

SEPTEMBER
2023


Meeting DOJ and SEC Post-Settlement Obligations: A Practical Guide



Table of Contents

Introduction	3
Commitments and Breaches	5
Certifying Compliance Program & Controls Effectiveness	12
Reporting Misconduct Allegations	15
Making the Best of a Government Monitor	17
Notes	22
Our Team	24





Meeting DOJ and SEC Post-Settlement Obligations: A Practical Guide

Introduction

No Longer Just a Matter of Paying the Fine and Moving On.

Corporate settlement agreements used to be straightforward—pay the penalty and move on. Now, these resolutions rival complex business transactions, including months of negotiations and multi-year post-resolution obligations. Satisfying post-settlement commitments is a business imperative, not just a legal obligation. Meeting, if not exceeding obligations, helps restore brand value and improves employee and investor stakeholder confidence.

DOJ policy requires prosecutors to consider the effectiveness of the company's compliance program in determining whether to bring charges and in negotiating plea and other agreements.¹ Companies may secure leniency by having an independent third-party or senior management certify the compliance program and control's effectiveness or, if not ready for certification, report on the company's progress.

Adopting a business mindset toward post-resolution obligations will identify significant revenue and cost savings opportunities. Compliance controls enhancements eliminate and improve efficiency. StoneTurn, for example, worked with a global bank to reduce the number of "key controls" for 17 risk types from 2000 to 200 controls. Layering this business mindset with a risk-based approach saved the bank untold time and money.

How a company addresses post-settlement obligations can go a long way in building (or re-building) government trust, which is critical if serious compliance issues arise. (The government estimates that between 10% and 20% of large corporate criminal resolutions have involved recidivist companies.)²

The consequences of violating post-resolution obligations are severe. One party (the government) decides whether a breach occurred. Under DOJ settlement agreements, the government can prosecute the organization for the underlying conduct and use any information the company provided at trial. And breaches are not academic. DOJ has committed to "hold accountable any company that breaches the terms of its DPA or NPA" and impose "serious consequences for violating their terms."³ DOJ rescinded Ericsson's DPA, forced the company to plead guilty and imposed a \$200 million+ penalty for breaching its DPA.⁴ Deutsche Bank incurred a one-year extension of its corporate monitorship for violating its DPA.⁵

Step-By-Step Post-Settlement Guide

StoneTurn developed this Post-Settlement Guide to help companies and their external counsel prepare for and manage post-resolution obligations. Our suggestions draw from StoneTurn's cross-disciplinary and industry expertise; past experience as regulators, auditors and prosecutors; our team's many risks and controls engagements; and years of experience serving as government-imposed and voluntary compliance monitors and consultants.

The Post-Settlement Guide includes four sections organized around requirements for DOJ non-prosecution agreements (NPA), deferred prosecution agreements (DPA), and plea agreements. The SEC and other agencies impose similar obligations (e.g., HHS Corporate Integrity Agreements).

- 1 Commitments & Breaches.** The Guide begins with basic steps companies should take to meet obligations and avoid breaches. These steps include starting early; developing an obligations register; conducting a root cause analysis to identify compliance program elements requiring remediation; creating a governance structure, developing assessment criteria, expected evidence and validation procedures; performing a "check and challenge" of the executability of corrective action plans; conducting "real-time" testing to keep the project on track; identifying and mitigating breach risks and scenarios; and keeping a "good deeds" scrapbook to evidence the company's good faith efforts in the event of a breach.
- 2 Certifying Compliance Program Effectiveness.** We follow with steps to meet DOJ and SEC requirements for senior management to certify compliance programs and controls effectiveness and how public companies can leverage their Sarbanes-Oxley processes to avoid duplication of efforts. Key steps include selecting a framework and criteria; identifying and assessing significant ethics and compliance risks and scenarios; evaluating the design and operating effectiveness of the risk response; executing a corrective action plan to cure deficiencies; implementing an evidence-based sub-certification waterfall; and arranging for an independent third party or internal audit to validate that the program meets the framework and criteria.
- 3 Duty to Report Misconduct Allegations.** The Post-Settlement Guide next considers DOJ's requirement for CEOs and CFOs to certify personally that the company reported to DOJ evidence or allegations of violations of the criminal laws that gave rise to the settlement. We suggest ensuring that all employees understand the obligation; developing an inventory of potential sources, recipients, reporters, and escalation systems; identifying reasonably likely breach scenarios and evaluating the effectiveness of the company's risk response; establishing a process to escalate misconduct allegations to the right decision-makers; and protecting the CEO and CFO with evidence-based sub-certifications and independent testing.
- 4 Making the Best of a Government Monitor.** The Post-Settlement Guide concludes with practical steps to prepare, liaise and maximize the value of a government-imposed monitor or independent consultant, starting with behaving like a client, not a criminal defendant and avoiding an adversarial relationship. We also suggest identifying the objectives and benefits of the monitorship; developing proposed assessment criteria; selecting candidates wisely; investing in an effective project management office; and collaborating on the Monitor's work plans and recommendations.

Commitments and Breaches

This section begins with tips for meeting post-settlement compliance obligations and follows with tips for avoiding breaches.

A. Meeting Post-Settlement Compliance Obligations

Organizations should address all criminal conduct, not just the specific violation. DOJ settlement agreements often include the corporate defendant's agreement "to commit no further crime."⁶ And, even if not explicit in the settlement agreement, the DOJ's updated criminal enforcement policy is tough on corporate recidivists, requiring prosecutors to "consider the full criminal, civil, and regulatory record of any company when deciding the appropriate resolution."⁷

- **Scenario-Based Risk Identification.**

Companies tend to limit risk identification to laws and regulations, not the scenarios that give rise to the violation. For example, breaching the Foreign Corrupt Practices Act (FCPA) is a legal risk; risk mitigation requires the identification of the fact patterns that are reasonably likely to materialize into an FCPA violation (e.g., vendor overpayments, excessive sales discounts, fake charitable contributions). To get to the scenario level, companies should include and brainstorm with the first line of defense (1st LoD) business personnel familiar with the ins and outs of the business.

- **Reliance on Ineffective Controls.**

Linking controls to risks is essential but too often not done. Companies and auditors tend to evaluate controls individually and focus on control objectives. However, meeting control objectives is different from mitigating risk.

Forensic auditors assess whether the suite of processes and controls ("control suite") brings the compliance risk scenario within risk appetite

Takeaways

- Address all potential criminal conduct, not just the specific violations leading to the settlement.
- Start now—don't wait for the company and government to finalize settlement terms.
- Create an obligations register.
- Conduct a root cause analysis to identify items requiring remediation.
- Create a governance structure and form a multi-disciplinary project team.
- Develop assessment criteria, expected evidence and validation procedures.
- Check and challenge the executability of corrective action plans and monitor completion.
- Conduct "real-time" testing to keep the project on track.
- Identify and mitigate breach risks and scenarios.
- Keep a "Good Deeds" scrapbook.

