

Characteristics of Cybersecurity and IT Involvement by the IA Activity

Christopher Calvin
University of Dayton
ccalvin1@udayton.edu

Marc Eulerich
University of Duisburg-Essen
marc.eulerich@uni-due.de

Matthew Holt
University of Dayton
mholt1@udayton.edu

August 2023

Abstract: We provide the first, large scale, global study on the characteristics associated with an internal audit function's involvement in IT and cybersecurity assurance. Using a unique dataset of 1,142 survey responses, we identify internal audit development (i.e., level of maturity) and two characteristics of internal audit knowledge availability (CAE IT certification and external sourcing) as being positively associated with the performance of IT assurance, cybersecurity assurance, or both. Our findings are informative to academia, laying the groundwork for further exploration of internal audit's engagement in IT and cybersecurity assurance. They are also informative to practice, as they provide insight to standard setters, practitioners, management, and governance bodies about characteristics that can enhance internal audit's ability to provide IT and cybersecurity assurance.

Keywords: Internal Audit Function, Cybersecurity, IT Audit

JEL-Classification: M42, M15, L86

Disclosure: The Internal Audit Foundation granted access to its “Assessing Internal Audit Practices Globally” survey data on conditions of anonymity and confidentiality. Although the data were provided by the Foundation, the views expressed in this study are those of the authors and do not necessarily present positions or opinions of the Foundation.

Acknowledgements: We are grateful to Martin Wagener and Annika Bonrath for their helpful comments. We also appreciate the University of Dayton and University of Duisburg-Essen for supporting this research. Any remaining errors are our own.

Characteristics of Cybersecurity and IT Involvement by the IA Activity

Abstract: We provide the first, large scale, global study on the characteristics associated with an internal audit function's involvement in IT and cybersecurity assurance. Using a unique dataset of 1,142 survey responses, we identify internal audit development (i.e., level of maturity) and two characteristics of internal audit knowledge availability (CAE IT certification and external sourcing) as being positively associated with the performance of IT assurance, cybersecurity assurance, or both. Our findings are informative to academia, laying the groundwork for further exploration of internal audit's engagement in IT and cybersecurity assurance. They are also informative to practice, as they provide insight to standard setters, practitioners, management, and governance bodies about characteristics that can enhance internal audit's ability to provide IT and cybersecurity assurance.

Keywords: Internal Audit Function, Cybersecurity, IT Audit

JEL-Classification: M42, M15, L86

Characteristics of Cybersecurity and IT Involvement by the IA Activity

I. INTRODUCTION

In recent years, the concept of cybersecurity has become increasingly relevant to corporate management and audit committees. Cybersecurity risks are now among the most dominant classes of business risks for companies and other forms of organization (Walton, Wheeler, Zhang, and Zhao 2021; Chartered Institute of Internal Auditors 2021; ECIIA 2022; World Economic Forum 2022, Wilkin, and Chenhall 2020). Cyberattacks can bring business operations to a halt and jeopardize the financial well-being of the company (e.g., Jiang, Legoria, Reichelt, and Walton 2021). Additionally, risks related to privacy of data in the custody of an organization, that pertain to others, present potential fiduciary and ethical problems which could damage the business model. However, since there are too few members on boards with relevant IT expertise (Boehm, Laube, and Riek 2018; Boehm, Curcio, Merrath, Shenton, and Staehle 2019), boards of directors and audit committees must rely on other partners to assist with governance related to IT systems and cybersecurity risks. Against this background, internal auditing provides independent and objective assurance and consulting services to improve governance, risk management, and internal controls (Eulerich 2021). The scope of an internal audit function (IAF) includes various organizational activities and internal auditors could be a valuable source of different types of IT-related assurance activities, e.g., in the field of information security, cybersecurity, or continuous IT assurance (e.g. No and Vasarhelyi 2017; Steinbart, Raschke, Gal, and Dilla 2012, 2013, 2018).

This paper focuses on the involvement of IAFs in cybersecurity and IT assurance tasks. We empirically examine characteristics of cybersecurity and IT involvement with a set of global data from 1,142 Chief Audit Executives (CAEs). Those characteristics include the maturity of the IAF,

whether the CAE holds an IT certification, and above-average outsourcing of the IAF. We also explore the role audit committee oversight plays.

Our findings contribute to the academic and practitioner knowledge bases on IAFs' IT-related assurance activities. Prior literature does not address why some IAFs engage in IT and cybersecurity assurance activities while others do not. We identify several characteristics associated with such engagement. Furthermore, ex-ante, one might assume the same characteristics are associated with IT assurance and cybersecurity, as they are closely related. However, our results highlight two key characteristics that are associated with cybersecurity assurance which are not associated with IT assurance. Finally, we have established a baseline understanding of IAFs' involvement in IT and cybersecurity that could be leveraged to perform future in-depth research in this area.

II. LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

The value proposition of the IAF is that the members of the internal audit profession assist boards and top-management in achieving organizational objectives by providing independent assurance regarding risk management, control, and governance processes.¹ It is well established that an IAF can add value to the financial reporting process of an organization (e.g., Coram, Ferguson, and Moroney 2008; Prawitt, Smith, and Wood 2009; Lin, Pizzini, Vargus, and Bardhan 2011; Ege 2015) and reduce the company's risk level (Carcello, Eulerich, Masli, and Wood 2018). More recently, there has been discussion about the role that IAFs should play in cybersecurity and protecting a company's information system (IS) (Slapničar, Vuko, Čular, Drašček 2022; Slapničar, Axelsen, Bongiovanni, and Stockdale 2022). While this is generally outside of the traditional

¹ Obtained from the Institute of Internal Auditors - <https://www.theiia.org/en/about-us/about-internal-audit/> (accessed February 10, 2023).

duties performed by IAFs, standard-setting bodies, global organizations, and even higher education institutions suggest that IAFs should be as involved as they would with the implementation of other risk mitigation strategies.

The IIA, for example, has published a great deal of literature suggesting that internal auditors should become more involved with information technology systems and cybersecurity controls assurance (ITCSA) (e.g., IIA 2016). The IIA has also published specific guidance about the role of the IAF in the context of ITCSA (see, for example, the IIA's series of the Global Technology Audit Guides (GTAGs)). More recently, in December 2022, the B20's Integrity and Compliance Task Force (the official business forum for the G20 summit) issued a policy paper recommending strengthening the position of IAFs with respect to cybersecurity assurance, highlighting the essential role they play in this area of risk mitigation.² In March 2023, Louisiana State University's (LSU) Center for Internal Auditing Excellence, a flagship internal audit education program created in partnership with the IIA, expanded its curriculum and rebranded itself to the LSU Center for Internal Auditing Excellence and Cybersecurity Risk Management.³ This push from the IIA and other bodies coincides with economic reasons for greater IAF participation in ITCSA due to increased risks in these areas; breaches and failures can damage an organization financially and reputationally. In a recent survey by Deloitte, 34.5% of executives responded that their organizations' accounting and finance data had been specifically targeted via cyberattack and 39.5% responded that they expect their finance and cybersecurity teams to work more closely together in the next year (Deloitte 2023).

