5 Tips For Meeting DOJ's New CCO Certification Requirements

By **Jonny Frank, Laura Greenman and Chris Hoyle** (June 30, 2022)

Jonny Frank

Laura Greenman

Chris Hoyle

In March, the U.S. Department of Justice Criminal Division Assistant Attorney General Kenneth Polite announced plans to require chief executive officers and chief compliance officers to certify to the effectiveness of the ethics and compliance program, particularly when the government does not impose a corporate monitor.[1]

The May Foreign Corrupt Practices Act plea agreement in U.S. v. Glencore International AG, in the U.S. District Court for the Southern District of New York, makes good on that plan and requires the CEO and CCO to certify the company met its compliance obligations under the agreement.[2]

Similarly, the April deferred prosecution agreement in U.S. v. Stericycle Inc., in the U.S. District Court for the Southern District of Florida, requires the company to certify that it "adopted and implemented all of the Monitor's recommendations."[3]

And the DOJ has signaled that CEO and CCO certifications will become a staple of all corporate settlement agreements.

Asking CEOs and CCOs to certify effectiveness of compliance programs sparked quite a ruckus. Critics worry CEOs and CCOs face undue personal liability and argue it will dissuade CCOs from accepting the role. But compliance certifications are not new. And the benefits of compliance certifications far outweigh the risks if companies and their counsel address them as rigorously as other certifications.

At a Securities Industry and Financial Markets Association anti-money laundering conference in May, Deputy Attorney General Lisa Monaco defended compliance officer certifications during a fireside chat.[4] She explained the DOJ intends CCO certifications to empower compliance officers, not punish them.

And at an International Bar Association conference in June, David Last, the head of the DOJ's Foreign Corrupt Practices Act Unit, predicted compliance certifications will ensure companies take compliance seriously and set CCOs up for success, not punishment.[5]

Under the Sarbanes-Oxley Act, CEOs and chief financial officers certify the effectiveness of controls over financial reporting, which is a certification of the effectiveness of the compliance program relating to the FCPA's controls and books and records requirements.

Some DOJ-imposed monitors require companies to certify the effectiveness of the compliance program before the monitor certifies. And the new policy is a natural extension of the DOJ policy requiring certifications relating to disclosing information to the DOJ.[6]

The U.S. Securities and Exchange Commission also requires certifications to compliance program effectiveness. The SEC's 2019 settlement with KPMG LLC required two certifications. First, as noted in the SEC's press release, during the independent consultant's work, the CEO must certify that KPMG implemented the independent consultant's

recommendations.[7]

Second, the CEO must certify the firm policies, procedures and controls "are adequate and sufficient to provide reasonable assurance of compliance with all professional standards relating to ethics and integrity."[8]

Compliance program attestations provide benefits beyond satisfying government authorities. First, the certification process, if performed effectively, will identify opportunities to save costs, maximize revenues, safeguard tangible and intangible assets, and enhance the CCO's power and prestige.

Second, certification strengthens the ethics and compliance program because it reinforces the first line of defense revenue-producing business units own the risk.

Third, a group-level certification boosts the significance, prestige and visibility of the compliance program.

Finally, if misconduct arises, certification demonstrates the company's commitment to ethics and compliance, helps it to defend the program in existence at the time of the misconduct[9] and obtained reduced penalties.[10]

Here, we present five critical steps CEOs and CCOs must take before certifying the effectiveness of the ethics and compliance program.

1. 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 risk management frameworks[11] are the most logical because for public companies, COSO is the de facto standard to identify and mitigate operational, compliance and reporting risks

Other acceptable frameworks include the U.S. Sentencing Guidelines criteria of an effective compliance program, the DOJ Criminal Division's guidance on Evaluation of Corporate Compliance Programs[12] and subsequent policy statements,[13] or the DOJ and SEC's FCPA resource guide.[14]

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.

