5 Steps To Meet CFTC Remediation Expectations

By **Jonny Frank and Chris Hoyle** (November 28, 2023)

Jonny Frank

Chris Hoyle

In recent remarks announcing updates to U.S. Commodity Futures Trading Commission enforcement policies,[1] Enforcement Director Ian McGinley emphasized the importance of remediation in mitigating the consequences of being a recidivist and avoiding the imposition of an independent monitor or consultant.

The updated policy weighs the "robustness and effectiveness of remediation" in determining whether to consider a company a recidivist.[2]

Similarly, the CFTC will consider whether it has confidence that the entity will remediate its misconduct without the help of a neutral third party and oversight in deciding whether to impose a monitor or consultant.[3]

Cut to the chase: Organizations that remediate effectively receive lesser penalties and escape third-party oversight, while those that delay or fail to remediate face harsher penalties and an independent monitor or consultant.

From a business perspective, remediation should more than pay for itself by safeguarding assets, cutting costs and increasing revenues.

Take the Foreign Corrupt Practices Act, for example. Bribery requires employees to misappropriate company assets to pay government officials. It is just as likely — if not more probable — that employees will exploit control deficiencies to embezzle for personal use.

This article summarizes five key elements of effective remediation.[4]

1. Start immediately, and make all efforts to complete the remediation before resolution.

Some companies take the old-fashioned approach of waiting until the investigation is complete to begin remediation. But delaying is a mistake.

Promising the CFTC that the company will remediate invites the CFTC to impose a monitor or consultant. Showing the company has finished remediation before settlement increases the possibility of a nonprosecution or deferred prosecution agreement, reduces the monetary penalty and avoids independent oversight.[5]

And, as a practical matter, key stakeholders tend to be exhausted by the end of an investigation, which makes it harder to remediate.

2. Conduct a root-cause analysis.

A root-cause analysis forms the foundation of effective remediation and attempts to answer the following questions:

- Why did the offenders engage in misconduct?

- How did they rationalize their misconduct?

- What ethics and compliance deficiencies allowed the misconduct to occur and go undetected?

There is no prescribed method for conducting a root-cause analysis of compliance violations and corporate misconduct, but resources to leverage as a starting point include:

- The Committee of Sponsoring Organizations of the Treadway Commission's "Internal Control-Integrated Framework";[6]

- COSO's Fraud Risk Management Guide;[7]

- The U.S. Department of Justice's evaluation of corporate compliance programs; and

- Donald Cressey's "fraud triangle."

For example, according to Cressey's Fraud Triangle, named after the 20th-century criminologist Donald Cressey, three conditions exist whenever misconduct occurs: pressure or incentive, rationalization, and opportunity. Understanding and identifying these factors are critical steps in early remediation.

3. Perform a read-across analysis.

"Read across" refers to how organizations detect similar misconduct elsewhere in the company — e.g., other geographies, business units, etc.

Consider an auditing process called negative assurance, which is intended to provide comfort to the company — and, if requested, the government — that the organization took appropriate steps to determine whether others engaged in similar misconduct.

In this process, search for indicators of misconduct. If there are none, it provides "negative assurance" that the procedures detected nothing to indicate misconduct.

Suppose root-cause analysis reveals the controls are well designed but not operating effectively. There, test operating effectiveness in a sample of other locations to gain assurance that the wrongdoing was limited to a single individual or location.

The process becomes more difficult if the root-cause analysis concludes that the misconduct arose from significant design deficiencies.

The company must decide whether the likelihood and significance of the underlying deficiencies warrants conducting a forensic audit to search for indications of misconduct, e.g., artificial intelligence, data analytics, transaction testing, etc.

4. Implement a corrective action plan.

Corrective action plans include enhancements to entity-level controls — e.g., corporate culture, risk assessment processes, etc. — and transaction-level controls to prevent and timely detect misconduct.

Corrective actions include manual and automated enhancements and, in today's world, must consider forensic technology and artificial intelligence.

Because they typically involve multiple workstreams, corrective action plans require project management to coordinate and report on the status of the corrective action plans.

To save time and reduce costs, companies should conduct a "check and challenge" of the executability of the corrective actions and obtain real-time assurance that workstreams adequately completed corrective actions as they meet key milestones.

5. Test design and operating effectiveness.

Testing and certification includes design and operating effectiveness.

Design effectiveness considers whether the risk response — i.e., policies, procedures and controls to prevent and detect the risk — if performed as prescribed by people possessing the authority and competence, mitigates the risk within risk appetite.

Operating effectiveness tests how the risk response works and whether the people performing it have the requisite authority and competence.

Testing requires objectivity; that is, the testing function cannot review its own work. Nor can the testing function be an advocate. For these reasons, organizations typically rely on internal audit or an independent third party to perform testing.

Testing procedures should draw from generally accepted audit standards because the validation process is like an audit. These standards include requirements for planning, risk assessment, scaling, addressing fraud risk, using the work of others, materiality, and entity- and transaction-level controls.

Validation requires audit knowledge and experience. Testing procedures include inspection of documents, interviews, process walk-throughs, sampling, reperformance of processes and controls, and transactional analysis.

While government regulation is in constant evolution, organizations can lead on tried-and-true tools and experience to find their path forward.

The DOJ and U.S. Securities and Exchange Commisssion sometimes require companies to certify to remediation and compliance program effectiveness.[8]

Jonny Frank and Chris Hoyle are partners at StoneTurn Group LLP.

[1] CFTC, Remarks of Enforcement Director Ian McGinley at the New York University School of Law Program on Corporate Compliance and Enforcement: "The Right Touch: Updated Guidance on Penalties, Monitors, and Admissions" (October 2023) https://www.cftc.gov/PressRoom/SpeechesTestimony/opamcginley2.

[2] CFTC, CFTC Releases Enforcement Advisory on Penalties, Monitors and Admissions (October 2023) https://www.cftc.gov/PressRoom/PressReleases/8808-23. See generally CFTC Division of Enforcement, Enforcement Manual (May 2020) ("Enforcement Manual") https://www.cftc.gov/sites/default/files/2021-05/EnforcementManual.pdf.

[3] The CFTC distinguishes between Monitors and Consultants. The CFTC imposes a "Monitor" which the CFTC selects if "the pervasiveness and/or severity of the misconduct and/or the absence of effective controls is such that the Division lacks confidence that the entity will remediate its misconduct without the assistance of a neutral third party and oversight. The CFTC requires a "Consultant," which the company selects if "the evidence persuades the Division that the entity requires the assistance of a neutral third party to advise regarding remediation but can otherwise remediate its misconduct without oversight.""

[4] For a deeper discussion of remediation of misconduct, see J. Frank, Remediation, Litigation Services Handbook: The Role of The Financial Expert 5th Edition, Chapter 13a (2015) https://stoneturn.com/wp-content/uploads/2016/02/Remediation_Litigation_Services_Handbook.pdf.

[5] Enforcement Manual §§ 6-7, supra.

[6] Committee of Sponsoring Organizations of the Treadway Commission ("COSO), Internal Control-Integrated Framework (2013) https://www.coso.org/guidance-on-ic.

[7] COSO, Fraud Risk Management Guide (2023) https://www.theiia.org/en/content/communications/press-releases/2023/may/coso-releases-fraud-risk-management-guide-2nd-edition/.

[8] See generally Department of Justice Criminal Division. Evaluation of Corporate Compliance Programs. (March 2023) https://www.justice.gov/criminal-fraud/page/file/937501/download.