burton, Columbia Southern University
- Roslyn Crews, Alabama A&M University
- Daphne Hamilton, Poarch Creek Indians
- Craig Lenz, Alabama College of Osteopathic Medicine
- Joelle Limbaugh, Alabama Power
- Wesley Manning, Poarch Creek Indians
- Phyllis Osby
- Annie Self, Southern Linc

ALASKA
- Margaret Baker, University of Alaska Anchorage College of Health
- Ashley Beeson, Gana- A'Yoo, Limited
- Brennan Cain, The Eyak Corporation
- Paul Carpenter, Northern Industrial Training

ARIZONA
- Angela Egelhoff, Endurance International
- Rich Hoffecker, The Red Flag Group
- Christina Lam, The Red Flag Group

ARKANSAS
- Nisha Aggarwal, Wal-mart Stores Inc
- Dan Brown, Interactive Services
- Linda Hartsock, Wal-mart Stores Inc
- Kara Moss, Wal-mart Stores Inc
- Missy Sleep, Wal-mart Stores Inc
- Rachel Smith, Wal-mart Stores Inc
- Junior Zuniga, Wal-mart Stores Inc

CALIFORNIA
- Leona Augerlavoie, CompuMail
- Valarie Baker, CalPERS
- Tamara Barnas, The Scripps Research Institute
- Alan Bennett, LA Co Metropolitan Transportation
- Stacey Caplan, SAP
- Hala Helm, Palomar Health
- Jerry Jackson, AltaMed Health Services
- Susan Jones, Amgen
- Cynthia Kerenyi, VHA Office of Research Oversight
- Paco Morales, Robert Half International
- Sherry Morimoto, Los Angeles Department Of Water And Power
- Andrea Mozqueda, Keck Graduate Institute
- Adam Odabashian, CalPERS
- Brittany Raygoza, Keck Graduate Institute
- Rebekah Rushton, Northridge Hospital Medical Center
- Alanna Rutan, The Scripps Research Institute
- Thomas Scott, Cruise Automation (GM Cruise LLC)
- Aurora Servin, General Atomics
- Andrea Troublefield, Calaveras Health & Human Services Agency
- Laura Weissbein, Credit Karma
- Lawrence Wold, CalPERS

COLORADO
- Mark Barela, National Renewable Energy Laboratory
- Jennifer Gomez, Centura Health
- Jim Hankins, Antero Compliance
- Jennifer Houghland, DMC Global Inc
- Michelle Rubalcava, Lockheed Martin
- Su Sim, CHFA
- David Williams, Williams Compliance Group LLC
- Samantha Williams, Williams Compliance Group LLC

CONNECTICUT
- Karen Allison

DELAWARE
- Clare Thomas, St. Francis Healthcare

FLORIDA
- Rica Calhoun
- Onelia Cano, Assurant
- Nivia Cox, FNF
- Juan DeLeon
- Trisha Hoover, Katmai Government Services
- Dianne LaFrance, Cognizant
- Steve Lee, Hellmann Worldwide Logistics
- Stephanie Linares, University of Miami
- Christopher Martin, UF Health Jacksonville
- Kerry Anne McClannahan, IAP Worldwide Services, Inc
- Raul Ordonez, Jackson Health System
- Autumn Smallwood, Moffitt Cancer Center
- Alex Soto, Dufry Group
- Brooke Tefft, Ring Power Corporation
- Eiko Witkowski

GEORGIA
- Alecia Bell, Morehouse School of Medicine
- Richard Escoffery, ACS Group
- Kim Gleeson, RSUI Group, Inc
- Christee Laster, Kaiser Permanente Medical Group
- Kristen Lilly
- Carolyn Miller, Georgia-Pacific LLC
- Stanford Smalls, Southwire
- Lori Spencer, Southeast Permanente Medical Group

ILLINOIS
- Brian Annulis, Ankura Consulting Group
- Richard Crusor, Cook County Government
- Michael Gooding, Fidelity Life Association
- Karen Habercoss, The University of Chicago Medicine & Biological Sciences
- Susan Lynch
- Charles McElravey, VMware Inc
- April Minkus, Law Offices of April Minkus
- Nicole Monaco, Videojet Technologies/ Danaher
- Mary Owen
- Jeff Parker, Allstate
- Elizabeth Rodriguez, IMEG
- Holly Skonecke, Allstate Insurance Company
- Latasha Thelemaque, State Farm
- Wendy Thomas, CDK Global