Applying the selected framework, the company and CCO must define the criteria they will consider before making a certification. Below are criteria drawn from COSO and DOJ guidance. For each of these criteria, the company should develop detailed points to consider for conducting the program assessment.

Control environment considers and broadly includes:

- Commitment to compliance and integrity;

- Governance and structure;

- Sufficiency and autonomy of compliance personnel and resources;

- Senior and middle management oversight;

- Three lines of defense risk management model;

- Speak-up culture and confidential and other mechanisms to report misconduct anonymously;

- Effective risk-based training and communications for directors, officers, employees and, where appropriate, agents and business partners;

- Incentives for compliance and disincentives for noncompliance, including clear and consistent disciplinary measures;

- Due diligence and integration of mergers and acquisitions; and

- Third-party management.

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. Key elements include:

- Risk assessment policy, including risk appetite;
- Sufficiently granular risk taxonomy;
- Process to identify risks, including new and emerging risks;
- Risk-rating scale based on the likelihood of occurrence and significance of effect;
- Key control activities inventory; and
- Process for communicating and reporting.

Risk response and control activities comprise the key policies, processes and controls — collectively, risk response or control activities 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. An effective risk response includes adequate data science and analytics tools and data quality to maintain preventive and detective risk indicators for the company to act timely.

Testing includes the company's program and processes to evaluate the design and test the operating effectiveness of the risk response and control activities. Because of the volume of testing and specific skills required — e.g., data analytics, risk and controls testing — organizations are building compliance testing functions outside of internal audit.

Incident response and remediation includes:

- Incident identification;
- Triage;
- Investigation;
- Remediation; and
- Trend analysis and reporting.

Most large companies possess mature investigative functions. But few have a defined remediation framework. Nor do many organizations have risk and control experts skilled and experienced in conducting a comprehensive root-cause analysis, read-across for potential similar misconduct, lessons-learned analysis — including incorporation into risk assessments — and testing of corrective measures.

The DOJ also expects companies to look at past misconduct. David Last, chief of the Fraud Section's FCPA unit, noted prosecutors may consider misconduct years ago, particularly if it involved similar misconduct or players. The DOJ will consider whether the company conducted a root-cause analysis, learned lessons and enhanced its compliance programs in the wake of misconduct.[15]

2. Address design and operating effectiveness.

Design effectiveness standing alone cannot support certification. CEOs and CCOs must also consider operating effectiveness before certifying the effectiveness of the compliance program.

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.

Testing operating effectiveness requires the company to conduct field reviews at a sample of locations, where the team inspects documents, conducts interviews, performs walk-throughs, tests transactions and reperforms processes and controls.

In his remarks at NYU Law's Program on Corporate Compliance and Enforcement, Polite explained the 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."

He noted the DOJ is "also interested in how a company measures and tests its culture — at all levels of seniority and throughout its operations — and how it uses the data from that testing to embed and continuously improve its ethical culture. There is a separate question of whether a company is demonstrating an ethical culture in practice."

3. Test response to material ethics and compliance risks.

Companies assess risks in terms of likelihood — e.g., probable, reasonably likely, remote — and effect — e.g., material, important, observed. The combination of these risk factors forms a risk rating — e.g., significant, medium and low. Before certifying, the CEO and CCO should ensure the company audits the effectiveness of material risks.

Testing risk response or control activities must be independent. The control owner and business unit cannot audit the risk response and control activities they developed or rely upon to mitigate ethics and compliance risk. Because testing often reveals weaknesses, the CEO and CCO must exercise judgment on whether the weaknesses prevent certification.

Auditors use the terms "deficiency," "significant deficiency" and "material weakness" to rate weaknesses in internal controls over financial reporting, or ICFR. A clean audit opinion requires no single or combination of deficiencies rise to a material weakness.[16] CEO and CCOs should apply a similar analysis.

4. Implement a subcertification waterfall.

A practical and common approach for management certifications is to establish a subcertification waterfall.

