

# Towards a Proactive Role of Internal Auditors in Anti-Money Laundry Compliance Review: An Egyptian Perspective

Sara H. Sabry

Pharos University in Alexandria, and Faculty of International Business and Humanities (EJUST) - Egypt

## Abstract

The banking sector is crucial to any financial sector's stability and prosperous. But Money laundering (ML) threatens such stability through its vicious consequences. Thus, the need for a solid and rigorous AML programs emerged. In the light of the drastic evolution of the business environment over the last decades to rely heavily on information technology (IT), The new role for internal auditors (IAs) needed to convoy such evolution by advancing from traditional and reactive role to a more proactive and strategic role. No study has closely investigated the impact of IAs involvement in IT governance on IAs effectiveness in AML compliance review. A survey was developed based on the prior literature and was administered IAs in the Egyptian Banking sector. In all, 39 usable questionnaires were received. Smart partial least square was used to analyse the responses, the results indicated that IAs involvement in IT governance structures and relational capabilities significantly affected the IAs effectiveness. But IT involvement in processes was found to be insignificant. The overall results should be useful to banks in general, seeking to utilize the IAs to the full their aptitude in combating ML through improving the IAs effectiveness in AML compliance review.

**Keywords:** IT governance, AML compliance review, Internal Auditors

## 1. Introduction

Money Laundering (ML) has been announced to be a major priority to fight against by the international community; this is mainly due to its destructive consequences on the integrity and stability of the financial sector and economy. ML is the process by which the source of assets (usually cash) is concealed to obscure the link between the funds and the original criminal activity (International Monetary Fund 2016). The Banking sector is the gatekeeper of any financial system and thus, is more vulnerable to ML and many other fraudulent activities. At the same time, almost all banks use intelligent systems to track and report any suspicious activity, such systems need certain controls because failure of handling them produces higher systematic risk. Thus, stronger internal controls are required to prevent ML. According to Basel Committee on Banking Supervision (BCBS), an efficient internal audit independently and objectively evaluates the effectiveness of banks' controls, risk management and governance processes (Basel Institute of Governance 2016). The BCBS requires banks to have internal audit function (IAF) with sufficient authority, stature, independence and resources. Thus, the involvement of IAs in IT governance creates new opportunities in the Banking sector to fight ML and assess such risk.

The Egyptian Banking sector after the 25<sup>th</sup> of January revolution is moving steadily towards becoming the biggest financial centre in the region through expanding to non-traditional services such as investment consultations, brokerage and mutual funds. Thus, more integrity and transparency is needed through combating ML, Kassem and Higson (2015) argues that reviewing ML research in Egypt showed a huge gap, thus the current study aims at filling this gap by evaluating the Egyptian Banking sector's ability to comply to AML programs through highlighting the major vital role of the IA, especially in such an intensive IT environment. This paper attempts to answer the following question: Does the banks IA's involvement in IT Governance contribute to effective AML compliance review? We have identified the research hypotheses according to the state of art in the extant literature. The data used to test the hypotheses were collected through a questionnaire, which was distributed among IAs in the Egyptian Banking sector and a response rate of 38% was reached, this paper is constructed as follows: the next section contains the conceptual framework and discussion of the literature review and thus the derivation of the research hypotheses, followed by a section to present the research methodology; target population, sample and research constructs. The third section discusses the research findings and the fourth section displays conclusions and discussion. The final section highlights the main research limitations and future research.

## 2. Conceptual Framework

### 2.1 AML Compliance in the Banking Sector

Banks are financial institutions offering a wide range of financial services to individuals and SMEs, those services include loans, deposits, transaction services, credit cards, insurance and investment products. All those services can be used to launder money domestically and internationally, thus threatening the effective functioning, stability and integrity of the Banking sector (Petrou 2009). Thus, the need for anti-money laundry (AML) programs emerged. Angell and Demetis (2005) highlighted that although AML in the Banking sector is

vital to the stability and integrity of such institutions. AML compliance consists of number of checks and processes to ensure that the client's details are verified. Domestically, the Egyptian ministry promulgated the AML law No.80 of 2002, which aims at combating ML practices in the Egyptian environment. The Central Bank of Egypt (CBE) created an independent ML unit; this unit's main aim is to receive information from financial institutions regarding the latter's suspicion in ML. This MLU has obliged the financial institutions to implement AML programs to ensure the obtainment of needed information about suspicious activities (Fouda 2010).