(i.e., the amount of risk an organization is willing to take to meet objectives). Forensic auditors evaluate and test whether the control suite is vulnerable to override, collusion, or other circumvention and whether it operates effectively, including the competency of the persons performing the controls. Given the consequences of recidivism, companies operating under a corporate resolution should reconsider the adequacy of their testing program.

- **Forensic Data Analytics.** Forensic data analytics is the corporate equivalent of smoke detectors. And even though DOJ policy emphasizes the importance of data analytics,⁸ most companies have only a rudimentary or developing data analytics strategy.⁹

Failure to invest in data analytics could be costly for organizations. The SEC and DOJ have publicly stated that they are actively using data analytics to identify irregular trends that might indicate criminal activity and require the department's attention. They have also reaffirmed an ongoing commitment to using and understanding the latest technological advances to identify potential misconduct proactively.¹⁰

Forensic analytics requires collaboration between forensic data analytics and risks and controls experts. Risk and controls experts know the red flags. Forensic data analytics experts know how to search through data to identify red flags before the misconduct becomes a three-alarm fire.¹¹

Start Now—Don't Wait to Finalize the Settlements. Post-resolution obligations require advanced preparation and dedicated resources, including governance, project management, dedicated multi-disciplinary skills, participation from all three lines of defense, and technological solutions. It is easy to anticipate the post-resolution commitments the DOJ and SEC require because both agencies rarely vary from prior agreements. Recent settlement agreements provide a detailed roadmap of what to expect.

Besides preparation, early planning is necessary to secure senior management's interest. Settling criminal and regulatory investigations is time-consuming and emotionally exhausting. Senior management's engagement—and appetite to invest resources—waned as soon as the company and government finalize settlement terms. Don't wait for the final settlement to prepare and line up resources.

Form a Steering Committee and Post-Resolution Project Office. Most companies create a governance structure comprised of a Steering Committee reporting to a Board Committee or senior management and a Post-Resolution Office (PRO) or Project Management Office (PMO) reporting to the Steering Committee. Governance helps avoid the natural tendency for companies to de-prioritize the settlement agreement and ensures efforts to comply with obligations remain on track.

Staff PRO/PMO with Multi-Disciplinary, Cross-Functional Resources. Meeting government obligations typically requires a handful of dedicated resources, although more will be necessary if the settlement includes a government-imposed monitor or consultant. The team should be knowledgeable of the industry and day-to-day business operations. Choose a well-respected, rising leader and recruit a team skilled in risk identification and mitigation, controls development and testing, data analytics, project management, root cause analysis, and implementing corrective actions.

Some companies assign only legal and compliance personnel to the PRO/PMO. However, including well-respected personnel from the business segments subject to post-resolution obligations is more effective and efficient.

Engaging the Three Lines of Defense (3LoD)



Companies must engage all 3LoD in meeting its post-resolution obligations.

For example:

- **1st LoD (Risk Owners)** – Accountable for identifying, owning and mitigating risks
- **2nd LoD (Risk and Control Functions)** – Responsible for design of risk and control management frameworks and monitoring
- **3rd LoD (Independent Assurance)** – Responsible for providing independent assurance on the effectiveness of Compliance Program

Create Measurable Assessment Criteria. DOJ and SEC resolution agreements require companies to take affirmative steps to enhance compliance controls. DOJ agreements on a disaggregated basis include over 30 obligations (e.g., fostering a high-level commitment to compliance; developing policies, procedures and controls to prevent and detect the misconduct that gave rise to the settlement; conducting periodic risk assessments; ensuring proper oversight; providing training and guidance; establishing an effective system for internal reporting; enhancing investigation and consequence management processes; managing third-party relationships; and testing the design and operating effectiveness of the compliance program and controls).¹²

Under DOJ agreements, companies must submit to the government work plans for enhancing and testing the compliance program and controls.¹³ Companies must also meet periodically and submit written reports on their progress and testing results to the government.¹⁴

Like Sarbanes-Oxley financial reporting certifications, companies must base their assessments on generally accepted frameworks and objective evidence. DOJ’s 2023 [Evaluation of Corporate Compliance Programs \(ECCP\)](#) and Committee of Sponsoring Organizations of the Treadway Commission’s (COSO) 2023 [Fraud Risk Management Guide: Second Edition](#) standards provide an excellent starting point. Companies, however, must customize the framework to their organization and decide upfront the evidence they will rely on to support their assessment and if required, certifications.¹⁵ We also suggest developing validation procedures upfront.

Below is a sample assessment criteria document. For illustrative purposes, we populated the table with the criteria, points to consider, expected evidence and validation procedures to assess boards of directors’ oversight of the compliance program.¹⁶

Table One: Sample Assessment Criteria Document

Topic	Points to Consider	Evidence	Validation Procedures
Commitment to ethics and integrity (DOJ Agreement, Attachment C ¶1)	<p>Does the Board:</p> <ul style="list-style-type: none"> • Include members with compliance experience; • Provide strong, explicit, visible support and commitment to compliance programs; • Oversee compliance risk assessments, internal investigations, and remediation efforts; • Evaluate the ethics and compliance program; • Require management reporting on the compliance and ethics program; • Ensure management maintains proper oversight of subsidiaries, affiliates, joint ventures, vendors and other third parties; • Factor management’s commitment to compliance in setting compensation; and • Prioritize ethical conduct over business objectives? 	<ul style="list-style-type: none"> • Board agendas. • Meeting minutes. • Communications to management regarding ethics and compliance. • Communications regarding major business decisions. (e.g., location of operations, service offerings, clients, vendors.) • Documentation evidencing Board oversight of control functions. 	<ul style="list-style-type: none"> • Review agendas and minutes. • Review Board communications to management. • Interview Board members.

“Check & Challenge” Corrective Action Plans.

Establishing detailed criteria, expected evidence and anticipated validation procedures upfront enables companies to identify deficiencies and opportunities for enhancements, cost savings and increased efficiency. Companies typically organize into workstreams to address these issues and, as a first step, require workstreams to develop corrective action plans.

Corrective action plans should have a consistent format that allows bundling into a single, integrated program. Corrective action plans should (1) describe the initiative; (2) itemize the work steps; (3) assign responsibility and accountability; (4) establish milestones and target dates; (5) identify required resources; and (6) note dependencies (e.g., technological solutions).