² Obtained from the B20 website - https://b20indonesia2022.org/view-doc-b20/policy_paper/MVY26ELP (accessed March 7, 2023).

³ See the press release at <https://www.lsu.edu/business/news/2023/3/world-renowned-lsu-center-for-internal-auditing-adds-cybersecurity-esg-2023.php> (accessed March 7, 2023).

In recent years, the digitization of corporate processes has dominated the strategy discussion within companies. However, transforming buzzwords such as ‘digitization’, ‘automation’, ‘data analytics’, ‘cloud service’, and ‘Big Data’ into actual, successful projects is a significant challenge. Although the concepts associated with these buzzwords offer a broad variety of benefits, nearly all of them generate myriad risks and challenges (e.g., Eulerich, Masli, Pickerd, and Wood 2022; Eulerich, Waddoups, Wagener, and Wood 2023b). Most of these new technologies have numerous cybersecurity risks, which is why cybersecurity has become a key priority in enterprise risk management. Current professional studies, such as the “Risk in Focus” study from the European Confederation of Institutes of Internal Auditors (ECIIA), rate cybersecurity as the number one risk for companies (ECIIA 2022). As organizations’ information systems gather more information than ever, some belonging to the entity and some belonging to others, the controls placed within and around these systems have become more important (e.g., Eulerich, Waddoups, Wagener, and Wood 2023a). Many controls that were once performed manually are now incorporated into an organization’s IS. Additionally, an ever-increasing number of companies have some portion of their IS maintained remotely by cloud service providers, which creates other risks. Also, as companies continue to move to the cloud, they will likely have much smaller IT and information security departments who traditionally are responsible for much of the work regarding ITCSA. Poorly designed IS controls can lead to unreliable systems that harm the organization even in the absence of any malice. In addition, malicious cyberattacks continue to increase (World Economic Forum 2022). Thus, organizations should continuously assess their overall IT and cybersecurity risk profile to be better prepared against attacks and other inherent risks.

IAFs recognize that their organizations expect them to provide value. One potential way for them to do that is to help reduce the frequency of, and fallout from, IT and cybersecurity-related

incidents. IIA “Three Lines” guidance suggests internal auditors are well-positioned to provide ITCSA since they offer independent and objective audit and consulting services for all first and second line activities and functions (Bantleon et al. 2020; IIA 2020b).⁴ In other words, all IT-related risks of an organization can be in the scope of the IAF. This includes IT systems and IT governance, but also Cybersecurity audits (Dzuranin and Malaescu 2016; IIA 2022). The IIA’s International Professional Practice Framework concretize this focus on the assurance of IT in their standard 2110.A2, which explains that one potential internal audit activity is to assess whether the organization’s IT governance supports the organization’s strategies and objectives. However, as will be discussed later, less than half of CAEs surveyed indicate that their IAFs have significant involvement in IT and cybersecurity assurance activities.

Although the advantages of linking internal audit activities and IT audit and/or cybersecurity audits seem obvious, and the standard setters define the framework for internal audit functions through numerous publications (e.g., IIA 2017, IIA 2020a, IIA 2022), the alignment in practice remains far from the envisioned path (Internal Audit Foundation and Crowe 2018; Kahyaoglu and Caliyurt 2018). There is a question as to why some IAFs have increased their participation in ITCSA, while others have not. It is important to better understand which characteristics drive IAFs to take a more active role in the assurance of IT-related risks through ITCSA. Thus, the development of our hypotheses is centered on two high-level dimensions which are expected to influence IAF participation in ITCSA: level of development and knowledge sets.

Internal Audit Function Development

⁴ “First line roles are most directly aligned with the delivery of products and/or services to clients of the organization, and include the roles of support functions. Second line roles provide assistance with managing risk” (IIA 2020b). These roles are the responsibility of management.

For an IAF to participate in ITCSA, it requires appropriate support from the organization. A less mature IAF will focus on more traditional areas of internal auditing, as the core responsibilities of the IAF would need to be fulfilled before adding additional duties such as contributing to ITCSA. Furthermore, lack of development may prevent adequate knowledge attainment to provide significant ITCSA support. Companies that value the IAF and sponsor its growth and progress will tend to have more mature IAFs that possess the capability to become involved in newer areas such as ITCSA. This leads to our first set of hypotheses:⁵

H1a: There is a positive association between the level of IAF development and participation in IT assurance.

H1b: There is a positive association between the level of IAF development and participation in cybersecurity assurance.

Internal Audit Function Knowledge Set

In addition to reaching a certain level of development, knowledge is a key dimension required for IAFs to participate in ITCSA. Abbott, Daugherty, parker, and Peters (2016) mention competence as integral to IAF effectiveness, and there is some question regarding whether IAFs possess, or can even obtain, the requisite skills to effectively participate in ITCSA. Even if an IAF is sufficiently mature, if it doesn't have personnel with necessary IT and cybersecurity skills, and cannot outsource those skills because they are in high demand, then the IAF will be unable to participate in ITCSA. This leads to our second set of hypotheses:

H2a: There is a positive association between access to ITCSA knowledge and participation in IT assurance.

H2b: There is a positive association between access to ITCSA knowledge and participation in cybersecurity assurance.

⁵ Ex ante, we have no reason to believe participation in IT assurance will differ from participation in cybersecurity assurance on the dimensions of IAF development and knowledge. However, the survey data used for this study separately asked respondents about cybersecurity assurance and the collection of all other IT assurance. To provide the richest analysis possible, we therefore examined each type of assurance individually as well as in combination.

Audit Committee Reliance on the Internal Audit Function

As mentioned in the introduction, governing bodies such as audit committees often rely on others for assistance with IT and cybersecurity governance due to a lack of relevant internal expertise and assurance being outside the scope of the board of directors. Since IIA Standards 1110, 1111, and 2060 require the IAF to report to an organization's board, it is naturally positioned to provide such risk assurance reliance through ITCSA engagement. On the other hand, we have already discussed a number of reasons why IAFs may engage in ITCSA even without serving the needs of a governing body. Thus, it is unclear whether the presence of an audit committee affects the likelihood that an IAF engages in ITCSA. We explore this with the following set of research questions:

RQ1a: Are IAFs that report to audit committees more likely to participate in IT assurance?