### *2.2 The role of IA in AML compliance review*

The international community realized the need to increase the responsibilities for IA with a special emphasis on combating ML carried by individuals (Naheem 2016), thus providing a unique opportunity and a heavy obligation for IA to take a more proactive role in combating ML rather than their existing reactive role. Notably, it is the responsibility of the management and governance structures to assess and detect ML activities, as part of this process; IA is considered one of the four core stones of the banking governance besides the audit committee (AC), management and the external auditor. Due to the globalization of the Banking sector, a shift in thinking of the role of IA of banking is required. Modisagae (2013) reasoned that the main success factor of AML program resides in the effectiveness of the IA of banking, where IA provides opportunities to align sound governance, Enterprise Risk Management (ERM) and to achieve greater compliance. Because IA is well positioned to assess internal control systems, it can continually assess the effectiveness of internal controls, accuracy of financial records and compliance to policies and regulations.

However, it needs to be noted that IA has a reactive nature regarding ML detection, not a proactive one; IA can only identify ML activity at the stage where a client has been directly involved in a suspicious activity. But Sinason (2003) argues that the position of IA enhances his/her ability to detect suspicious transactions specially those related to ML in customer account. Where it is required according to IIA practice advisory 1210.A2-1, it is the responsibility of IA to grasp the key indicators of fraud sufficiently to warrant an investigation. Additionally, IA is required to be aware of ML indicators as a type of fraud (Institute of Internal Audit, IIA 2004). The extent of the integration between the financial institution and IAF is a vital key success factor for an effective AML compliance (Axelod & Ross 2012).

One of the new recommendations by the FATF requires from the banking sector to develop a sound AML programme, these programs should be reviewed by an independent individual, but the FATF did not specify who will perform the review (Financial Action Task Force 2013). Additionally, Modisagae (2013) argues that this independent review should be executed by the IA to ensure that AML programme is robust and fully aligned with the regulatory requirements. Also, the author elaborated that IA should perform periodic compliance audits, to assess the level of adherence to the so forth set compliance framework and at the same time provide an auditing report regarding non-compliance issues. Notably, the more effective the AML compliance review conducted by IA, the more effective the AML programme, the less ML is likely to happen. IA effectiveness is the main highlight of many researches ( Arena & Azzone, 2009; Lenz & Hahn, 2015).

### *2.3 The IA involvement in IT governance and AML compliance review effectiveness*

Corporate governance practices have assumed a new emphasis across the USA, Asia, Europe and UK. There has been a strong emphasis on internal elements of governance such as internal control, the role of IA and the audit committee. The latter two roles are perceived as critical elements in the assurance process. Nowadays, many if not all large organizations rely heavily on IT, that is why corporate governance, especially IT governance, has gained momentum in recent years. Where, technology affects every facet of organizational activities on a daily basis. Information Systems Audit and Control Association (ISACA, 2002) defined IT governance as “a structure of relationships and processes to direct and control the organization with the purpose of achieving organizational goals by adding value while, maintaining the balance between risk and return over IT and its processes.

In the same spirit, Héroux & Fortin, (2013) noted that IT governance consists of structures, processes and relational capabilities that ensure the organizational sustainability and extension of the organizational strategy and objectives. The authors explained that *structures* consist of formal positions and roles for making IT related decisions; internal auditor's involvement in IT governance structure is indicated for example by the membership of IT chief internal auditor in an IT committee. While, *processes* stand for the implementation of IT management techniques and procedures; indicated for example by the usage of IT internal auditor of IT governance framework. Whereas, for relational capabilities, they are the active participation of, and collaborative relationships among corporate executives, IT management and business management; indicated for example by the presence of close cooperation between chief internal auditor and the corporate security officer. Accordingly, the essential role of IT in corporate business processes results in organizational dependency on IT. Auditors need to assess the effectiveness of IT controls as part of their own audit assessments of the organization's internal control system. Thus, confirming the important role of IAs in IT governance.

Anderson et al. (2012) argued that due to the pervasive nature of ML techniques, IAs need to develop a

special set of skills such as forensic internal auditors, IT internal auditors and fraud internal auditors. At the same time, IAs need to develop an understanding of the nature of ML, it is vital to comprehend various areas of risk, internal controls and red flag indicators. This phenomenon highlights the new demands, challenges and opportunities for the banking sector at large and for IAs in specific. According to Ferguson et al. (2013) IT governance reduces risks, by improving key internal control areas, and by foreseeing material accounting misstatements. Thus, it can be postulated that internal auditor's involvement in IT improves IA's effectiveness in conducting AML compliance review. Hence, the research hypotheses can be formulated as follow:

**H1: The involvement of IA in IT governance is positively related to the effectiveness of AML compliance review.**

**H1a: The involvement of IA in IT governance processes is positively related to the effectiveness of AML compliance review.**

**H1b: The involvement of IA in IT governance structures is positively related to the effectiveness of AML compliance review.**

