COSMOS
Navigate the Compliance Universe

The Complete Compliance and Ethics Manual 2023
Structuring the CECO and Compliance Function for Success

By Donna C. Boehme[1] , [2]

Why This Is Important

In an ideal world, a company that is establishing a new chief compliance and ethics officer position (CECO) would dedicate considerable time and effort to high-level strategic thinking, contemplating the mandate for the function, the proper positioning, independence and empowerment for the officer, the competencies and experience necessary for the new position, and the resources required to do the job. After all, as your mother always told you, anything worth doing is worth doing well. But all too frequently, as reflected in the steady parade of companies with failed compliance programs in the headlines, the CECO position is created in haste and repented at leisure—sometimes under the watchful eye of a prosecutor or corporate monitor. In today's perilous regulatory environment where carefully nurtured corporate reputations and brands can be destroyed on the strength of a single individual act, revealed at the speed of a single Tweet or blog post, the CECO (together with the company's compliance program) is the company's first line of defense (after the business itself).[3] Compliance-savvy boards and senior management could make no better use of their scarce time than ensuring that their CECO and compliance function are structured for success, in a manner that is fit-for-purpose for their organization's size, scope, risk profile, industry, business structure, and culture.[4]

To facilitate this important endeavor, this chapter sets out a principles-based analysis based on six key criteria or features that are relevant to any CECO in any organization: true compliance subject matter expertise, empowerment, independence, seat-at-the-table, line of sight, and adequate resources—so that companies can structure their CECOs and compliance functions strategically for success and detect, fix, and prevent corporate misconduct or other big problems, before prosecutors, regulators, investors, plaintiff lawyers, or other stakeholders compel them to do so on terms that they demand (e.g. huge fines and penalties, blacklisting, reputational damage, class actions, and court ordered monitors, to name a few).[5] It is fairly easy to see from recent headlines that the companies involved would have fared much differently had they been able to discover and remedy their problems early, before landing squarely in media headlines, prosecutor's crosshairs, and a crisis/PR management war-zone.

The compliance profession has evolved rapidly over the last two decades, building its subject matter expertise (SME) in compliance, ethics, and culture, and establishing itself as a separate and independent profession that is needed by management in these modern times to lead its approach to its compliance, ethics, culture, and reputation issues.[6] The emergence of a new model of compliance, known as "Compliance 2.0," is being felt in corporate C-suites, boardrooms, and in policymaking both nationally and internationally, as more and more boards, C-suites, and government gatekeepers begin to understand the role of compliance and the experienced CECO in designing and managing the organization's approach to compliance, ethics, culture, and reputation issues. They are noting that the model for compliance governance is really the single most important indicator of whether a compliance program will succeed or fail. Compliance 2.0 is the new and improved model for compliance programs that are structured to succeed, in contrast to the old legacy model of Compliance 1.0—where the general counsel or an in-house counsel without true compliance SME is expected to design and

manage compliance. I call this the "DIY Compliance" version of Compliance 1.0,[7] where the person with no prior compliance SME does no more than an elementary "check the box" version of compliance based on (a lawyer's reading of) the seven elements of the FSG, and assumes that everything will magically "work" to fulfill the compliance mandate. Oh, but there is so much more to true compliance SME than that! A JD or golden legal resume is no substitute for true compliance SME earned on the ground and in the field.

As further discussed below, compliance SME is not taught in law schools. Producing the FSG elements is only the tip of the iceberg! Not only must the CECO and team be skilled and experienced in the best practices of how each element is designed and optimally operated, but also how they work in combination and in parallel to establish and nurture the right culture of ethical leadership, one that is sustainable and that acts as the umbrella and floor for an effective program that will work to successfully achieve the unique compliance mandate. One need only do a quick scan of Compliance 1.0 "train wrecks" over the last decade (i.e., "Ripped From the Headlines") to understand what happens when a CECO with no true compliance SME attempts to drive the compliance and culture train, usually with a mandate that runs at cross-purposes with the mandate of compliance (as further discussed below under "Structuring for Success: The Six Essential Features—Empowerment."