INDIANA
- Aaron Love, MISO Energy

KANSAS
- Debbie Sackuvich, Louis Dreyfus Company LLC

LOUISIANA
- Paul Avery, Fluor Federal Petroleum Operations, LLC
- Valerie Clark, Louisiana Dept of Children & Family Services
- Paola Corrada, Pan-American Life Insurance Group
- Mark Garrison, LOOP LLc
- Arlene McCarthy, self-employed

MAINE
- Carissa Hanratty, Avangrid

MARYLAND
- Bethany Alt, Flagship Rehabilitation
- Tracie Andrews, Lockheed Martin Corp
- Denise DeZolt, Laureate Education
- Kristin Diamond, Flagship Rehabilitation
- April Doss, Saul Ewing Arnstein & Lehr LLP
- Melissa Grocia, Shimadzu Scientific Instruments, Inc
- Michael Guzman, Flagship Rehabilitation

MASSACHUSETTS
- Julie Basha, Fresenius Medical Care NA
- Michael Ferguson, Kroll

MICHIGAN
- Kathryn Clampitt-Voiles, Judson Center
- Gary Forward, Guardian Industries
- Kara Gordon, The Dow Chemical Company
- Kelly Scott, CareWell Services Region 3B Area Agency on Aging
- Karie Steuer, Perrigo Company PLC

MINNESOTA
- Pamela Kemp, Tennant Company
- Katie Regenscheid, Prime Therapeutics
- Kristin Selph, Shapiro & Zielke, LLP
- Robyn Singer, Xcel Energy

MISSOURI
- Angela Campbell, H&R Block
- Tammy Pierce, Preferred Family Healthcare
- Kyle Wachs, Kansas City Power & Light

NEW JERSEY
- Marta Borbon, Brother International Corporation
- David Levin, Lockheed Martin
- David Marcus, Wakefern Food Corp
- Lindsay Seitz, DoubleCheck Software, LLC

NEW MEXICO
- Kathy Silva, Sandia National Laboratories

NEW YORK
- Leon Bukhman, Con Edison Company of NY
- Christina Corbellati, Person Centered Services of WNY
- Elisa Galuppo, The Resource Center
- Danielle Gordon, Memorial Sloan Kettering Cancer Center
- Omer Hussain, United Bank For Africa
- Julie Swanson, The Resource Center

NORTH CAROLINA
- Heather Aherne, The Fresh Market
- Brad Glazer, GlaxoSmithKline

- Celeste Goddard, Merz North America, Inc
- Shelley Medford, Messer Financial Group
- Stephanie Poole, Grifols
- Laura Rodgers, ECM Solutions Group
- Connie Wilkinson, LifePoint Hospitals Inc

OHIO

- James Grasso, STERIS
- Craig Hanson, Wal-mart Stores Inc
- Joan Hartman, OhioHealth
- Kristy Heath, Toledo Clinic
- Grace Ho, The Timken Company
- Jim Holmes, Treasurer's Office Franklin City Ohio
- Bae Hunt, Medical Mutual of Ohio
- Brianna Weir, STERIS Corporation

OKLAHOMA

- Robyn Burk, Chesapeake Energy
- Ryan Daugherty, Cherokee Nation
- Kimberly Johnson, Cherokee Nation
- Kearby Lamson, Sonic Drive-In
- William Turner, American Fidelity Assurance

PENNSYLVANIA

- Carly Chronister, Flagship Rehabilitation
- Allison Firely
- Patrick Hromisin, Saul Ewing Arnstein & Lehr LLP
- Jennifer Leone, Lannette Co.
- Angel Mazack, United Health Group
- Margaret McKeon, Philadelphia College of Osteopathic Medicine
- Claudia Pankowski, Buckeye Partners
- Linda Toth

SOUTH CAROLINA

- Matt Bayne, Fluor Govt Group
- John Harman, Benefitfocus
- Wesley Jarmulowicz, Vinnell Arabia LLC
- Pam Johnston, Dennis Corporation
- Justin Lee, DHEC