**H1c: The involvement of IA in IT governance relational capabilities is positively related to the effectiveness of AML compliance review.**

### 3. Research Methodology

Given our objective was to explore the proactive role of IA in IT governance in the banking sector and its influence on conducting an effective AML compliance review. A survey was, therefore, an appropriate research method to use (Héroux & Fortin 2013). All the statements were selected and adapted, if necessary, from existing instruments, using a five point-Likert scale. Five academics revised the questionnaire, we enhanced our comprehension of the role of IA in IT governance through a prior pilot study; this study involved sending the questionnaire to ten IAs in the Egyptian banking through emails, the pilot study aimed to test the reliability and validity of the statements developed. The reliability of the constructs was assessed using Cronbach's Alpha of 0.70 or more is considered highly reliable.

Cronbach's Alpha for IA involvement in IT governance processes was 0.948, for IA involvement in IT governance relational capabilities was 0.811, for IA involvement in IT governance structures was 0.872 while that of IA effectiveness was 0.948. To assess the validity of constructs, Average Variance Extracted (AVE) of 0.50 or more is considered valid. AVE for IA involvement in IT governance processes was 0.655, for IA involvement in IT governance relational capabilities was 0.630, for IA involvement in IT governance structures was 0.653, and for IA effectiveness was 0.762.

In addition, all statements yielding a factor loading less than 0.7 were excluded as follow; 8 out of the 13 items measuring the IA involvement in IT governance, 7 items out of the 23 items measuring the IA involvement in IT governance processes, 6 out of 9 items measuring IA involvement in IT governance relational capabilities and finally, 4 out of 12 items measuring the IA effectiveness in AML compliance review were all excluded (Table 1). This pilot study and the conceptual framework helped us develop our final questionnaire.

#### 3.1 Sample and survey administration

According to Elkhatab (2013) judgment sampling should be used when limited category of respondents have the required qualifications. Therefore, a judgment sample was used in the present study. Accordingly, the questionnaire was distributed among IAs who gained a certain qualification; Certified Internal Auditor (CIA) and\ or Certified Information System Auditor (CISA) and\ or Certified Public Accountant (CPA) and\ or other accounting designation. And most importantly, were engaged in retain auditing. The principle rationale behind this is based on the assumption that these qualified participants would have sufficient knowledge and expertise, which is expected to yield reliable and valid results.

The administration of the questionnaire involved developing the questionnaire via Google docs, to protect the participants' privacy and to ensure the ease of use for participants. This was followed by sending the questionnaire and cover letter link through personal messages to IAs in the Egyptian banking sector through the professional network; LinkedIn, to ascertain the qualifications of respondents. Accordingly, it was sent to 102 IAs, followed by a second and third reminder, one week apart. Response rate was 38.2% (39 respondents). Second, there was a departure from normality for the dependent and independent variables; assessed using skewness, kurtosis and normality plots). Finally, Smart PLS-SEM (Partial Least Square- Structure Equation Modelling) was used to test the research hypotheses.

#### 3.2 Measurement of constructs

##### 3.2.1 Independent variables

IA involvement in IT governance forms our independent variable, it was measured on three levels; IA involvement in IT governance structures, processes and relational capabilities, Which were measured using items developed in the light of (Héroux & Fortin 2013). First, IA involvement in IT governance structures was

measured using 5 items. Second, IA involvement in IT governance processes was measured using 16 items. Third, IA involvement in IT governance relational capabilities was measured using 3 items. The respondents were asked to indicate their agreement on each of the 24 statements based on a five-point Likert scale.

### 3.2.2 *Dependent variable*

IA effectiveness in AML compliance review forms our dependent variable. Though, many researches emphasized the need to measure IA effectiveness, but there is no generally acknowledged measure for this purpose (Karagiorgos et al. 2010). Based on the above consideration and according to the extant literature, the dependent variable is assessed by eight items that were developed from (Anderson et al., 2012; Arena & Azzone, 2009; Cahill, 2006; Cohen et al., 2010; Lenz & Hahn, 2015), the respondents were asked if banking IA is effective in AML compliance review when IA is skilful, competent, independent, objective, reports directly to AC, meets expectations of the AC, improves department's performance and finally, improves organizational performance. The respondents were asked to indicate the degree to which they agreed with each item based on a five-point Likert scale.

## 4. Results and Discussion

This study aims at describing the banking IA's involvement in IT governance and to investigate this involvement's impact on IA effectiveness in AML compliance review. First, general demographic characteristics of the respondents are provided. Second, according to our first objective, a descriptive analysis of IA's involvement in IT governance in structures, processes and relational capabilities, and IA effectiveness in AML compliance review are discussed. Finally, the results of smart PLS will be deliberated.