Table Two: Sample Summary Corrective Action Plan

Enhance the Compliance Risk Assessment Framework			
What: Enhance the Compliance Risk Assessment framework to define the approach, scope and process to identify and assess the Company’s most material compliance risks and meet regulatory requirements. Steps include identifying and assessing the inherent risks applicable to Company’s business activities; assessing design and testing operating effectiveness of key preventive and detective controls; quantifying the residual risks; and identifying instances that exceed the risk appetite.			
Why: The 1 st and 2 nd LoD need to understand the material risks and what controls the organization relies upon to mitigate the risks to identify any residual risks which exceed the Company’s risk appetite.			
How: Collaboration between the 1 st and 2 nd LoD in defining the methodology to develop and implement the framework across the organization.			
Accountable Party: CCO		Responsible Party: Deputy CCO	
Milestones		Deadline	Status
1	Identify resources required for conducting the Compliance Risk Assessment.	March 2023	Completed
2	Draft methodology and overall Framework documents.	May 2023	Completed
3	Finalize methodology and Framework documents.	June 2023	Completed
4	Conduct Training on Compliance Risk Assessment.	July 2023	In Progress
5	Implement the Compliance Risk Assessment.	September 2023	Not Started
6	Issue Compliance Risk Assessment Reporting to management.	December 2023	Not Started
Risks and Dependencies		Other Comments	
Technology development of Compliance Risk Assessment platform.			

StoneTurn recommends that an independent third party “check and challenge” the executability and monitor the completion of corrective action plans. The quality of corrective action plans will vary significantly, particularly in large remediation projects involving multiple workstreams. Workstreams invariably underestimate the time and resources necessary to complete milestones and inadequately account for dependencies and other obstacles. “Check and challenge” helps to drive consistency and on-time projects.

Implement a Project Dashboard. Project dashboards enable the PRO/PMO to track and report on the status of the efforts to meet post-resolution obligations. Dashboards can be as simple as manually prepared spreadsheets. However, most companies engage in-house or third-party data experts to customize the dashboard.

Value of a “Check & Challenge”



Third Party Validation of Corrective Action Plans Enables Companies to Identify Potential Remediation Pitfalls

- Is the timeline realistic and achievable?
- Are there sufficient resources to complete the remediation?
- Will the corrective actions adequately address the root cause(s) of the deficiency?
- Are there material risks and dependencies to completing the remediation?
- Is the accountable owner appropriate?
- Is the scope of the remediation sufficient?

Table Three: Sample Project Dashboard

Workstream	Maturity Status		Design Effectiveness		Operating Effectiveness	
			Testing Status	Rating	Testing Status	Rating
1. Culture of Integrity and Compliance	Designed		In Progress		Not Started	
2. Three Lines of Defense Framework	Operational		Completed	Effective	In Progress	

Perform Frequent and Real-Time Testing and Assurance. The DOJ ECCP devotes an entire section to “Continuous Improvement, Periodic Testing, and Review.”¹⁷ In determining whether to file charges and what penalty to impose, Federal prosecutors must assess whether the company proactively audits the program’s effectiveness and revises it based on lessons learned. Similarly, when determining whether to impose a corporate monitor, DOJ considers “if, at the time of the resolution, the corporation has adequately tested its compliance program” and suggests prosecutors to consider imposing a monitor if the company’s “compliance program and controls are untested.”¹⁸

Testing typically occurs at two levels. The PRO/PMO should validate that the workstream met the milestone before it marks and reports to the Steering Committee that the milestone is closed. Companies also arrange for a third-party consultant or the internal audit function to conduct independent testing. Most opt for an independent consultant known to the government, particularly if the settlement agreement requires the CEO and CCO to certify the compliance program.

Testing should cover design and, after implementation, operating effectiveness. Testing procedures draw from generally accepted audit standards because the validation process is akin to an audit.¹⁹ These standards include requirements for planning, risk assessment, scaling, addressing

fraud risk, using the work of others, materiality, and entity and transaction-level controls.

“Design effectiveness” considers whether the risk response (i.e., policies procedures and controls to prevent and detect the risk), if performed as prescribed by persons possessing the necessary authority and competence, mitigates the risk within risk appetite. Operating effectiveness tests how the risk response works in practice and whether the persons performing it possess the necessary authority and competence.²⁰

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

B. Avoiding & Mitigating Breaches

Conduct a Breach Risk Assessment. Just as risk assessment forms the foundation of an effective compliance program, so does it underpin avoiding post-resolution breaches. A risk-based approach allows the company to prioritize its resources and demonstrate its efforts to comply with the settlement agreement in case of a breach.

Breaches tend to arise from the unexpected. Convene a group of legal, compliance and business personnel to identify the scenarios that might give rise to a breach. After identifying potential risks and scenarios, evaluate the probability and impact on an inherent and residual basis. Be careful not to underestimate the consequences of a potential breach nor the likelihood that the government will discover the violation.

Table Four: Sample Breach Risk Assessment

Ref.	Obligation	Scenario	Response	Mitigation
A1	Should the Company learn of any evidence or allegation of conduct that may constitute a violation of the FCPA antibribery or accounting provisions had the conduct occurred the Company shall promptly report such evidence or allegation to the [Regulator].	A supervisor does not report allegations received from employees because the supervisor regards the allegation as factually incorrect.	<ol style="list-style-type: none"> Including misconduct allegations as a standard agenda topic. Supervisor sub-certifications. 	Independently test whether meetings include allegations as a standard agenda item.

Reduce Out-of-Appetite Risks.

A risk-based approach sets risk appetite and responds to risks and scenarios outside risk appetite. Develop and implement enhanced processes and controls to reduce out-of-appetite breach risks to an acceptable level.

For example, DOJ settlement agreements require companies to inform the government of allegations it receives relating to the illegal conduct at issue in the investigation.²¹ Evidencing the importance it places on this obligation, DOJ requires the CEO and CFO to certify that the company has satisfied this reporting requirement.

It is easy for large companies to breach this obligation because they typically have many channels for receiving allegations (e.g., media and regulator inquiries). The Ericsson and Deutsche Bank post-settlement violation agreements demonstrate that the consequences for failing to report misconduct are severe.²² Companies can mitigate this risk by adopting processes and controls to collect and funnel all misconduct allegations to a central function to decide whether it must report the issue.

Keep a Good Deeds Scrapbook. Companies can mitigate breaches by demonstrating good faith efforts to comply with post-resolution obligations.

However, companies need to keep contemporaneous records of their activities and accomplishments. Obtaining proof after the breach is difficult and less persuasive.

StoneTurn recommends that the PRO/PMO maintain a contemporaneous diary of examples. We refer to this exercise as keeping a good deeds scrapbook (e.g., turning down revenue opportunities because of ethical concerns). These examples will go a long way if the company defends a breach.

Good Deeds Scrapbook



Take credit for and document the strengths of your Compliance Program. Companies who have no evidence (e.g., a whistleblower program with no reports) of the Compliance Program working are at a disadvantage.

Good Deeds may include:

- Declining business due to potential ethical concerns.
- Performing read across analyses in other businesses/regions for breaches identified in one business/region.
- Documentation of positive speak up culture (e.g., whistleblower allegations which were investigated through completion).

Certifying Compliance Program & Controls Effectiveness

DOJ Requires CEOs & CCOs to Certify Compliance Program Effectiveness. In 2022, DOJ instituted a policy requiring CEOs and CCOs to certify the effectiveness of the ethics and compliance program as part of NPAs, DPAs and plea agreements.²³ The SEC enforcement orders often carry a similar requirement albeit limited to the CEO, not the CCO.²⁴

DOJ's announcement caused considerable 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 from company officers are not new, nor have they spurred lawsuits against individual members of management or dissuaded candidates from taking these positions. Sarbanes-Oxley, for example, has required CEO and CFO certifications for almost 20 years.