TENNESSEE

- Adam Balfour, Bridgestone
- Diana Lutz, FedEx
- Thomas Southerland, FedEx Express

TEXAS

- Vicky Ashmore, McCamey County Hospital District
- Brenda Balderaz, South Texas College
- Cecilia Gonzalez, UTIMCO
- Marilyn Gutierrez, Huawei Technologies USA Inc
- Kateeka Harris, Tarrant County College District
- Renita Holland, Bayview Loan Servicing
- Ashley Johnson, McCamey County Hospital District
- Sara Krause, Travis County
- Chidimma Mbamalu, Energy Transfer Partners
- John Minor, Houston Community College
- Ronald Nelson, Vantage Drilling International
- Paul Plata, University of Texas Rio Grande Valley
- Rebekah Rutland, Parsley Energy
- Cameron Schneider, DISA Global Solutions
- Szende Smith, TxDOT

- Elizabeth St. James, HMS Corporation
- Jana Terry, Beckstead Terry PLLC
- Sunela Thomas, AT&T Inc
- Steven Williams
- Adrienne Wilson

UTAH

- Bre Madsen, Credit Karma

VIRGINIA

- Irene Henrich, Flagship Rehab
- Michael Johnson, Clear Law Institute
- Michael Lawrence, USG
- Kimberly Rupert, SAIC

WASHINGTON

- Thomas Dynes, Boeing Company Ethics & Bus Conduct
- Katrina Higggason, Zillow Group
- Phuong Nguyen, The Boeing Company
- Jessica Shaw, WRPS

WISCONSIN

- Kristin Manney, Oshkosh Corp
- Kevin Tubbs, Oshkosh Corp

DISTRICT OF COLUMBIA

- Anjali Desai, Farmer Mac
- Judith Kassel, Saul Ewing Arnstein & Lehr
- Heather Mills, KPMG
- Rebecca Miner, AARP Services, Inc
- Dorinda Tucker, The George Washington University
- Clinton Yu, Barnes & Thornburg LLP

PUERTO RICO

- Lina Vega, Universidad Metropolitana

BAHAMAS

- Grace Neeley Sweeting

BRAZIL

- Taciana Alves, Engeform
- Ricardo Bocutti, JBS SA
- Andre Damaso, JBS SA
- Luciana de Andrade, Perisson Andrade, Massaro e Salvaterra Advogados
- Antonio Fernandez, Alcon
- Marina Ferro e Silva, Avery Dennison
- Natacha Marly, ENGIE
- Bruno Massard, KPMG
- Marcelo Massaro, Perisson Andrade, Massaro E Salvaterra Sociedade de Advogados
- Ana Mellone, ENGIE Brasil
- Rodrigo Merg, VMware,Inc
- Priscilla Moraes, Deloitte
- Priscila Palhares, Makro Group
- Renata Palma Rozzante de Castro, Herrera Castro Advogados
- Carolina Souza, Petrobras Transporte S.A.
- Benny Spiewak, ZCS LLC

CANADA

- Kristy Ivans, College of Physicians and Surgeons of Alberta
- Leanne Minckler, CPSA
- David Rothwell, TransCanada Pipelines
- Camilla Chalmers, Great-West Lifeco
- David Gore

CHINA

- Yuhua Rong, Cardinal Health

FRANCE

- Adrien Mezouari, L'Oréal

GERMANY

- Jens-Peter Wulf, Avaloq

HONG KONG

- Daniel Tsui, 3M
- Clark Tung, Cook Medical
- Chuu Yee Wong, CBRE Limited
- Dickens Wong, 3M

ITALY

- Milica Karunc, Unicredit S.P.A
- Antonio Ruocco, General Cable Co.

LUXEMBOURG

- Deloge Florence, FANUC Europe Corporation

MALAYSIA

- Nurfarah Zafirah Foo Abdullah, Molex
- Thomas Aker, Ericsson Malaysia Sdn. Bhd.

