Does one size fit all?

The modernization of an AML Audit into a Financial Crime Audit

Jay Smith, CAMS-Audit

ACAMS® | Advancing Financial Crime Professionals Worldwide

Contents

1 EXECUTIVE SUMMARY

Does one size fit all? Can an anti-money laundering (AML) audit mitigate an institution's every risk of financial crime? As bribery and corruption regulations continuously expand and new regulations, such as the Foreign Account Tax Compliance Act (FATCA), emerge, the need for more comprehensive in-house risk policies has increased significantly. Corporate leaders have come to realize that other risks, such as sanctions and fraud, threaten the reputation of every institution. Therefore, even though current regulations only require an AML audit to be conducted, it is considered a management best practice to have an independent audit within the organization for other types of financial crime risks.

This white paper postulates that a robust independent financial crime (FC) audit will enable the organization to detect and deter a broader set of financial crime risks, and why all organizations can easily adopt such FC audits because the steps and processes are already established for their mandatory AML audits. Although the focus of an independent FC audit is to "kill two birds with one stone," it does not recommend consolidating the AML and FC audit into a consolidated FC program.

The white paper will refer to the results of a survey that was conducted for the sole purpose of this paper. (Appendix 7.2) The survey shows that compliance professionals strongly feel that their current AML audit programs can be, and should be, expanded to include other financial crime risks. This paper will also explain how auditing the management best practice of "knowing your employee" can help to mitigate asset misappropriation risks. In 2014, asset misappropriation was identified by PricewaterhouseCoopers (PWC) as the most prevalent economic crime reported by financial institutions.[1]

This white paper will also highlight the need for independent audits to be completed by qualified individuals. This is currently not a requirement in some offshore jurisdictions. Furthermore, some institutions have their AML audits completed by their external financial auditor as part of their annual audit process. Although convenient, these financial auditors may not be qualified to spot the signs of the broader range of financial crimes.

Overall, this white paper will conclude that every organization will benefit from a FC audit, and that in this instance, one size does fit all.

[1] http://www.pwc.com/gx/en/economic-crime-survey/economic-crimes/index.jhtml

2 BACKGROUND

Independent auditing of an anti-money laundering/counter-terrorist financing (AML/CTF) program is a regulatory requirement highlighted in Section 352 of the USA PATRIOT Act[2] and is carried out by organizations to check the effectiveness of their AML/CTF controls and systems. In general, independent auditing refers to the scrutiny of an organization's AML/CTF program by an objective person or department that is unrelated to the AML/CTF functions within the organization, or by an independent third party. A thorough AML/CTF audit will help the organization understand if their program is up-to-date with the legislation, and highlight any loopholes in the controls and systems, so that corrective measures can be implemented. Section 352 of the USA PATRIOT Act and the Financial Action Task Force (FATF) Recommendation 18 requires an AML/CTF program to include the following;

1. Development of internal policies, procedures and controls
2. Designation of a compliance manager
3. Ongoing training for employees
4. An independent audit function to test the system[1,3]

The points mentioned above are just an indication of the minimum requirements of an AML/CTF program as required by law, but should not act as the exhaustive framework. As highlighted by FATF Recommendations in 2012, AML/CTF programs should be planned with a risk-based approach. Therefore, in addition to the requirements mandated by legislation, AML/CTF best practice would mandate incorporating the following aspects: AML/CFT risk assessment in the areas of products, customer types, geographic business locations, and other relevant aspects:

1. Enterprise-wide approach
2. AML and OFAC monitoring system
3. Documentation
4. Reporting, constant follow-up and escalation, as well as including the review of reports such as suspicious activity reports (SARs) and currency transaction reports (CTRs)
5. Know your customer/Customer Identification Program (KYC/CIP)
6. Customer due diligence (CDD) and enhanced due diligence (EDD)
7. Information sharing as required under Section 314

2 USA Patriot Act of 2001, http://www.sec.gov/about/offices/ocie/aml/patriotact2001.pdf

3 FATF Recommendations, International Standards on combating money laundering and the financing of terrorism & proliferation.