Nor are compliance program certifications 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. The new policy is a natural extension of the DOJ policy requiring certifications relating to disclosing information to the DOJ.²⁵

In May 2022, Deputy Attorney General Lisa Monaco defended the announcement, explaining DOJ intends CCO certifications to empower compliance officers, not punish them.²⁶ Further, the head of the DOJ's FCPA Unit predicted compliance certifications would ensure companies take compliance seriously and set CCOs up for success, not punishment.²⁷

[Note: A previous version of this section appeared under the title, *Great Expectations: Certification of Ethics and Compliance Program Effectiveness*, in the July 2023 issue of Compliance and Ethics Professional Magazine published by the Society of Corporate Compliance and Ethics. Copyright 2023 CEP Magazine, a publication of the Society of Corporate Compliance and Ethics (SCCE).]

Takeaways

- Corporate settlements often require CEOs and CCOs to certify compliance program effectiveness.
- Expect requests for compliance program certifications aside from corporate settlements (e.g., board of directors).
- 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.
- Leverage past DOJ and SEC settlement agreements to anticipate the terms.
- Utilize the Sarbanes-Oxley Act financial reporting controls management assertion and external auditor audit processes.
- Before the CEO and CCO/CECO certify:
 1. Select a framework and criteria.
 2. Identify and assess significant ethics and compliance risks and scenarios.
 3. Evaluate the design and operating effectiveness of the risk response.
 4. Execute a corrective action plan to cure deficiencies.
 5. Implement an evidence-based sub-certification waterfall.
 6. Have an independent third party or internal audit validate that the program meets the framework and criteria.

Compliance Certifications Likely to Reach Beyond Post-Settlement Obligations. 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 compliance program's effectiveness when the misconduct occurred.²⁸ Counsel can also use certifications to meet DOJ *ECCP*, DOJ *Corporate Enforcement Voluntary Self-Disclosure Policy*²⁹ and the SEC Seaboard Factors³⁰ expectations companies use to test remediation and compliance program effectiveness. Boards of directors and company management might use certifications to satisfy their duty of oversight.³¹

DOJ Settlement Agreements and SEC Orders Illustrate Certification Terms. Companies and counsel can review past DOJ and SEC settlement agreements to anticipate the terms. For example, Glencore's FCPA plea agreement requires the CEO and CCO to certify that the company implemented a compliance program that 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."³² 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."³³ 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.³⁴

Benefits Beyond Meeting Post-Resolution Obligations. 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.

Critical Steps for Certifying Compliance Program Effectiveness.

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



Select a Framework and Criteria. Certification requires a framework against which the CEO and CCO measure and certify compliance program effectiveness. Sarbanes-Oxley, for example, requires management to identify its framework underpinning the certification of financial reporting controls effectiveness.

The COSO risk management frameworks are the most logical. Because most companies already use COSO as the framework for certifying financial reporting controls' effectiveness, they can apply the same process to certify compliance controls' effectiveness.³⁵ Other acceptable frameworks include the DOJ ECCP and the U.S. Sentencing Guidelines criteria of an effective compliance program,³⁶ and the DOJ and SEC's FCPA Resource Guide.³⁷

- StoneTurn suggested steps to establish assessment criteria in **Section One** of this guide.
- Employ those same steps to develop the CEO and CCO certification criteria.



Identify and Assess Significant Ethics & Compliance Risks and Scenarios. Risk identification and assessment form the cornerstone of an effective ethics and compliance program. 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 consists of the company’s program and processes to evaluate the design and test the operating effectiveness of the risk response and control activities.

The company should arrange independent testing to support the CEO and CCO’s certifications.

Control owners and business units are not independent. Instead, CEOs and CCOs should rely on testing by an independent third party or internal audit, assuming the function is independent.



Evaluate the Design and Test the Operating Effectiveness of the Risk Response. Companies must assess the design and test the operating effectiveness of their response to ethics and compliance risks utilizing a risk-based approach. As we discuss in [Section One](#), design effectiveness refers to whether the company’s policies, processes, and controls—if they are performed as prescribed by personnel with the necessary authority and competency to perform the control —bring the risk within risk appetite. Operating effectiveness refers to how the policies, processes, and controls work in practice and whether the personnel performing the control possess the necessary authority and competency to perform the control effectively.

Companies evaluate design effectiveness by: (1) reviewing policies, processes and controls; (2) conducting interviews and control walkthroughs with business personnel; (3) evaluating vulnerability to collusion, override and other circumvention methods; and (4) competency and authority assessment. Companies validate operating effectiveness through: (1) additional interviews and walkthroughs; (2) observations of controls and processes; (3) sample transaction testing; (4) re-performance; and (5) competency and authority assessment.



Execute a Corrective Action Plan to Cure Deficiencies. [Section One](#) outlines StoneTurn’s steps for developing and executing corrective plans to bring the risk response within risk appetite. Those same steps apply to the CEO and CCO certification process.

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. The sub-certification process should require attestors to maintain evidence on which their attestation relies.

By implementing an evidence-based 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.



Arrange Independent Testing. 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. Maintaining documentation of periodic tests and reviews helps to support the overall certification and evidence that the company engaged in meaningful efforts to review its compliance program.

Reporting Misconduct Allegations

DOJ corporate settlement agreements require companies to “promptly report” to DOJ “any evidence or allegation of misconduct that may constitute a violation of the criminal laws that gave rise to the settlement, including foreign conduct that would have been illegal if it had occurred in the U.S.”³⁸ The government regards this obligation so seriously that DOJ requires the CEO and CFO to certify personally that (1) they are aware of the company’s disclosure obligations and (2) the company reported all disclosable information.³⁹

The obligation seems straightforward. But, as we discussed, the Ericsson⁴⁰ and Deutsche Bank⁴¹ cases demonstrate the severe consequences if the DOJ becomes aware of misconduct allegations the companies failed to disclose to them directly.

Here, we present critical steps companies should take to meet and avoid breaches of disclosure obligations and to protect CEOs and CFOs before they certify personally that the company has completed its disclosure obligations.

Communicate Reporting Requirements Across the Company. Because the commitment extends company-wide, all employees must understand the reporting obligation. And, if a breach occurs, the company cannot afford to explain that employees were not aware of their duty to report.

Senior management should send an initial communication stressing the seriousness of the commitment and emphasizing that it applies throughout the company. Business and infrastructure function leaders should reinforce the message in emails, town halls, intranet postings, newsletters and other communications.

Some companies include the disclosure obligation as a standing agenda at all company meetings. Albeit monotonous, including it as a standing agenda item bolsters its importance.

Develop an Inventory of Channels, Escalation Systems, and Tools.