### 4.1 *Demographic Characteristics*

Demographic characteristics of the respondents regarding gender, years of experience, the IA use, certification and areas of responsibilities (Table 2). The respondents were made of 94.7% males and 5.3% females, indicating a high dominance of males in the sample. 71% of the respondents have more than 7 years of experience in the internal auditing profession. 68.4% of the respondents use IIA's Global Technology Audit Guides (GTAG) and IIA International Standards for the Professional Practice of Internal Auditing. 52.6% gained their CIA, 26.3% have CISA. 89.7% of the respondents conducted general internal auditing, while 74.4% were engaged in retail auditing.

### 4.2 *PLS Results analysis*

It was suggested that banking IA involvement in IT governance positively influences IA effectiveness in AML compliance review. First, it was proposed that IA involvement in IT governance structures is positively correlated with IA effectiveness (H1a). Looking at (Table 3, Panel A), The results suggested that IA is more involved in IT governance structures when IA executive is a member of the IT security steering committee and is invited to the committee meetings (mean= 2.179). The analysis showed that oversee of board committee over IT related risks and activities had the highest correlation with the IA effectiveness; where skills (0.535), IA competence (0.568), objectivity (0.492), reporting to AC (0.439), meeting AC expectations (0.488). The overall correlation of IA involvement in IT governance structures is positively correlated to IA effectiveness ( $R^2=0.515$ ), indicating a reasonable positive correlation, while p-value= 0.025 (less than 0.05, two tailed test), also, T-statistics= 2.250 (more than 1.96). Thus, at a confidence level of 95%, the first hypothesis was supported (Table 4, Panel A).

Second, the second hypothesis proposed that IA involvement in IT governance processes is positively correlated with IA effectiveness in AML compliance review (H1b). In light of Table 3, Panel B: 81% of the sample use risk assessment in planning overall IT audit (mean= 1.72), IA evaluates IT strategic planning process (mean= 1.67), also evaluates data integrity (mean= 1.8), where 84% of the sample their AC provides inputs to IT internal audit planning (mean= 2.15), while 92% of the sample agreed that IA of banking evaluates IT- related compliance with external requirements (mean= 1.85). The results also suggested that higher IA involvement in IT governance processes is related to IA's evaluation of IT security (mean=1.56) and privacy procedures (mean= 1.64). It was concluded that IA involvement in IT governance processes is positively correlated with IA effectiveness in all manners where IA's skills were mostly correlated with IA evaluation of privacy procedures (0.536); IA's competence was mostly correlated with AC input provides input to IT internal audit planning (0.550), IA's independence, objectivity and reporting directly to AC were mostly correlated with IA evaluation of data integrity (0.554, 0.450 and 0.464 respectively). Regarding IA effectiveness in meeting the AC's expectations, IA's evaluation of the IT asset safeguarding was highly correlated (0.526), while IA effectiveness in improving department's performance and organizational performance was positively correlated with IA's evaluation of IT security and IA's review of IT projects (0.370, 0.549 respectively). The overall correlation of the IA's involvement in IT governance processes was 0.527 (p-value=0.450) and T-statistics= 0.756. Thus, at confidence level of 95%, the second hypothesis was rejected (Table, Panel A).

Third, it was suggested that IA involvement in IT governance relational capabilities is positively correlated with IA effectiveness in AML compliance review (H1c), Panel C (Table 3); the results suggested that higher IA involvement in IT governance relational capabilities is due to IA training on IT control (mean=2.08). It was found that IA training on IT controls had the most correlation with IA's skills, competence, and independence objectivity, reporting directly to AC, meeting the AC expectations and improving the organizational performance (0.573, 0.627, 0.653, 0.446, 0.513, 0.597 and 0.591 respectively). Also, AC collaboration with IA executive in charge of IT internal audits had the highest correlation with IA improving the department's performance. The overall correlation between IA involvement in IT governance relational capabilities with IA effectiveness in AML compliance review was 0.806 (p-value= 0.000 and T-statistics= 6.175). Thus, at a confidence level of 95%, the third hypothesis is supported. Finally, it was concluded that there is a significant positive correlation between IA involvement in IT governance and IA effectiveness in AML compliance review with  $R^2=0.695$  (P-value=0.000 and T-statistics= 10.958). Hence, at a confidence level of 95%, the main hypothesis (H1) is supported (Table 4).