8. Regulatory examinations by the designated authorities such as FINRA, SEC and others.[4,5]

However, the question remains: Why are these guidelines only limited to AML/CTF but not mandatory for other financial crimes such as tax evasion, bribery and corruption, sanction and fraud? Also, should employee due diligence be conducted in the same manner as due diligence for customers? In many cases, screening of employees is neglected and could not only turn into an AML/CTF risk, but more importantly, even reputational risk depending on the nature of the business.

Apart from money laundering, all institutions are acutely aware that they are exposed to the greater range of financial crime, including bribery, corruption, cyber-crime, fraud and sanctions, and have adopted different systems and programs to combat these risks. However, they are not required by law to independently audit these financial crime defences, and constantly rely on their own internal audit committees to check these programs, disregarding the importance of impartial, objective assessments of these pervasive financial and reputational risks.

3 FINANCIAL CRIME AUDIT METHODOLOGY

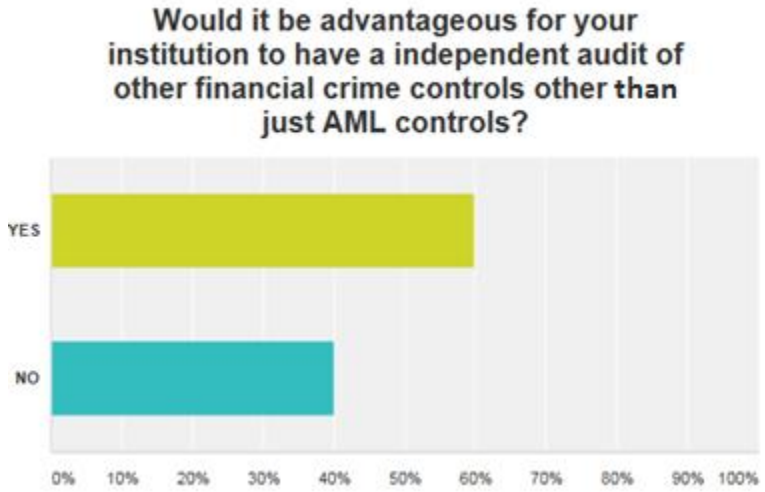
AML policy and procedures have gotten better in determining what processes and controls are needed to mitigate AML risks. As these regulatory requirements expand, the risks and mandatory controls have evolved with them to enhance protection against AML risks. A FC audit methodology will expand on a typical AML audit methodology to include testing controls that mitigate the other financial crime risks. The objectives of a FC audit should include:

- The effectiveness of the institution's overall compliance function in timely identification, analysis, monitoring and reporting of the principal FC risks, which the institution is exposed to, and the responsiveness of these compliance functions to changing risk dynamics
- The appropriateness and successful implementation of management decisions, and their adherence to director's directives
- Policies and procedures of the institution are up-to-date and effectively implemented
- Compliance with regulatory and procedural requirements, and the approved policies of the institution.

4 Goldzung, Laura H, Managing AML audit expectations, http://www.amlauditservices.com/Articles/Goldzung_PCRM_Nov%202013.pdf

5 The role of an effective independent review of your institution's anti- money laundering (AML) program by Pricewaterhouse Coopers, https://www.pwc.com/en_US/us/financial-services/regulatory-services/assets/pwc_aml_role.pdf

Do these objectives sound remarkably familiar? They should, as there are very similar to the objectives of a typical AML audit. The only difference is its focus on the broader scope of FC risks. Hence, initiating a FC audit can be easily accomplished as many of the planning, executing, reporting and monitoring processes are already established for the AML audit. In the survey, 60 percent of participants felt that having an independent FC audit is beneficial to reducing FC risks. One respondent went as far to say, "Who would answer no!" Full results of the survey are available in Appendix 7.3.



