Securing a C-ADR: Key steps for compliance programme readiness and independent reviews

By Mike Roos and Jonny Frank

In 2024, the National Prosecuting Authority (the "NPA") published the Corporate Alternative Dispute Resolution ("C-ADR") Directive (the "Directive"). Similar to US Deferred Prosecution Agreements, C-ADRs enable qualifying companies to avoid criminal prosecution by resolving the investigation at the pre-trial stage.

The Directive lists criteria the NPA considers in deciding whether to grant a C-ADR (including disclosure, cooperation, misconduct seriousness and pervasiveness). Criteria 8 pertains to compliance programmes, which, if in existence and effective, "will weigh in favour of a Corporate ADR".

However, the Directive, provides no specific guidance on what constitutes an effective compliance programme. We seek to fill the gap based on international best practices[1] and StoneTurn's extensive experience serving as a voluntary and government-imposed compliance consultant.

Elements of effective remediation

Prosecutors and regulators are likely to examine how the company remediated the misconduct under investigation and addressed the past instances of misconduct. There are five elements to effective remediation:

1. **Root Cause Analysis (RCA): Investigations determine what happened while RCA discovers how the misconduct occurred.**

Sample questions include:

- What was the perpetrator's motivation?
- Were any systemic issues identified?
- Did the company anticipate the risk?
- What controls failed?
- Were supervisors negligent in overseeing the employees involved in the misconduct?
- Why did bystanders not report the misconduct?
- How did the company fund the corruption?
- What opportunities did the company miss to detect the misconduct?[2]

2. Read across

This element refers to the procedures the company uses to build on the root-cause analysis to discern the full extent of wrongdoers' misconduct; and detect similar misconduct elsewhere in the organisation (including other geographies and business units)[3].

3. Risk assessment

Companies should conduct a risk assessment based on the RCA and Read Across findings. The risk assessment should be scenario-based; that means determining what misconduct scenarios might arise from the RCA and Read Across findings. How likely are these to occur? What would be the impact? Remediation must address risks that are reasonably likely to occur and, if they occurred, would have a significant legal, financial, reputational or market impact on the company.

4. Corrective Action Plan (CAP)

Remediation plans commonly fail because they address only the immediate problem, not the broader issues underlying the misconduct. To be effective, the CAP must address RCA and Read Across findings and significant risks identified in the risk assessment. Remediation tends to slip as the immediate crisis fades and new problems arise. To mitigate that risk, the corrective action plan should include specific milestones and timelines and have the support of good governance and solid project management[4].

5. Independent testing

The NPA Directive clarifies that a critical consideration for a C-ADR is its willingness to subject such a programme to review and monitoring by an external compliance evaluator[5].

Steps to take to prepare for an independent review

The company should prepare for an independent evaluation and set up a Project Management Office ("PMO"). An effective PMO minimises disruption to the business and allows for a streamlined and "less painful" evaluation. Senior leadership and business buy-in are essential for an effective working relationship.

1. Conduct self-assessment

Companies benefit from conducting self-assessment, looking at the organisation from the evaluator's perspective. Self-assessment helps the company to anticipate the recommendations and enables candid discussion during the evaluation. It also positions the company to negotiate and potentially push back on the evaluator's scope and work plan.

2. Document production and tracking

The external compliance evaluator will make numerous document requests, often broad and general, because they do not know the company. General and broad information requests can put the company in a difficult position because it must balance between overproducing irrelevant documents and being accused of withholding documents. We recommend collaborating with the evaluator to avoid over and under production.

3. Interviews

The external compliance evaluator will also request interviews and walkthroughs of company processes. The company must prepare employees for interviews (which can be done by alleviating concerns). Labour unions may also raise concerns that the company must consider as part of the interviewing process (such as by demanding union counsel to be present at interviews). The company should consider how best to collect the information from the interview (by requesting a PMO member to take notes and post-interview debriefing). The company must demonstrate its usefulness in attending interviews (including clarifying answers after the interview, suggesting and arranging follow-up interviews and communicating action items). Even more important, the company should avoid interfering with the interviews, appearing defensive or becoming adversarial.

The company must prepare employees for interviews (which can be done by alleviating concerns). Labour unions may also raise concerns that the company must consider as part of the interviewing process (such as by demanding union counsel to be present at interviews).

Guidelines on testing compliance programmes and controls

This process requires forensic audit and investigation skills, knowledge and experience in risks and controls.

1. **Independence**
   The testing function must be independent - it cannot serve as an advocate or review its work. As an example, the Chief Compliance Officer lacks the independence to evaluate and test the compliance programme and control the compliance function developed or implemented. Likewise, it would impair the independence of internal or external counsel to conduct testing.
2. **Conflict of interest**
   The testing function cannot be subordinate to the function, department or business under evaluation. As an example, a conflict of interest would arise if an internal audit simultaneously tested compliance controls and reported to the Chief Compliance Officer.
3. **Testing the compliance programme** differs fundamentally from testing controls. Compliance programme testing considers entity-wide issues and activities, such as the corporate culture, risk assessment, technology, compliance and internal audit functions, incident response and remediation. For testing, the organisation and evaluator must first agree on the compliance programme elements and then on the assessment criteria and benchmarks. The testing process applies standard audit procedures to assess the design[6] and validate the operating effectiveness[7] against the agreed-upon criteria and benchmarks.
4. **Compliance controls testing** pertains to the critical policies, processes and controls ("controls suite") the organisation relies upon to prevent and timely detect breaches of the laws and regulations in the investigation. Testing assesses whether the controls suite adequately mitigates legal and regulatory risks.
   Broadly summarised, the process entails the following:
   (1) setting risk appetite;
   (2) selecting applicable laws and regulations;
   (3) identifying breach scenarios;
   (4) linking the scenarios to the control suite;
   (5) linking risks to mitigating policies, processes and controls;
   (6) auditing control suite design effectiveness;
   (7) auditing operating effectiveness, assuring control suite found to be effective; and
   (8) identifying deficiencies, significant deficiencies or material weaknesses.

