A principles-based approach for auditing board reporting

CAMS-Audit White Paper
A principles-based approach for auditing board reporting

Introduction

Regulatory requirements and guidance around independent testing of Board of Directors (BOD) data gathering and BOD reporting processes is sparse, but applicable processes support key Bank Secrecy Act (BSA)/anti-money laundering (AML) and Office of Foreign Assets Control (OFAC) governance activities. As such, it is incumbent on internal audit to understand applicable risks, process objectives and regulatory expectations and ensure their test programs drive sufficient testing of each. This is a challenging task that requires consideration of numerous factors. This white paper provides discussion of key factors and principles-based guidance to assist with test plan design and execution. By no means is the discussion or principles-based guidance conclusive. The white paper provides a snapshot of key factors and principles that I have found most helpful in my experience.

Background

As an internal auditor in a large financial institution (FI) I see first-hand the pivotal role the BOD plays in providing oversight and strategic guidance to drive BSA/AML and OFAC compliance. The BOD is an independent group of directors with oversight over the FI, including the BSA/AML and OFAC compliance programs. The BOD is well-positioned to oversee key risks and objectives, provide an effective challenge to Senior Management and/or offer their support where applicable. At its best, the BOD provides strong oversight and guidance strengthening the BSA/AML and OFAC compliance programs and contributing to the safety and soundness of the FI. However, recent enforcement actions brought by U.S. regulators against large FIs highlight systemic issues with BSA/AML and OFAC
A principles-based approach for auditing board reporting

compliance and specifically BOD oversight. Fortunately internal audit has tools at its disposal to assist the BOD in achieving their objectives.

As part of risk-based independent testing, internal audit supports the BOD by conducting regular audits of BSA/AML and OFAC compliance data gathering and BOD reporting processes. The simple objective of this work is to verify that there are sustainable compliance processes in place to provide the BOD accurate, complete and timely data related to money laundering, terrorist financing and compliance risk and program effectiveness.

**Insight into the Board**

A key step in auditing data gathering and BOD reporting is to understand the BOD and their mandate. BOD members are extremely accomplished, knowledgeable and competent individuals with a mandate to provide independent oversight of and strategic guidance for their FIs. The scope of the BOD’s mandate includes BSA/AML and OFAC compliance programs, but it is important to note that while BOD members have considerable expertise, it may not include explicit compliance and/or regulatory expertise. As such, BOD members rely on subject matter experts, including senior management, the Chief AML Officer and the Chief Auditor to provide regular BSA/AML and OFAC training and to communicate key messages regarding risk and program effectiveness to them in a timely and succinct fashion.

Information communicated to the BOD must be carefully crafted to meet regulations and regulatory expectations, strike a balance between too much and just enough information and be sufficiently straight-forward so that a reasonably knowledgeable individual can understand it. It should also effectively prioritize higher risk items, drawing attention
A principles-based approach for auditing board reporting

where attention is needed. It is important to note that BSA/AML and OFAC compliance is just one of the risk sub-sets the BOD is mandated to oversee. As such, the information presented to the BOD must be clear, concise and memorable so that key messages are conveyed economically and get sufficient attention.

**Regulatory requirements – The Letter of the Law**

**Key Audit Consideration:** Strong audit work programs drive comprehensive coverage of applicable laws and regulations. For U.S.-centric auditors, key laws to consider include the BSA, the U.S.A. PATRIOT Act and OFAC. Building a strong audit work program also includes developing an understanding of formal BSA/AML and OFAC compliance guidance, which in the U.S. is delivered in the BSA/AML FFIEC examination manual (2010). The FFIEC examination manual is specifically designed to provide guidance to U.S. regulators for carrying out BSA/AML and OFAC exams and is an invaluable tool for AML auditors. Laws like the BSA identify AML program requirements and the FFIEC BSA/AML examination manual provide context for the law and guidance on how examiners design test steps to cover the requirements. Taken together, the law and the guidance provide a great starting point for a well-designed audit workplan.