Of the 23 percent of respondents who said that their organization did not have any independent and regular reviews of their other FC programs, the reason was consistent: cost. While this paper makes no attempt to adopt an apathetic attitude towards the obvious cost of FC auditing, we emphasize that companies need to have very clear expectations of the cost of regulatory compliance and recognize the necessity of staying ahead of financial criminals. The recent spate of high profile regulatory action against institutions such as HSBC, JPMorgan Chase Bank, N.A., TD Bank and N.A. cements the fact that no one is immune to financial crime, nor the penalties of non-compliance. [6]

Although funding the more expensive financial crime audit could increase the cost of compliance, there are several ways to mitigate the cost apart from passing the costs on to the customer, or allowing it to eat into the bottom line. Possible sources of funding include savings achieved from an institutional-wide implementation of:

- Adoption of cloud-based systems to reduce document retention costs

[6] www.bankersonline.com/security/bsapenaltylist.html.

- Streamlining of processes into electronic platforms
- Reduction of travel and training expenditure by using teleconferences, webinars, and/or online modules.

Implementing a robust FC audit should not be evaluated purely on the basis of cost. As important a consideration as that may be, it must be evaluated based on what is reasonably and morally expected of a quality financial institution. Once these companies successfully implement an effective FC audit strategy, the benefits of greater customer confidence and the derived savings from preventing a financial crime will appreciably outweigh the cost and effort of preventive action.

3.1 Financial Crime Audit Risk Assessment

Initiating the FC audit is arguably the most challenging phase that the company will face. Where do you start and what should be your focus? Which FC risk should get the most attention?

A FC audit risk assessment (FCARA) should be conducted to identify which areas of the operation are most vulnerable to financial crime. The first place to start would be the current AML risk assessment, as most organizations tend to integrate the audits of other FC risks into their AML risk assessment in some form or another. In our survey, 73 percent of respondents confirmed that their AML risk assessment already includes some form of oversight on other financial crime risks. The risk elements that are already identified in the current AML risk assessment are the ones that are most relevant, and/or prevalent in your industry or business.

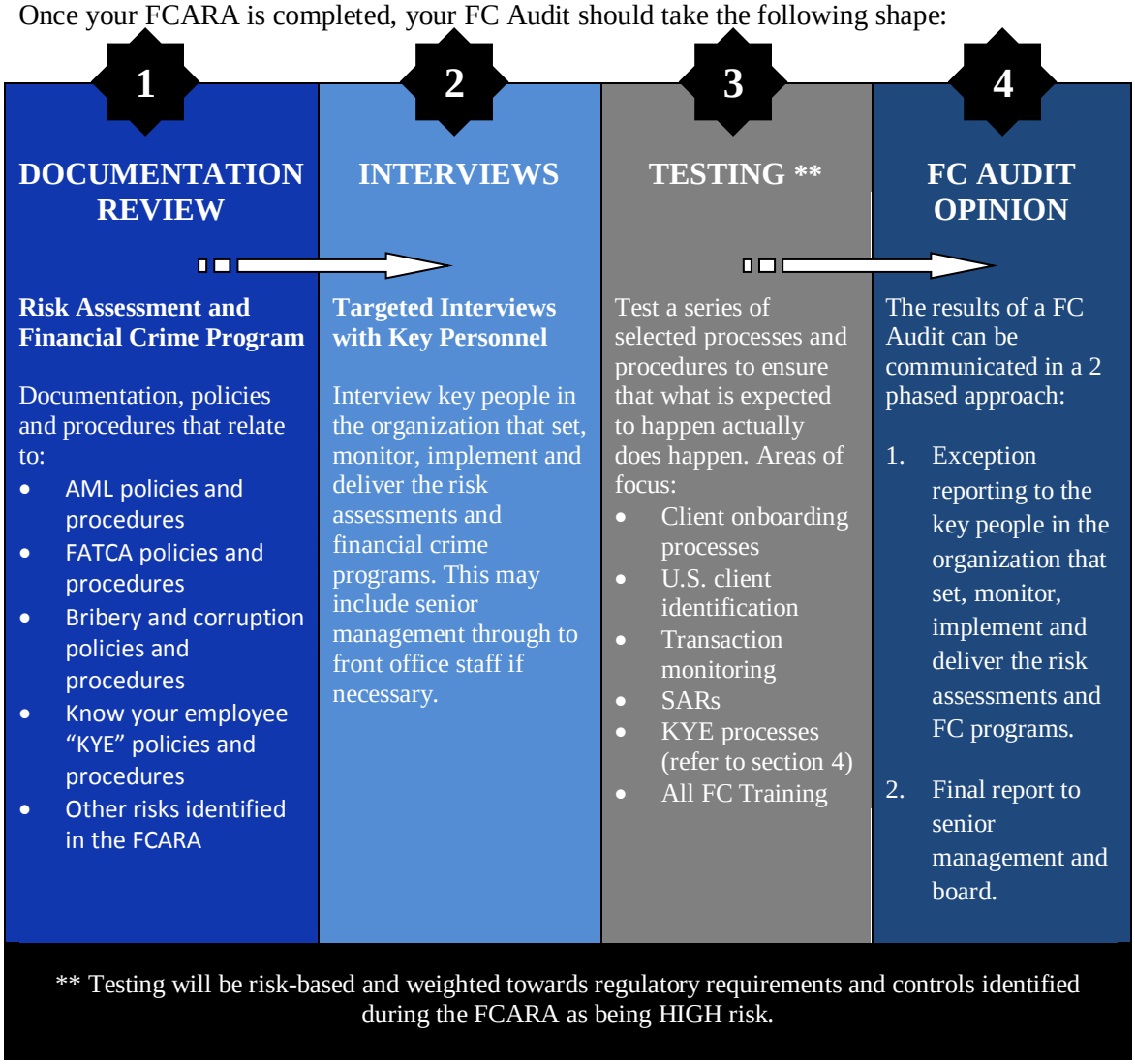
In addition to the vulnerabilities that are listed in the AML risk assessment, it is important to run through and evaluate other potential FC risks that do not appear to affect the organization at the moment. Vulnerabilities such as asset misappropriation, fraud, bribery, corruption, cyber-crime, data theft and insider dealing are just some of the major threats to all businesses, and usually take place under the radar unbeknownst to the business owner. Having an audit that ensures that the tell-tale signs are identified and reported could help rein in a financial or reputational disaster before it happens.

