The Influence of Internal Audit on Information Security Effectiveness: Perceptions of Internal Auditors

ABSTRACT

This paper presents the results of a survey of internal auditors' perceptions about the nature of the relationship between the information security and internal audit functions in their organization and the effect of that relationship on their organization's information security efforts. We find that internal auditors perceive that increasing the frequency with which they review some information security activities improves the quality of the relationship between the two functions. However, the quality of their relationship with the information security function does not affect either the number of security incidents or the number of audit findings related to information security issues. We also find that internal auditors report that the frequency of audit reviews of information security affects the number of audit findings related to information security, but does not affect the number of security incidents. We discuss the implications of our findings for both research and practice.

Keywords: Internal audit, information systems security, information security governance, perceptions, survey

The Influence of Internal Audit on Information Security Effectiveness: Perceptions of Internal Auditors

I. INTRODUCTION

It is important to regularly monitor and assess the effectiveness of information security controls and processes (NIST 2012, p. 7). However, the value of monitoring and assessment is enhanced when done by someone who was not responsible for designing, implementing, and performing the activities being reviewed (ITGI 2012a, MEA02.05). One way to provide independent monitoring and assessment is to have the internal audit function periodically review and evaluate the organization's information security activities. Thus, the internal audit function can potentially contribute to effective governance and management of IT by providing an independent assessment of controls and processes (ITGI 2012a).

Until recently, little was known about the effect of internal audit activities on an organization's information security program. Steinbart et al. (2012) conducted in-depth interviews at four organizations and found that information security professionals believed that a good relationship with internal audit improved overall information security effectiveness in several ways. One perceived benefit of a good relationship with internal audit was that it made it easier to obtain management support for and employee compliance with information security policies (Steinbart et al. 2012). In addition, information security professionals indicated that internal audit feedback was useful in improving the design of role-based access controls (Steinbart et al. 2012). Subsequent research involving a survey of information security professionals from multiple industries (Steinbart et al. 2013) validated those anecdotal accounts, finding that a good relationship between the information security and internal audit functions improved the information security professionals' perceptions about the overall effectiveness of information security.

Steinbart et al. (2013) also found that the extent and frequency of internal audit reviews of various information security processes affected the quality of the relationship between the internal audit and information security functions. They also report that information security professionals believed that internal auditors could be more involved in reviewing their organization's information security. Thus, an important strategic question concerns the allocation of internal audit resources to information security reviews. In most firms, internal audit has responsibilities to review multiple operational and financial reporting aspects. In many public companies, considerable internal audit resources are devoted to assisting management in the review and evaluation of internal controls over financial reporting required by S-OX Section 404 (Lin et al. 2011). Thus, management must view information security effectiveness as a priority in order to support the use of internal audit resources to review this area. Therefore, it is important to assess the value of internal audit reviews of information security. This study makes an important contribution by surveying internal auditors to learn how audit reviews of information security program components affect: (1) the relationship between the internal audit

and information security functions and (2) the effectiveness of information security. We also examine whether the quality of the relationship between internal audit and information security itself affects the effectiveness of either information security or the internal audit process.

The remainder of this paper is organized as follows. Section two reviews the relevant literature and develops the hypotheses that were tested. Section three describes the research method, section four presents our results and section five concludes with a discussion of the implications of our findings for both research and practice.

II. BACKGROUND AND HYPOTHESES

A fundamental tenet of information security is the principle of "defense-in-depth," which involves the use of multiple layers of preventive, detective, and corrective controls to protect information resources. Internal audit review and assessment of various components of an information security program is a detective control. Frequent internal audit review of information security may also serve as a preventive control—if information security personnel are aware that their work is being actively monitored by internal audit, they are more likely to remain in compliance with corporate information security policies and procedures. Normative frameworks clearly indicate that such review and assessment is a critical component of effective information security. For example, the monitoring, evaluating, and assessing of controls is one of the five top-level categories of enabling processes in the COBIT 5 Framework (ITGI 2012a, 2012b) deemed necessary for effective governance and management of information technology. Similarly, NIST Special Publication 800-53 identifies security assurance, which is defined as "the measure of confidence that the security functionality is implemented correctly, operating as intended, and producing the desired outcome" as one of the key components to effective information security (NIST 2012, pp. 18-19).

Yet there has been scant research into the role of internal audit in information security. Ransbotham and Mitra (2009) included "audit controls," by which they meant monitoring and assessment, as one of three elements necessary to reduce the risk of security compromise. In their model, such monitoring played an indirect role in improving information security by providing feedback that could be used to improve the effectiveness of the other technologies and processes comprising an organization's information security program. Although Ransbotham and Mitra did not empirically test that research proposition, subsequent accounting research found that a good relationship between the internal audit and information security functions produces benefits. For example, a good relationship between the two functions results in a higher level of compliance with Sarbanes-Oxley requirements (Wallace et al. 2011) and is inversely related to the number of security incidents and security-related audit findings (Steinbart et al. 2013). In addition, Steinbart et al. (2012) report that information security professionals believed that audit feedback helped them to improve the effectiveness of access controls. Thus, there is some evidence that internal audit can contribute to information security effectiveness. However, respondents to Steinbart et al.'s (2013) survey of information security professionals rated the

average quality of the relationship between the information security and internal audit functions at only 3.4 on a 5-point scale, indicating that there was room for improvement.

Although the information security and internal audit functions share a high-level, common goal of maximizing the effectiveness of the organization's efforts to protect its information resources, the task of developing and managing proper relationships between the two functions involves a host of complex behavioral issues (Dittenhofer et al. 2010). On one hand, the practitioner literature notes that differences in attitudes and behaviors often make it difficult for the information security group to develop good relationships with other compliance-oriented functions, such as records management (Anderson 2012). On the other, auditors must not impair their objectivity and independence (Behn et al. 1997; Carcello et al. 1992; Schroeder et al. 1986; Stoel et al. 2012). Therefore, it is important to understand the factors that determine the quality of the relationship between the information security and internal audit functions.

Steinbart et al. (2013) found that the frequency and scope of internal audit's review of various information security components had a positive influence on information security professionals' perceptions of the quality of relationship with internal audit. However, respondents to their study rated the frequency and scope of internal audit involvement at only 2.84 on a five-point scale. Thus, it appears that information security professionals view internal audit reviews positively, but that in many organizations the extent of such internal audit involvement is relatively low. Steinbart et al.'s (2013) finding, however, only represents the perspective of information security professionals. It is also important to understand what internal auditors believe about their level of involvement in reviewing information security activities and the value of having a good relationship with the information security function. If auditors and information security professionals agree about the level of internal audit involvement in information security and the benefits to cultivating a good relationship between the two functions, then research can focus on identifying and appropriately adjusting the factors that contribute to and hinder that relationship. But, if the two functions disagree about the extent of current audit involvement in reviewing information security and the merits associated with having a good relationship between the two functions, then research needs to examine the causes of that disagreement and how to rectify it. Thus, one objective of this study is to examine the following research question:

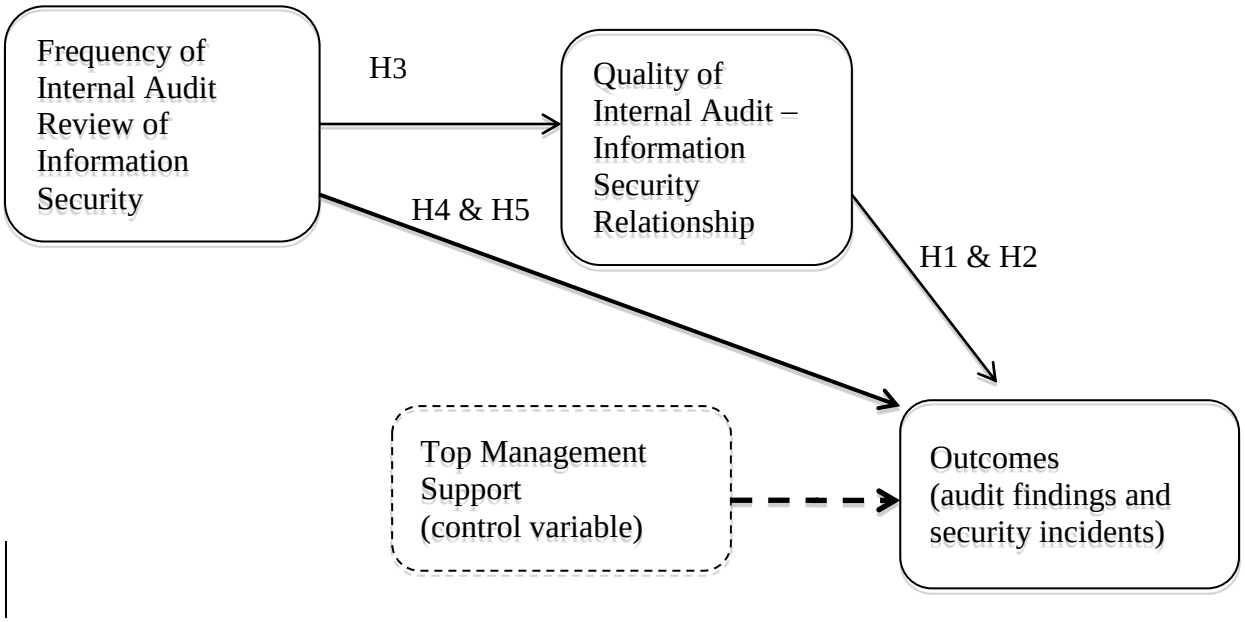
> RQ1: From the perspective of internal auditors, how does the quality of the relationship between the internal audit and information security functions affect outcomes (audit findings and security incidents)?

Steinbart et al. (2012) identified a number of factors that can affect the quality of the relationship between the internal audit and information security functions, including the auditor's technical competence, attitude (friendly or adversarial), communication skills, and the extent of interaction. Of those factors, perhaps the one that can most quickly be changed is the frequency of audit reviews. Therefore, the second objective of this study is to examine the effects of such interaction:

RQ2: From the perspective of internal auditors, how does the frequency of reviews of their organization's information security program affect: (a) their relationship with the information security function and (b) information security outcomes (security incidents and audit findings)?

Figure 1 presents the research model we use to investigate those questions.

Figure 1. Research Model and Hypotheses (dashed lines = control variables)



Benefits From A Good Relationship Between Internal Audit and Information Security

Prior research suggests that there should be positive organizational benefits associated with a good relationship between the internal audit and information security functions. Wallace et al. (2011) found that a good relationship between the internal audit and information security functions resulted in better compliance with Sarbanes-Oxley. Further, Steinbart et al. (2013) found that a good relationship between the two functions improved the information security professionals' perceptions of the overall effectiveness of the organization's information security efforts. One explanation for these findings is Steinbart et al.'s (2012) report that information security professionals believed that internal audit feedback helped them improve the design of access controls. Steinbart et al. (2012) also report that auditors believed the quality of the relationship between the two functions affected audit efficiency: a poor relationship between the two functions led to efforts by information security to hide evidence of problems from the auditors, whereas a good relationship between the two functions resulted in information security helping internal auditors to identify and focus attention on the areas representing the greatest risk. Thus, a good relationship between the internal audit and information security functions may result in an increased number of audit findings that information security professionals can use to improve the design and operation of various components of the organization's information

security program, which in turn should reduce both the frequency and severity of security incidents.

The preceding discussion leads to the following hypotheses:

> H1: Internal auditors' perceptions about the quality of the relationship between the internal audit and information security functions will be positively related to the number of audit findings related to information security.
>
> H2: Internal auditors' perceptions about the quality of the relationship between the internal audit and information security functions will be negatively related to the frequency of security incidents.

Steinbart et al. (2013) also found that top management support (i.e., investment of resources, communication about the importance of information security policies, etc.) was positively associated with overall information security effectiveness. Therefore, as shown in Figure 1, we treat top management support for information security as a control variable when we test whether the quality of the relationship between internal audit and information security improves effectiveness.

Benefits of Internal Audit Reviews of Information Security

One's ability to understand another is related to the frequency and extent of interaction (Cronin and Weingart 2007; Huber and Lewis 2010). The more aspects of information security that internal audit reviews, and the more frequently it does so, the greater the opportunity for the two functions to develop a shared understanding. In turn, mutual understanding improves communication effectiveness (Cronin and Weingart 2007; Huber and Lewis 2010), which should improve the overall quality of the relationship. Indeed, Steinbart et al. (2013) found that the frequency of internal audit reviews of information security activities was positively related to information security professionals' perceptions about the quality of the relationship between the internal audit and information security functions. Therefore, our third hypothesis is:

> H3: The frequency of internal audit reviews of various aspects of their organization's information security activities will be positively associated with internal auditors' perceptions about the quality of the relationship between the internal audit and information security functions.

Further, as discussed earlier, internal audit reviews of information security should also directly improve information security effectiveness by providing advice (in the form of audit findings) that information security professionals can use to improve the design of various controls and procedures, thereby reducing the number and severity of security incidents. This leads to our final two hypotheses:

> H4: The frequency of internal audit reviews of various aspects of their organization's information security activities will be positively associated the number of audit findings related to information security.

H5: The frequency of internal audit reviews of various aspects of their organization's information security activities will be negatively associated with the number and severity of security incidents.

III. METHOD

We created a web-based survey instrument to collect internal auditors' perceptions about the quality of the relationship between the internal audit and information security functions at their current employer, the frequency of audit reviews of various components of the organization's information security program, and the overall effectiveness of information security. We solicited and obtained assistance from ISACA's director of research to post an announcement of the survey on ISACA's main national webpage, which described the survey's purpose and included a link to the survey. About one week later, we posted an additional link to the survey on ISACA's LinkedIn CISA site and posted two additional messages on LinkedIn in subsequent weeks.

To build the survey instrument, we adapted the questions used by Steinbart et al. (2013) to assess information systems professionals' perceptions, changing the wording to make the questions appropriate for internal auditors. We then asked internal auditor practitioners to review the instrument and made a few additional modifications based on that feedback. Appendix A presents the questions used to measure each construct.

Independent Variables

Level of IA Review

We asked respondents to indicate how often internal audit reviews the eight aspects of information security listed in Appendix A on a five-point scale ranging from not-at-all to often. Higher scores represent more frequent internal audit review of various aspects of information security.

Top Management Support (control variable)

Eight Likert-style questions were used to capture respondents' perceptions about top management's support for information security. Four questions focused on top management's current level of support and four asked about the trend in that support over the past 3 years. Each set of questions asked whether management provided adequate resources, communicated the importance of information security, believed that information security was important, and was more proactive or reactive in regards to information security. Responses to the eight questions were averaged to create an aggregate measure of top management support, with higher scores indicating greater support.