NETHERLANDS

- Abdulaziz Bassam, Aramco Overseas Company
- Daniela Meirelles, Booking.com B.V.
- Daniel Post, Booking.com

NIGERIA

- Olukayode Dada, Udo Udoma & Belo-Osagie

PERU

- Giovanni Marotta, SOS Children's Village

PHILIPPINES

- Dennis Odra, Reckitt Benckiser

SAUDI ARABIA

- Ahmed Hilal, Saudi Aramco

SINGAPORE

- Puay Huang Cynthia Chan, Tan Tock Seng Hospital Pte Ltd
- Clara Choo, 3M
- Geraldine Goh, Marina Bay Sands Pte Ltd

SLOVENIA

- Snežana Harnik, NLB Skladi d.o.o., Ljubljana, VAT^{46788719}

SOUTH KOREA

- Jee Eun Kim, The Red Flag Group (att. Jenna Kim)

THAILAND

- Jonathan Blaine, DFDL (Thailand) Ltd.

UNITED ARAB EMIRATES

- Joanne Norman, Emirates Global Aluminium

UNITED KINGDOM

- St.John Bent, FTI Consulting LLP
- Kiran Hundal, Salesforce
- Alpa Piparia, Compliance in Action Limited
- Roma Poonja, FTI Consulting Ltd

by Joe Murphy, CCEP, CCEP-I

GDPR and your compliance program

Joe Murphy (joemurphyccep@gmail.com) is a Senior Advisor at Compliance Strategists, SCCE's Director of Public Policy, and Editor-in-Chief of Compliance & Ethics Professional *magazine.*

The world is buzzing about the EU's General Data Protection Regulation (GDPR); Europe now sets the global standard for protecting privacy. GDPR is a pervasive regulatory system that tends to stick to anything that touches it. It is detailed and requires knowledge of the special terminology of privacy.

Murphy

It also is backed by huge fines. The privacy bureaucrats can extract up to 4% of a company's global turnover for violations. I have been told that they will probably not go after such large amounts of money in small cases. But most governments are quite fond of revenue, and the temptation under this amorphous area of regulation may be overwhelming.

But here is the special concern for us. Because the concept of privacy is so broad and the regulations so pervasive, they invite abuse by regulators in dealing with company compliance and ethics programs. Compliance and ethics, by its nature, involves interaction with "data subjects" (i.e., humans), thus giving the privacy sheriffs license to control and restrict our work.

European privacy regulators already have demonstrated indifference about other areas of the law. Protecting the environment? Fighting corruption? Unearthing cartels? A muscular approach to privacy comes first.

So in France, when companies worked to adopt speak-up programs, the French privacy regulator had a field day denouncing these efforts and dreaming up regulatory schemes to fence them in. Spanish regulators even purported to muffle abused employees by forcing them to reveal their identities if they wanted to report their bosses' crimes and abuses. After all, it can be impossible to retaliate against employee insolence unless you know who had the nerve to speak up.

Now commentators are raising the alarm that GDPR will make anti-corruption due diligence more difficult and undermine the fight against bribery, and privacy regulators may undercut all company efforts to comply with the law and act ethically.

Conducting an investigation of alleged misconduct in your company? Doing training? Testing employees? Due diligence on new hires? Audits of company records? Whatever you do, if it involves contact with human beings, plan to spend time talking with privacy mavens.

Here is the issue. Privacy is one value, and one only. Society needs organizations to take effective steps to prevent and detect wrongdoing. If privacy merits the grand regulatory scheme of GDPR, then certainly company compliance and ethics work deserves at least as much protection. It is time for the EU and other governments to step up and enact legislation that protects compliance efforts and bars future roving regulators from hijacking our work to expand their own regulatory kingdoms.[1] ✳

[1] Joseph E. Murphy: "Policies in conflict: Undermining corporate self-policing" Rutgers U.L., Rev. 421, 2017. Available at https://bit.ly/2LP0tlY.

Takeaways

August 2018

Compliance & Ethics PROFESSIONAL

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

Anti-bribery/compliance pitfalls at the U.S. state level

Don McCorquodale and Susan Carr (page 29)

- The United States state and local government sales market is very large.
- The state and local sales markets permit easy access to decision makers.
- Significant compliance issues must be addressed when selling directly to state and local government employees and leaders.
- A compliance strategy must be incorporated into corporate sales planning.
- Failure to address compliance issues can lead to severe penalties and public scrutiny.