The steps to plan and operationalize your FCARA should be:

- Identify what your annual regulatory requirements are (i.e., AML/FATCA)

- Confirm weaknesses, control deficiencies and opportunities that have been identified in the AML risk assessment
- Identify other possible vulnerabilities that are un-related to AML/CTF (i.e., fraud, bribery, corruption)
- Identify AML risk assessment processes and activities where the FC audit can integrate and align with to "kill two birds with one stone."

Once your FCARA is completed, your FC Audit should take the following shape:



This approach is methodical and robust, and adopts an enterprise wide oversight with particular focus on areas where FC risks are highest.

This methodology undertakes a "point in time" audit to assess the organization's compliance with AML, FATCA and the competence of the internal systems to protect against other financial and reputational risks. It will also complete work to assess the controls surrounding

data protection procedures and information technology (IT) security contracts/programs. (NOTE: This will not include a detailed audit of the integrity of the IT programs as it is suggested that this should be completed by a content expert in IT.) The schedule for certain FC tests can be completed on a periodic basis depending on where the risk is highest. Obviously AML requirements will still have to be included annually.

3.2 Review of Training Records

Ensuring that employees are trained to understand and identify what constitutes a FC risk is critical to an institution's protection against these malicious activities. Training employees on the risks of money laundering is a regulatory requirement, but educating them on other FC risks is not, despite these risks being just as important, and possibly a greater reputational risk, to the institution. In the survey, more than half of respondents noted that their compliance training only included AML, FATCA, fraud, bribery and corruption-related topics. FC audits should broaden the focus of the audit to include the review of other financial crime training material.