Tips on assessment and reporting

The NPA Directive is neither specific in the requirements for an independent report, nor is there a single internationally accepted method for reporting the results of compliance programmes and compliance control testing. The US Department of Justice (DOJ) uses certifications in its settlement agreements. Corporate Compliance Monitors, for example, must certify whether the compliance programme, including its policies and procedures, are reasonably designed and implemented to prevent and detect violations of laws" and regulations giving rise to the settlement[8]. For audits of internal controls over financial reporting, the Public Company Accounting Oversight Board ("PCAOB") requires auditors to issue an "opinion on whether the company maintained, in all material respects, effective internal control over financial reporting". The auditor can issue such an opinion if there are no "material weaknesses," which the PCAOB defines as a "deficiency, or a combination of deficiencies, in internal control over financial reporting[9], such that there is a reasonable possibility that a material misstatement of the company's annual or interim financial statements will not be prevented or detected on a timely basis" (emphasis in the original)[10]. **A reasonable possibility** is a likelihood that is "reasonably possible" or "probable"[11]. The PCAOB also requires the auditor to provide the basis of the opinion[12].

We recommend adapting the PCAOB approach. For compliance programmes, we regard a certification that the programme is "reasonably designed and implemented" as an opinion that compliance programme and controls are free of a deficiency or a combination of deficiencies such that there is a reasonable possibility that a material violation of the laws at issue in the investigation will not be prevented or detected on a timely basis[13].

Conclusion

The NPA's Corporate ADR Directive offers a significant opportunity for companies to mitigate legal risks through proactive remediation and compliance. By adhering to international best practices, conducting thorough independent reviews and rigorously testing compliance programmes, organisations can position themselves favourably for a C-ADR. With the guidance outlined in this article, companies are equipped to meet the Directive's requirements and establish a culture of integrity that deters future misconduct.

Footnotes

1. See DOJ, Criminal Division. 2023. Evaluation of Corporate Compliance Programs ("ECCP"). https://www.justice.gov/criminal-fraud/page/file/937501/download.
2. See generally, J. Frank et al. 2024. "A primer in root cause analysis: A critical step in the remediation of compliance violations." https://stoneturn.com/insight/root-cause-analysis-compliance-remediation/.
3. See generally J. Frank et al. 2024. "Sweeping skeletons out of the corporate closet: 'Read Across' and 'Remediation'." https://stoneturn.com/insight/sweeping-skeletons-out-of-the-corporate-closet-read-across-and-remediation/.
4. See J. Frank et al. 2024. "Remediation roadmap: 5 steps for timely and cost-effective corrective action." https://stoneturn.com/insight/remediation-roadmap-5-steps-for-timely-and-cost-effective-corrective-action/.
5. See J. Frank et al. 2024. "Where's the beef? Demonstrating 'timely & appropriate' Remediation." https://stoneturn.com/insight/demonstrating-timely-appropriate-remediation/.
6. Design effectiveness assesses whether the policies, processes and controls, assuming they operate effectively, meet the objectives. Design effectiveness also considers vulnerability to collusion, management override or other circumvention.
7. Operating effectiveness tests how the compliance programme elements work in practice, including the competency and authority of the persons responsible and involved in carrying out the processes.
8. See, as an example, Plea agreement, attachment D, U.S. v. Binance, 23 Cr. 178 (W.D.Wash. 2023). For management, the settlement agreements typically require the CEO and CCO to certify that the "compliance programmes are reasonably and effectively designed to detect and prevent" violations of the laws and regulations at issue in the settlement. Id. at Attachment D. The DOJ has not explained why management certifies that the compliance programmes are "reasonably and effectively designed" and monitors certify that they are "reasonably designed and implemented." From an auditor's perspective, the difference is that management's certification would cover only design effectiveness, while the monitor's certification encompasses both design and operational effectiveness. However, there is no reason why the DOJ would expect a lower standard from management than the monitor.
9. PCAOB. 2007. An audit of internal control over financial reporting that is integrated with an audit of financial statements, reporting on internal control. Auditing Standard 2201, 85(c). https://pcaobus.org/oversight/standards/auditing-standards/details/AS2201.
10. Id. at A7. The PCAOB defines "deficiency" as "when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis." Id. at A.3. The PCAOB defines "significant deficiency as a "deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight of the company's financial reporting." Id. at A.11.
11. Id.
12. Id. at 85.d.
13. See J. Frank et al. 2023. Certification of ethics and compliance programme effectiveness. SCCE CEP. https://stoneturn.com/insight/certification-of-ethics-and-compliance-program-effectiveness/.

About the authors

Mike Roos, a Partner with StoneTurn, has 25 years of experience in forensic accounting, investigations and expert witness work. He has extensive experience in conducting Foreign Corrupt Practices Act (FCPA) and anti-bribery/anti-corruption investigations, investigative due diligence, corporate governance and integrity and compliance monitoring. Most recently, he presented evidence to the US DOJ relating to an FCPA matter in Africa.

Jonny Frank helps organisations and counsel remediate misconduct and address regulatory findings. He joined StoneTurn from PwC, where he was a Partner, and globally led the fraud risk & controls practice. Jonny also served as the Executive Assistant United States Attorney, Eastern District of New York, a Senior Faculty Fellow at the Yale School of Management and an Adjunct Associate Professor at Fordham University Law School and Brooklyn Law School.