GM is a perfect example of a mandate conflict that caused a large-scale compliance train wreck. According to media reports, in-house legal counsel was busy "quietly" settling cases and giving PowerPoint training on the "69 Naughty Words" that employees must absolutely avoid in all communications, rather than diligently getting to the root of the ignition switch defect and resolving it with a prompt recall, before the affected cars resulted in the deaths of at least 167 customers![8] That list itself became a regrettable "smoking gun" for the company, demonstrating management's ambivalent approach to open and transparent discussion of problems and concerns, one of the hallmarks of a strong culture of ethical leadership that is supported by a strong, successful, and effective compliance program. Bottom line: so many other Compliance 1.0 train wrecks in the media headlines could have had different paths and outcomes if the company had understood the value of an independent, empowered, Compliance 2.0 program[9] that is structured and built to succeed! The analysis is even more striking when you consider that in many of these Compliance 1.0 train wrecks, employees, or other parties had attempted to raise specific concerns to management, but in each of these cases, the company failed to detect or avoid, follow through, and address (fix) the problems before they had to parachute into the crisis zone. A few examples:

Compliance 1.0 Case Studies (Recent Train Wrecks Ripped From the Headlines)

1)**Walmart Mexican bribery scheme**: A former employee reported the scheme, but the local international counsel, who had repeatedly recommended a full outside investigation into the reports, resigned after a few members of the C-suite decided to "hush up" the bribery investigation by sending it back to the very local counsel who had been involved in the problem conduct in the first place! That local counsel then dutifully closed the investigation with "nothing to see here" as the primary takeaway. While the *New York Times* investigative reporters won a Pulitzer Prize, Walmart lost some key executives and became embroiled in an expansive bribery investigation extending to a number of jurisdictions well beyond Mexico. Fortunately, Walmart has taken substantive steps in response to the scandal, hiring a new CCO with true compliance SME who then overhauled the compliance program making many improvements reflected in the Compliance 2.0 model, and setting an example for companies and their boards everywhere.[10] I have covered the issue and its implications more extensively here.[11]

2) **Siemens FCPA scandal**: I have written about this one in further detail here,[12] but suffice it to say that the company failed to detect and fix the misconduct (despite being notified of the misconduct by a whistleblower) before its Compliance 1.0 failures hit the prosecutor's desk and media headlines.

3) **GM's delayed ignition switch recall**: The classic poster child for "DIY Compliance" discussed briefly above is most notable for the mandate conflict that detoured the legal department from achieving the mandate of the compliance program. Even if the lawyers had understood the compliance mandate, they lacked the true compliance SME required to design and manage their program. A CCO with true compliance SME would have understood that the "69 Naughty Words" training was sending the wrong message to the organization and undermining the speak-up and trust culture that companies should be working hard to encourage.

4) **VW emissions fraud scandal**: The VW emissions fraud scandal is another widely publicized Compliance 1.0 collapse.[13] Like Walmart, the German auto giant emerged from its epic Compliance 1.0 failure by reaching for a true compliance SME (the former Daimler CECO), who was installed as a new member of the company's supervisory board. In 2016 the company installed a new CCO reporting directly to the CEO, with unfiltered access to the board.[14] In a 2017 interview, Stephanie Davis, the company's new CCO, commented:

> [t]he compliance function at VW Group of America has been newly elevated. I report to the chief executive, I sit on the executive team as a member of management, and that is new. I report directly to the CEO of VW Group of America and I have an independent relationship with the board, so I report at least on an annual basis to them. I am focused on making sure this never happens again. We still are complying with the terms of the consent decrees.[15]

5) **Wells Fargo fake accounts scandal**: The Wells Fargo fake accounts scandal, which resulted in a long list of terrible consequences, including a rare restriction on growth by the Federal Reserve Board, reflects a nearly perfect storm of Compliance 1.0 failures.[16] As Mike Volkov, former federal prosecutor and recognized thought leader for the compliance profession, has noted in his blog series on the matter:

> [emphasis added] *If someone asks you what was the most important lesson learned from the Wells Fargo fiasco, you can confidentially respond – the absence of an independent and empowered compliance function. It is easy to imagine how such a function, if it had a seat at the business table, would have responded to a proposed sales incentive program that rewarded sales staff based on the number of accounts opened rather than focusing on promoting customer service. Numbers of accounts bears no relation to quality of service, and in the end an ethics and compliance program officer would have pointed out the problem with the sales incentives program based on its skewed and illogical incentives.*[17]

The appalling breakdown of Wells Fargo's compliance processes could have been predicted by the compliance function's lack of authority, inadequate line of sight into risks and the business units, toothless oversight, and absence of a seat at the senior management table where incentives and culture were discussed, all in a highly decentralized operation. In fact, with a true compliance SME at the helm, the program could have been designed with the right checks, balances, and mechanisms necessary to bring the embattled bank's culture, compliance, and retaliation problems to the forefront where management could have addressed them before the scandals reached the attention of regulators and prosecutors. For instance, strict investigation guidelines (including confidentiality and non-retaliation monitoring) and training, as well as a nondiscretionary board escalation policy,[18] might have prevented the board from being blind-sided by the ever-expanding fake accounts scandal and the fact that over 5,300 employees had been fired in connection with the fraudulent activity, including many employees who had tried to report their concerns to the company's internal ethics line.[19] A true compliance