Areas of focus for the FC audit should be:

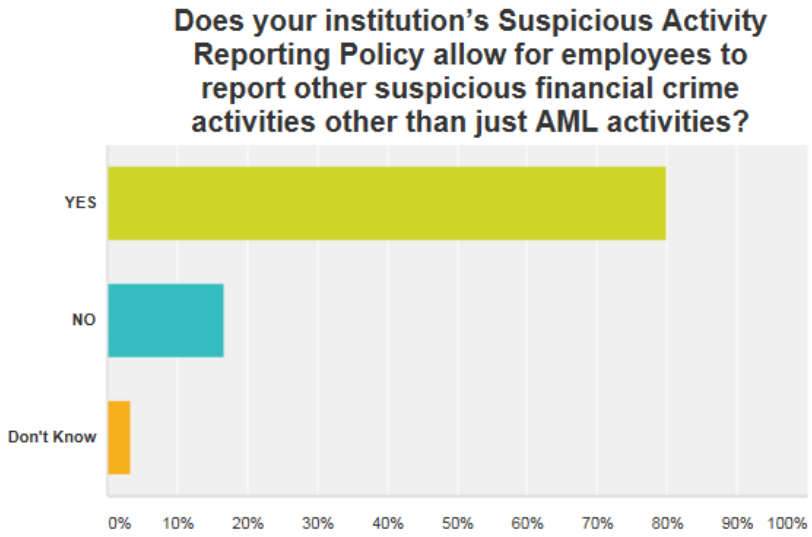
- Are FATCA requirements included in the training?
    - Can employees identify U.S. client activities
    - Do employees understand reporting requirements
- Are employees educated on bribery and corruption?
- Assess the effectiveness of fraud training.
- Are employees reminded about data protection and other IT security threats?

Just like the assessment of AML training, each area of focus should be concentrated on completeness, frequency and effectiveness of the FC training. It is critical that employees understand why they are completing these courses. Completing a FC audit and identifying gaps in this process will mitigate an institution's risk against financial crime.

3.3 Suspicious Activity Reporting

SARs or Suspicious Transaction Reports (STRs) are mandatory regulatory requirements in most reputable jurisdictions. Maintaining a clearly defined channel for personnel to raise any concerns in relation to suspicious activities, without fear of reprisals, is critical in minimizing your institution's risks to AML and other FC activities. Eighty percent of the surveyed

respondents felt that their institution's SARs policy already allows for employees to report other suspicious activities other than AML activities.



According to BankersOnline.com:

> Most of the BSA SAR reportable conditions across the sectors are in fact fraud and not money laundering… Better risk assessment processes are leading, responsively, to better detection and reporting of both AML and non-AML activity... The radar screen must be all-encompassing.[7]

When auditing an institution's SARs process, the main objective should be to identify any potential vulnerability to money laundering and other financial crimes. It is also not unusual for an auditor to discover potential suspicious activities during the audit process. Thus, it is important that auditors should have sufficient training and expertise to recognize unusual and suspicious activities beyond AML.

4 KNOW YOUR EMPLOYEE

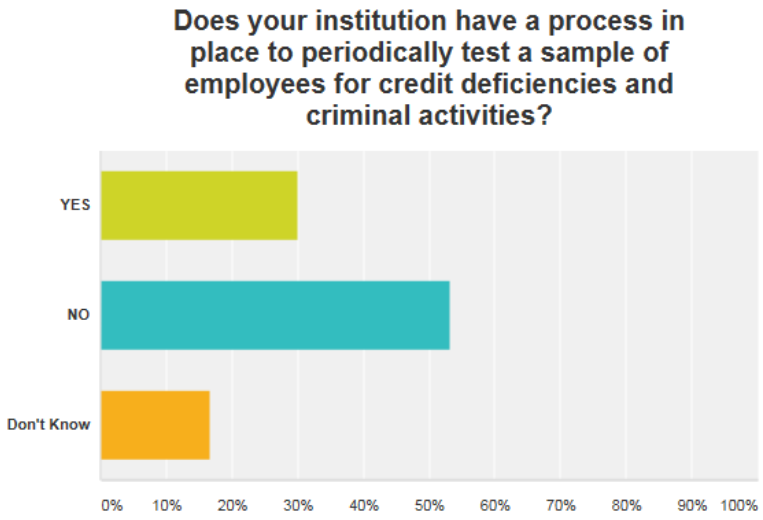
4.1 Why should you audit your know your employee processes?