## 5. Conclusion

Generally, the participants' responses appear to be positive about the set of indicators which were examined with regards to IA involvement in IT governance; structures and relational capabilities, and IA effectiveness. Descriptive results suggested that IA involvement in IT governance structures was mainly consisting of inviting IA to different IT steering committee meetings and the inclusion of IT audit matters in periodic audit reports. Also, IA involvement in IT governance relational capabilities was mainly concentrating on the collaboration between AC and IA, the type of training the IA gets, it can be reasoned that two levels of IA involvement in IT governance (structures and relational capabilities) proved to be significantly correlated with IA effectiveness, these results exhibits an extension to (Héroux & Fortin 2013) work by examining the impact of those two levels of involvement on IA effectiveness in AML compliance review.

However, there are some exceptions manifested in the respondents' perception of an insignificant influence of IA involvement in process on IA effectiveness, this is due to the immature level of the internal auditing profession in a country like Egypt. Moreover, the overwhelming majority of respondents recognized that IA involvement in IT governance structures and relational capabilities are more extensive than IA involvement in IT governance processes, the descriptive results suggest that there is an opportunity for further improvement with regards to the banking IA involvement. Based on the above results, respondents identified that IA contribution to the organizational performance is the most crucial element in IA effectiveness in AML compliance review. The results also indicate that IA involvement in IT governance significantly influenced the IA effectiveness in conducting AML compliance review in the banking sector in Egypt. Based on the above discussion, this research contributes to the literature in three areas. First, this study addressed the important role of IA in Egypt where the internal auditing profession is still developing. Second, this study highlights various elements that contribute to IA effectiveness and more specifically in AML compliance review. Finally, this research provides practical insights to the banking sector, suggesting that IA needs to go beyond boundaries, taking a more proactive, unique and indispensable role to muddle through the dynamicity of the banking sector, forming a vital defence line in combating ML.

## 6. Limitations and Further Research

This research aimed at investigating the impact of IA involvement in IT governance on IA effectiveness in AML compliance review. This involvement needs to be extended beyond IT governance and to cover other aspects of corporate governance. In addition, IA effectiveness was measured only by 8 items; those indicators can be prolonged in further research. Also, this research sample was affected by the number of qualified respondents imposing a great limitation to the study. Future research can uncover other determinants of IA involvement in IT governance. Furthermore, a cross regional comparative study could also be conducted to compare between IA involvements in IT governance across different regions.

## References

- Anderson, U.L. et al., 2012. A post-SOX examination of factors associated with the size of internal audit functions. *Accounting Horizons*, 26(2), pp.167–191.
- Angell, I.O. & Demetis, D.S., 2005. Systems thinking about anti-money laundering: considering the Greek case. *Journal of Money Laundering Control*, 8(3), pp.271–284.
- Arena, M. & Azzone, G., 2009. Identifying organizational drivers of internal audit effectiveness. *International Journal of Auditing*, 13(1), pp.43–60.
- Axelod, R.M. & Ross, K., 2012. Effective AML Compliance. *Internal Auditor*, August, pp.71–73.
- Basel Institute of Governance, 2016. *Basel AML Index 2016 Report*,
- Cahill, E., 2006. Audit committee and internal audit effectiveness in a multinational bank subsidiary: A case