Incidents or allegations of suspected or actual criminal conduct (collectively “misconduct allegations”) can arise from numerous channels, including hotlines, employees, comments to supervisors, media and regulatory inquiries, customers, vendors, etc. Differentiate among sources, reporters, and receivers.

The inventory helps determine where to develop and implement policies, processes and controls and facilitates proper risk assessment and control testing.

To avoid issues falling through the cracks, companies should create an inventory of (1) potential sources and reporters; (2) receiving and escalation channels; and (3) systems and tools the receiving and escalation channels use to ensure they capture and report allegations of criminal conduct.

Takeaways

- Corporate settlements require CEOs and CFOs to certify personally that the company reported to DOJ evidence or allegations of violations of the criminal laws that gave rise to the settlement.
- Because the commitment extends company-wide, all employees must understand the reporting obligation.
- Develop an inventory of potential sources, recipients, reporters and escalation systems.
- Identify reasonably likely breach scenarios.
- Evaluate the effectiveness of the company’s risk response.
- Establish a process to escalate misconduct allegations to the right decision-makers.
- Protect the CEO and CFO with evidence-based sub-certifications and independent testing.

Identify Potential Breach Scenarios.

As discussed in **Section One**, the best defense against breaches is to anticipate how they might materialize. For example, violations have occurred because receivers mistakenly believed the allegation had been closed, non-U.S. employees did not understand the reporting obligation, and internal counsel erroneously concluded the alleged misconduct did not constitute a potential violation of the law(s) requiring disclosure.

Identifying potential breach scenarios should include workshops involving business and control function representatives who understand the channel processes and likely misconduct risks.

The discussions should focus on identifying:

(1) scenarios (e.g., receiver not recognizing an allegation is being made) that might lead to a failure to identify, escalate and report allegations of criminal conduct; (2) controls or other mitigating factors in place to prevent or timely detect failure to escalate or report allegations of criminal conduct; and (3) impact on the risk profile.

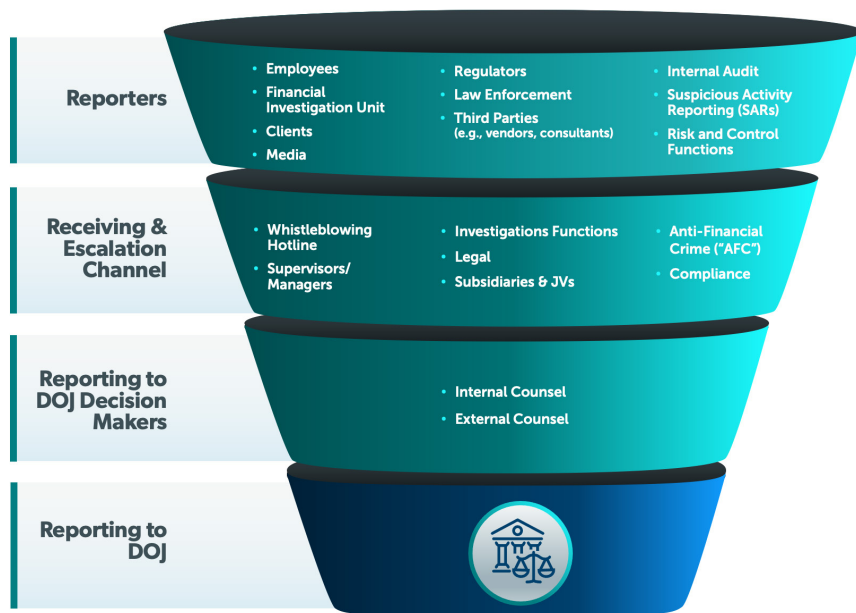
Evaluate the Effectiveness of the Risk Response. Companies must assess the design and test the operating effectiveness of their escalation and reporting policies and processes, as well as the controls to prevent or timely detect failure to escalate and report allegations of criminal conduct. **Section One** outlines StoneTurn's steps for conducting design and operational effectiveness testing.

Cure Deficiencies. **Section One** outlines StoneTurn's steps for developing and executing corrective plans to bring the risk response within risk appetite. Those same steps apply to the escalating and reporting misconduct allegations process.

Establish a Process to Escalate Misconduct Allegations to the Right Decision-Makers. Most companies rely on internal and external counsel to decide whether to report a misconduct allegation to DOJ. The company must develop a process to triage and ensure all potentially reportable matters reach the team charged with responsibility for reporting. The diagram on the right depicts a high-level overview of a financial institution's reporter, receiving, escalation, and reporting process.

Protect the CEO and CFO with Sub-Certifications and Independent Testing. As a matter of necessity, CEOs and CFOs must rely on senior management and their respective teams to support their certification. Like they do Sarbanes-Oxley certifications, companies can develop a waterfall of quarterly sub-attestations from two or three levels below the c-suite, certifying they understand the reporting obligations and have escalated received or known potential criminal misconduct.

CEOs and CFOs usually want the added protection of an internal audit or third-party testing of the reporting process before executing a certification to the DOJ. The testing evaluates the design and validates the operating effectiveness of escalation policies and procedures to provide evidence to support the CEO's and CFO's certifications.



Making the Best of a Government Monitor

No company asks the government to impose a monitor, an independent auditor, or an independent compliance consultant (we collectively refer to these as “government-imposed monitor,” although the roles and relationship are very different). Companies can avoid government-imposed monitors if they remediate early and demonstrate that the enhanced compliance program is “tested, effective, adequately resourced, and fully implemented at the time of a resolution.”⁴²

But sometimes a government-imposed monitor is inescapable.⁴³ This section suggests actions for companies to reduce costs, save time and minimize management distraction based on our experience as a government-imposed and voluntary monitor, independent auditor, and independent consultant to over 25 companies.

Behave Like a Client, Not a Criminal Defendant.

The government repeatedly emphasizes that it does not impose monitors for punitive purposes.⁴⁴ Corporate defendants often feel otherwise, particularly after lengthy, adversarial settlement discussions.

However, companies must regard themselves as the Monitor’s client, no matter how disappointed they may be about the government imposing one. Most companies consider the Monitor only negatively; their sole objective is to survive the monitorship with the least cost, risk and distraction. They adopt a reactive and submissive approach, responding subserviently to monitor information requests and recommendations. Instead, posture the company as the Monitor’s client.

The company-to-auditor relationship provides a good model. Like monitors, external auditors are mandatory and independent. Both relationships entail independent third-party assurance — financial statements and financial reporting controls for the external auditor, compliance program and controls for a monitor.

Develop a Positive Relationship. There are limits, however, to assuming the role of the Monitor’s client. Remember that the Monitor has another client, namely, the prosecutor or regulator that appointed it. And because it is independent, the Monitor never regards itself as working for the company, even though you pay the bills.

Gaining the Monitor’s trust is crucial. Monitors feel at risk because they sign reports and issue certifications in their individual capacities. Companies gain trust by working to help the Monitor mitigate that risk. Companies, for example, should raise both positive and negative matters proactively.