RQ1b: Are IAFs that report to audit committees more likely to participate in cybersecurity assurance?

III. RESEARCH DESIGN

Tests of the Characteristics of Cybersecurity and IT Involvement by the IA Activity

We test H1, H2, and RQ1 using the following equation that models IAF involvement in their organizations' cybersecurity and IT efforts as functions of potential characteristics of involvement and a control set of IAF and organization traits:

$$\text{Involvement} = \alpha + \beta_1 \text{Maturity} + \beta_2 \text{ITCert} + \beta_3 \text{Sourcing} + \beta_4 \text{AC} + \text{controls} + \epsilon \quad (1)$$

In the above model, *Involvement* represents one of three indicator variables: *Cyber*, *IT*, and *CyberIT*, which are equal to one if a survey respondent indicated that their IAF had significant involvement in the organization's cybersecurity, IT, or cybersecurity and IT efforts, and are equal to zero otherwise. The variables of interest in Eq. (1) are *Maturity*, *ITCert*, *Sourcing*, and *AC*.

Maturity is a variable equal to zero, one, two, three, or four if a respondent answered that their IAF had an initial, infrastructure, integrated, managed, or optimizing level of maturity per the IIA-Netherlands' Internal Audit Ambition Model, respectively.⁶ This measure is used to capture the level of development of the IAF used to test H1a and H1b. Because we expect more developed IAFs to be those engaged in higher-level activities such as ITCSA, we predict a positive coefficient on β_1 .

Additional variables of interest in the above models, used to test H2a and H2b, include *ITCert* and *Sourcing*. *ITCert* is an indicator variable equal to one if a survey respondent indicated that they held an IT-related certification, and equal to zero otherwise.⁷ Certifications represent a respondent's skillset. Regardless of whether the organization hired a CAE because it desires their particular IT-related skillset, or a CAE's personal skillset, it influences the activities and priorities of the IAF. We predict that IT skills held by IAF supervisors will be associated with more IAF involvement in the ITCSA efforts of the organization. Therefore, we predict a positive coefficient on β_2 . *Sourcing* is an indicator variable equal to one if a survey respondent indicated that their organization outsources or co-sources IAF services greater than the sample mean (eleven percent), and equal to zero otherwise.⁸ For organizations that do not possess IAF employees with the necessary skills to effectively participate in ITCSA, outsourcing serves as another way to fill the knowledge gap (e.g., Abbott, Parker, Peters, and Rama 2007). Thus, we expect outsourcing will be associated with ITCSA participation and predict a positive coefficient on β_3 .

We include in Eq. (1) one final variable of interest, *AC*, which is an indicator variable equal to one if a survey respondent indicated that their organization has an audit committee, and equal to

⁶ There is no concept of "zero maturity," therefore we set the lowest level of maturity, "initial," equal to zero.

⁷ As noted below, our sample is restricted to Chief Audit Executives.

⁸ The use of a mean split provided more variation than a median split, as the median was only five percent.

zero otherwise. As noted in our discussion of RQ1, it is unclear whether the presence of an audit committee will influence an IAF's involvement in ITCSA. Thus, we make no prediction for β_4 and include it for exploratory purposes. A significant, positive coefficient suggests the presence of an audit committee contributes to an IAFs engagement in ITCSA, while a significant, negative coefficient, or insignificant coefficient, suggests otherwise.

Control variables in Eq. (1) include *Funding*, *AdminRptMgmt*, *FuncRptBoard*, *Private*, *NonProfit*, *Government*, and *OtherOrg*, all defined in Appendix A.⁹ We include country and industry fixed effects and estimate the models using logistic regression with robust standard errors. For ease of interpretation, we present odds ratio coefficients for all results.

Sample Selection

Our sample is comprised of respondents to the IIA's "Assessing Internal Audit Practices Globally" survey. The survey was administered during the second half of 2021 and received responses from over 3,600 practitioners from 159 countries and territories. From the initial pool of respondents, we eliminated those who were not CAEs, as IA staff were not presented with the survey questions relied upon in this study. We then eliminated any CAE respondents who did not answer all questions used to derive regression variables, resulting in a final sample of 1,142 observations.

Sample Descriptive Analysis

Summary statistics, presented in Table 1a, show that 38 percent of respondents indicated that cybersecurity (*Cyber*) is an area in which their IAF has significant involvement. 38 percent also indicated that IT is an area in which their IAF has significant involvement (*IT*) while 25 percent

⁹ To ensure our model is not subject to multi-collinearity concerns, we calculated its variance inflation factor (VIF). The minimum VIF observed was 1.01 and the maximum VIF observed was 3.65, suggesting multi-collinearity is not an issue.

of the sample indicated that they have significant involvement in both cybersecurity and IT (*CyberIT*). The average maturity level of IAFs in our sample is 2.42 out of four (*Maturity*). IT certifications are held by 17 percent of respondents in our sample (*ITCert*), 27 percent use co-sourcing or outsourcing to staff their IA activity (*Sourcing*), and 83 percent of organizations in our sample have an audit committee (*AC*).

INSERT TABLE 1A HERE

To provide additional descriptive insight into the sample, we also perform ten cross-section analyses that yield preliminary evidence about dimensions on which the IAF's involvement in IT and/or cybersecurity differ. The summary of these analyses is presented in Table 1b. We find that larger IAFs, sufficiently funded IAFs, IAFs whose CAEs have an IT-related certification, IAFs which outsource a portion of their services, IAFs that operate in organizations with audit committees, IAFs that report functionally to the board, more mature IAFs, IAFs located in North America, and IAFs serving the finance industry tend to be more involved in both IT and cybersecurity assurance activities. The results for IAF maturity and IPPF conformance, IAF size, CAE certification, and service sourcing, and audit committee presence provide preliminary support for our hypotheses. Additionally, the result for audit committee presence provides an initial finding related to our research question. The results for sufficient funding, functional reporting, North American IAFs, and finance industry IAFs are unrelated to our hypotheses but are nonetheless intuitive. Involvement in ITCSA is a costly activity that will require sufficient funding to support. Functional reporting to the board helps position the IAF to provide ITCSA assurance to a governance body. North American IAFs operate in a highly regulated capital market that places significant value on investor and asset protection. Finally, IAFs in the finance industry work for organizations with heightened levels of IT and cybersecurity risk. Surprisingly, though public

companies are associated with many of these same characteristics in practice (audit committees, larger IAFs, more mature IAFs, capital market regulation, etc.), there was no evidence that IAFs in public companies are more likely to engage in ITCSA.