Specific to BOD reporting, the 2010 FFIEC BSA/AML manual states that FIs must inform the Board, or a committee thereof, and senior management, of compliance initiatives, identified compliance deficiencies, and corrective action taken, and notify directors and senior management of SARs filed. Other than reporting identified compliance deficiencies, the BSA does not require a more detailed synopsis of program effectiveness.
A principles-based approach for auditing board reporting

**Risk:** Audit work programs that are not firmly grounded in BSA/AML and OFAC laws and FFIEC BSA/AML guidance are destined to raise concerns from the regulators and may fail to provide adequate assurance that BOD reporting meets minimum regulatory requirements. It also could increase the likelihood that if BOD reporting omits key BSA/AML and OFAC compliance risk assessment and program effectiveness data that the omission may not be identified and corrected. Omitted data could deprive BOD members of information necessary to achieve their mandate. Finally, if foundational, “block and tackle” elements, like regulatory requirements are omitted from audit work programs it signals to regulators that there may be a fundamental lack of understanding of the work and may lead to additional scrutiny of internal audit in future examinations.

**Regulatory Expectations – The Spirit of the Law**

**Key Audit Consideration:** In today’s zero tolerance regulatory environment, designing audit work programs to meet the letter of the law is a starting point, but in no way guarantees a satisfactory assessment from regulators or adequate coverage of money laundering and terrorist financing (ML/TF) risk. The fact is that minimum regulatory requirements are not sufficient to effectively prevent and detect ML/TF. Criminal and terrorist interests are often advanced organizations constantly evolving their operations and ML/TF techniques to evade detection. As such, to keep pace with criminal and terrorist interests and effectively prevent and/or detect ML/TF, FIs must evolve their compliance programs quickly. Regulators must test for compliance with regulations, but they also have a vested interested in the objective or spirit of the regulations, which is to prevent and/or detect ML/TF. As such, regulators are continuously pushing program evolution and their expectations for BSA/AML and OFAC compliance have risen noticeably each year since 2001. The question is,
A principles-based approach for auditing board reporting

in the absence of documented laws and regulations to guide FIs, how do regulators communicate their expectations? Also, how can FIs be expected to follow a set of expectations and best practices that are not completely clear and may not be consistently enforced?

The answer is there is no one source of information that adequately captures the complete set of regulatory expectations and that complying with expectations is difficult and potentially impossible to do perfectly. Getting a handle on regulatory expectations requires proactive monitoring of the regulatory environment and prudent relationship management with one’s own regulators. Some sources that I leverage include regulatory enforcement actions, commentary from regulators at training events, such as conferences, Senate testimony, formal regulatory feedback for my own organization and discussions held with regulators as part of regular relationship management activities. Information obtained from each of these data sources must be proactively aggregated and understood. If evidence of a change in regulatory expectations is strong and a trend can be extrapolated, it is incumbent on the AML auditor to build in applicable test steps in the audit work plan and begin auditing clients against the new, higher standards. This work can produce productive friction at the client-level as new regulatory expectations are introduced and this is okay. However, to ensure an effective partnership with the client, it is helpful to proactively communicate changes in regulatory expectations and the impact to the client as it becomes known. This will allow the client to begin to comply with the new expectations prior to the audit, helping them to enhance their risk management practices and saving them from being cited unnecessarily in the audit report.
A principles-based approach for auditing board reporting

**Risk:** Failure to understand regulatory expectations for BOD reporting when designing and executing data gathering and BOD reporting independent testing can have significant negative implications. Laws and regulations around BOD reporting are unspecific and guidance is sparse. However, regulators expect the BOD to provide active oversight over BSA/AML and OFAC compliance and to do this they require timely, accurate and concise reporting of key risks and program effectiveness. As such, independent testing must be designed to support this expectation and verify BOD reporting effectively supports the BOD's mandate. Failure to do this could lead to insufficient BOD reporting and limit the BOD's effectiveness.

**Audit risk assessment and strategy**

**Key Audit Considerations:** BOD reporting for large FIs is the culmination of complex data aggregation, analysis and review processes. Often times these processes are a mix of system-based and/or manual processes executed in various levels of the organization. The extent of the processes and the data involved present a high likelihood of execution error. Data can be easily overlooked, system feeds can fail and data can be misunderstood resulting in incorrect conclusions and sub-optimal positioning in BOD reporting. Even well-designed processes run by skilled professionals have error rates. The BOD can be relied upon to question material data inconsistencies, but are less likely to identify small, but potentially significant gaps in reporting or analysis.