Takeaways

- Behave like a client, not a criminal defendant.
- Develop a positive relationship; avoid an adversarial relationship.
- Identify objectives and benefits.
- Set the proper tone with employees.
- Develop proposed assessment criteria.
- Select candidates wisely.
- Invest in an effective PMO.
- Collaborate on the Monitor’s work plans and recommendations.

Avoid an Adversarial Relationship. Monitorships risk becoming adversarial when the relationship takes on the feel of litigation. Companies understandably want to keep track of the information they provide to the Monitor. But they must strike a delicate balance.

The relationship sours if the Monitor feels that the company or its buffer counsel impedes the flow of information. For example, preparing employees for monitoring team interviews is good practice. But the relationship will surely spoil if the Monitor perceives the company is coaching witnesses.

Set the Right Tone for Employees. The organization should be aware of the Monitor, its role and mandate. Companies benefit from their employees understanding why there is a Monitor and what they are focused on. Management can set the right tone by socializing the importance of Monitor's roles and responsibilities and acknowledging the benefits the company will experience by engaging with the Monitor.

Identify Objectives and Benefits. To be a client is to derive benefits from the service provider. The test of a successful monitorship is whether the company acknowledges it benefited even if it resisted having a monitor.

Don't underestimate the value of third-party assurance, particularly for a company seeking to restore trust with customers, investors, lenders, employees, regulators and other stakeholders in the wake of significant corporate misconduct. Nor should companies discount the benefit of a fresh, objective perspective from a compliance subject matter expert.

Effective monitors will also provide business benefits. Including industry and business process subject matter experts on the monitorship team often lead to suggested operational efficiencies and cost-cutting measures. StoneTurn's methodology, for example, helps companies weed out out-of-date and redundant controls.

Develop Proposed Assessment Criteria.

Monitors typically have a two-fold mandate: (1) oversee the company's compliance with its settlement obligations; and (2) opine on the effectiveness of the company's compliance program and controls.⁴⁵ DOJ agreements require monitors at the end of their terms to certify whether the company's policies, procedures and controls are "reasonably designed and implemented" to prevent and detect violations of laws that gave rise to the settlement. However, the agreements do not specify the criteria for the monitor's certification.

Companies should develop proposed assessment criteria as soon as it becomes apparent that the government might impose a monitor. **Section One** of the Guide provides a template for creating assessment criteria.

Companies can use the proposed assessment criteria to self-evaluate and develop a corrective action plan. Companies should also use the proposed assessment criteria to vet candidates and obtain buy-in during selection.

Select Candidates Wisely. Agencies vary in selection process. The SEC allows the defendant to select a monitor so long as the candidate is “not unacceptable.”⁴⁶ The DOJ permits companies to recommend candidates but leaves the final selection to the government.⁴⁷ **Issues to consider and inquire of candidates include:**

- **Assessment and Certification Criteria.**

Ask candidates to provide and commit to the criteria against which it will measure the company’s compliance program and controls. The quality and detail of the candidate’s criteria shed light on the candidate’s experience and enable the company to gather the evidence to meet the future monitor’s expectations. Having the criteria upfront and in writing ensures no surprises.

- **Detailed Work Plan.**

Besides criteria, ask candidates to propose a work plan for testing the company’s compliance program and controls. Experienced monitors can provide detailed draft work plans including documents they propose to review, planned interviews and walkthroughs, sampling techniques, field visits, transaction testing and re-performance. The work plan should also confirm that candidates understand the monitorship is forward-looking, not an exercise to detect or investigate misconduct.

- **Team Composition.**

Monitorship engagements require cross-disciplinary knowledge, skills and experience, including industry experts, forensic auditors, data scientists and risk and controls experts. Beware and avoid inexperienced resources learning at the company’s expense. Ask candidates to identify the consultants they expect to engage on the project and vet them just as the company conducts diligence on the monitor candidate.

- **Commitment to Rely on Company Resources and Work Product.**

Settlement agreements allow monitors to rely on studies, reviews, sampling and testing methodologies and other work conducted by or on behalf of the company as well as the company’s internal resources including legal, compliance and internal audit so long as the Monitor trusts the quality of the work product or resources.⁴⁸ The standard for relying on the company’s work and resources is similar to the standard external auditors apply to rely on the work of internal audit.⁴⁹

The company likely has had a third-party or internal audit test the areas the future monitor will evaluate. Relying on this work and resources helps avoid unnecessary costs and duplicative business disruptions. Companies should also consider allocating resources to the monitorship, which saves money and ensures the transfer of knowledge when the monitorship ends. Request candidates to confirm their willingness to rely on company work product and accept company resources.

- **Knowledge Transfer.** Conversely, the monitorship team will develop knowledge, skills and work product useful for the company. For example, business leaders, compliance, and internal audit would benefit from the results of monitor-performed risk assessments and monitor-developed compliance program and controls testing procedures. Ask candidates about how they propose to transfer knowledge. For example, will they train the company’s internal auditors to test compliance controls and share testing scripts when the monitorship ends?
- **Communication.** Request monitor candidates to explain their proposed communication plans. For example, will they share findings and recommendations in real-time or defer them to the written reports? Will the candidate share draft reports and if so, how much will it allow the company to comment?
- **Fees.** When it comes to fee estimates, transparency is critical. Candidates should be able to identify assumptions and variables impacting fees (e.g., number and location of field visits). If the candidate has audit and monitoring experience, they likely will be able to budget fees for tasks listed in the work plan. Companies should request candidates submit a detailed budget upfront based on the work plan, and continue to track ongoing activity and related fees to avoid surprises and properly manage costs.

Invest in an Effective Project Management Office (PMO). An effective PMO is key to building and maintaining a healthy company-to-monitor relationship. Take care in selecting employees to serve in the PMO. Investing in strong individuals to lead the PMO ensures buy-in from senior management and a smooth company-to-monitor relationship.

- **Monitor Boot Camp.** At the beginning of the monitorship, the PMO often serves as a “tour guide” function, helping the monitor team to understand the company’s business, structure, and culture. Many organizations find it helpful to begin the monitorship with an onsite orientation that includes senior management representatives, external counsel, PMO, single points of contact (SPOCs), etc. The boot camp provides an opportunity to introduce the Company and its key representatives, explain its compliance program and organization structure and acquaint the monitor team with the underlying facts. It further allows for frank discussion on open audit and regulatory findings, so the monitor team does not duplicate work and is aware of open deficiencies. It also enables the Company to identify the remediation plan for these and whether it will be “good enough” from the monitor team’s perspective.
- **Information Requests.** The PMO typically serves as a central repository for: (1) processing information requests; (2) arranging for review of potentially privileged information; (3) liaising with business leaders; (4) preparing and observing employee meetings; (5) socializing and coordinating the response to findings and recommendations; and (6) periodic reporting to senior management and the board.

The company and monitor should agree up-front on the process for addressing the Monitor document requests. (e.g., single collection point, turnaround time, PMO to direct which documents are to be reviewed/ classified/ redacted by counsel before sharing) and meeting requests (e.g., agreeing attendees from PMO or external counsel).