- study. *Journal of Banking Regulation*, 7(1–2), pp.160–179.
- Cohen, J., Krishnamoorthy, G. & Wright, A., 2010. Corporate governance in the post-Sarbanes-Oxley era: Auditors' experiences. *Contemporary Accounting Research*, 27(3), pp.751–786.
- Elkhatib, H., 2013. The perceptions of audit committees' role in an emerging market: the case of Egypt. *Journal of Economic and Administrative Sciences*, 29(2), pp.85–98.
- Ferguson, C. et al., 2013. Determinants of Effective Information Technology Governance. *International Journal of Auditing*, 17(1), pp.75–99.
- Financial Action Task Force (FATF), 2013. *Methodology for assessing compliance with FATF recommendations and evaluation of the effectiveness of AML/CFT systems*,
- Fouda, I.M., 2010. *CORRUPTION AND MONEY LAUNDERING IN EGYPT*,
- Goodwin-Stewart, J. & Kent, P., 2006. The use of internal audit by Australian companies. *Managerial Auditing Journal*, 21(1), pp.81–101.
- Harvey, J., 2004. Compliance and reporting issues arising for financial institutions from money laundering regulations: a preliminary cost benefit study. *Journal of Money Laundering Control*, 7, pp.333–346. Available at: <http://dx.doi.org/10.1108/13685200410810047>.
- Héroux, S. & Fortin, A., 2013. The internal audit function in Information Technology Governance: A Holistic Perspective. *Journal of Information Systems*, 27(1), p.189. Available at: <http://search.proquest.com/library.capella.edu/docview/1428835140?accountid=27965>.
- Information Systems and Audit ISACA, 2002. *Auditing Guideline, IT Governance*,
- International Federation of Accountants (IFAC), 2002. *E-Business and the Accountant*.
- International Monetary Fund, I., 2016. *The IMF and the Fight Against Money Laundering and the Financing of Terrorism*, Available at: <http://www.imf.org/external/np/exr/facts/aml.htm>.
- Karagiorgos, T., Drogalas, G. & Dimou, A., 2010. Effectiveness of Internal Control System in the Greek Bank Sector. *The Southeastern Review of Business Finance & Accounting*, pp.1–11.
- Kassem, R. & Higson, A., 2015. Institutional Repository Combating fraud : Is Egypt ready? Insights from the literature. *Journal of Emerging Trends in Economics*, 6(5), pp.290–298.
- Kranacher, M., Riley, R.A.J. & Wells, J.T., 2010. *Forensic Accounting and Fraud Examination*.
- Lenz, R. & Hahn, U., 2015. A synthesis of empirical internal audit effectiveness literature pointing to new research opportunities. *Managerial Auditing Journal*, 30(1), pp.5–33.
- Mihret, D.G., 2013. The role of internal auditing in risk management. , pp.1–17.
- Modisagae, T., 2013. *The Role of Internal Audit in the Independent Review of Anti-Money Laundering Compliance in South Africa*. University of Pretoria.
- Naheem, M.A., 2016. Risk of Money Laundering in the US : HSBC case study. *Journal of Money Laundering Control*, 19(3), pp.225–237.
- Peterson, R., 2004. Crafting information technology governance. *Information Systems Management*, 21(4), pp.7–22.
- Petrou, A.P., 2009. Foreign Market Entry Strategies in Retail Banking: Choosing an Entry Mode in a Landscape of Constraints. *Long Range Planning*, 42(5–6), pp.614–632. Available at: <http://dx.doi.org/10.1016/j.lrp.2009.09.001>.
- Sarens, G. & De Beelde, I., 2006. Internal auditors' perception about their role in risk management. *Managerial Auditing Journal*, 21(1), pp.63–80. Available at: <http://www.emeraldinsight.com/doi/abs/10.1108/02686900610634766>.
- Sinason, D.P. & W. h., 2003. The role of internal auditor's in fighting terrorist financing. *Internal Auditing Journal*, March/Apri, pp.11–18.
- The Institute of Internal Auditors (IIA), 2004. *Internal auditing role in sections 302 and 404 of the Sarbanes Oxley Act*,

**Tables**

**Table 1**

Constructs Reliability and Validity

	Cronbach's Alpha	Composite Reliability	(AVE)	Factor
<b>Panel A: IA involvement in IT Governance Structure</b>				
1-Presence of an IT steering committee(s): IA senior executive/officer is a member of the IT committee, invited to IT committee meetings.				0.849
2-Presence of an IT project committee(s): IA senior executive/officer is a member of the committee invited to committee meetings.				0.925
3-Presence of an IT security committee: IA senior executive/officer is a member of the committee invited to committee meetings.	0.872	0.903	0.653	0.804
4-Presence of an IT architecture committee: IA senior executive/officer is A member of the committee invited to committee meetings.				0.758
5-Board committee (other than the audit committee) oversees IT-related risks and/or IT-related audit activities				0.784
<b>Panel B: IA involvement in IT Governance Relational Capabilities</b>				
1-Audit Committee collaborates with the IA senior executive/ officer or the officer/ manager in charge of IT internal audits in identifying and addressing IT risks.				0.765
2-Officer/manager responsible for IT security collaborates with the IA senior executive/ officer or the officer/manager in charge of IT internal audits in identifying and addressing IT-related risk.	0.811	0.872	0.630	0.765
3-Internal auditors are trained on IT control.				0.815
<b>Panel C: IA effectiveness in AML Compliance Review</b>				
1-IA is effective in AML compliance review when IA skillful.				0.828
2-IA is effective in AML compliance review when IA is competent.				0.893
3-IA is effective in AML compliance review when IA is independent.				0.932
4-IA is effective in AML compliance review when IA is objective.				0.869
5-IA is effective in AML compliance review when IA reporting directly to AC.	0.948	0.957	0.762	0.841
6-IA is effective in AML compliance review when IA meets expectations of the AC.				0.901
7-IA is effective in AML compliance review when IA improves department's performance.				0.782
8-IA is effective in AML compliance review when IA improves organizational performance.				0.886