INSERT TABLE 1B HERE

Pearson and Spearman correlations between dependent variables and independent variables of interest are presented in Table 2. With the exception of a positive, but insignificant association between IA sourcing and IT involvement, the univariate correlations generally provide support for our hypotheses (based on Pearson correlations). However, since these correlations do not control for other correlated variables, we defer further discussion to multivariate analyses.

INSERT TABLE 2 HERE

IV. RESULTS

Hypothesis 1 Test Results

Results from our estimates of Eq. (1) are presented in Table 3. Consistent with H1a and H1b, the coefficient on *Maturity* is positive and significant when using *Cyber*, *IT*, and *CyberIT* as our dependent variables (z-stats: 6.077, 4.847, and 5.240, respectively). These results provide evidence that more developed IAFs are associated with having a more significant role in the assurance related to cybersecurity and IT in their respective organizations.

INSERT TABLE 3 HERE

Hypothesis 2 Test Results

Results for our tests of H2 are also contained in Table 3. Consistent with H2a and H2b, the coefficient on *ITCert* is positive and significant when using *Cyber*, *IT*, and *CyberIT* as our dependent variables (z-stats: 4.646, 3.901, and 3.972, respectively). Consistent with H2b, but not H2a, the coefficient on *Sourcing* is positive and significant when using *Cyber* as the dependent

variable (z-stat: 1.773), but not when using *IT* or *CyberIT* (z-stats: 0.635 and 1.340, respectively). These findings suggest that, as predicted, the IAF's involvement in cybersecurity and IT is associated with CAEs having relevant skillsets. Since CAEs serve in a supervisory and planning capacity, rather than a hands-on auditing capacity, this association suggests the personal specializations of CAEs influence the areas in which their IA activities are involved.¹⁰ These findings also suggest that missing skillsets can be co-sourced or outsourced, but that sourcing tends to be used for cybersecurity assurance, rather than more general IT assurance. A possible explanation for this is that cybersecurity is a newer threat that incumbent IAFs are less equipped to address, versus IT risk, which has existed for longer and for which IAF management and staff are better trained to handle.

Research Question 1 Analysis

Our analysis of RQ1 is also presented in Table 3. The coefficient on *AC* is positive and significant when using *Cyber* as the dependent variable (z-stat: 2.337), but not when using *IT* or *CyberIT* (z-stats: 0.328 and 1.287, respectively). These findings suggest that audit committees may increase pressure on IAFs to serve as cybersecurity assurance providers. Similar to our findings for *Sourcing*, it is possible that due the longer history of IT risk for companies, the presence of an audit committee may not be related to IT assurance in the same way. In other words, more developed IAFs may be involved with IT assurance at this point, regardless of whether or not the organization has an audit committee.

¹⁰ Alternatively, it is possible that companies who wish for their IA activities to be involved in cybersecurity and IT hire internal auditors with that particular skillset, but those hiring efforts would more likely be at the hands-on (i.e., staff) level. Since we do not have relevant data from staff survey respondents, we are unable to further disentangle these possibilities.

V. SUPPLEMENTAL ANALYSIS

To further explore the relationships tested in H1 and H2, we performed a path analysis to examine how IAF development impacts ITCSA directly and indirectly through sources of knowledge. Results of the analyses (untabulated, presented visually in Figures 1-3) show that *Maturity* (i.e., development) impacts ITCSA directly as well as indirectly through *ITCert*. This implies that the more developed an IAF is, the more likely the IAF will participate in ITCSA, and will do it by obtaining the requisite knowledge internally.

INSERT FIGURE 1 HERE

The level of IAF development is negatively associated with outsourcing, which is to be expected.¹¹ The more developed an IAF is, the more likely it will have greater internal knowledge that pertains to ITCSA, and thus the less likely it will resort to outsourcing to fill in knowledge gaps. In line with the results of our primary tests, the role played by *Sourcing* is not consistent between *Cyber* and *IT*. As shown in Figure 1, *Sourcing* is positively and significantly associated with engagement in *Cyber*. However, Figures 2 and 3 demonstrate that Sourcing is not significantly associated with *IT* or *CyberIT*. Again, we posit that the difference may be due to the newness of IAF participation in cybersecurity-related activities, relative to more general IT. As cybersecurity is newer, IAFs may be more likely to outsource, because they may be less likely to have the requisite knowledge in-house.

INSERT FIGURES 2 AND 3 HERE

¹¹ Path analysis coefficients are presented as odds ratios. Therefore, a coefficient less than one implies lower odds (i.e., a negative association).

VI. CONCLUSION

This paper investigates characteristics associated with an IAFs' involvement in cybersecurity and IT assurance. We posit that for an IAF to engage in ITCSA, it must be sufficiently developed and have access to requisite IT and cybersecurity knowledge. Using a unique dataset of 1,142 survey responses from CAEs, we perform the first academic examination, to the best of our knowledge, of the IAF's involvement in ITCSA on a global scale. We identify a characteristic of IAF development (maturity) and two characteristics of IAF knowledge availability (CAE IT certification and external sourcing) that are associated with the performance of IT assurance, cybersecurity assurance, or both.

Our results contribute to the academic discussion about the evolving role of internal auditors in ITCSA. Existing literature has yet to shed light on why, despite repeated encouragement from the IIA to engage in ITCSA and the IAF's natural position to provide ITCSA as both an assurance and value-add activity, some IAFs include IT and cybersecurity in their audit plans while others do not. Through descriptive and regression analysis, we provide support that variation in IAFs' development and knowledge availability are two explanations for these differences. These findings represent a first step in this area and pave the way for future research into the IAF's ITCSA involvement. Such research could include more targeted surveys aimed at identifying additional characteristics that impact the likelihood of an IAF's ITCSA involvement or examining potential interactions between these characteristics. It could also include experiments to explore how an IAF's ITCSA involvement affects other assurance aspects of the organization, such as external audit reliance, or how it influences capital market responses, such as investor decisions. As a final suggestion, experimental and qualitative methods could be combined to gain an understanding of the effectiveness of internal auditors (versus other assurance providers) in ITCSA activities.

Our results also contribute to the practical knowledge about IAFs' involvement in ITCSA. The standard-setting body for the internal audit profession, the IIA, has been a proponent of IAF ITCSA involvement, and identifying the characteristics associated with that involvement can assist the IIA in providing more detailed guidance in this area. IAF practitioners who wish to pursue an ITCSA strategy can use knowledge of these characteristics to identify potential gaps in their ability to engage in ITCSA. Furthermore, management and boards can use this knowledge to better understand how they can position and equip their IAFs to offer more assurance in the fields of cybersecurity and IT.

