Internal Audit: Raising the Bar in Auditing Financial Crime Risk
Exiger is a global regulatory and financial crime, risk and compliance company. Exiger arms financial institutions, multinational corporations and governmental agencies with the practical advice and technology solutions they need to prevent compliance breaches, respond to risk, remediate major issues and monitor ongoing business activities. Exiger works with clients worldwide to assist them in effectively managing their critical challenges while developing and implementing the policies, procedures and programs needed to create a sustainable compliance environment. A global authority on regulatory compliance, the company also oversees some of the world’s most complex court-appointed and voluntary monitorships in the private and public sectors, including the monitorship of HSBC. Exiger has four principal business units being: Exiger Advisory; Exiger Analytics, including DDIQ, the groundbreaking cognitive computing and intelligent search platform; Exiger Diligence and Exiger Insight 3PM. Exiger operates through offices in New York City, Silver Spring (DC Metro), Toronto, Vancouver, London, Hong Kong, and Singapore.
Banks have faced a raft of fines, consent orders and deferred prosecution agreements (“DPAs”) stemming from weak sanctions and AML programs in recent years. Since 2013, New York’s Department of Financial Services (“DFS”) has entered into 38 consent orders on these grounds. Many other well-known banks have been fined for violations of the Bank Secrecy Act and sanctions violations, including Standard Chartered ($300 million), BNP Paribas ($8.9 billion) and Commerzbank AG ($1.45 billion). Such penalties are not limited to the United States. In the United Kingdom, the Financial Conduct Authority (“FCA”) fined Barclays £72 million for its poor handling of financial crime risks and Deutsche Bank £227 million for manipulating Libor. The cost of these judgments is measured not only in eye-watering fines but also in immense reputational damage.

Enforcement actions of this type highlight the potential failure of managers and internal auditors to prevent, detect and deter non-compliant activity. While responsibility for this type of activity ultimately lies with senior management and the front line, repeated compliance failures raise serious questions about the effectiveness of an internal audit (“IA”) function.

Assess Controls to Ensure They Achieve Risk Management Outcomes

Regulatory breaches persist even though internal auditors have developed robust methodologies for evaluating the design and operating effectiveness of preventative and detective controls. Unfortunately, IA’s efforts do not always lead to measures that effectively identify poor risk management outcomes, address the root causes of control failures, properly assign accountability for these deficiencies or indeed ensure due dates leave enough elapsed time for controls to properly mature. Shortcomings in the control environment often persist in cases where corporate leaders are willing to accept a higher degree of residual risk than is warranted or fail to implement sustainable solutions, adopting sticky plaster fixes that are not wholly effective, without being held accountable for these bad decisions.

In September 2013, the Chartered Institute of Internal Auditors (“CIIA”) issued guidance that, as part of its evaluation of the design and effectiveness of policies and procedures, internal audit in the financial services sector should “consider whether the outcomes

achieved by these policies and processes are in line with the objectives, risk appetite and values of the organization”. Although the CIIA refreshed its guidance in September 2017, this statement still holds true. While this recommendation can be applied throughout a financial institution, evaluating outcomes is particularly valuable in addressing the AML, sanctions and anti-bribery and corruption (“ABC”) issues that are increasingly attracting scrutiny from regulators and law enforcement agencies.

IA can assure the board and senior management that internal controls are both fit for purpose and effectively managing risk through controls-based testing and focusing on the outcomes controls are designed to achieve. IA can thus avoid the unfortunate situation where controls are tested mechanically and assessed as “green” or “satisfactory”, even while outcomes remain sub-par. Audit functions that fail to dig deeper may fail to identify poor risk outcomes, leaving an institution vulnerable to financial crime and regulatory action. Most critically, IA must direct the business to ensure that bad actors are prevented from opening accounts through strong front-end controls. Given that criminals will often target institutions with a softer reputation for fighting financial crime, IA must guide the business to build a reputation that their institution is tough on this.

IA can only play the vital role it needs to if the institution has audit staff who understand regulatory requirements, the financial crime risks associated with its products and services, the regulatory expectations of an effective financial crime risk management framework and how to provide assurance over it. Auditors need to understand financial crime typologies so that they can identify gaps in the firm’s defenses. Since few auditors are available who have this unique blend of skills, those who do are in fierce demand. Board audit committees and senior management should therefore ensure that chief auditors have the skilled resources they need to more effectively provide assurance over the financial crime risk and control environment.