The concept of know your employee (KYE) is not new to internal audits, nor is it new to AML best practices. However, incorporating KYE into a FC audit highlights new control weaknesses that have never been identified before. In their 2014 Economic Survey, PWC identified asset

[7] Abel, Alan S., Update: Auditing the AML Program – What's New? , www.BankersOnline.com.

misappropriation as the most commonly reported crime,[8] typically committed by those affected by the global economic slump, even those with jobs as these people struggle to maintain a certain lifestyle.

The survey revealed that 53 percent surveyed identified that their institution does not have a process to periodically assess employees' credit deficiencies and criminal activities.



4.2 How can you audit this sensitive process?

So where should institutions start the process to KYE? The perfect starting point is at the beginning, during the recruitment process. After employment, supervisors should continue to monitor their staff's behavior so as to identify and report any situations that might be considered suspicious. Although this should already be standard practice in most organizations, companies should enhance the KYE process to include an audit of the personal activities of employees.

KYE audits of individuals should focus primarily on senior management, middle managers and other professionals with key access into the corporate system. The inclusion of who to monitor should be risk-based and weighted towards individuals with previous policy violations, individuals working in cash sensitive areas, newly promoted managers, and individuals with key system access.

The following table proposes a sample policy for KYE testing:

[8] http://www.pwc.com/gx/en/economic-crime-survey/economic-crimes/index.jhtml.

Senior Management	To be tested once every three years
Employees with Previous Violations	To be tested one year after violation
Employees working in Cash Sensitive Areas	To be tested once every three years
Employees with "Key" system access	To be tested once every three years
Newly Promoted Managers	To be tested one year after promotion

The KYE audit should include the completion of a questionnaire that requires employees to attest to various policies and provide supporting documents. Additional questions should include:

- Details of audited person and their immediate family. Such as:
    - Marital status
    - Dependents
- Overview of financial interest and dealings, and other external appointments such as:
    - History of dealings with credit agency
    - Members of immediate family holding any directorships

Auditees will not be required to provide details of quantities or monetary amounts, unless the materiality of the holding is a conflict of interest. During the interviews, the FC auditor will also inquire into the auditee's understanding of company policies, code of ethics, independence and how such workplace policies affect them on a personal basis.

If a KYE audit is not feasible, there are a number of internal monitoring systems that organizations can use, for example:

- A portfolio review
- Review of reactivated accounts
- Exception reports
- 'Same name' reports – When an account holder has same name, especially last name, as employee accessing account;
- Transfer Reports – Transfers that have been completed soon after a change of address or similar customer detail changes

- Behavioral pattern analysis[9] – This should already be included in the annual training for managers

The recommendations described in the KYE audit section are subject to jurisdictional rules and regulations, and legal advice should be sought before implementing such. Upon execution, corporate leaders must make it clear that such a policy benefits the institution, employees, shareholders and the customers.

5 WHO SHOULD CONDUCT THE AUDIT

5.1 Independence

Although not a requirement in some jurisdictions, the AML audit can be completed by anyone who is independent of the institution and/or of the compliance function. Most institutions have their own internal audit committee look into other financial crimes, hence the absence of independent auditing. The absence of independent auditing provides an opportunity for individuals to engage in financial crimes, often resulting in financial and reputational risks to the institutions. Furthermore, independent audits reduce the chances of collusion.

5.2 Qualification

Who should, and who is qualified to conduct the FC audit is another topic entirely and is beyond the focus of this white paper. However, it is worth mentioning that the increased scope of a FC audit may be beyond the abilities of a regular external or internal auditor, CPA or CA. An auditor specializing in the studies of financial crime would be better suited to consult on FATCA, bribery, corruption, sanction and fraud requirements.

Specifically relating to IT systems, although a FC audit could help to assess the controls surrounding data protection procedures and IT security contracts/programs, the detailed audit of the integrity of the IT programs should be left to a competent IT security expert.

6 CONCLUSION

Although most reputable jurisdictions only mandate the completion of an independent AML audit, it is categorically clear that much more is needed to protect today's institutions from a

[9] Erlick Companys, S.A., P&P Manual for the Prevention of ML and TF, http://www.erlick.com.uy/PP_Manual_en.pdf.

larger array of FC risks. Most companies have already subconsciously included other FC risks under their AML audits, but until an objective, enterprise-wide investigation into the other non-AML/CTF risks is conducted, these businesses remain vulnerable to a vast array of liability and reputational dangers that might only be caught when it is too late.