Dependent Variables

Perceived Quality of the Relationship

Four Likert-style questions asked respondents about the quality of the relationship between internal audit and information security. Three were the same items used in Steinbart et al.'s (2013) survey of information systems professionals; a fourth item asked whether respondents felt that the two functions worked together to assure information systems were secure and reliable. Responses to all four questions were averaged, with higher scores representing a better quality relationship.

Outcome: Information Security Effectiveness

We assessed information security effectiveness two ways: in terms of audit findings and security incidents. The survey instrument included two Likert-style questions about audit findings. One question asked respondents about the percentage of internal audit findings that were related to information security in the most recent year, the other asked them to assess the trend in the number of internal audit findings related to information security over the past three years. The survey instrument also included two Likert-style questions about security incidents. One question asked about the number of security incidents (breaches, denial of service attacks, etc.) that the organization experienced during the past year. The second asked respondents to assess the trend in the number of information security incidents over the past three years. Responses to the two questions about incidents were reverse coded so that higher scores represented more incidents.

IV. RESULTS

Demographics

Table 1 provides basic demographics about respondents. 29 (67%) of the respondents were male; 18 (43%) were under the age of 40; and 34 (79%) possessed the Certified Information Systems Auditor (CISA) certification. In terms of total work experience, 11 (26%) had less than 10 years; 18 (43%) had 11-20 years, and 13 (31%) had over 20 years. In addition, 13 (33%) had more than 10 years work experience with their current employer. 21 (49%) respondents worked for publicly traded companies; 14 (32%) worked for privately-held companies and 8 (19%) worked for nonprofits.

Table 1. Demographics and Audit Review Descriptive Statistics

	Frequency	Percentage
Respondent gender:		
• Male	29	67%
• Female	14	33%
Respondent age:		
• Under 40	18	43%
• 40 or older	25	57%
Respondent's certifications (could be multiple):		
• CPA/CA	7	16%
• CISA	34	79%
• CISM	8	19%
• CIA	6	14%
• CISSP	3	7%
• None	2	5%
• Other (CRISC, CGEIT, etc.)	17	40%
Respondent total work experience (years):		
• 10 or less	11	26%
• 11-20	18	43%
• Over 20	13	31%
Respondent work experience with current employer (years):		
• 10 or less	30	67%
• Over 20	13	33%
Nature of organization		
• Publicly traded for profit	21	49%
• Privately held for profit	14	33%
• Non-profit	8	18%
Industry:		
• Government	3	7%
• Manufacturing	1	2%
• Financial Services	18	42%
• Technology	2	5%
• Healthcare, education, and other professional services	11	26%
• Mining and Construction	3	7%
• Other	5	11%

Construct Reliability

Before testing the research model, we first assessed the reliability of our constructs. Table 2 presents the results of the initial factor analysis for the reflective constructs. We followed Bentler and Wu's (1995) suggestion of only retaining those indicators that have loadings greater than .50, resulting in no items being dropped. For the formative construct, Level of IA Review, we examined variance inflation factor (VIF) for any issue of multicollinearity (Peter et al. 2007, Cenfetelli and Bassellier (2009). The VIF for this construct is below the 3.3 threshold identified by Diamantopoulos and Siguaw (2006) that would indicate a multicollinearity problem. Table 3 shows the reliability and correlations among those constructs. Table 3 presents descriptive statistics for each construct (panel A) and also shows that they exhibited adequate convergent and discriminant validity (panels A and B) with all AVE scores greater .50 and larger than cross-correlations with other constructs. We also tested for common methods bias, because respondents answered questions about both the independent and dependent variables. The Harmon one-factor test indicated that one factor accounts for only 32% of the total variance in the independent and dependent measures, well below the 50% threshold for common method bias (Podaskoff and Organ 1986). In summary, the measures exhibit sufficient reliability to test the hypotheses.

Table 2: Factor Analysis – Model Constructs

	QUAL_REL	FINDINGS	INCIDENTS	TMS
QUAL_REL1	**0.7845**	-0.0592	-0.0184	-0.0735
QUAL_REL2	**0.6677**	-0.0291	-0.0328	-0.0442
QUAL_REL3	**0.7866**	-0.0411	0.1254	0.0811
QUAL_REL4	**0.9458**	-0.0365	-0.055	0.0533
FIND1	-0.07	**0.896**	-0.1709	0.2203
FIND2	-0.0171	**0.8672**	0.0104	0.203
INCID1	0.0706	0.0489	**0.822**	0.2887
INCID2	-0.0972	-0.2274	**0.7117**	0.2483
TMS1	0.2086	-0.0586	-0.052	**0.5093**
TMS2	0.0132	0.1478	0.0922	**0.7674**
TMS3	0.1598	0.1185	0.2845	**0.7796**
TMS4	0.021	0.1942	0.3789	**0.8772**
TMS5	-0.1736	0.2403	-0.1413	**0.4526**
TMS6	0.0065	0.0377	-0.1217	**0.5856**
TMS7	-0.0875	0.148	-0.0413	**0.5455**
TMS8	-0.14	0.2151	0.0702	**0.7008**

Table 3: Construct Validation

Panel A: Construct Values and Reliability Measures

Construct	Mean	Std. Dev.	CR	AVE	Cronbachs Alpha
FREQ_IA_REV	3.60	1.12	1.000	1.000	1.000
QUAL_REL	3.31	1.09	0.873	0.637	0.809
FINDINGS	3.31	1.39	0.875	0.777	0.716
INCIDENTS	4.41	1.46	0.743	0.592	0.700
TMS	3.42	0.91	0.899	0.531	0.884

CR: Composite Reliability
AVE: Average Variance Extracted

Panel B: Construct Correlation Table

Construct	FREQ_IA_REV	QUAL_REL	FINDINGS	INCIDENTS	TMS
FREQ_IA_REV	**1.000**				
QUAL_REL	0.453	**0.637**			
FINDINGS	0.224	(0.051)	**0.777**		
INCIDENTS	0.173	(0.006)	(0.097)	**0.592**	
TMS	0.307	0.012	0.240	0.350	**0.531**

Note: Latent Variable square root of the AVE on the diagonal.

Table 4. Descriptive statistics for constructs

	Mean (Median)*	Range
Internal Audit Reviews of Information Security Topics:		
• Business Continuity and Disaster Recovery	3.44 (3.0)	1-5
• Identity and Access Management	4.07 (4.0)	1-5
• Logging and System Monitoring	3.49 (4.0)	1-5
• Firewalls and Other Network Access Devices	3.26 (3.0)	1-5
• Encryption policies (including key management)	2.88 (3.0)	1-5
• Backup Procedures	3.77 (4.0)	1-5
• Change Management Controls	4.02 (4.0)	1-5
• Security Policies	3.88 (4.0)	1-5
Effectiveness of Information Security:		
• Incidents	5.40 (6.00)	1-7
• Trend in incidents	3.42 (4.00)	1-6
• Audit findings related to information security	3.65 (4.00)	1-7
• Trend in audit findings	2.98 (3.00)	1-6