Clear Accountability

So how does a financial institution avoid the regulatory and reputational costs of poor AML and sanctions controls? One approach, which the regulators are currently taking, involves making senior bank staff formally accountable. In the United States, the DFS has, for example, mandated that senior compliance officers annually certify the effectiveness of certain aspects of their AML programmes. In a similar spirit, the United Kingdom’s FCA has introduced an accountability regime, called the Senior Managers Regime (“SMR”), which requires firms to

---

clarify and document individual accountability for senior management responsibilities, including for financial crime risk management. Although the trend of personal accountability appears to be here to stay, it has significant limitations. Many employees are hesitant to take on such burdens. For example, since the DFS rules went into effect in 2017, there has been anecdotal evidence that compliance employees are already leaving banks for consultancies and other institutions to avoid being forced to sign off on AML programs in which they lack either confidence or management support to fix sustainably.

In this environment, institutions need clarity as to who is accountable for lapses so they can meet compliance challenges head on. Moreover, there must be clarity regarding the responsibilities and expectations of IA. For internal auditors themselves, the concept of accountability for organizational failure is not new. In its International Standards for the Professional Practice of Internal Auditing (“Standards”), the Institute of Internal Auditors (“IIA”) stresses the importance of individual accountability. It mandates that auditors have the “knowledge, skills and other competencies needed to perform their individual responsibilities” and requires that they “make appropriate recommendations to improve the organization’s governance processes” particularly as they relate to “effective organizational performance management and accountability”.

The IIA defines internal auditing as “an independent, objective assurance and consulting activity, designed to add value and improve the organization’s operations”. It assists “the organization in accomplishing its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes”. If the board and senior management recognize IA as an assurance “consultant” and give it the stature and resources to become robust and strong, it can act as a safety net for management and compliance officers. By providing IA with the appropriate number of staff with expertise in financial crime, a financial institution can identify issues early, remediate them thoroughly and relieve some of the excessive pressures placed on compliance officers and executives. This can lead to an internal control environment that is not only sustainable and effective but tailored to the firm’s risk appetite.

Financial Crime Risk Auditing
There are many ways for financial institutions to strengthen their controls and improve the effectiveness of their financial crime audit programs. IA is best placed to play the vital role needed when the board audit committee challenges the function to raise the bar - so that it continues to improve its capability to uncover issues missed by the first and second lines, and find them before the regulators do.

(5) Ibid.
The following nine best practices can help IA, through its independent assurance and consulting activity, contribute to reducing the risk of facilitating financial crime and regulatory sanction of financial institutions.

1) Elevate Internal Audit’s Structure

IA may struggle to obtain support from management to remediate audit issues properly, escalate overdue findings or hold management accountable for failures to address control issues. For example, in its summary of the issues involving Commerzbank’s shortcomings, the DOJ explained that “the head of Commerzbank’s internal audit division stated in an email to a member of the firm’s senior management that Iranian bank names in payment messages going to the United States were being ‘neutralized’”. They warned “it raises concerns if we consciously reference the suppression of the ordering party in our work procedures in order to avoid difficulties in the processing of payments with the USA”. Indeed, IA’s warnings were not heeded and Commerzbank had to forfeit $563 million and pay a $79 million fine.

While DPAs and regulatory fines have brought compliance to the forefront, problems occur if IA lacks board and senior management support to function efficiently and effectively. It is therefore important that IA not only has direct access to the board in line with IIA standards, but that senior managers understand the impact of financial crime and regulatory risk on organizational objectives. Senior managers are more likely to take IA’s role seriously if those financial and reputational risks are made clear to them. Therefore audit’s reporting to senior management and the board needs to be insightful, and not just a regurgitation of audit results. Audit must provide on at least a quarterly basis, an opinion on the state of the control environment using audit judgment and data derived from audit results. The opinion should relate to the control environment in a global business, function, region or country, and state whether for example it is “satisfactory”, “requires improvement” or is “unsatisfactory”. This should be accompanied by a supporting explanation that provides insight to management on what all the audit results collectively mean based on factors such as: the level of unmitigated risk in high risk areas, overdue or open audit issues, key audit results, open regulatory issues and change projects in train. The assessment should include root causes and also the trend in the control environment to give management a sense of whether it is “stable”, “improving” or “deteriorating”.

While DPAs and regulatory fines have brought compliance to the forefront, problems occur if IA lacks board and senior management support to function efficiently and effectively.

Samar Pratt
Managing Director

stature is sufficiently elevated within the organization so that it is capable of providing insightful reporting to the board before the regulators do.

2) Assess the Compliance Culture
Regulators now look to financial institutions to have a “culture of compliance” that encourages employees to voice concerns around compliance matters. Without a strong compliance culture, the best designed controls will be severely impaired in their execution. For this reason, it is imperative that IA takes organizational culture into consideration when performing regulatory or financial crime audits, and to assess management action plans to instill a strong compliance culture. In these instances, it is important that auditors dig deeper to find out where the break-down in the escalation of issues is occurring.