SME could have designed an investigation system and supporting infrastructure (including incentives) that would have helped the company to manage its risks more successfully. It is disheartening to think how an independent, empowered compliance and ethics function with clear authority and positioning could have made a difference in this perfect storm of a Compliance 1.0 train wreck. But at the same time, it is encouraging to see that government gatekeepers and policymakers in the US and around the globe are increasingly showing that they understand the value of a modern Compliance 2.0 function and program that is structured and built to succeed (and more than just window dressing), as discussed below.

Regulatory Scrutiny Around the World on the CECO Role (progress toward a consensus)

The Federal Sentencing Guidelines for Organizations (FSGO) set out for organizational compliance and ethics a roadmap of those elements viewed as critical to strong, effective programs, including senior management commitment and resources. An endless number of panel discussions and articles have been devoted to so-called "tone from the top,"[20] which is often mistaken by CEOs as "talk at the top" (as coined by Joe Murphy, recognized C&E expert and author of *501 Ideas for Your Compliance and Ethics Program*) [21] in the form of a video or annual letter to the troops. In fact, the most robust form of "high-level commitment"— one that is now heavily scrutinized by prosecutors and regulators—is the proper structuring and resourcing of the CECO position, and by extension, the overall compliance program. That is because how well the CECO is positioned is the single most important indicator of whether the program will succeed or fail. A board of directors or CEO who has established an independent, empowered modern Compliance 2.0 function and program shows by these very decisions their "high level commitment" to a strong compliance program that works to achieve its mandate and is more than mere window dressing. As discussed further here,[22] choices have consequences, and government gatekeepers are increasingly scrutinizing those choices.

For these reasons, the CECO position demands the close attention and deliberation of the governing authority. Under the FSGO, the board has a key role to oversee the company's compliance and ethics program, and this starts with ensuring that management has properly structured the CECO position.[23] In addition, the 2010 amendments to the FSGO reflected government's strong preference for the CECO to have "direct reporting obligations" to the governing authority, intended to create a direct CECO channel to the board (or independent board committee), unfiltered by any other senior officer. Former federal prosecutor Michael Volkov asks two basic questions to gauge the strength of a compliance program: "Does the [CECO] have independent authority and reporting access?" and "Does the [CECO] have the resources needed to carry out the job?"[24] This year, the Department of Justice and Securities Exchange Commission's Joint Resource Guide on the Foreign Corrupt Practices Act specifically observed that the CECO *[emphasis added] "must have appropriate authority within the organization, adequate autonomy from management, and sufficient resources to ensure that the company's compliance program is implemented effectively."*[25]

The CECO also has the attention of standard-setting bodies outside the US. In 2010, 38 signatory nations to the OECD Good Practice Guidance for Internal Controls, Ethics and Compliance[26] endorsed the CECO standard of a "senior corporate officer, with adequate level of autonomy from management, resources and authority." Similarly, the Canadian Competition Bureau has stated in its Corporate Compliance Programs brochure that the chief compliance officer *[emphasis added] "must be in a position to act effectively, in that there is independence, professionalism, empowerment, financial support and a solid understanding of what is taking place within the business."*[27] Focus on the empowered CECO continues worldwide. In 2012 the French Competition Authority adopted "Procedural Notice on the French Settlement Procedure," setting out the requirements for an effective compliance program, including a CECO who is *"empowered"* to implement and oversee the compliance program

[emphasis added] *"with the necessary autonomy and means to fulfill [the] role."*[28] Also in 2012, the Chilean competition agency (Fiscalía Nacional Económica, the "FNE") published new Guidelines on Competition Law Compliance Programs, including this specific guidance on the CECO role:

> Finally, to the extent that the degree of market power justifies it and there are sufficient resources, the person responsible for enforcing the correct implementation of the compliance program must have full autonomy and independence within the company (for example, that person reports directly to the Board of Directors and can be removed only under specifically defined conditions).[29]

The list of regulatory and standard-setting bodies around the world that are issuing guidelines for effective C&E programs continues to expand annually. These guidelines are increasingly addressing the seniority, positioning, empowerment, authority, independence, and resources assigned by companies to the CECO role. These include:

