COSMOS
Navigate the Compliance Universe

CEP Magazine - July 2023

Jonny Frank (jfrank@stoneturn.com) is Partner for StoneTurn in New York, NY, USA.

Kat Nolan (knolan@stoneturn.com) is Senior Consultant for StoneTurn in New York, NY, USA.

Great expectations: Certification of ethics and compliance program effectiveness

By Jonny Frank, JD, LLM, and Kat Nolan, CPA, CFE

In March 2022, the United States Department of Justice (DOJ) Criminal Division Assistant Attorney General Kenneth Polite announced plans to require chief executive officers (CEOs) and chief compliance offices (CCOs) to certify the effectiveness of the ethics and compliance program as part of all non-prosecution agreements, deferred prosecution agreements, and plea agreements.[1] The U.S. Securities and Exchange Commission (SEC) often imposes a similar requirement.

DOJ's announcement has caused concern within the compliance community. Critics worry CEOs and CCOs will face undue personal liability and argue it would dissuade CCOs from accepting the roles. But certifications are not new, nor have they spurred lawsuits against individual members of management and dissuaded candidates from accepting promotions or appointments to senior roles.

The Sarbanes-Oxley Act, for example, has required public company CEOs and chief financial officers (CFOs) to certify the effectiveness of controls over financial reporting for almost 20 years. These certifications have not resulted in lawsuits against CEOs and CFOs absent intentional misconduct or gross negligence. Nor has Sarbanes-Oxley dissuaded candidates from accepting CEO and CFO positions.

As mentioned, compliance program certifications aren't new. DOJ has long required compliance monitors to certify compliance program effectiveness. Some monitors require management to certify compliance program effectiveness before the monitor certifies. And the new policy is a natural extension of the DOJ policy requiring certifications relating to disclosing information to DOJ.[2]

In May 2022, Deputy Attorney General Lisa Monaco defended the announcement, explaining DOJ intends CCO certifications to empower compliance officers, not punish them.[3] Further, the head of the DOJ's Foreign Corrupt Practices Act (FCPA) Unit predicted compliance certifications would ensure companies take compliance seriously and set CCOs up for success, not punishment.[4]

Companies should expect requests for compliance program certifications to expand beyond post-incident settlements. For example, counsel can use CCO and third-party certifications to demonstrate the effectiveness of the compliance program in effect when the misconduct occurred.[5] Counsel can also use certifications to meet DOJ *Evaluation of Corporate Compliance Programs*[6] and *Corporate Enforcement Voluntary Self-Disclosure Policy*[7] expectations companies use to test remediation and compliance program effectiveness, as well as the SEC Seaboard Factors.[8] Boards of directors and company management might use certifications to satisfy their duty

of oversight.[9]

Examples from recent DOJ plea agreements and SEC orders

In recent DOJ plea agreements and SEC orders, the government required CEOs and CCOs to certify the company's ethics and compliance program effectiveness, specifically related to the misconduct at hand.

The Glencore FCPA plea agreement, for example, requires the CEO and CCO to certify that the company implemented a compliance program that meets the requirements outlined in the plea agreement and that the program is "reasonably designed to prevent and detect violations of the Foreign Corrupt Practices Act and other applicable anti-corruption laws throughout the Company's operations."[10] Similarly, Danske Bank's plea agreement requires CEO and CCO certification that "the Bank's compliance programs are reasonably and effectively designed to deter and prevent violations of money laundering, anti-money laundering, and bank fraud laws throughout the Bank's operations."[11] The SEC's order against a Big Four accounting firm for cheating on training exams requires the CEO to certify the adequacy and effectiveness of the firm's integrity culture, ethics, and integrity training and guidance.[12]

Benefits of the compliance program attestations

Compliance program attestations provide benefits beyond satisfying government authorities. The certification process, if performed effectively, should:

- Identify opportunities to save costs, maximize revenues, and safeguard tangible and intangible assets;
- Enhance the power and prestige of the compliance function;
- Reinforce the first line of defense revenue-producing business units' risk ownership; and
- Demonstrate the organization's commitment to ethics and compliance.

Five critical steps when certifying effectiveness

Whether pre- or post-settlement, CEOs and CCOs should take these five critical steps before certifying the effectiveness of the ethics and compliance program.