Quality of Relationship between information security and internal audit		
• Members of information security and internal audit work together to assure information systems are secure and reliable	3.60 (4.00)	1-5
• There is little friction between internal audit and information security	3.16 (4.00)	1-5
• The relationship between internal audit and information security staff is close and personal	2.95 (3.00)	1-5
• There is a good working relationship between internal audit and information security	3.53 (4.00)	1-5
Top management support for information security		
• In my organization, top management provides adequate resources for information security	3.33 (4.00)	1-5
• In my organization, top management regularly communicates with employees about the importance of information security	3.21 (4.00)	1-5
• In my organization, top management believes that information security is an important issue	3.79 (4.00)	1-5
• In my organization, top management is more proactive as opposed to reactive with respect to information security issues	3.05 (3.00)	1-5
• Considering the past 3 years, I think top management's commitment to providing adequate resources for information security has	3.56 (4.00)	1-5
• Considering the past 3 years, I think top management's communication of the importance of information security issues has	3.45 (3.00)	1-5
• Considering the past 3 years, I think top management's view of the importance of information security has	3.51 (4.00)	1-5
• Considering the past 3 years, I think top management's anticipation of information security issues has	3.43 (3.00)	1-5

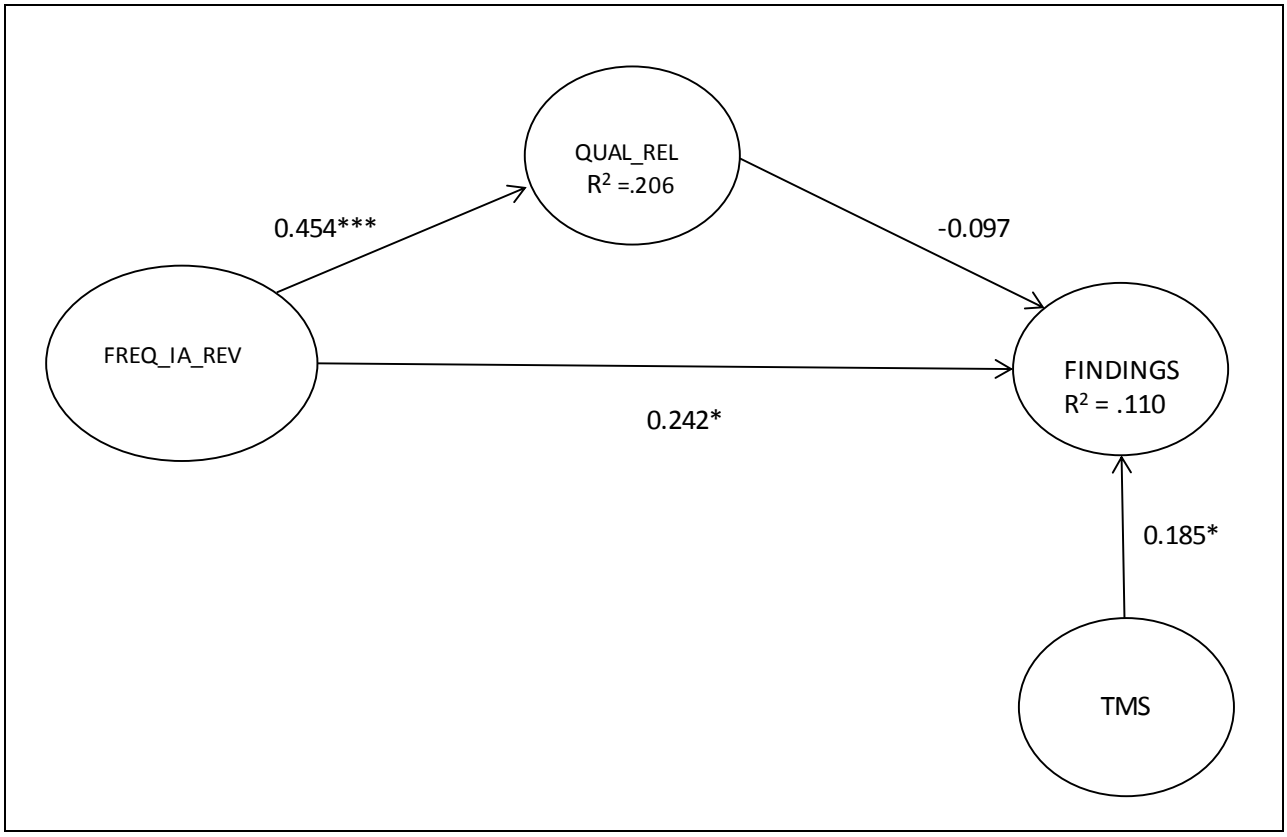
Table 4 shows the frequency of audit reviews varied across the eight areas of information security. Identity access controls and change management controls were reviewed most frequently, and encryption policies were reviewed least often. Overall, respondents rated the quality of the relationship between the internal audit and information security functions to be positive, but with potential for further improvement (Table 3 shows that the mean for the construct was 3.31 on a five-point scale, and Table 4 shows that the median for 3 of the 4 items comprising the construct was 4.0). Respondents also perceived that top management was supportive of information security, but that, too, could be increased (Table 3 shows that the mean for the construct was 3.42 on a 5-point scale, and Table 4 shows that the median score for five of

the eight items comprising the construct was 4.0). Table 4 also shows that respondents reported that between ten to fifteen percent of audit findings related to information security issues, and that the number of security-related audit findings had decreased over the past three years. Respondents also reported experiencing a number of security incidents in the past year (mean response was 16-20; median response was 21-25), but that number had slightly decreased from what it was three years earlier.

Model Fit

We used Partial Least Squares (PLS) to test the hypotheses in the research model because it does not assume multivariate normal distribution and is mathematically rigorous with small sample sizes (Hair et al. 2011; Lee et al. 2011). Consistent with Hair et al. (2011) recommendations, we ran 5000 bootstrapping repetitions. Figures 2 and 3 provide the results of the measurement and structural model for audit findings and security incidents, respectively.