ISO 37001 Certification: Understanding and navigating the process

Maurice L. Crescenzi, Jr. (page 36)

- The International Organization for Standardization (ISO) is a non-governmental organization that facilitates the international unification of industrial standards and management systems.
- Registrars or "certifying bodies" issue ISO certifications, and leading practices suggest it is best to obtain ISO certifications from accredited registrars.
- ISO 37001 establishes a standardized management system for managing the risk of bribery and corruption in both the public and private sectors.
- Although ISO 37001 has been received positively in the international ethics and compliance community, there is an accompanying sentiment that it does not introduce anything fundamentally new.
- How quickly and widely ISO 37001 will be adopted in the public and private sectors remains to be seen.

Making the most of the FCPA Corporate Enforcement Policy

Valerie Charles (page 46)

- The Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy encourages organizations to voluntarily disclose FCPA violations.
- Companies need to cooperate with the Justice Department if investigations occur and remediate the cause of the violation.
- There are five key capabilities of an effective compliance program.
- Compliance officers must determine the company's level of willingness to embrace the Enforcement Policy.
- Data analysis can help compliance officers understand the costs and benefits of working with the FCPA Enforcement Policy.

Establishing ethics compliance for the banking sector in Bosnia and Herzegovina

Mujo Vilašević (page 50)

- Transitional and integration processes toward the European Union give specific challenges to each transitional country.
- The banking sector has had its development in Bosnia and Herzegovina and has reached the point where it has higher standards of regulation than the country itself.
- The Compliance function has been introduced formally in the banking sector via new regulatory framework.
- Ethics compliance is a completely new approach and challenge in Bosnia and Herzegovina, which will help the path of development for the banking sector in general.
- Institutional support by state bodies will be conditio sine qua non for establishing ethics compliance.

Compliance: Addressing the intensifying age of statutory regulations

Ken Chamberlain (page 54)

- We've said goodbye to the old and have entered a new world of Compliance.
- The emphasis is now on an ever-changing regulatory framework for business.
- The tide of regulatory enforcement is accelerating.
- Effective risk and compliance infrastructures are absolutes.
- Make compliance, risk assurance, and whistleblowing solutions workable.

Your settlement with the government requires an Independent Review Organization: Now what?

Bert F. Lacativo and Adam Lampert (page 62)

- Begin searching for and interviewing Independent Review Organization (IRO) candidates as soon as it becomes apparent that the settlement agreement will require one.
- Choose your IRO carefully to ensure that it has the credentials, experience, and independence necessary to accomplish the tasks outlined in the settlement agreement.
- Begin preparing the information that the IRO will need to perform its assigned tasks so that it can be completed within the normal 60-day reporting timeframe.
- Ensure that claims and compliance process maps, policies, and procedures are prepared, because the IRO will likely be required to review them as part of their work.
- Be prepared to respond quickly to questions and requests from the IRO, and agree on a timeframe to review its findings and respond, if necessary.

Five ways to reduce the likelihood of a third-party breach

Dov Goldman (page 67)

- Prioritize the access given to third parties and create an inventory of them to reduce the risk of a data breach.
- Use a SaaS solution to centralize third-party documentation and workflows to help reduce risk.
- Designate responsibility and accountability to the board of directors/senior leadership to alleviate risk.
- Collaborate across job functions and form a third-party risk management committee to regularly review/update standard risk management processes.
- Ultimately, information security is more about managing risk and building customer trust than building widgets.

SCCE'S UPCOMING EVENTS

Learn more about SCCE educational opportunities at **corporatecompliance.org/events**

August 2018

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
29	30	31	1	2	3	4
5	6 **BASIC COMPLIANCE & ETHICS ACADEMY®** Washington, DC	7	8 **WEB CONFERENCE:** New Department of Defense Cyber Rules	9 CCEP Exam	10	11
12	13 **WEB CONFERENCE:** Privacy: Individual Rights and Consumer Protections	14	15	16	17 **REGIONAL CONFERENCE** Columbus, OH	18
19	20 **BASIC COMPLIANCE & ETHICS ACADEMY®** São Paulo, Brazil	21	22	23 CCEP-I Exam	24 **REGIONAL CONFERENCE** São Paulo, Brazil	25
26	27	28	29	30	31	1