Risk and vulnerabilities are ever evolving and rules, both regulatory and societal expectations, change constantly. What used to be called a "friends and family discount" may today be easily construed as a conflict of interest. And if your friend or family sets you up for a job interview or helps you expedite a process, does an appreciation gift form facilitation payment or a bribe?

Just because regulatory requirements mandate an AML audit does not mean that the largest or most dangerous risks are AML related. The truth is, many companies are already (sub-consciously) completing more than just an audit of AML controls. They understand that other FC risks are present and are already affecting their businesses and reputations. But what about the risks that are lurking beneath and are a ticking time-bomb waiting to explode? Perhaps it is time to face up to reality and acknowledge that a broader, more objective FC audit is no longer optional in today's business environment.

7 APPENDIX

7.1 Acronyms

AML – Anti Money Laundering

CTF – Counter-Terrorism Financing

FCARA – FC Audit Risk Assessment

FATF – Financial Action Task Force

FC – Financial Crime

FATCA – Foreign Account Tax Compliance Act

PWC – Price Waterhouse Coopers

SARs – Suspicious Activity Reports

STRs – Suspicious Transaction Reports

7.2 Survey Results

The survey was carried out between April 2014 and June 2014. This survey was completed by 30 respondents in 10 different sectors (refer to question 2). The respondents were from LinkedIn AML Groups and members of the Association of Bermuda Compliance Officers (ABCO). I used Survey Monkey to complete the survey and analyze the data.

1. What kind of jurisdiction are you currently working in?		
Answer Options	**Response Percent**	**Response Count**
Offshore Jurisdiction	60.0%	18
Onshore Jurisdiction	40.0%	12
	answered question	30

2. What sector is your institution in? *Multiple categories may apply.		
Answer Options	**Response Percent**	**Response Count ***
Accounting	6.7%	2
Banking	36.7%	11
Broker	3.3%	1
Corporate Service Provider	10.0%	3
Gaming	6.7%	2
Insurance	6.7%	2
Money Service Business	3.3%	1
Securities	10.0%	3

Trust	26.7%	8
Other (please specify)	13.3%	4
	answered question	30

3. What form of financial crime is of the greatest concern for senior management?

Answer Options	Response Percent	Response Count
Asset misappropriation	10.0%	3
Bribery and corruption	0.0%	0
Cybercrime	3.3%	1
Data Theft	6.7%	2
Fraud	0.0%	0
Insider Dealing	3.3%	1
Money Laundering	70.0%	21
Tax fraud	3.3%	1
Other (please specify)	3.3%	1
	answered question	30

4. Does your institution have a policy in place to carry out an independent and regular review (by either an internal or external party) of all components of its AML program?

Answer Options	Response Percent	Response Count
YES	90.0%	27
NO	10.0%	3
Don't Know	0.0%	0
	answered question	30

5. Does your institution have a policy in place to carry out an independent and regular review (by either an internal or external party) of other financial crime programs (i.e. FATCA, Fraud, bribery, etc?)

Answer Options	Response Percent	Response Count
YES	73.3%	22
NO	23.3%	7
Don't Know	3.3%	1
	answered question	30

6. Would it be advantageous for your institution to have an independent audit of other financial crime controls other than just AML controls?

Answer Options	Response Percent	Response Count
YES	60.0%	18
NO	40.0%	12
Additional Comments?		8
	answered question	30

7. Does your institution's AML Risk Assessment include other financial crime risks?

Answer Options	Response Percent	Response Count
YES	73.3%	22
NO	16.7%	5
Don't Know	10.0%	3
answered question		30

8. If YES to question 7, what other financial crimes are included?
*** Multiple responses per respondent.**

Answer Options	Response Percent	Response Count *
Fraud	64.0%	16
Bribery & Corruption	52.0%	13
Cybercrime	32.0%	8
FATCA	80.0%	20
Tax Evasion	40.0%	10
Other (please specify)	16.0%	4
answered question		25
skipped question		5

9. If NO to question 7, does your institution's overall Risk Assessment include other financial crime risks or has your institution created a separate risk assessment for the other financial crime risks?