Figure 2. Structural Model

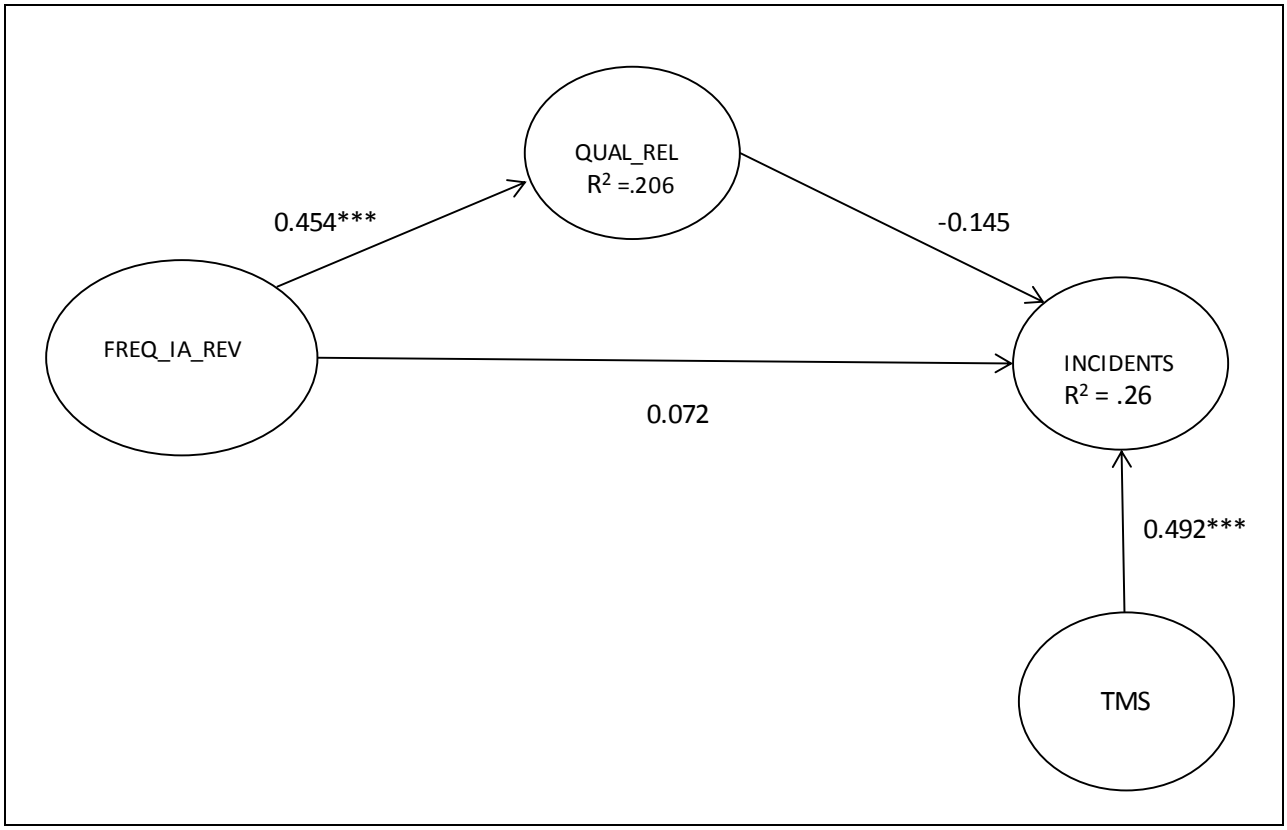


* P-value <. 10 (one-tailed)

** P-value <. 05 (one-tailed)

*** P-value <. 01 (one-tailed)

Figure 3. Structural Model



* P-value <. 10 (one-tailed)
** P-value <. 05 (one-tailed)
*** P-value <. 01 (one-tailed)

Although there are no overall 'goodness of fit' statistics in PLS (Hulland 1999), there are two means of understanding the predictability of a model in PLS: endogenous R^2 values, or amount of explained variance, and Q^2, or predictive relevance. R^2 values are 0.206 for the Relationship Quality construct, and 0.110 and 0.260 for the Audit Findings and Information Security Incidents Information Security Effectiveness outcome variables, respectively. The Stone-Geisser Q^2 values (Geisser 1974; Stone 1974) are 0.388 for Relationship Quality, 0.759 and 0.557 for Audit Findings and Information Security Incidents, respectively. Q^2 values for an endogenous construct that are greater than zero indicate that its explanatory latent construct exhibit predictive relevance (Hair et al. 2011). Thus, our model satisfies accepted standards for research seeking to identify predictive relationships.

Hypothesis Tests

Hypotheses 1 and 2 predict that internal auditors' perceptions about the quality of the relationship between the internal audit and information security functions will be positively related to the overall effectiveness of information security, both in terms of number of audit findings (H1) and security incidents (H2), after controlling for the effects of top management

support. As shown in Figures 2 and 3, neither path is significant. Thus, hypotheses 1 and 2 are not supported.

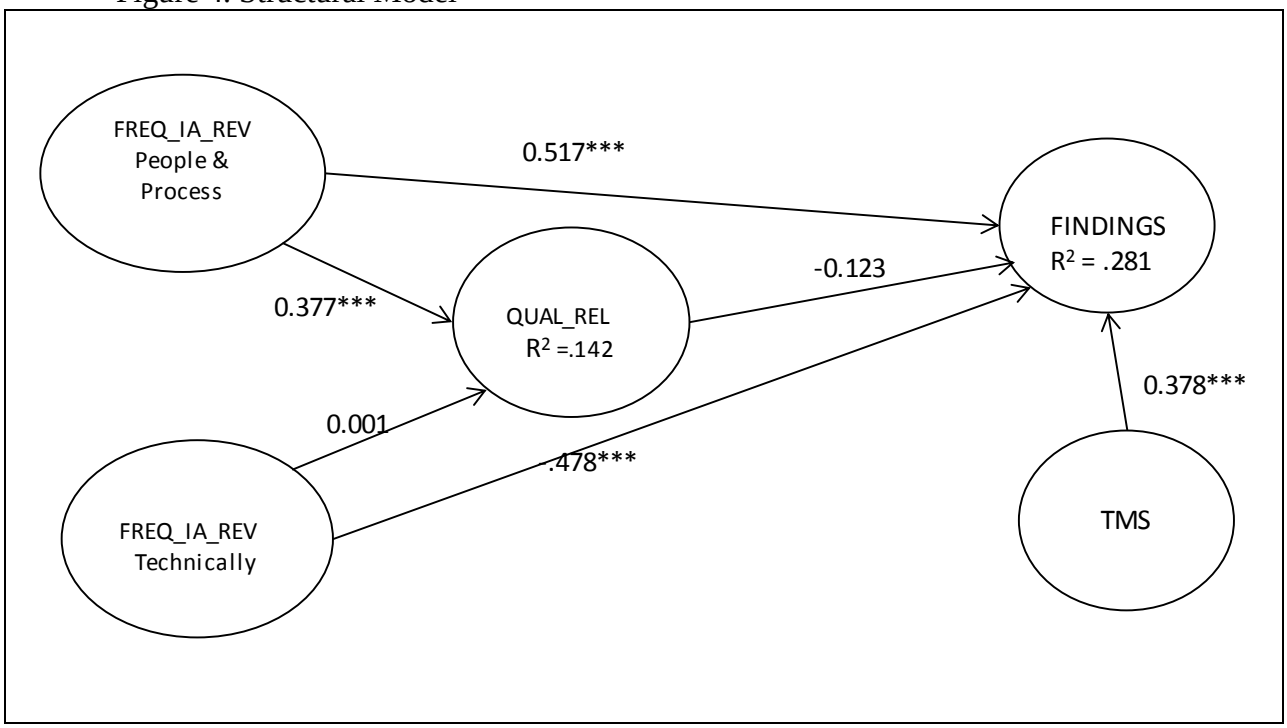
Hypothesis 3 predicts that the frequency of internal audit's review of information security activities will be positively associated with the quality of the relationship between the internal audit and the information security functions. In both figures 2 and 3 the path from audit review to relationship quality is positive and significant ($p < .01$). Thus, Hypothesis 3 is supported.

Hypotheses 4 and 5 predict that the frequency of internal audit reviews of information security will be positively (negatively) related to the number of audit findings (security incidents). Figure 2 shows that the path from audit reviews to findings is significant ($p < .10$), indicating that increased frequency of audit reviews of various information security activities results in more audit findings related to information security. Further, Figure 3 shows that the path from audit reviews to security incidents is not significant. Thus, neither H4 nor H5 are supported.