Where the government-appointed monitorship is imposed outside of the U.S., the company should anticipate translation and data privacy issues and share their perspectives on the potential impact of local legal considerations (e.g., codetermination agreements, local labor regulations).

- **Communication & Reporting.** The PMO likely will coordinate communication and reporting among the stakeholders. It is helpful if the company and monitor agree up-front on a communications plan, including frequency of status reports and meetings with senior management. Consider whether and how to include the board of directors. Some settlement agreements explicitly require board involvement and accountability. Boards often want to be kept apprised even if the settlement agreement does not require board involvement.

Collaborate on Monitor Work Plans and Recommendations

- **Monitor Work Plans.** DOJ settlement agreements require monitors to submit a work plan before commencing its initial review.⁵⁰ Make sure to hold a boot camp or provide other orientation (e.g., show me presentations, walk-throughs) to help the monitor gain sufficient information to develop a detailed work plan. Ask the Monitor to share a draft before it submits the work plan. Use the work plan to identify opportunities for the monitor to rely on company work products and resources and assess whether the proposed work steps are in scope.

- **Monitor Recommendations.** Settlement agreements require companies to implement Monitor recommendations or raise an objection to the government if the company and monitor cannot agree. Companies rarely lodge objections, particularly if they and the monitor develop a positive working relationship and communicate frequently.

The number of recommendations can range widely depending on the status of its remediation efforts and the maturity of its compliance controls. Companies can anticipate and potentially avoid recommendations by self-assessing the program against the criteria and agreeing on a corrective action plan before the monitor issues a recommendation. The monitor will note the remediation plan in its report instead of issuing a formal recommendation.

Some monitors make highly prescriptive recommendations; others make them broad. Gain clarity of the monitor’s expectations – or voice the company’s preference – to avoid a deadlock later in the process. Develop a correction plan, including senior-level responsibility/accountability, milestones, and timelines. As discussed in **Section One**, StoneTurn recommends developing a dashboard to track and keep the Monitor updated on the program’s status.

Demonstrate Sustainability

As the end of monitorship approaches, the company should demonstrate its commitment to maintain its culture of integrity and enhanced ethics and compliance policies, processes and controls. Words alone are insufficient. Instead, discuss and agree with the Monitor upon a post-monitorship plan (e.g., Board oversight, periodic management certifications, regularly scheduled internal audit of compliance program.)



Conclusion

This guide is a resource for companies seeking to navigate the complex landscape of DOJ and SEC corporate settlement agreements.

We recommended the steps outlined above to help companies fulfill their post-resolution obligations, mitigate the risk of future violations and rebuild trust with stakeholders and the public. Our guide acknowledges that every organization’s post-resolution journey is unique, and flexibility in implementing these steps is important. StoneTurn encourages companies to tailor their strategies to their specific circumstances, industry, and risk profile while maintaining regulatory compliance and ethical standards at the forefront.

Companies should not be surprised by CEO/CCO certifications, nor should they consider them as punitive. Instead, organizations can leverage them as empowerment tools for ethics, compliance, and integrity. Additionally, there are opportunities to learn from prior monitorships to understand how to prepare for and effectively navigate such a process when faced with required remediation. Finally, if a monitor is assigned, organizations can take advantage of a monitorship like they would a compliance consultant: the fee and fines will be paid either way, and companies can reap various benefits through the monitorship experience and knowledge gained.

Notes

- 1 DOJ, Principles of Federal Prosecution of Business Organization, §9-28.300 (2023). <https://www.justice.gov/jm/title-9-criminal>; DOJ Criminal Division, *Evaluation of Corporate Compliance Programs* (March 2023) (“ECCP”). www.justice.gov/criminal-fraud/page/file/937501/download
- 2 DOJ Office of Public Affairs, *Deputy Attorney General Lisa O. Monaco Delivers Remarks on Corporate Criminal Enforcement*, September 2022 <https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-corporate-criminal-enforcement>.
- 3 DOJ Office of Public Affairs, *Deputy Attorney General Lisa O. Monaco Gives Keynote Address at ABA’s 36th National Institute on White Collar Crime*, October 28, 2021. <https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute>.
- 4 DOJ Office of Public Affairs, *Ericsson to Plead Guilty and Pay Over \$206M Following Breach of 2019 FCPA Deferred Prosecution Agreement*, March 2, 2023 (“Ericsson Plea Agreement Violation”). <https://www.justice.gov/opa/pr/ericsson-plead-guilty-and-pay-over-206m-following-breach-2019-fcpa-deferred-prosecution>.
- 5 Deutsche Bank Aktiengesellschaft, Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1935 for the Fiscal Year Ended December 31, 2022, p.13 (March 2022) (“Deutsche Bank 2022 Annual Report”). <https://investor-relations.db.com/files/documents/sec-filings-for-financial-results/Form-20-F-2022.pdf>.
- 6 See, e.g., *U.S. v. Danske Bank, Plea Agreement*, 22 Cr. 679 (SDNY)), December 12, 2022 (“Danske Bank”). www.justice.gov/opa/press-release/file/1557611/download.
- 7 DOJ, Office of Public Affairs, *Deputy Attorney General Lisa O. Monaco Delivers Remarks on Corporate Criminal Enforcement*, September 15, 2022 www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-corporate-criminal-enforcement.
- 8 See ECCP, *supra* note 2, at Part II, ¶B (requiring prosecutors to consider whether “compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions”).
- 9 White & Case, *Use of Data Analytics in Compliance Programs*, June 13, 2023. <https://www.whitecase.com/insight-our-thinking/2023-global-compliance-use-data-analytics-compliance-programs>.
- 10 Dylan Tokar, Assistant Attorney General, on Eve of Exit, Touts Data’s Growing Role in Crime Fighting, *The Wall Street Journal*, July 17, 2023. <https://www.wsj.com/articles/assistant-attorney-general-on-eve-of-exit-touts-datas-growing-role-in-crime-fighting-a22112cb>.
- 11 Jonny Frank, *Forensic Analytics Can Find Needs in Multiple Haystacks*, *Law360*, April 30, 2013. www.law360.com/articles/436990/forensic-analytics-can-find-needles-in-multiple-haystacks.
- 12 See, e.g., *Danske Bank, supra* note 6, at Attachment C.
- 13 See, e.g., *Danske Bank, supra* note 6, at Attachment D.
- 14 *Id.*
- 15 See, e.g., *Danske Bank, supra* note 6, at *Attachments E and F* (requiring certifications respectively that company reported misconduct and implemented an effective compliance program); see also *The Matter of Ernst & Young LLP*, Exchange Act Release No. 95167 ¶56 (June 2022) (“EY SEC Order”) (requiring EY’s Principal Executive Officer to certify whether the firm’s policies and procedures are “adequate and sufficient to provide reasonable assurance of compliance with all relevant professional standards”). <https://www.sec.gov/litigation/admin/2022/34-95167.pdf>
- 16 See, e.g., *Danske Banke, supra*, Attachment C ¶1 (requiring the defendant to “ensure that its directors and senior management provide strong, explicit, and visible support and commitment to its Compliance Programs”).
- 17 ECCP, *supra*, note 2, at Part III, ¶A.
- 18 DOJ, Criminal Division, Revised Memorandum on Selection of Monitors in Criminal Division Matters, March 1, 2023 (“DOJ Selection of Monitors”). www.justice.gov/criminal-fraud/file/1100366/download.
- 19 See, e.g., Public Accounting Oversight Board, *An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements*, Auditing Standard 2201 (2007) (“PCAOB AS 2201”). <https://www.pcaobus.org/oversight/standards/auditing-standards/details/AS2201>.
- 20 PCAOB AS 2201, at ¶42-45 (defining design effectiveness for financial report controls as “whether the company’s controls, if they are operated as prescribed by persons possessing the necessary authority and competence to perform the control effectively, satisfy the company’s control objectives and can effectively prevent or detect errors or fraud that could result in material misstatements in the financial statements”).
- 21 See, e.g., *Danske Bank, supra* note 6, at Attachment E.
- 22 Ericsson Plea Agreement Violation, *supra* note 4. Deutsche Bank 2022 Annual Report, *supra* note 5.