**Panel D: IA involvement in IT Governance Processes**

1-AC provides input to IT internal audit planning.				0.804
2-Risk assessment is used in planning Overall IT internal audit.				0.859
3-Risk assessment is used in planning Execution of the individual elements of IT internal audits.				0.830
4-IT governance and control frameworks (e.g., COBIT, ITGI) used in Performing IT internal audits.				0.736
5-IA evaluates IT strategic planning process (including IT investment planning).				0.830
6-IA evaluates IT-related compliance with external requirements (e.g., laws and regulations) affecting IT.				0.763
7-IA evaluates Attribution of responsibility for IT risk				0.786
8-IA evaluates Data integrity.	0.965	0.968	0.655	0.917
9-IA evaluates Privacy procedure.				0.827
10-IA evaluates IT.				0.899
11-IA evaluates IT asset management and safeguarding.				0.863
12-IA evaluates IT-related threat and risk management methods to ensure continuity of processing.				0.792
13-IA evaluates IT-related disaster-recovery procedural plan, testing and documentation.				0.721
14-IA evaluates IT cost controls.				0.702
15-IA evaluates IT performance.				0.854
IA reviews IT projects.				0.821

**Table 2**  
 Participants Demographics

Demographics Information		Frequency	percentile
<b>Gender</b>	Male	37	94.7
	Female	2	5.3
<b>Years of experience as bank internal auditor</b>	1-3 years	6	15.8
	4-7 years	5	13.2
	More than 7 years	27	71.1
<b>IA uses</b>	Computerized audit techniques	4	10.5
	Control Risk Self-Assessment (CRSA)	3	7.9
	Governance frameworks (e.g., COSO)	3	7.9
	IIA International Standards for the Professional Practice of Internal Auditing	26	68.4
<b>Certification</b>	Certified Internal Auditor (CIA)	20	52.6
	Certified Public Accountant (CPA)	3	7.9
	Certified Information Systems Auditor (CISA)	10	26.3
	Accounting designation (CA, CMA or CGA)	5	13.2
<b>What areas of responsibility does the internal audit activity oversee (choose all that apply)</b>	General internal auditing	35	89.7
	IT auditing	26	66.7
	Fraud auditing	26	66.7
	Retail Auditing	29	74.4
	Environment, Health, and Safety	19	48.7
	Compliance	28	71.8
	Risk management	29	74.4
	Forensic Auditing	14	35.9

**Table 3**  
 Descriptive statistics

	Mean	Mdn	Min	Max	SD	Strongly Agree		Agree		Neutral		Disagree		Strongly Disagree	
						N	%	N	%	N	%	N	%	N	%
						<b>Panel A: IA involvement in IT Governance Structure</b>						2.980			
1-Presence of an IT steering committee(s): IA senior executive/officer is a member of the IT committee, invited to IT committee meetings.	2.359	2	1	5	1.187	12	30.8	12	30.8	7	17.9	7	17	1	2.6
2-Presence of an IT project committee(s): IA senior executive/officer is a member of the committee invited to committee meetings.	2.308	2	1	5	1.066	10	26.3	14	36.8	8	21.1	5	13	1	2.6
3-Presence of an IT security committee: IA senior executive/officer is a member of the committee invited to committee meetings.	2.179	2	1	4	0.93	12	31.6	13	34.2	9	23.7	4	10	0	0
4-Presence of an IT architecture committee: IA senior executive/officer is A member of the committee invited to committee meetings.	2.564	2	1	5	1.081	5	13.5	14	37.8	10	27	6	16	2	5.4
5-Board committee (other than the audit committee) oversees IT-related risks and/or IT-related audit activities	2.513	2	1	5	1.318	13	34.2	6	15.8	10	26.3	5	13	4	10
<b>Panel B: IA involvement in IT Governance Processes</b>						1.894									
1-AC provides input to IT internal audit planning.	1.744	1	1	4	0.898	21	55.3	11	28.9	4	10.5	2	5.3	0	0
2-Risk assessment is used in planning Overall IT internal audit.	1.718	1	1	5	0.904	20	52.6	11	28.9	6	15.8	0	0	1	2.6
3-Risk assessment is used in planning Execution of the individual elements of IT internal audits.	2.154	2	1	5	1.167	23	60.5	9	23.7	5	13.2	0	0	1	2.6
4-IT governance and control frameworks used in Performing IT internal audits.	2.103	2	1	4	0.955	14	36.8	15	39.5	6	15.8	2	5.3	1	2.6
5-IA evaluates IT strategic planning process (including IT investment planning).	1.667	1	1	5	0.915	17	44.7	14	36.8	6	15.8	1	2.6	0	0
6-IA evaluates IT-related compliance with external requirements (e.g., laws and regulations) affecting IT.	1.846	1	1	5	1.144	22	57.9	13	34.2	2	5.3	1	2.6	0	0
7-IA evaluates Attribution of responsibility for IT risk	2.026	2	1	5	1.165	22	57.9	11	28.9	2	5.3	2	5.3	1	2.6
8-IA evaluates Data integrity (effectiveness of IT controls).	1.795	1	1	4	1.042	20	52.6	11	28.9	4	10.5	1	2.6	2	5.3
9-IA evaluates Privacy procedures (effectiveness of IT controls).	1.641	1	1	4	0.862	20	52.6	11	28.9	2	5.3	5	13	0	0
10-IA evaluates IT security (security access, evaluation of, and compliance with, standards and procedures, effectiveness of IT controls).	1.564	1	1	4	0.778	23	60.5	10	26.3	3	7.9	2	5.3	0	0
11-IA evaluates IT asset management and safeguarding.	1.744	1	1	5	1.006	24	63.2	10	26.3	3	7.9	1	2.6	0	0
12-IA evaluates IT-related threat and risk management methods to ensure continuity of processing.	1.667	1	1	5	0.996	22	57.9	11.2	28.9	3	7.9	2	5.3	0	0
13-IA evaluates IT-related disaster-recovery procedural plan, testing and documentation.	2.154	2	1	5	1.188	25	65.8	9	23.7	2	5.3	2	5.3	0	0
14-IA evaluates IT cost controls.	1.795	1	1	4	0.992	16	42.1	12	31.6	3	7.9	6	15	1	2.6
15-IA evaluates IT performance.	2.256	2	1	5	1.192	20	52.6	11	28.9	3	7.9	3	7.9	1	2.6
16-IA reviews IT projects.	2.436	2	1	5	1.15	20	52.6	11	28.9	2	5.3	5	13	0	0
<b>Panel C: IA involvement in IT Governance Relational Capabilities</b>						2.248									
1-Audit Committee collaborates with the IA senior executive/ officer or the officer/ manager in charge of IT internal audits in identifying and addressing IT risks.	2.385	2	1	4	1.028	8	21.1	13	34.2	9	23.7	6	15.8	2	5.3
2-Officer/manager responsible for IT security collaborates with the IA senior executive/ officer or the officer/manager in charge of IT internal audits in identifying and addressing IT-related risk.	2.282	2	1	5	1.176	9	23.7	13	34.2	10	26.3	6	15.8	0	0
3-Internal auditors are trained on IT control.	2.077	2	1	5	1.047	14	36.8	8	21.1	10	26.3	4	10.5	2	5.3