Supplemental Analyses

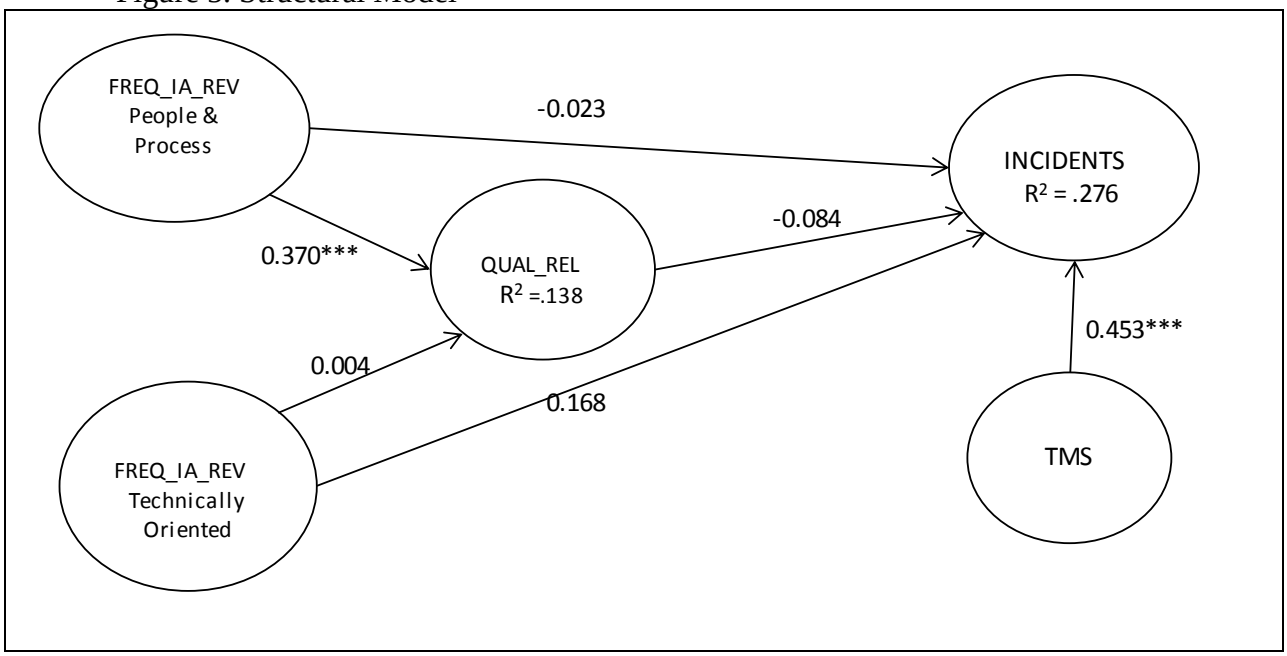
The preceding analysis shows that more frequent internal audit reviews of information security improve the quality of the relationship between the internal audit and information security functions. However, frequency of internal audit reviews has only a marginally significant ($p < 0.10$) direct influence on findings and does not directly influence security incidents. As in Steinbart (2013), we treated the frequency of audit reviews as a single, second-order formative construct based on responses to questions about the frequency with which internal auditors reviewed eight separate aspects of information security. If a second-order construct is not significant, re-fitting the model with first-order constructs may provide richer information on the impact of the individual constructs (Albers 2010). Consequently, we defined two first-order constructs for audit review frequency, based on discussions in the practitioner literature. Four items (identity and access management, backup procedures, security policies, and change management) focus on "softer" people-related issues and are considered important in a financial audit, whereas the other four items (encryption, firewalls, logging, and BC/DR) are more technically-oriented (Singleton 2009, 2010a, 2010b). A factor analysis of the responses to the eight questions confirms the loading on two distinct constructs. Therefore, we decided to retest hypotheses H3-H5 with models that divide audit review activities into two formative constructs. Figures 4 and 5 show the results of testing these revised models.

Figure 4. Structural Model



* P-value <. 10 (one-tailed)
** P-value <. 05 (one-tailed)
*** P-value <. 01 (one-tailed)

Figure 5. Structural Model



* P-value <. 10 (one-tailed)
** P-value <. 05 (one-tailed)
*** P-value <. 01 (one-tailed)

Figures 4 and 5 show that differentiating the two types of audit reviews provides additional insights into how the frequency of reviews affects the quality of the relationship between the internal audit and information security functions. Specifically, frequency of audit reviews that focus on the "softer" people and process aspects of information security have a significant ($p < 0.01$) positive effect on the quality of the relationship between the internal audit and information security functions, but audit reviews of the more technical aspects of information security do not.

Figure 4 shows that the explanatory power of the model (i.e., R^2 value) for audit findings improves to 0.281 when the types of audit review are separated, compared to 0.110 in the model where the types of findings are treated as a single, second order factor. In addition, the frequency of both types of audit reviews directly affects audit findings, albeit in different directions. More frequent audit reviews of the people-oriented aspects of information security are positively related ($p < 0.01$) with audit findings related to information security. In contrast, more frequent audit reviews of the more technical aspects of information security result are negatively related ($p < 0.01$) with audit findings.

Figure 5 shows that separating the types of audit review only slightly increases the R^2 for security incidents, to 0.276 in the model with separate factors for types of audit review, compared to 0.260 in the model where audit review types are treated as a single factor. However, neither type of audit review is significantly related to information security incidents.

V. DISCUSSION

We extend prior research by investigating how frequency of audit reviews of information security affect internal auditors' perceptions of the quality of the relationship between the internal audit and information security functions and the effect of audit reviews on both audit findings and security incidents. Before discussing the implications of our findings, it is important to acknowledge the study's limitations. The principal limitation is the small sample size. Nevertheless, respondents had extensive work experience and therefore were subject-matter experts who could provide insightful and reliable input. Indeed, a strength of the study is that instead of general perceptions about the effectiveness of information security, we collected data about the number of audit findings and security incidents. Another limitation is that the cross-sectional nature of the study precludes testing the temporal relationship between audit findings and future rates of security incidents. However, we note that cross-sectional surveys can provide useful data for assessing causal relationships, as shown in the following discussion.

We predicted and found that more frequent audit reviews of information security improve internal auditors' perceptions about the quality of their relationship with the information security function. Similarly, Steinbart et al. (2013) found that frequency of audit reviews of information security improve information security professionals' perceptions about the quality of their relationship with the internal audit function. Thus, both groups agree that greater involvement by internal audit (in the form of audit reviews) improves the quality of the relationship between the

two functions. However, as shown in Table 4, internal auditor responses to the frequency of audit reviews were only slightly above the midpoint on a five-point scale that ranged from not at all to often, similar to the results that Steinbart et al. (2013) report in their survey of information security professionals. Taken together, the results of both studies suggest that internal auditors could be more involved in reviewing various aspects of their organization's information security function and that such increased involvement is likely to improve the quality of the relationship between the two functions.

However, this study did not find any evidence that the quality of the relationship between the internal audit and information systems functions affects outcomes. Whereas Steinbart et al. (2013) found that information security professionals believe that the quality of the relationship between the internal audit and information security functions improves the effectiveness of information security, this study found no relationship between internal auditors' beliefs about the quality of this relationship and the number of reported security incidents. One explanation for this difference in results is that Steinbart et al. (2013) included *perceptions* of information security quality as one of the three components of their outcomes dependent measure, whereas the present study exclusively used internal audit findings and information security incidents as outcome measures. Another possibility is that a good relationship improves security by identifying vulnerabilities that need to be addressed, but the remediation efforts are not timely enough to reduce the number of incidents. Alternately, attackers may simply find other avenues to exploit. Further research, particularly of a longitudinal nature, is needed to better understand how the quality of the relationship between the information security and internal audit affects the overall effectiveness of an organization's information security program.