As with all studies, our method of analysis comes with some limitations. First, the survey answers we relied upon are the perceptions of the survey participants, as we do not directly measure the level of each IAF's ITCSA involvement. It is therefore possible that self-perception bias leads to an above-average evaluation of the dimensions surveyed (i.e., internal auditors present themselves in an overly positive manner). The survey's confidentiality, as well as absence of repercussions for any negative responses given, should mitigate much of this concern. The survey was also limited in which company data it collected. Certain measures we've used in this study would more appropriately be scaled by company size, complexity, or a similar construct. As these scaling measures were not collected, we implemented unscaled measures in our models. Future research could explore whether scaling IAF characteristics by company characteristics affects our inferences.

REFERENCES

- Abbott, L. J., B. Daugherty, S. Parker, and G. F. Peters. 2016. Internal audit quality and financial reporting quality: The joint importance of independence and competence. *Journal of Accounting Research* 54 (1): 3–40.
- Abbott, L. J., S. Parker, G. F. Peters, and D. V. Rama. 2007. Corporate governance, audit quality, and the Sarbanes-Oxley Act: Evidence from internal audit outsourcing. *The Accounting Review* 82 (4): 803–835.
- Bantleon, U., A. d'Arcy, M. Eulerich, A. Hucke, B. Pedell, and N. V. S. Ratzinger-Sakel. 2020. Coordination Challenges in Implementing the Three Lines of Defense Model. *International Journal of Auditing* 25(1): 59–74.
- Boehm, J., N. Curcio, P. Merrath, L. Shenton, and T. Stähle. 2019. *The risk-based approach to cybersecurity*. Available at: <https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity> (last accessed March 3, 2023).
- Boehm, R., S. Laube, and M. Riek. (2018). A fundamental approach to cyber risk analysis. *Variance* 12 (2): 161–185.
- Carcello, J., M. Eulerich, A. Masli, and D. A. Wood. 2018. The value to management of using the internal audit function as a management training ground. *Accounting Horizons* 32 (2): 121–140.
- Chartered Institute of Internal Auditors. 2021. *Mind the gap: Cybersecurity risk in the new normal*. Available at: <https://www.iiia.org.uk/media/1691585/cyber-security-risk-in-the-new-normal-report.pdf> (last accessed March 3, 2023).
- Coram, P., C. Ferguson, and R. Moroney. 2008. Internal audit, alternative internal audit structures and the level of misappropriation of assets fraud. *Accounting & Finance* 48 (4): 543–559.
- Deloitte. 2023. Almost Half of Executives Expect a Rise in Cyber Events Targeting Accounting and Financial Data in Year Ahead. Available at: <https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/almost-half-execs-expect-rise-in-cyber-events-targeting-accounting-and-financial-data.html> (last accessed March 3, 2023).
- Dzuranin, A. C., and I. Malaescu. 2016. The current state and future directions of IT audit: Challenges and opportunities. *Journal of Information Systems* 30 (1): 7–20.
- European Confederation of Institutes of Internal Auditors (ECIIA) (2022): Risk in Focus 2023 – Hot topics for internal auditors. Available at: <https://www.iiia.org.uk/policy-and-research/research-reports/risk-in-focus> (last accessed March 3, 2023).

- Ege, M. S. (2015). Does internal audit function quality deter management misconduct? *The Accounting Review* 90 (2): 495–527.
- Eulerich, M. (2021). The new three lines model for structuring corporate governance – A critical discussion of similarities and differences. *Corporate Ownership & Control* 18 (2): 180–187.
- Eulerich, M., A. Masli, J. Pickerd, and D. A. Wood. 2022. The impact of audit technology on audit task outcomes: Evidence for technology-based audit techniques. *Contemporary Accounting Research* (forthcoming).
- Eulerich, M., N. Waddoups, M. Wagener, and D. A. Wood. 2023a. Development of a Framework of Key Internal Control and Governance Principles for Robotic Process Automation (RPA). Working Paper.
- Eulerich, M., N. Waddoups, M. Wagener, and D. A. Wood. 2023b. The dark side of robotic process automation (RPA): Understanding risks and challenges with RPA. Working Paper.
- Internal Audit Foundation and Crowe. 2018. *The future of cybersecurity in internal audit*. Available at: <https://www.crowe.com/-/media/Crowe/LLP/folio-pdf/The-Future-of-Cybersecurity-in-IA-RISK-18000-002A-update.pdf> (last accessed March 3, 2023).
- Institute of Internal Auditors (IIA). 2016. *Assessing cybersecurity risk: roles of the three lines of defense*. Available at: <https://global.theiia.org/standards-guidance/Member%20Documents/GTAG-Assessing-Cybersecurity-Risk.pdf> (last accessed March 3, 2023).
- Institute of Internal Auditors (IIA). 2017. International Standards for the Professional Practice of Internal Auditing. Available at: <https://www.theiia.org/globalassets/site/standards/mandatory-guidance/ippf/2017/ippf-standards-2017-english.pdf> (last accessed March 3, 2023).
- Institute of Internal Auditors (IIA). 2020a. *Global Technology Audit Guides (GTAG): Assessing Cybersecurity Risk*. Altamonte Springs, FL.
- Institute of Internal Auditors (IIA). 2020b. *The IIA's Three Lines Model*. Available at: <https://www.theiia.org/globalassets/site/about-us/advocacy/three-lines-model-updated.pdf> (last accessed March 3, 2023).
- Institute of Internal Auditors (IIA). 2022. *Global Technology Audit Guides (GTAG): Auditing cybersecurity operations: Prevention and detection*. Altamonte Springs, FL.
- Jiang, W., Legoria, J., Reichelt, K., and Walton, S. (2021). Firm Use of Cybersecurity Risk Disclosures. *Journal of Information Systems*, forthcoming.
- Kahyaoglu, S., and K. Çaliyurt. 2018. Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal* 33 (4): 360–76.