Panel D IA effectiveness in AML Compliance Review													1.903		
1-IA is effective in AML compliance review when IA skillful.	1.949	2	1	4	0.959	15	40.5	14	37.8	5	13.5	2	5.4	1	2.7
2-IA is effective in AML compliance review when IA is competent.	1.816	2	1	4	0.942	14	36.8	14	36.8	5	13.2	4	10.5	1	2.6
3-IA is effective in AML compliance review when IA is independent.	1.923	2	1	4	0.971	16	43.2	12	32.4	5	13.5	3	8.1	1	2.7
4-IA is effective in AML compliance review when IA is objective.	1.872	2	1	4	0.911	17	44.7	10	26.3	8	21.1	3	7.9	0	0
5-IA is effective in AML compliance review when IA reporting directly to AC.	2	2	1	4	0.877	16	42.1	14	36.8	5	13.2	3	7.9	0	0
6-IA is effective in AML compliance review when IA meets expectations of the AC.	2.692	3	1	5	1.158	14	37.8	12	32.4	9	24.3	2	5.4	0	0
7-IA is effective in AML compliance review when IA improves department's performance.	1.923	2	1	4	0.917	16	43.2	10	27	9	24.3	2	5.4	0	0
8-IA is effective in AML compliance review when IA improves organizational performance.	1.051	1	1	2	0.221	16	42.2	10	27	9	24.3	2	5.4	0	0

**Table 4**  
 IA involvement in IT governance  
**Panel A: P-value and T statistics**

Constructs	T Statistics	P Values
IA involvement in processes-> IA effectiveness in AML compliance review	0.756	0.450
IA involvement in relational capabilities-> IA effectiveness in AML compliance review	6.175	0.000
IA involvement in structures-> IA effectiveness in AML compliance review	2.250	0.025

  

Panel B: R2				
	R2	R <sup>2</sup> Adj	T-Stat	P Values
IA effectiveness in AML compliance review	0.695	0.669	10.958	0.000

**Panel C: Variables Correlation**

	IA effectiveness in AML compliance review	IA involvement in processes	IA involvement in relational capabilities	IA involvement in structures
IA effectiveness in AML compliance review	1.000			
IA involvement in processes	0.527	1.000		
IA involvement in relational capabilities	0.806	0.693	1.000	
IA involvement in structures	0.515	0.429	0.421	1.000