Select a framework and criteria

A certification needs a framework from which the CEO and CCO can certify the effectiveness of the ethics and compliance program.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) risk management frameworks are the most logical because, for public companies, COSO is the de facto standard to identify and mitigate operational, compliance, and reporting risks.[13] Other acceptable frameworks include the U.S. Sentencing Guidelines criteria of an effective compliance program,[14] the DOJ Criminal Division's guidance on the *Evaluation of Corporate Compliance Programs* and subsequent policy statements like the "Monaco Memo,"[15] and the DOJ and SEC's FCPA resource guide.[16]

Although these frameworks have their differences, they include five common elements: (1) control environment, (2) risk identification and assessment, (3) risk response and control activities, (4) testing and monitoring, and (5) incident response and remediation. The company and CCO must define the criteria for these common

elements to assess the compliance program. For example, the company should consider various factors when evaluating the control environment, including the governance and structure, sufficiency, and autonomy of compliance personnel; three lines of defense risk management model; and the speak-up culture.

Identify and assess significant risks and scenarios

Risk identification and assessment form the cornerstone of an effective ethics and compliance program that companies should perform periodically based on continuous access to operational data and information.

Risk response and control activities comprise key policies, processes, and controls the company relies upon to prevent and detect reasonably likely and high-impact ethics and compliance risk events. The risk response or control activities should link to specific risks and include a combination of preventive, detective, manual, and automated control activities. Testing includes the company's program and processes to evaluate the design and test the operating effectiveness of the risk response and control activities.

Testing risk response and control activities must be independent. The control owner and business unit should not assess the risk response and control activities they developed or rely upon to mitigate ethics and compliance risks.

DOJ also expects companies to look at past misconduct. David Last, chief of the DOJ Criminal Division Fraud Section's FCPA unit, noted that prosecutors can consider misconduct years ago—especially if it involved similar misconduct or players. DOJ will consider whether the company conducted a root cause analysis, learned lessons, and enhanced its compliance programs in the wake of misconduct.[17]

Correct design and operating effectiveness deficiencies

Companies must assess the design and operation of the vital control activities identified above before certifying compliance program effectiveness.

Design effectiveness refers to whether the company's policies, processes, and controls—if they operate as prescribed by competent personnel—bring the risk within risk appetite. Operating effectiveness refers to how the policies, processes, and controls work in practice and the competency of personnel performing them.

Generally speaking, companies evaluate design effectiveness by (1) reviewing policies, processes, and controls, (2) conducting interviews and control walkthroughs with business personnel, and (3) evaluating vulnerability to collusion, override, and other circumvention methods. Companies assess operating effectiveness through (1) additional interviews and walkthroughs, (2) observations of controls and processes, (3) sample testing, (4) re-performance, and (5) competency assessment. Any weaknesses identified will be rated to determine if they equate to a deficiency, significant deficiency, or material weakness.[18]

In his remarks at The New York University School of Law's Program on Corporate Compliance and Enforcement, Polite explained DOJ considers "whether the company is continuously testing the effectiveness of its compliance program, and improving and updating the program to ensure that it is sustainable and adapting to changing risks."[19]

Implement a sub-certification waterfall

A practical and common approach for management certifications is establishing a sub-certification waterfall. Sub-certification entails identifying accountable owners throughout the organization to certify the compliance program's effectiveness in their responsible business.

By implementing a sub-certification waterfall, the company (1) assigns accountability for the effectiveness of the program throughout the organization, (2) provides valuable and timely information to the CEO and CCO to identify potential areas that require attention, (3) helps to socialize and strengthen the importance of the compliance program, and (4) displays the organization's commitment to compliance and reinforces the message that all employees are risk managers.

Test the certification

Besides the sub-certification, companies should arrange for independent testing by internal audit or a third party. Testing is essential if the certifications come after significant misconduct; a positive report will help counsel and the company demonstrate that the organization successfully enhanced its ethics and compliance program.

Conclusion

DOJ and SEC requirements for CEO and CCO certifications of the ethics and compliance program understandably sparked concern in the compliance community, but there is no cause for alarm. The benefits of compliance certifications far outweigh the risks if companies and their counsel address them rigorously as other certifications. Compliance certifications will boost the program's significance, prestige, and visibility and strengthen the program by reinforcing that the first line of defense revenue-producing business units own the risk.