Similarly, whereas Steinbart et al. (2012) reported that internal auditors believe that a good relationship with the information security function improves audit effectiveness by helping them to focus on higher-risk areas, this study found that the quality of the relationship between the internal audit and information security functions does not affect the number of audit findings. On the one hand, this lack of a significant relationship indicates that efforts to improve the quality of the relationship between the two functions do not produce any objective benefits. On the other, this finding does not necessarily suggest that the quality of the relationship is unimportant. Clearly, an adversarial relationship between the auditor and auditee is not desirable as it is likely to increase the effort required to conduct an audit and may encourage the auditee to deliberately hide evidence. Moreover, our results show that a good relationship with the information security function does not *reduce* the number of audit findings related to information security issues. This can be interpreted in a positive light as evidence that cultivating a positive relationship with the auditee does not impair the auditor's independence and objectivity with respect to detecting and reporting findings related to information security.[1]

We also extended prior research by investigating whether audit reviews directly affect either the number of audit findings or security incidents, in addition to any indirect effects mediated by the quality of the relationship between internal audit and information security. Our

[1] We thank an anonymous reviewer for suggesting this positive interpretation of our results.

results provide evidence of a marginally significant positive relationship between more frequent reviews of various aspects of information security and the number of security-related audit findings. When we decomposed audit activities into two sub-constructs: one that addresses softer "people-related" information security topics and another that addresses technical information security topics, we found that more frequent reviews of "soft" issues resulted in an increased number of audit findings related to information security. At the same time, more frequent review of technical issues actually resulted in fewer audit findings.

The first result is intuitive: increased frequency of review produces more audit findings because the auditor is expending more effort and time on a given area. Although the result for increased frequency of reviews of the more technical aspects of information security seems counterintuitive, there is a plausible explanation. Active internal audit review of technical information security issues may serve as a preventive control. If information security personnel know that their activities are likely to be reviewed, they are more likely to be in compliance with best practices; therefore, there will be fewer internal audit findings in this area. In addition, it may be easier to correct audit findings related to technical aspects of information security than to fix issues associated with people and processes. Therefore, more frequent audit reviews of the technical aspects of information security will, over time, uncover fewer problems. Alternatively, this result may reflect the limits of internal audit's information security knowledge and expertise. Initial reviews of technical aspects of information security reveal issues in need of remediation, but after that "low-hanging fruit" has been addressed, additional scrutiny yields diminishing returns[2]. Clearly, additional research is needed to further investigate this apparently complex relationship between the frequency of different types of internal audit information security reviews and the number of internal audit findings.

Finally, while we found that the frequency of audit reviews affected the number of audit findings, it did not influence the number of information security incidents. There are several possible explanations for the lack of association between audit review and incidents. Because of time lags between finding an issue, reporting it, and addressing it, there may have not been enough time to address audit findings in order to prevent an incident. Alternatively, resource constraints may have resulted in a decision to not address audit findings. Moreover, there are numerous vectors that can be used to attack organizations, and audit reviews may not have identified all of them. Further, there is often a significant time lag of months or even years between the time when a security incident happens and it is discovered (Verizon 2012). Thus, reported incidents in our study may have predated audit reviews. Additional research, preferably longitudinal in nature, is needed to better understand this issue.

VI. CONCLUSION

This study extends prior research about the quality of the relationship between the information security and internal audit functions by collecting data from internal auditors about

[2] We thank an anonymous reviewer for suggesting this possible explanation.

their perceptions and actual audit activities. Consistent with prior research,w e found that greater interaction between the internal audit and information security functions, in the form of more frequent audit reviews of information security activities, improves the quality of the relationship between the two functions. However, relationship quality does not affect either the number of audit findings or security incidents. We did find, however, that frequency of audit reviews of information security directly affects the number of audit findings, independent of relationship quality. When considered as a single construct, frequency of audit reviews has a marginally significant positive relationship with the number of audit findings. Decomposition of the audit review construct, however, reveals a more nuanced picture of the relationship. More frequent audit reviews of the "softer" people and process aspects of information security increase the number of audit findings related to information security. At the same time, more frequent audit reviews of the technical aspects of information security result in fewer audit findings. At the same time, frequency of audit reviews had no effect on the number of security incidents, regardless of whether considered as a single construct or two constructs. Clearly, more research is needed to understand how internal audit reviews contribute to the overall effectiveness of information security.

REFERENCES

Anderson, K.A. 2012. A Case for a Partnership Between Information Security and Records Information Management. *ISACA Journal* 12 (2): 40-44.

Albers, S. "PLS and success factor studies in marketing" in Handbook of Partial Least Squares: Concepts, Methods, and Applications, Vinzi, V.E., Chin, W.W., Henseler, J., and Wang, H. (ed), Springer, Berlin 2010.

Behn, B., Carcello, J., Hermanson, D.R., and Hermanson, R.H. 1997. The determinants of audit client satisfaction among clients of big 6 firms. *Accounting Horizons* 11 (1): 7-24.

Bentler, P.M. and Wu, E.J.C. 1995. *EQS for Windows User's Guide*. Encino, Ca.: Multivariate Software.

Bou-Raad, G. 2000. Internal auditors and a value-added approach: The new business regime. *Managerial Auditing Journal* 15 (4): 182-187.

Bradach, J.L. and Eccles, R.G. 1989. Price, authority, and trust: From ideal types to plural forms. *Annual Review of Sociology* 15: 97-118.

Carcello, J., Hermanson, R., and McGrath, N. 1992. Audit quality attributes: the perceptions of audit partners, preparers, and financial statement users. *Auditing: A Journal of Practice and Theory* 11 (1): 1-31.

Cenfetelli, R. and Bassellier, G. 2009. Interpretation of formative measurement in information systems research. *MIS Quarterly* 33 (4): 689-707.

Chapman, C. 2001. Raising the bar. *Internal Auditor* 58 (2): 55-59.

Chin, W.W. "Partial Least Squares is to LISREL as principal components analysis is to common factor analysis. *Technology Studies*, 2:. 315-319.

Chin, W. W. "The Partial Least Squares Approach to Structural Equation Modeling," in *Modern Business Research Methods*, G. A. Marcoulides (ed.), Lawrence Erlbaum Associates, Mahwah, NJ, 1998.

Cronin, M.A., and Weingart, L.R. 2007. Representational gaps, information processing, and conflict in functionally diverse teams. *The Academy of Management Review* 32 (3): 761-773.

Collins, R. 1999. Auditing in the knowledge era. *Internal Auditor* 56 (3): 26-29.

Diamantopoulos, A., and Siguaw, J. A. 2006. Formative Versus Reflective Indicators in Organizational Measure Development: A Comparison and Empirical Illustration, *British Journal of Management* (17), 2006, pp. 263-282.

Dittenhofer, M.A., Ramamoorti, S., Ziegenfuss, D.E., and Evans, R.I. 2010. *Behavioral dimensions of internal auditing: A practical guide to professional relationships in internal auditing.* Orlando, FL. The Institute of Internal Auditors Research Foundation.

Donathan, C. 2012. So you want to be an IT auditor? *Internal Auditor* 69 (5): 26-27.

Geisser, S. 1974. A predictive approach to the random effects model. *Biometrika* 61 (1): 101–107.

Hair, J.F., C.M. Ringle, and M. Sarstedt. 2011. PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice* 19 (2): 139-151.

Henderson, J.C. 1990. Plugging into strategic partnerships: The critical IS connection. *Sloan Management Review* 31 (3): 7-18.

Huber, G.P., and Lewis, K. 2010. Cross understanding: implications for group cognition and performance. *The Academy of Management Review* 35 (1): 6-26.

Hulland, J. 1999. Use of partial least squares (PLS) in strategic management research: A review of four recent studies. Strategic Management Journal, 20 (2), 195-204.

IIA (Institute of Internal Auditors). 2011. International Standards for the Professional Practice of Internal Auditing. Available at https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Standards.aspx

ITGI. 2012a. *COBIT 5: Enabling Processes.* (IT Governance Institute: Rolling Meadows, IL).