- Lin, S., M. Pizzini, M. Vargus, 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.
- No, W. G., M. A. Vasarhelyi. 2017. Cybersecurity and continuous assurance. *Journal of Emerging Technologies in Accounting* 14 (1): 1-12.
- Prawitt, D. F., J. L. Smith, and D. A. Wood. 2009. Internal audit quality and earnings management. *The Accounting Review* 84 (4): 1255–1280.
- Slapničar, S., T. Vuko, M. Čular, and M. Drašček. 2022. Effectiveness of cyber security assurance by internal auditors. *International Journal of Accounting Information Systems* 44: 100548.
- Slapničar, S., M. Axelsen, I. Bongiovanni, and D. Stockdale. 2022. *The pathway model to five lines of accountability in cybersecurity governance*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4176559 (last accessed March 3, 2023).
- Steinbart, P. J., R. L. Raschke, G. Gal, W. N. Dilla. 2012. The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems* 13 (3): 228-43.
- Steinbart, P. J., R. L. Raschke, G. Gal, W. N. Dilla. 2013. Information security professionals' perceptions about the relationship between the information security and internal audit functions. *Journal of Information Systems* 27 (2): 65-86.
- Steinbart, P. J., R. L. Raschke, G. Gal, W. N. Dilla. 2018. The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society* 71: 15-29.
- Walton, S., Wheeler, P. R., Zhang, Y., Zhao, X; An Integrative Review and Analysis of Cybersecurity Research: Current State and Future Directions. *Journal of Information Systems* 1 March 2021; 35 (1): 155–186. <https://doi.org/10.2308/ISYS-19-033>
- Wilkin, C. L., R. H. Chenhall. 2020. Information technology governance: Reflections on the past and future directions. *Journal of Information Systems* 34 (2): 257-92.
- World Economic Forum. 2022. *Global cybersecurity outlook 2022: Insight report*. Available at: <https://www.weforum.org/reports/global-cybersecurity-outlook-2022> (last accessed March 3, 2023).

Figure 1: Path analysis of IAF maturity's impact on cyber activities

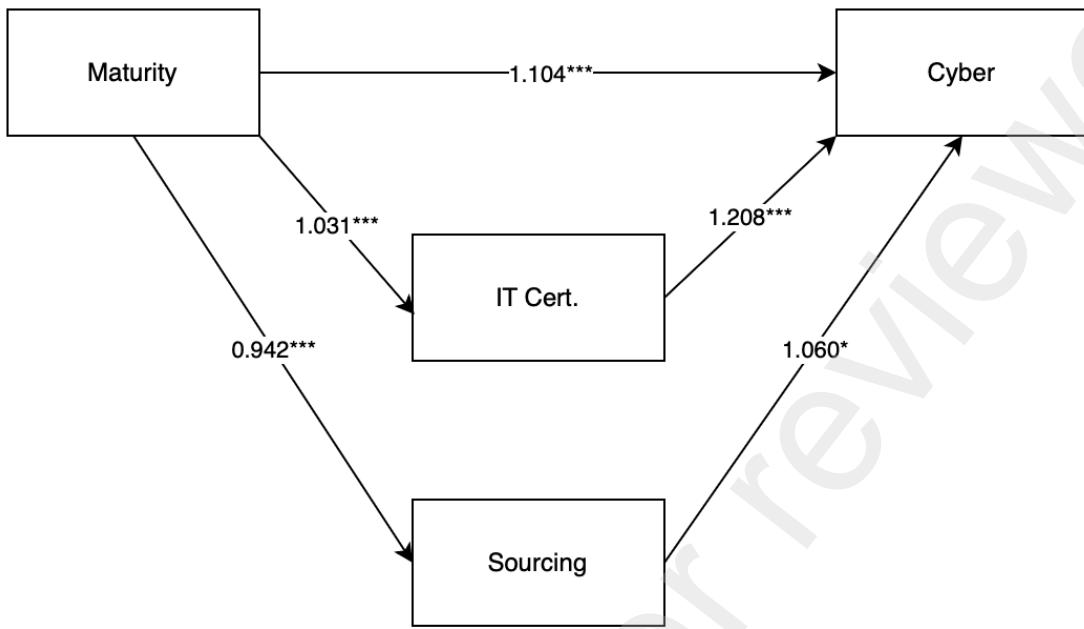


Figure 2: Path analysis of IAF maturity's impact on IT audit activities

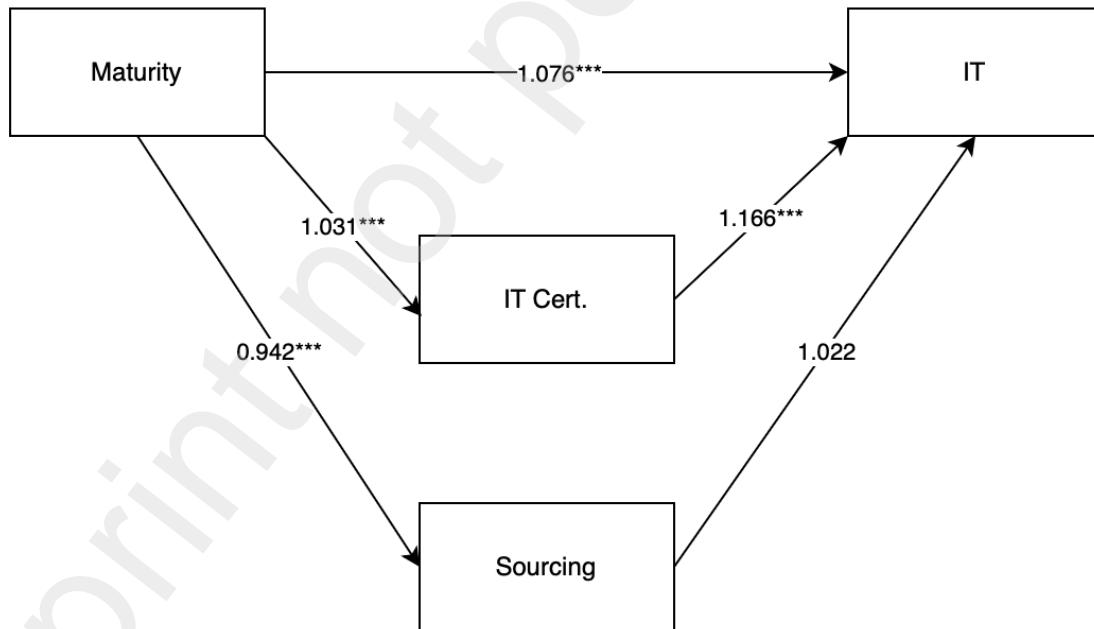


Figure 3: Path analysis of IAF maturity's impact on combined IT audit and cyber activities