Takeaways

- Corporate settlements often require chief executive officers (CEOs) and chief compliance officers (CCOs) to certify compliance program effectiveness.
- CCOs should expect requests for compliance program certifications aside from corporate settlements (e.g., board of director requests).
- CCO compliance program certifications provide benefits beyond satisfying regulator and prosecutor expectations, including identifying opportunities to save costs, maximize revenues, safeguard tangible and intangible assets, and enhance the CCO's power and prestige.
- Public companies can leverage their Sarbanes-Oxley Act financial reporting controls certification process.
- The CCO certification process includes (1) selecting a framework and criteria, (2) identifying and assessing significant ethics and compliance risks and scenarios, (3) correcting design and operating effectiveness deficiencies, (4) implementing a sub-certification waterfall, and (5) testing the certification.

1 Kenneth Polite, "Assistant Attorney General Kenneth A. Polite Jr. Delivers Remarks at NYU Law's Program on Corporate Compliance and Enforcement (PCCE)," March 25, 2022, New York, NY, remarks as prepared for delivery, https://www.justice.gov/opa/speech/assistant-attorney-general-kenneth-polite-jr-delivers-remarks-nyu-law-s-program-corporate.
2 Plea agreement, United States v. Glencore International A.G., (S.D. N.Y. 2022), https://www.justice.gov/criminal/file/1508266/download.
3 Al Barbarino, "DOJ Defends New CCO Certifications Amid Industry Worry,"*Law360*, May 26, 2022, https://www.law360.com/articles/1496108/doj-defends-new-cco-certifications-amid-industry-worry.
4 Anna Bianca Roach, "FCPA chief clarifies compliance certification efforts," *Global Investigations Review*, June

14, 2022, https://globalinvestigationsreview.com/just-anti-corruption/article/fcpa-chief-clarifies-compliance-certification-efforts.
5 U.S. Department of Justice, *Principles of Prosecution of Business Organizations*, §9-28.800, 2019, https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations.
6 U.S. Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs*, updated March 2023, https://www.justice.gov/criminal-fraud/page/file/937501/download.
7 U.S. Department of Justice, Criminal Division, *Corporate Enforcement and Voluntary Self-Disclosure Policy*, updated January 2023, https://www.justice.gov/criminal-fraud/file/1562831/download.
8 U.S. Securities and Exchange Commission, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions*, Release No. 44,969, October 23, 2001, https://www.sec.gov/litigation/investreport/34-44969.htm.
9 In Re McDonald's Corporation Stockholder Derivative Litigation, C.A. No. 2021-0324-JTL, 2023 WL 407668 (Del. Ch. Jan. 26, 2023), https://courts.delaware.gov/Opinions/Download.aspx?id=343130.
10 United States v. Glencore, Attachment H, 91-92, https://www.justice.gov/criminal/file/1508266/download.
11 Plea agreement, United States v. Danske Bank A/F (S.D. N.Y. 2022), https://www.justice.gov/opa/press-release/file/1557611/download.
12 In the Matter of Ernst & Young LLP, Exchange Act Release No. 95167 (June 28, 2022), ¶56, https://www.sec.gov/litigation/admin/2022/34-95167.pdf.
13 Committee of Sponsoring Organizations of the Treadway Commission, "Guidance on Internal Control," last accessed April 26, 2023, https://www.coso.org/sitepages/internal-control.aspx?web=1.
14 U.S. Sent'g Guidelines Manual §8B2.1 (U.S. Sent'g Comm'n 2013), https://guidelines.ussc.gov/gl/%C2%A78B2.1.
15 Lisa O. Monaco, "Further Revisions to Corporate Enforcement Policies Following Discussions with Corporate Crime Advisory Group," memorandum, September 15, 2022, https://www.justice.gov/opa/speech/file/1535301/download.
16 U.S. Department of Justice, Criminal Division, and U.S. Securities and Exchange Commission, Enforcement Division, *FCPA: A Resource Guide to the U.S. Foreign Corrupt Practices Act, Second Edition*, July 2020, https://www.justice.gov/criminal-fraud/file/1292051/download.
17 Ines Kagubare, "FCPA Unit chief clarifies DOJ approach to corporate recidivism," *Global Investigations Review*, December 9, 2021, https://globalinvestigationsreview.com/just-anti-corruption/corporate-liability/fcpa-unit-chief-clarifies-doj-approach-corporate-recidivism.
18 Public Company Accounting Oversight Board, "AS 2201: An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements," Release No. 2007-005A, June 12, 2007, https://pcaobus.org/oversight/standards/auditing-standards/details/AS2201.
19 Polite, "Remarks at NYU."