Corporate culture is an especially challenging indicator of a financial institution’s ability to manage financial crime and regulatory risk. It is incumbent upon IA to educate board members and senior management about the root causes of failures in compliance culture and provide them with the information they need to respond to emerging issues. IA should identify metrics that indicate whether the business is driving an effective compliance culture, such as audit issue “re-open” rates. IA should also assess the effectiveness of “balanced scorecards” that are in place to assess the compliance of front line revenue generators and ensure that the incentivization process is set up to drive the right behaviors.

3) Quarterly Business Monitoring
To monitor the risk profile of the institution, IA should conduct quarterly monitoring through regular meetings with the business and reviews of relevant management information. Ideally IA should also evaluate the progress of management action plans – especially those relating to high risk audit issues, reassess relevant issues and identify any meaningful changes. Ultimately, management should empower IA to monitor those functions that bear on financial crime risks. Finally, once the business declares victory in having addressed an audit issue, the three lines of defense model crumbles if IA does not check this thoroughly. IA must therefore have an effective issues validation process, that carefully examines the evidence and re-tests newly implemented controls, to ensure sustainable control improvements.

4) End-to-End Financial Crime Audits Across the First & Second Lines of Defense
Providing appropriate time to plan and complete audits is crucial, as well as assessing the controls in place to manage financial crime risks “end-to-end” across the first and second lines of defense. This type of financial crime outcome-based auditing inevitably takes longer as it is risk-based and assesses controls and outcomes “end-to-end”. Failure to test in this way will
result in IA not being able to flush out control issues that standalone audits of, for example, know your customer (“KYC”) or transaction monitoring activities, will never be able to identify because of the interconnected nature of process, systems and data within a financial institution’s financial crime compliance program. IA must challenge long-standing controls that do not yield results. To do this, auditors need sufficient time to evaluate and identify the root causes of control failures or poor outcomes across the various lines of defense.

After testing outcomes, IA should compare its audit results against the understanding that the business has of its own control issues, as well as second line compliance testing results, to assess whether these lines of defense have raised all the appropriate red flags and identified similar issues. If not, they should find out why. Only by conducting a rigorous examination across the first two lines of defense can internal auditors identify whether the outcomes are acceptable. The inclusion of this final step, assessing the intersection of an institution’s goals and its outcomes across the first and second lines of defense, creates a three lines of defense model that is more effective in rooting out compliance issues.

5) Risk-Based Audit Plan & Sampling Approach
The most effective audit departments adopt a risk-based approach to annual audit planning. This involves maintaining an “audit universe” that is risk-assessed annually and refreshed quarterly as part of quarterly business monitoring, so that adjustments can be made to the audit plan to reflect changes in the risk profile. Resources are often limited and significant time can pass between audits on cyclical plans, so it is important to consider the risk that a part of the business presents before auditing it. Moving from cycle-based to risk-based auditing however does not mean focusing exclusively on high-risk areas. Some work may still need to be cyclical, especially in cases of low or moderate risk and recurring high risk.

A risk-based approach can be proactively employed in sampling to test both preventative and detective controls. Although many banks employ random sampling during audit testing, most financial crime compliance fines are not the result of the 95% of the time that a control works effectively. Rather, penalties arise from issues that are often unknowns, which a targeted risk-based sample has a greater chance of detecting.

6) Make Recommendations That Address Root Causes & Specify Expected Outcomes
IA needs the authority and skill to make recommendations that enable management to take corrective actions. Effective actions are those that target the risk, root causes and clearly identify “who did not do what to whom” to
ensure clear accountability for failures to minimize repeat control issues. Recommendations must encapsulate the risk management outcomes that the business needs to achieve. IA must play a role in agreeing with management the actions they plan to take so that IA has some “skin in the game”, although this should never impact IA’s independence. IA must make clear to the business that time lines for completion should not just reflect the time required to implement the control enhancement, but also to embed it into business-as-usual operations and to evidence the required outcomes.

One common response to IA findings is that only once the organization receives a new system or technical solution, the concern will be addressed. While this may be warranted in some cases, the reality is that management is being negligent if it fails to mitigate ongoing risk while waiting for a new tool. Finding resources and approval for new solutions can take years, especially in an environment where profit-seeking takes precedence over compliance. Yet, the efficacy of such a new system does not excuse delayed action. Even partial improvement is better than the inaction of waiting. If at the next audit or follow-up review the risk has not been mitigated, at least partially, the issue should be escalated up the chain of command – ultimately to the COO, CEO or board audit committee if the risk is very high. Whatever the historical justification, it is vital once recurrent issues are identified and escalated that mitigating controls become part of the management action plan.