September 2018

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10 **BASIC COMPLIANCE & ETHICS ACADEMY®** Las Vegas, NV	11 **WEB CONFERENCE:** FOFAC Sanctions: The Iran Nuclear Deal	12	13 **WEB CONFERENCE:** How to Have a Wildly Successful Career in Compliance CCEP Exam	14	15
16	17	18	19	20	21 **REGIONAL CONFERENCE** Washington, DC	22
23	24 **BOARD AUDIT COMMITTEE COMPLIANCE CONFERENCE** Scottsdale, AZ **BASIC COMPLIANCE & ETHICS ACADEMY®** Madrid, Spain	25	26	27 CCEP-I Exam	28 **REGIONAL CONFERENCE** Dallas, TX	29

REGIONAL CONFERENCES

August 17 • Columbus, OH

August 24 • São Paulo, Brazil

September 21 • Washington, DC

September 28 • Dallas, TX

October 4 • Sarajevo, Bosnia and Herzegovina

November 16 • Seattle, WA

December 7 • Philadelphia, PA

BASIC COMPLIANCE & ETHICS ACADEMIES

August 6–9 • Washington DC

September 10–13 • Las Vegas, NV

October 1–4 • Dallas, TX

November 12–15 • San Diego, CA

December 10–13 • Orlando, FL

INTERNATIONAL BASIC COMPLIANCE & ETHICS ACADEMIES

August 20–23 • São Paulo, Brazil

September 24–27 • Madrid, Spain

November 26–29 • Rio de Janeiro, Brazil

BOARD AUDIT COMMITTEE COMPLIANCE CONFERENCE

September 24–25 • Scottsdale, AZ

COMPLIANCE & ETHICS INSTITUTE

October 21–24 • Las Vegas, NV

Dates and locations are subject to change.

2019 SCCE Events

Internal Investigations Workshops

January • San Diego, CA

June • Orlando, FL

Utilities & Energy Compliance & Ethics Conference

February 10–12 • Houston, TX

Board Audit Committee Compliance Conference

February 18–19 • Scottsdale, AZ

European Compliance & Ethics Institute

March 10–13 • Berlin, Germany

Higher Education Compliance Conference

June 9–12 • Orlando, FL

18th Annual Compliance & Ethics Institute

September 15–18 • National Harbor, MD

WEB CONFERENCES

Stay up-to-date on compliance issues and hot topics without leaving your desk. Expert-led web conferences are added throughout the year. If you missed a must-hear session, past sessions are archived so you can listen when it's convenient for you. Visit corporatecompliance.org/webconferences to see our latest and archived web conferences.

BASIC COMPLIANCE & ETHICS ACADEMIES

January 21–24 • Orlando, FL
February 4–7 • Scottsdale, AZ
March 18–21 • Chicago, IL
April 15–18 • San Diego, CA
May 13–16 • Minneapolis, MN
June 3–6 • Washington, DC
August 5–8 • New York, NY
September 30–October 3 • Anaheim, CA
October 21–24 • Orlando, FL
December 2–5 • Houston, TX
December 16–19 • Nashville, TN

INTERNATIONAL

January 13–16 • Dubai, UAE
February 11–14 • Hong Kong
May 6–9 • Amsterdam, Netherlands
July 15–18 • Singapore
August 26–29 • São Paulo, Brazil
September 23–26 • Madrid, Spain

REGIONAL COMPLIANCE & ETHICS CONFERENCES

January 25 • Southern California
February 21–22 • Anchorage, AK
March 1 • Minneapolis, MN
March 15 • New York, NY
March 29 • Boston, MA
April 12 • Scottsdale, AZ
April 26 • Tampa, FL
May 3 • Chicago, IL
May 10 • Richmond, VA
May 17 • San Francisco, CA
June 7 • Atlanta, GA
June 21 • Nashville, TN
August 16 • Columbus, OH
October 11 • Washington, DC
October 25 • Dallas, TX
November 15 • Seattle, WA
December 6 • Philadelphia, PA

INTERNATIONAL

January 17 • Dubai, UAE
July 19 • Singapore
August 30 • São Paulo, Brazil
October 3 • Sarajevo, Bosnia

Plan your year at corporatecompliance.org/events

SCCE™
Society of Corporate Compliance and Ethics

Conference dates and locations are subject to change.