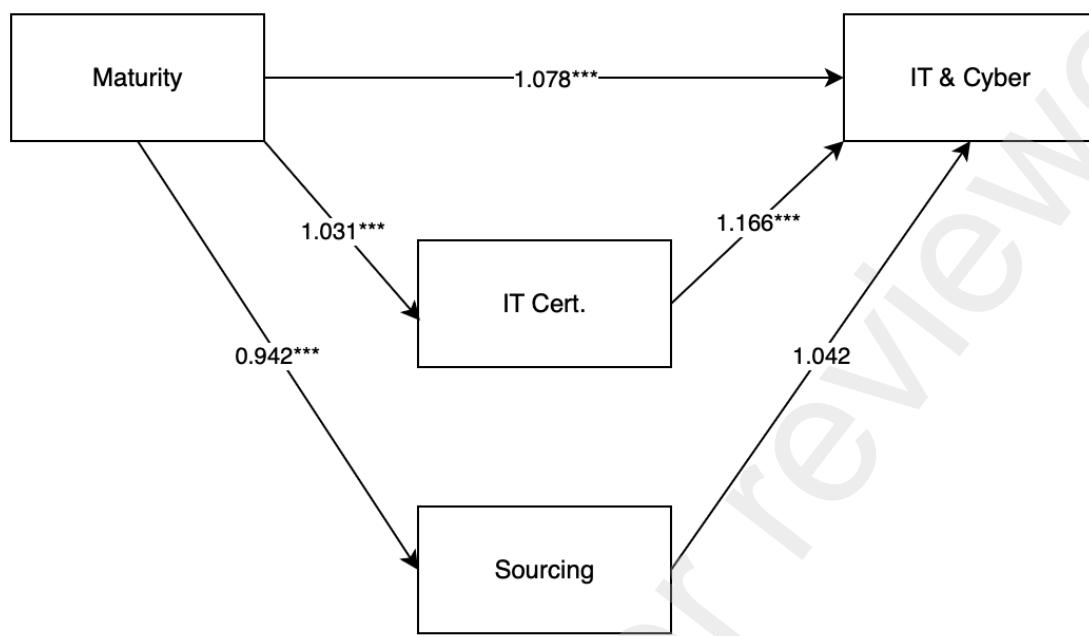


Table 1a: Descriptive Statistics (Sample)

	mean	sd	min	p25	p50	p75	max
Cyber	0.38	0.49	0.00	0.00	0.00	1.00	1.00
IT	0.38	0.49	0.00	0.00	0.00	1.00	1.00
CyberIT	0.25	0.43	0.00	0.00	0.00	1.00	1.00
Maturity	2.42	1.03	0.00	2.00	2.00	3.00	4.00
ITCert	0.17	0.37	0.00	0.00	0.00	0.00	1.00
Sourcing	0.27	0.44	0.00	0.00	0.00	1.00	1.00
AC	0.83	0.37	0.00	1.00	1.00	1.00	1.00
Funding	3.33	1.13	1.00	2.00	4.00	4.00	5.00
AdminRptMgmt	0.81	0.39	0.00	1.00	1.00	1.00	1.00
FuncRptBoard	0.74	0.44	0.00	0.00	1.00	1.00	1.00
Private	0.17	0.38	0.00	0.00	0.00	0.00	1.00
NonProfit	0.06	0.23	0.00	0.00	0.00	0.00	1.00
Government	0.25	0.44	0.00	0.00	0.00	1.00	1.00
OtherOrg	0.01	0.07	0.00	0.00	0.00	0.00	1.00
Observations	1142						

This table presents summary statistics for all dependent and independent variables used in regression analysis. All variables are defined in Appendix A.

Table 1b: Descriptive Statistics (Cross-Section Analyses)

		Cyber	IT	CyberIT
IA Maturity	low	0.28	0.31	0.18
	high	0.50	0.46	0.33
	diff	0.22***	0.15***	0.15***
IT Certification	no	0.35	0.35	0.23
	yes	0.55	0.52	0.40
	diff	0.20***	0.17***	0.17***
Sourcing	no	0.31	0.34	0.21
	yes	0.45	0.41	0.29
	diff	0.14***	0.07***	0.08***
Audit Committee	no	0.25	0.33	0.17
	yes	0.41	0.39	0.27
	diff	0.16***	0.06**	0.10***
Size	low	0.33	0.31	0.20
	high	0.47	0.49	0.34
	diff	0.14***	0.18***	0.14***
Funding	low	0.32	0.34	0.21
	high	0.44	0.42	0.30
	diff	0.12***	0.08***	0.09***
Functional Reporting	mgmt	0.29	0.32	0.20
	board	0.42	0.40	0.27
	diff	0.13***	0.08***	0.07***
Org Type	other	0.38	0.39	0.26
	public	0.39	0.37	0.24
	diff	0.01	-0.02	-0.02
North America	no	0.35	0.35	0.23
	yes	0.46	0.44	0.31
	diff	0.11***	0.09***	0.08***
Finance	no	0.36	0.35	0.23
	yes	0.44	0.46	0.32
	diff	0.08***	0.11***	0.09***

This table presents descriptive cross section analyses across ten different dimensions. All variables are defined in Appendix A. For size and maturity, high and low were determined by a mean split. For funding, high and low were determined by a split on whether survey respondents indicated the funding for their IAFs was mostly sufficient. The symbols ***, **, and * are used to denote statistical significance at the 1%, 5%, and 10% levels, respectively, for t-tests of means.

Table 2: Pearson (Bottom) and Spearman (Top) Correlations

Variables	Cyber	IT	CyberIT	Maturity	ITCert	Sourcing	AC
Cyber	1.000	0.327***	0.503***	0.194***	0.069**	0.034	0.090***
IT	0.453***	1.000	0.476***	0.164***	0.061**	0.029	0.056*
CyberIT	0.738***	0.742***	1.000	0.163***	0.096***	-0.007	0.028
Maturity	0.258***	0.195***	0.216***	1.000	0.016	-0.074**	0.107***
ITCert	0.151***	0.124***	0.146***	0.047	1.000	-0.026	0.011
Sourcing	0.090***	0.045	0.060**	-0.049*	0.016	1.000	0.038
AC	0.125***	0.050*	0.087***	0.132***	-0.002	0.023	1.000

This table presents the Pearson (bottom half) and Spearman (top half) correlations for all dependent variables and independent variables of interest used in regression analysis. We have excluded control variables for brevity. All variables are defined in Appendix A. The symbols ***, **, and * are used to denote statistical significance at the 1%, 5%, and 10% levels, respectively.

