JUSTICE DEPARTMENT ENFORCEMENT GUIDELINES PROVIDE PLAYBOOK FOR EVALUATING FINANCIAL CRIMES COMPLIANCE PROGRAMS

The Department of Justice (DOJ) recently released updated guidance (Guidance) for prosecutors when evaluating a financial institution's financial crimes compliance program. The Guidance focuses on three core principles, considering whether a compliance program is:

1. 'Well-designed' **2.** Adequately resourced and functioning effectively **3.** Working in practice[1]

The DOJ makes clear that they expect compliance programs to be specifically-tailored and continuously evolving, providing "…revisions to corporate compliance programs in light of lessons learned."[2] As a result, the Guidance explicitly highlights expectations regarding how a financial institution executes its risk assessment, but also how it makes use of the results and learns from its peers.

However, there are additional areas of focus that financial institutions should evaluate in light of the DOJ's risk-based approach, including training, reporting, third-party management, testing and governance.

This paper discusses several of these themes in greater detail below.

RISK ASSESSMENT

The Guidance makes clear that the DOJ will use the financial crime risk assessment as the core process in evaluating whether a financial institution has a well-designed compliance program. Specifically, the DOJ will consider whether the company has analyzed and addressed the varying risks presented by, among other factors, "the location of its operations, the industry sector, the competitiveness of the market, the regulatory landscape, potential clients and business partners, transactions with foreign governments, payments to foreign officials, use of third parties, gifts, travel, and entertainment expenses, and charitable and political donations."[3] Financial institutions are also expected to consider whether the compliance program was specifically tailored to the outcome of the risk assessment and whether assessment criteria are regularly updated.

In light of this Guidance, financial institutions must be learning and acting on the results of their risk assessments. Banks should examine whether their risk assessment criteria, methodology and timing are current. Periodic reviews, which

1. JM 9-28.000 Principles of Federal Prosecution of Business Organizations, Justice Manual ("JM"), available at https://www.justice.gov/jm/jm-9-28000-principlesfederal-prosecution-business-organizations., JM 9-28.800.
2. Id. at JM 9-28.80.
3. https://www.justice.gov/criminal-fraud/page/file/937501/download

are merely a 'snapshot in time' versus a comprehensive data and event-driven update, may not meet the DOJ standards. Additionally, financial institutions should understand whether the results of their risk assessments have led to meaningful updates to policies, procedures, and controls – if not, significant modifications may be required to be considered well-designed and effective. Financial institutions that do not currently have a process to track and incorporate lessons learned from their risk assessments, as well as insights from other companies operating in the same industry and/or geographical region, should take action now.[4]

In evaluating the effectiveness of the risk assessment process, compliance departments must also evaluate the quality of their compliance data. Specifically, they must understand whether compliance and control functions have sufficient access to the types of data that allows them to do their job, whether any impediments restrict access to required data, and whether institutions are taking corrective action to address them. The implication here is two-fold. Firstly, data quality and efforts to remediate data gaps should be prioritized. Secondly, institutions should be investing in technological advancements across the entire financial crimes compliance program, so the firms do not fall behind their peers' compliance advancements. Therefore, investments in risk assessment technology are essential. Not only because the assessments are expected to form the cornerstone of the compliance program, but because they are expected to be evolving and increasingly data-driven.

TRAINING AND COMMUNICATION

The Guidance indicates that training is another indicator of a well-designed and effective financial crimes compliance program, namely, whether the training is appropriately provided to, and understood by, all impacted personnel. A risk-based training program is crucial.

Institutions should evaluate current training programs to understand:

- Whether employees in specific high risk and/or control functions have received targeted training, including areas where the institution has previously identified control breaches

- Whether supervisors received different or supplemental training given their duty to ensure the day-to-day effectiveness of the compliance program

In examining their training programs, institutions should also pay careful attention to their record-keeping processes. Being able to track which employees require training and proving they were trained effectively is critical to proving the success of a program. Training must also incorporate prior compliance incidents to ensure the material is timely and up to date.

Training content should also be evaluated. For example, institutions should be testing their employees on what they have learned, and then providing additional training based on the results. Capco has observed instances where training modules contained the appropriate content but failed to be offered in a language and format relevant to a global audience. Additionally, we have observed training which has not been updated to address lessons from prior instances of misconduct – given the expectation that firms learn from their experience and their peers, we believe this is a critical time to evaluate the effectiveness of training programs. Firms should evaluate the need to include case studies from industry events, if their employees can ask questions about training content, and whether they have established methods to measure training effectiveness.

4. Id.

CONCLUSION

The Guidance represents a general regulatory trend toward tailoring compliance programs to the specific risks of the financial institution, which now includes a requirement to remain aware of peer institutions. Data quality remains a crucial impediment to effective compliance programs; therefore, firms should take action to remediate their gaps, but also to invest in data analytics. The amount of data financial institutions have in their systems of record regarding the customers (including from financial crimes compliance activities) could prove tremendously insightful in developing a more robust understanding of the client and identifying economic activities. By aggregating and analyzing this data, financial institutions could vastly improve their client relationships and their own bottom lines.

For more information, please contact

Randall Sawyer
US Capital Markets Partner
randall.sawyer@capco.com

Spencer Schulten
Executive Director and US Head of Financial Crimes Compliance
spencer.schulten@capco.com

WWW.CAPCO.COM

CAPCO