Given this, the BOD reporting process should be assessed with a proportionately high risk score and audited at least annually. The method in which applicable processes are audited is also an important consideration. In large organizations, lines of business and legal
A principles-based approach for auditing board reporting

entities complete similar data gathering and reporting processes that feed to a centralized data repository. This data is then aggregated and analyzed, conclusions are prioritized and BOD reporting is developed. The end product is socialized with BOD members and formally presented to the BOD by the Chief AML Officer. Wherever similar processes with identical objectives are executed by multiple control performers across different silos, horizontal process audits must be considered. The benefits of horizontal process audits include timely and comprehensive coverage of a single process, easy comparison of processes across silos and enhanced identification of global insights. Positive outcomes of horizontal audits include recommendations to increase efficiency and effectiveness through adoption of organizational best practices and a clear picture of organizational process effectiveness and risk management capabilities. Traditional vertical audits of individual lines of business and legal entities provide incremental assurance that processes are effective, but require many audits and subsequent aggregation of those audits to deliver the same opinion on organizational effectiveness yielded by a single horizontal audit.

There are several key aspects of BOD reporting that require a high level of attention, including, but not limited to data validation processes, prioritization and positioning of key issues in the reporting and escalation of instances of non-compliance with BSA/AML and OFAC laws and regulations. However, I think it is important to specifically highlight important audit considerations regarding key performance and key risk indicators (KPIs and KRIs). KPIs and KRIs are statistical measures calculated based on compliance program, operational and sales data that are helpful in quantifying process effectiveness and risk. Examples of each as it relates to suspicious activity monitoring and reporting include the alert to suspicious activity report (SAR) ratio (KPI) and the geographic distribution of SAR
A principles-based approach for auditing board reporting

reports (KRI). These specific metrics provide objective measures of SAR efficiency and ML/TF risk by geography. Used correctly, KPIs and KRIs are powerful tools that allow efficient measurement of both process effectiveness and risk. However, used incorrectly they can yield misleading results.

Key questions to answer when auditing KPIs and KRIs are:

1. Does the organization have the appropriate number and types of metrics to adequately describe both process effectiveness and risk?

Too few metrics can hamper adequate measurement of the data and too many metrics can lead to confusion as various data elements are considered and potentially conflict. Appropriate numbers and types of KPIs and KRIs should be included to adequately describe each of the key BSA/AML and OFAC processes and to define primary ML/TF risks on an organization and/or line of business or legal entity basis.

2. Is there an effective process to ensure accurate calculation of KPIs and KRIs?

A lack of adequate controls over a key spreadsheet can result in unauthorized revisions to metric calculations yielding incorrect results.

3. Are upper and lower bands designed to trigger reporting set too tight or not tight enough?

An upper band requiring a twenty-five percent spike in suspicious activity reports (SAR) before escalation to the BOD may never result in escalation even if SAR reports increase by an otherwise significant amount.

4. Is analysis of KPIs and KRIs resulting in appropriate conclusions?
A principles-based approach for auditing board reporting

What is significant to some is not significant to others. Also, spikes in metrics can be misleading; pointing to one conclusion when another is potentially more appropriate. Professional judgment is required to interpret metrics and as such, it is important that there is a process for conclusions based on metrics to be vetted by management prior to inclusion in BOD reporting.

5. Finally, is there a continuous review process to ascertain that the current metrics and triggers continue to effectively measure what they are designed to measure?

Metrics must be updated and/or replaced as applicable to account for and align with changes to the organization’s risk profile and the evolving regulatory environment.

Risk: If BOD reporting for BSA/AML and OFAC compliance does not adequately communicate ML/TF risks and program effectiveness it is unlikely to comply with regulatory expectations. In addition, there is a risk that inadequate BOD reporting will not provide the BOD with sufficient information to effectively exercise their mandate. Inconsistencies in BOD reporting may be identified by the BOD, but there is also the chance that the BOD will fail to identify the error and make significant decisions based on bad data. Consistently flawed BOD reporting could have lasting negative effects for the organization.

Closing

In setting out to write this white paper I hoped to add value by discussing key factors to consider regarding independent testing of data aggregation and BOD reporting, as well as providing principles-based approaches to completing the work. This information should be useful as you begin to plan your audit of data aggregation and BOD reporting processes or are in the midst of annual planning and considering which audits should be in place for the
A principles-based approach for auditing board reporting

upcoming year. I made a case to rate data aggregation and BOD reporting processes as high risk and consider doing horizontal audits on an annual basis. I also identified one of the keys of BSA/AML and OFAC independent testing generally, which is to go beyond regulatory requirements and audit to regulatory expectations. Finally, I focused on KPIs and KRIs. These metrics are ubiquitous in large FIs and play a central role in BSA/AML and OFAC compliance programs. As such, it is important to understand the risks they present and potential pitfalls associated with them. Hopefully my principles-based approach yielded some straight-forward insights for you to consider and from which to potentially benefit.