In other words, companies identify accountable owners throughout the organization to certify the effectiveness of the compliance program in their responsible business. Companies utilize this method for various certifications, including the Sarbanes-Oxley Act and the Volcker Rule. A subcertification waterfall brings numerous benefits to an organization.

First, it assigns accountability for the effectiveness of the program throughout the organization. Second, it can provide the CEO and CCO with useful and timely information to identify potential areas that require attention. Third, it helps to socialize and strengthen the importance of the compliance program.

Subcertifications allow more employees to understand how their roles and responsibilities play a key role in the overall compliance program. Finally, it displays the organization's commitment to compliance and reinforces the message that all employees are risk managers.

5. Test the certification.

Just as Sarbanes includes an ICFR audit, companies should consider arranging for internal audit or similar function to test the CEO and CCO certifications of effectiveness of the compliance program.

Testing is particularly useful if the certifications come in the wake of significant misconduct.

A positive report will help counsel and the company demonstrate the organization successfully enhanced its ethics and compliance program.

Testing can save time and reduce cost if internal audit or other reviewer starts early and provides real-time assurance as the organization implements remediation.

Conclusion

The DOJ's plan to require CEO and CCO certification of the compliance program understandably sparked jitters. But there is no cause for alarm. Companies routinely have employees execute attestations and certifications. And the business and legal benefits outweigh the costs and risks.

Jonny Frank is a partner, Laura Greenman is a managing director and Chris Hoyle is a partner, at StoneTurn Group LLP.

[1] DOJ, Assistant Attorney General Kenneth A. Polite Jr. Delivers Remarks at NYU Law's Program on Corporate Compliance and Enforcement (PCCE) (2022) 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. SDNY (2022), https://www.justice.gov/usao-sdny/press-release/file/1508166/download.

[3] Deferred Prosecution Agreement, United States v. Stericycle Inc. S.D. Fl (2022), https://www.justice.gov/opa/press-release/file/1496416/download.

[4] A. Barbarino, DOJ Defends New CCO Certifications Amid Industry Worry, Law360 (May 2022).

[5] A. Roach, DOJ FCPA Chief Clarifies Compliance Certification Efforts, Global Investigations Review (June 2022).

[6] See, e.g., Deferred Prosecution Agreement, United States v. Deutsche Bank Aktiengesellschaft, EDNY (2021); Deferred Prosecution Agreement, United States v. The Boeing Company, ND Tex.(2021); Non-Prosecution Agreement, American Century Companies, Inc. (2021).

[7] KPMG LLP SEC Order , ¶73 (2019). See also Wedbush Securities Inc. SEC Order ¶35 (2021); KT Corporation SEC Order , No. 3-20780, ¶4 (2022).

[8] Id at ¶80.

[9] DOJ, Principles of Prosecution of Business Organizations, §9-28.800 (2019); US Sentencing Guidelines Commission ("USSC"), US Sentencing Guidelines ("USSG"); Effective Compliance and Ethics Program, USSG §8B2.1 (2020).

[10] USSC, Primer on Fines for Organizations (2022).

[11] See COSO, Internal Control — Integrated Framework (2013); COSO, Guidance on Enterprise Risk Management (2022).

[12] DOJ, Evaluation of Corporate Compliance Programs (June 2020).

[13] DOJ, Corporate Crime Advisory Group and Initial Revisions to Corporate Criminal Enforcement Policies (October 2021).

[14] DOJ Criminal Division and SEC Enforcement Division, FCPA Resource Guide, Second Edition (July 2020).

[15] I. Kagubare, FCPA Unit Chief Clarifies DOJ Approach to Corporate Recidivism. Global Investigations Review (December 2021) (available at https://globalinvestigationsreview.com/just-anti-corruption/corporate-liability/fcpa-unit-chief-clarifies-doj-approach-corporate-recidivism).

[16] PCAOB, AS 2201: An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements (2007).