ITGI. 2012b. *COBIT 5 for Information Security.* (IT Governance Institute: Rolling Meadows, IL).

Ko, D., Kirsch, L., and King, W. 2005. Antecedents of knowledge transfer form consultants to clients in enterprise system implementations. *MIS Quarterly* 29 (1): 59-85.

Lee, L., S. Petters, D. Fayard, and S. Robinson. 2011. On the use of partial least squares path modeling in accounting research. *International Journal of Accounting Information Systems* (12): 305-328.

Lin, S., M. Pizzini, M. Vargas, and I.R. Bardhan. 2011. The role of the internal audit function in the disclosure of material weaknesses. *The Accounting Review* 86 (1): 287-323.

Lindenberg, S.M. and Foss, N. 2011. Managing joint production motivation: the role of goal framing and governance mechanisms. *The Academy of Management Review* 36 (3): 500-525.

Marcoulides, G.A., and Saunders, C. 2006. PLS a silver bullet? *MIS Quarterly* 30 (2): iii-ix.

Mata, F., Fuerst, W., and Barney, J. 1995. Information technology and sustained competitive advantage: a resource-based analysis. *MIS Quarterly* 19 (4): 487-505.

McCann, D. 2009. Doing the Internal Audit – Management dance. *CFO.com*, (November 10, 2009). Available at www.cfo.com/article.cfm/14453909 – accessed on July 31, 2012.

Nagy, A.L. and Cenker, W.J. 2002. An assessment of the newly defined internal audit function. *Managerial Auditing Journal* 17 (3): 130-137.

National Institute of Standards and Technology (NIST). 2012. *Special Publication 800-53, Revision 4: Information Security – Security and Privacy Controls for Federal Information Systems and Organizations.*

Peter, S., Straub, D., and Rai, A. 2007. Specifying formative constructs in information systems research. *MIS Quarterly*, 31(4): 623-656.

Podsakoff, P.M., and Organ, D. W. 1986. Self-reports in organizational research: Problems and prospects. *Journal of Management*, 12(2): 531-544.

Ransbotham, S. and Mitra, S. 2009. Choice and chance: a conceptual model of paths to information security compromise. *Information Systems Research* 20 (1): 121-139.

Ray, G., Muhanna, W. A., and Barney, J.B. 2005. Information technology and the performance of the customer service process: A resource-based investigation. *MIS Quarterly* 29 (4): 625-651.

Rockart, J. 1988. The line takes the leadership – IS management in a wired society. *Sloan Management Review* 29 (4): 55-64.

Ross, J.W., Beath, C.M., and Goodhue, D.L. 1996. Developing long-term competitiveness through IT assets. *Sloan Management Review* 38 (1): 31-42.

Schroeder, M., Solomon, I., and Vickrey, D. 1986. Audit quality: the perceptions of audit-committee chairpersons and audit partners. *Auditing: A Journal of Practice and Theory* 5 (2): 86-94.

Singleton, T. W. 2009. "What Every IT Auditor Should Know About Scoping an IT Audit," *ISACA Journal (Volume 4):*

Singleton, T. W. 2010a. "The Minimum IT Controls to Assess in a Financial Audit (Part I)," *ISACA Journal (Volume 1):*

Singleton, T. W. 2010b. "The Minimum IT Controls to Assess in a Financial Audit (Part II)," *ISACA Journal (Volume 2):* 6.

Spira, L.F. and Page, M. 2003. Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal* 16 (4): 640-661.

Steinbart, P.J., Raschke, R., Gal, G., and Dilla, W. 2012. The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems* (13): 228-243.

Steinbart, P.J., Raschke, R., Gal, G., and Dilla, W. 2013. Information Security Professionals' Perceptions about the Relationship between the Information Security and Internal Audit Functions. *Journal of Information Systems* 27 (2).

Stewart, J., and Subramanian, N. 2010. Internal audit independence and objectivity: emerging research opportunities. *Managerial Auditing Journal* 25 (4): 328-360.

Stoel, D., Havelka, D., and Merhout, J.W. 2012. An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners. *International Journal of Accounting Information Systems* 13: 60-79.

Stone, M. 1974. Cross-validatory choice and assessment of statistical predictions. *Journal of the Royal Statistical Society* 36 (2): 111–147.

Sundaramurthy, C. and Lewis, M. 2003. Control and collaboration: Paradoxes of governance. *The Academy of Management Review* 28 (3): 397-415.

Tucci, L. 2009. How CISOs can leverage the internal audit process. http://searchcompliance.techtarget.com/news/1362909/How-CISOs-can-leverage-the-internal-audit-process.

Van Peursem, K.A. 2005. Conversations with internal auditors: The power of ambiguity. *Managerial Auditing Journal* 20 (5): 489-512.

Wallace, L., Lin, H., and Cefaratti, M.A. 2011. Information security and Sarbanes-Oxley compliance: an exploratory study. *Journal of Information Systems* 25 (1): 185-212.

APPENDIX A – Construct Items

Construct: Frequency of Internal Audit Review of Information Security (FREQ_IA_REV) – 8 questions

Eight questions that asked respondents about the frequency of internal audit reviews of information security: (responses on a 5-point scale from Not at All to Often)

1. Business Continuity and Disaster Recovery Plans
2. Identity and Access Management Controls
3. Logging and system monitoring
4. Firewalls and other network access devices
5. Encryption policies (including key management)
6. Backup procedures
7. Change Management Controls
8. Security policies

Construct: Perceived Quality of Relationship Between Internal Audit and Information Security (QUAL_REL) – 4 questions

(responses on a five-point scale from Strongly Disagree to Strongly Agree)

1. There is little friction between internal audit and information security
2. The relationship between internal audit and information security staff is close and personal
3. There is a good working relationship between internal audit and information security
4. Members of information security and internal audit work together to assure information systems are secure and reliable

Construct: Perceived Effectiveness of the Organization's Information Security – 2 constructs:

Sub-construct 1: Security Incidents (INCIDENTS) – 2 questions

1. During the past year how information security incidents (breaches, denials of service, etc.) did you have? (7 ordinal responses, from zero to more than 25)
2. Compared to 3 years ago, the number of information security incidents has (significantly decreased through significantly increased, plus the option to indicate no problems)

Sub-construct 2: Audit Findings (FINDINGS) – 2 questions

1. Consider the total number of audit findings listed in formal internal audit reports during the most recent fiscal year, what is the percentage of internal audit findings related to information security? (7-point scale, from 0% to more than 25%)
2. Would you say that the number of internal audit findings specifically related to information security this year versus three years ago has (significantly decreased to remained the same to significantly increased PLUS we had none)

Construct: Perceptions of Top Management Support for Information Security (TMS)– 8 questions

Current situation (responses on a 5-point scale from Strongly Disagree to Strongly Agree):

1. In my organization, top management provides adequate resources for information security
2. In my organization, top management regularly communicates with employees about the importance of information security
3. In my organization, top management believes that information security is an important issue
4. In my organization, top management is more proactive as opposed to reactive with respect to information security issues

Trend in top management support (responses on 5-point scale from significantly decreased to significantly increased, with 3 = remained constant)

5. Considering the past 3 years, I think top management's commitment to providing adequate resources for information security has
6. Considering the past 3 years, I think top management's communication of the importance of information security issues has
7. Considering the past 3 years, I think top management's view of the importance of information security has
8. Considering the past 3 years, I think top management's anticipation of information security issues has