- Good Practice Guidance on Internal Controls, Ethics, and Compliance[30]
- UK Bribery Act[31]
- Anti-Corruption Ethics and Compliance Handbook for Business[32]
- Compliance Matters: What Companies Can Do Better To Respect EU Competition Rules[33]
- The ICC Antitrust Compliance Toolkit[34]
- Corporate Compliance Programs[35]
- Law on the Protection of Whistleblowers (Whistleblower Protection Act)[36]
- Guidelines for Competition Compliance Programs – Guidelines on the Structuring and Benefits of Adopting Competition Compliance Programs[37]
- ISO 37001 – Anti-bribery Management Systems [38]
- General Data Protection Regulation (GDPR)[39]

What the Surveys Tell Us

Recent well-regarded surveys underscore the fact that Compliance 2.0 is steadily becoming the modern model of compliance adopted by companies worldwide. According to reports, more compliance executives are confident and optimistic about their authority and agency, and are being afforded the tools and resources to fulfill their compliance mandate. According to Deloitte's 2016 survey, 60% of compliance professionals expected an increase in budget.[40] Even more promising is DLA Piper's 2017 Compliance Report, which found that 84% of compliance executives felt they had "sufficient resources, clout, and board access"[41] to run their compliance programs effectively, an increase from 77% in the DLA Piper 2016 survey.[42] Surveys such as DLA Pipers' also demonstrate an encouraging trend in CECO structuring, notably concerning the essential features of independence and C-suite inclusivity.

A strong indicator of this encouraging trend is the growing representation of stand-alone CCO/CECO positions in the compliance profession. While the percentage of stand-alone CCOs varies drastically on the size of the company in question, the 2015 Deloitte Compliance Trends survey found that 59% of respondents indicated their top compliance job is a stand-alone position, up from 50% in 2014 and 37% in 2013.[43] Gone are the days when companies in want of an official "chief compliance officer" could simply slap a new title on their GC and be done with it. Even former GE general counsel and highly vocal advocate for the in-house bar, Ben Heineman, agreed that "...the CCO's core job is to operationalize formal rules through engagement with the GC, CFO, and other experts and leaders within the company. Unless the company is very small and resource constrained, the GC should not also be the CCO."[44]

Equally crucial to the creation of a stand-alone role is the position, authority, and connectivity the CECO has within a business' hierarchy. A telling measure of the transition to 2.0 can be seen in the make-up of the C-Suite. In Deloitte's 2016 survey, 43% of respondents confirmed that the CCO held a seat on the CEO's executive management committee, or its equivalent.[45] Meanwhile, a consensus is being reached by compliance-savvy businesses that CCO reporting structures should evolve to reflect the trend of CCO independence and encourage the E&C function through empowerment. According to reports, more compliance executives are confident and optimistic about their empowerment and levers of authority, including direct reporting to the C-suite or higher. The percentage of compliance officers reporting to the CEO jumped from 25% to 39% from 2016 to 2017, while the percentage who reported to the GC or CLO dropped from 44% to 34%.[46] Likewise, the 2018 LRN Program Effectiveness Report found that 43% of boards have instituted a direct reporting channel from CECO to the board.[47]

What the Settlement Agreements Tell Us (the stakes have been raised)

Other clear indicia that the stakes have been raised are the number of settlement agreements and consent decrees that place the compliance function firmly in the spotlight. A long line of healthcare settlement agreements have yielded a now-standard undertaking, that the CECO "should not be, and should not be subordinate to, the general counsel or the chief financial officer."[48] More recently, prosecutors and regulators have taken aim at the compliance programs of large financial institutions involved in money-laundering, mortgage fraud, and LIBOR rate rigging, to name a few areas of headline-making scandals. In the HSBC settlement agreement, prosecutors not only demanded a separation of legal from compliance (independence), but also elevation of the CECO role to the top 50 managers (empowerment and seat at the table), revised reporting lines for firm-wide compliance officers (independence and line of sight), reformed mandate (empowerment), and a nine fold increase of the compliance budget (resources).[49] Major overhauls of compliance functions at other big banks tell a similar story.[50] Even in the absence of an actual settlement agreement, banks are feeling the heavy pressure from regulators and investors (and in at least one case, Senate investigating committees) and reforming their compliance functions to add one or more of the essential features discussed in this chapter.[51] At press time for this chapter, Citigroup is working on improvements to its anti-money laundering compliance program, first flagged in 2012 in a consent decree from one of its regulators.[52]

How can companies get ahead of this wagon train for effectively structured CECOs and compliance functions/programs? How can CECOs evaluating potential in-house positions better define their due diligence process? A review of the following essential CECO features is a start.