7) Integrate Data Analytics Into Your Audit Methodology

It is impossible to fulfill the internal audit mandate today using manual processes alone. Few IA departments have successfully integrated data analytics into their audit methodology, for example, to aid in the continuous monitoring of critical elements of the control environment – to detect controls that have broken down or where there is latent crystallized risk waiting to blow up. Many have failed to advance from simple computer-assisted audit techniques that are not very good at detecting emerging or hidden risk. But data is much easier to access than in bygone years and analytical tools are more powerful. In the right hands, they are also easy to use. Refashioning a financial crime audit program to use data analytics to drive efficiency and developing methodologies that include technology-driven audit tests that are repeatable, auditable and not highly manual should be a priority. IA must learn to tap efficiently into the vast volumes of transactional, customer and other operational data that is available and use it in a targeted way to improve its ability to proactively root out control breakdowns.

“IA must learn to tap efficiently into the vast volumes of transactional, customer and other operational data that is available and use it in a targeted way to improve its ability to proactively root out control breakdowns.”

Samar Pratt
Managing Director
It does not have to cost the earth either. Successful implementation of data analytics requires it to be well planned and integrated into the audit methodology, and sufficiently resourced with appropriately skilled staff. It must be introduced gradually, targeting specific risks and taking each critical business process and control at a time. Consider adopting a pilot approach by testing a specific area of the financial crime program, such as the exiting of customers who exceed your institution’s risk appetite. Run analytics across your recent transaction history and compare it against your list of exited customers to identify those that may still be active after the supposed exit date to identify failures in exit controls. Once results are proven through a small pilot, the chief auditor can present a more compelling business case to the audit committee to enable a step change in the use of data analytics in the IA methodology. Where budgetary constraints inhibit investment, IA should look to the second line and understand how compliance is using data analytics to find hidden pockets of unidentified risk and explore opportunities for IA to leverage this resource.

8) Utilize Financial Crime Compliance Experts
All of this relies on an institution’s ability to employ and utilize the right experts. To ensure that IA has the right individuals with the required level of knowledge and experience, IA should conduct an annual skills and training needs assessment which reviews the risk-based plan against the current skill set of the audit team. This assessment will identify potential gaps in the financial crime skills needed to complete the annual audit plan. In cases where specific training cannot provide the expertise to tackle complex audits, IA should engage external experts and ensure some skills transfer to their employees. Professionals who have worked in financial crime roles can provide much needed expertise. Outside experts will be able to explain which controls are most vital and where a program might lack appropriate coverage. These experts do not need to be full-time internal auditors. Such specialists are available through internal secondments, a guest auditor program or the hiring of external consultants.

In cases where specific training cannot provide the expertise to tackle complex audits, IA should engage external experts and ensure some skills transfer to their employees. Professionals who have worked in financial crime roles can provide much needed expertise. Outside experts will be able to explain which controls are most vital and where a program might lack appropriate coverage. These experts do not need to be full-time internal auditors. Such specialists are available through internal secondments, a guest auditor program or the hiring of external consultants.
9) Learn from the Past & the Mistakes Made by Others
A truly valuable IA function will be dynamic, learning from the past and from other institutions. Auditors must consider issues previously raised by regulators, other assurance functions in the first and second line and external consultants. Reviewing consent orders, thematic reviews and generally staying abreast of current regulatory developments, including external fines, can also aid auditors in planning and scoping audits. Understanding these reports and concerns is invaluable for assessing the effectiveness of a financial institution’s control environment and the sustainability of its financial crime compliance program. Most IA departments include internal issue reviews as part of their audit work. To raise the audit team’s awareness of the failings of their peers however, IA departments should include this as a requirement as part of the planning process in their IA manual and dedicate a specific place in their work papers to document any findings identified. Going through this exercise prior to any financial crime audit will give the audit team an insight into what the regulators are focused on and where audit should make sure controls are working effectively.

In light of the continuing fines from regulators and a recent increased focus on individual accountability, IA must continue to challenge itself by raising the bar and digging deeper to identify poor risk outcomes in the first line as well as inadequate risk oversight by the second line. IA must refashion its financial crime audit program to harness data analytics to create technology-driven audit tests that can identify critical control breakdowns or crystallized risk that the rest of the organization has missed. IA must also help institutions move towards implementing more effective financial crime compliance solutions by challenging management to implement sustainable fixes that not only address root causes of control failures but also achieve intended risk management outcomes.

IA is the third and final line of defense against financial crime breaches. Indeed, regulators are eager for IA to aid their supervisory efforts and to ‘rely’ on their work. A robust IA function is one which has both the expertise and the resources it needs to raise the bar on its financial crime audit program. Such investment can not only help minimize the regulatory risk of a consent order, large fine or a DPA – and the reputational damage that comes with them – but also minimize an institution’s financial crime residual risk exposure and, at the same time, strengthen its ability to disrupt financial crime itself.
For more information, contact:

Samar Pratt  
Managing Director  
spratt@exiger.com

Erika Peters  
Associate Managing Director  
epeters@exiger.com