Table 3: Characteristics of IA Activity Involvement in Organizations' Cybersecurity and IT Efforts

	(1) Cyber	(2) IT	(3) CyberIT
<i>Variables of Interest</i>			
Maturity	1.700*** [6.077]	1.475*** [4.847]	1.676*** [5.240]
ITCert	2.541*** [4.646]	2.172*** [3.901]	2.325*** [3.972]
Sourcing	1.339* [1.773]	1.120 [0.635]	1.284 [1.340]
AC	1.831** [2.337]	1.087 [0.328]	1.461 [1.287]
<i>Control Variables</i>			
Funding	1.133* [1.779]	1.019 [0.266]	1.091 [1.131]
AdminRptMgmt	0.727 [-1.599]	0.676** [-1.964]	0.755 [-1.270]
FuncRptBoard	0.923 [-0.352]	0.873 [-0.623]	0.754 [-1.108]
Private	1.295 [1.007]	0.756 [-1.038]	1.029 [0.095]
NonProfit	0.658 [-1.045]	0.455* [-1.902]	0.560 [-1.235]
Government	0.368*** [-3.180]	1.012 [0.039]	0.680 [-1.113]
OtherOrg	1.554 [0.445]	0.626 [-0.301]	1.018 [0.013]
Constant	0.080*** [-4.789]	0.361** [-2.062]	0.065*** [-4.583]
Observations	1,057	1,044	1,004
Industry Fixed Effects	Y	Y	Y
Country Fixed Effects	Y	Y	Y
Pseudo R2	0.151	0.131	0.146

This table presents the results from estimating Eq. (1) using logistic regression with robust standard errors. All variables are defined in Appendix A. Coefficients represent odds ratios. Z-stats are presented below each coefficient. The symbols ***, **, and * are used to denote statistical significance at the 1%, 5%, and 10% levels, respectively.

Appendix: Variable Definitions

Variable	Measurement	Survey Question and Relevant Response(s)
<i>Cyber</i>	An indicator variable equal to one if a survey respondent indicated that their IA activity had significant involvement in the organization's cybersecurity efforts, and equal to zero otherwise.	
<i>IT</i>	An indicator variable equal to one if a survey respondent indicated that their IA activity had significant involvement in the organization's IT efforts, and equal to zero otherwise.	Please indicate the areas where your internal audit activity has a significant level of involvement. Select all that apply. <ul style="list-style-type: none"> • Cybersecurity • Information Technology (IT) (not covered in other choices)
<i>CyberIT</i>	An indicator variable equal to one if a survey respondent indicated that their IA activity had significant involvement in the organization's cybersecurity and IT efforts, and equal to zero otherwise.	
<i>Maturity</i>	A variable equal to zero, one, two, three, or four if a respondent answered that their IA activity had an initial, infrastructure, integrated, managed, or optimizing level of maturity per the IIA-Netherlands' Internal Audit Ambition Model, respectively.	Which of the following best describes the maturity of your organization's internal audit activity? <ul style="list-style-type: none"> • Level 1 – Initial: Functioning at an initial stage of development, with ad hoc or unstructured activity • Level 2 – Infrastructure: Developing administrative infrastructure, along with policies, processes, and procedures • Level 3 – Integrated: Integrated into the organization and generally conforms to The IIA's Standards • Level 4 – Managed: Well-managed with a visible role in the organization and a long-term vision and plan

		<ul style="list-style-type: none"> • Level 5 – Optimizing: Optimizing value with continuous improvement for both internal audit and the organization
<i>ITCert</i>	An indicator variable equal to one if a survey respondent indicated that they held an IT-related certification, and equal to zero otherwise.	Which of the following professional certifications and/or qualifications do you have? Select all that apply. <ul style="list-style-type: none"> • IT-related certification(s) / qualification(s) (includes information systems and security of information technology)
<i>Sourcing</i>	An indicator variable equal to one if a survey respondent indicated that their organization outsources or co-sources IA services greater than the sample mean, and equal to zero otherwise.	In a typical year, what percentage of internal audit services are outsourced or co-sourced?
<i>AC</i>	An indicator variable equal to one if a survey respondent indicated that their organization has an audit committee, and equal to zero otherwise.	Does your organization have an audit committee? <ul style="list-style-type: none"> • Yes • No
<i>Funding</i>	A variable equal to one, two, three, four, or five if the respondent indicated that funding for their IA activity is not sufficient, generally sufficient, somewhat sufficient, mostly sufficient, or completely sufficient, respectively.	In your opinion, in a normal year (disregarding pandemic factors), how sufficient is the funding for your internal audit activity? <ul style="list-style-type: none"> • Completely sufficient • Mostly sufficient • Somewhat sufficient • Generally insufficient • Not at all sufficient
<i>AdminRptMgmt</i>	An indicator variable equal to one if a survey respondent indicated that their IA activity reports administratively to a member of management, and equal to zero otherwise.	What is the primary administrative* reporting line for the chief audit executive (CAE) or head of internal audit in your organization?

FuncRptBoard

An indicator variable equal to one if a survey respondent indicated that their IA activity reports functionally to the audit committee or board, and equal to zero otherwise.

Private

An indicator variable equal to one if a survey respondent indicated that their organization is privately held, and equal to zero otherwise.

NonProfit

An indicator variable equal to one if a survey respondent indicated that their organization is a non-for-profit or nonprofit, and equal to zero otherwise.

- Chief executive officer (CEO), president, head of government agency
- Chief financial officer (CFO) or equivalent
- Chief compliance officer (CCO) or equivalent
- Chief operating officer (COO) or equivalent
- Chief risk officer (CRO) or equivalent
- Controller or financial director
- General or legal counsel

*Administrative reporting refers to oversight of day-to-day matters, expense approval, human resource administration, internal policies and procedures.

What is the primary functional* reporting line for the chief audit executive (CAE) or head of internal audit in your organization?

- Audit committee
- Board of directors, or equivalent

*Functional reporting refers to oversight of the responsibilities of the internal audit function, including approval of the internal audit charter, the audit plan, evaluation of the CAE, compensation for the CAE.

What kind of organization do you currently work for?

- Privately held organization (not listed, family-owned)
- Public sector (including federal/national, state/provincial, local/city, government-sponsored

<i>Government</i>	An indicator variable equal to one if a survey respondent indicated that their organization belongs to the public sector, and equal to zero otherwise.	enterprises, international or multinational organizations)
<i>OtherOrg</i>	An indicator variable equal to one if a survey respondent indicated that their organization is something other than public, privately held, public sector, or nonprofit, and equal to zero otherwise.	<ul style="list-style-type: none"> • Not-for-Profit/Nonprofit (NPO) or Nongovernmental Organization (NGO) • Other

This appendix defines the variables used in regression analysis and the survey questions from which they were derived. All survey data was obtained from the IIA's "Assessing Internal Audit Practices Globally" survey.