Answer Options	Response Percent	Response Count
YES	33.3%	8
NO	12.5%	3
Not Applicable	54.2%	13
Additional Comments?		2
answered question		24
skipped question		6

10. Do you feel that your institution's current AML program mitigates exposure to other financial crime risks?

Answer Options	Response Percent	Response Count
YES	70.0%	21
NO	23.3%	7
Don't Know	6.7%	2
Additional Comments?		1
answered question		30

11. Do you anticipate that your institution's budget for compliance will increase with greater emphasis on Cybercrime and FATCA implementation?

Answer Options	Response Percent	Response Count
YES	63.3%	19
NO	30.0%	9
Don't Know	6.7%	2

	answered question	30

12. Does your institution's Suspicious Activity Reporting Policy allow for employees to report other suspicious financial crime activities other than just AML activities?

Answer Options	Response Percent	Response Count
YES	80.0%	24
NO	16.7%	5
Don't Know	3.3%	1
answered question		30

13. If NO to question 12, why are staff not allowed to report other suspicious activities?

Answer Options	Response Percent	Response Count
Staff have not been trained to recognize other threats.	14.3%	2
Legislation does not permit other suspicious activities from being reported.	0.0%	0
Your local Financial Intelligence Unit will only investigate AML suspected activities.	14.3%	2
Don't Know	21.4%	3
Other (please specify)	50.0%	7
answered question		14
skipped question		16

14. How often is your AML training rolled out?

Answer Options	Response Percent	Response Count
Monthly	6.7%	2
Quarterly	6.7%	2
Bi-Annually	6.7%	2
Annually	66.7%	20
Don't Know	0.0%	0
Other (please specify)	13.3%	4
answered question		30

15. What financial crime topics are included in your Compliance training program? * Multiple responses per respondent.

Answer Options	Response Percent	Response Count *
AML	86.7%	26
FATCA	56.7%	17
Tax Evasion	30.0%	9
Fraud	53.3%	16
Bribery & Corruption	53.3%	16
Cybercrime	13.3%	4
All of the above	16.7%	5
Don't Know	0.0%	0

Other (please specify)	3.3%	1
	answered question	30

16. Does your institution have a Know Your Employee Policy?		
Answer Options	**Response Percent**	**Response Count**
YES	53.3%	16
NO	43.3%	13
Don't Know	3.3%	1
	answered question	30

17. Does your institution have a process in place to periodically test a sample of employees for credit deficiencies and criminal activities?		
Answer Options	**Response Percent**	**Response Count**
YES	30.0%	9
NO	53.3%	16
Don't Know	16.7%	5
	answered question	30

18. Before an employee is hired or promoted into a position of trust and/or given various system access, does your institution have a process in place to research if the employee has any credit deficiencies and criminal activities?		
Answer Options	**Response Percent**	**Response Count**
YES	46.7%	14
NO	30.0%	9
Don't Know	23.3%	7
Additional Comments?		4
	answered question	30

7.3 Resources

Abel, Alan S., Update: Auditing the AML Program – What's New?, www.BankersOnline.com.

Erlick Companys, S.A., P&P Manual for the Prevention of ML and TF, http://www.erlick.com.uy/PP_Manual_en.pdf.

FATF Recommendations, International Standards on combating money laundering and the financing of terrorism & proliferation.

Goldzung, Laura H., Managing AML audit expectations, http://www.amlauditservices.com/Articles/Goldzung_PCRM_Nov%202013.pdf.

http://www.pwc.com/gx/en/economic-crime-survey/economic-crimes/index.jhtml.

The role of an effective independent review of your institution's anti- money laundering (AML) program by Pricewaterhouse Coopers, https://www.pwc.com/en_US/us/financial-services/regulatory-services/assets/pwc_aml_role.pdf.

USA Patriot Act of 2001, http://www.sec.gov/about/offices/ocie/aml/patriotact2001.pdf.

www.bankersonline.com/security/bsapenaltylist.html.