- 23** 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>.
- 24** See, e.g., In the Matter of KPMG, Exchange Act Release No. 4051 ¶80 (June 17, 2019)(requiring the CEO to certify that KPMG policies, processes and controls are “adequate and sufficient to provide reasonable assurance of compliance with all professional standards relating to ethics and integrity”). www.sec.gov/litigation/admin/2019/34-86118.pdf
- 25** See, e.g., Plea Agreement, United States v. Glencore International A.G., (S.D. N.Y.) (May 2022) (“Glencore”). <https://www.justice.gov/criminal/file/1508266/download>.
- 26** 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>.
- 27** 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>.
- 28** DOJ, *Principles of Prosecution of Business Organizations*, ¶9-28.800, 2019, <https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations>.
- 29** DOJ, Criminal Division, *Corporate Enforcement and Voluntary Self-Disclosure Policy*, updated January 2023, <https://www.justice.gov/criminal-fraud/file/1562831/download>.
- 30** SEC, *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* (Seaboard Factors), October 23, 2001, <https://www.sec.gov/litigation/investreport/34-44969.htm>.
- 31** In Re McDonald’s Corporation Stockholder Derivative Litigation, C.A. No. 2021-0324-JTL, 2023 WL 407668 (Del. Ch. January 26, 2023), <https://courts.delaware.gov/Opinions/Download.aspx?id=343130>.
- 32** Glencore, *supra* note 25, at Attachment H.
- 33** Danske Bank, *supra* note 6.
- 34** EY SEC Order, *supra* note 15, at ¶56.
- 35** Committee of Sponsoring Organizations of the Treadway Commission, *Guidance on Internal Control* (2013). <https://www.coso.org/sitepages/internal-control.aspx?web=1>.
- 36** U.S. Sentencing Guidelines Manual §8B2.1 (U.S. Sent’g Comm’n 2013), <https://guidelines.uscourts.gov/gl/%C2%A78B2.1>.
- 37** DOJ, Criminal Division, and SEC, 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>.
- 38** See, e.g., *Danske Bank*, *supra* note 6, at ¶13
- 39** See, e.g., *Glencore*, *supra* note 25.
- 40** Ericsson Plea Agreement Violation, *supra* note 4.
- 41** Deutsche Bank 2022 Annual Report, *supra* note 5.
- 42** See generally, Jonny Frank, 8 Critical Actions to Enjoy the Carrot & Avoid the Stick of DOJ’s Corporate Enforcement Policies, Corporate Compliance Insights, November 16, 2022. <https://www.corporatecomplianceinsights.com/doj-carrot-stick/>; see also Jonny Frank & Simon Platt, Five Ways to Eliminate the Need for a Corporate Monitor, New York Law Journal, December 11, 2017. https://stoneturn2017.wpenginepowered.com/wp-content/uploads/2018/03/NYLJ_Five-Ways-to-Eliminate-the-Need-for-a-Corporate-Monitor.pdf
- 43** See DOJ Selection of Monitors, *supra* note 18.
- 44** Id.; See also Acting Deputy Attorney General Craig S. Morford, *Selection and Use of Monitors in Deferred Prosecution Agreements and Non Prosecution Agreements with Corporations* (2008). www.justice.gov/sites/default/files/dag/legacy/2008/03/20/morford-useofmonitorsmemo-03072008.pdf
- 45** See, e.g., *Glencore*, *supra* note 25.
- 46** See Jonny Frank, Chapter 8: SEC & DOJ-Imposed Monitors, SEC Compliance and Enforcement Answer Book, Practising Law Institute (June 2023).
- 47** DOJ Selection of Monitors, *supra* note 18, at Part E.
- 48** See, e.g., *Glencore*, *supra*, note 25, at Attachment H¶7.
- 49** See Public Accounting Oversight Board, Consideration of the Internal Audit Function, Auditing Standard 2605 (2022). https://pcaobus.org/oversight/standards/auditing-standards/details/as-2605-consideration-of-the-internal-audit-function_1528.
- 50** See, e.g., Glencore Plea Agreement, *supra* note 25, at Attachment D ¶¶10 – 11



StoneTurn serves its clients from 15 offices across the U.S., U.K., Germany, Brazil, Singapore and South Africa. We have also assembled an unmatched global network of senior advisers – virtually all of whom have more than 20 years of experience in their respective disciplines—from diverse industries and geographies. Through this network, we supplement our teams with experienced, on-the ground professionals in nearly 100 countries, as needed, to assist our clients in any jurisdiction around the world.

Our experience extends worldwide. That’s because we understand solving complex issues often requires the expertise of resources around the globe—and with such a reach, our team can more efficiently and effectively assess global compliance programs for companies across geographies.

Our Team

Julia Arbery

jarbery@stoneturn.com

Laura Greenman

lgreenman@stoneturn.com

Patricia Latorre

platorre@stoneturn.com

Kaitlyn Cecala

kcecala@stoneturn.com

Chris Hoyle

choyle@stoneturn.com

Lisa Van Houten

lvanhouten@stoneturn.com

Michele Edwards

medwards@stoneturn.com

Ksenia Ioffe

kioffe@stoneturn.com

Rae Vogelman

rvogelman@stoneturn.com

Jonny Frank

jfrank@stoneturn.com

Ryan LaRue

rlarue@stoneturn.com

Brad Wilson

bwilson@stoneturn.com

Leaving no stone unturned.

StoneTurn, a global advisory firm, assists companies, their counsel and government agencies on regulatory, risk and compliance issues, investigations and business disputes. We serve our clients from 15 global offices across five continents.



[StoneTurn.com](https://www.stoneturn.com)