The Sunk Costs of Cybersecurity Testing: Who Bears Responsibility?

Natalie Epp

James Pentikis

Saeed Roohani
Bryant University

This paper intends to bring further clarity regarding the role of the auditor when there is a consideration of a cybersecurity. It seems there is an expectation gap between what the public expects and what the auditor role is, and that cybersecurity testing requires additional skills and efforts. Are auditors currently compensated for the cybersecurity testing? Do they want the scope of the audit to expand to include cybersecurity assessment? Will this lack of clarity impact the corporate governance model that is based on transparency and monitoring? There is limited data available regarding cybersecurity audits and whether such audits lower the threat of cybersecurity. Our analysis suggests that auditors should not have direct responsibility for testing the cybersecurity of a client, rather direct testing should be accomplished by a third party, primarily an auditor specialist. Also, it is time to expect the auditor to become familiar with general cybersecurity skills and standards.

Keywords: auditor responsibility, cybersecurity audit, audit specialist, risk of cybersecurity, cybersecurity standards

INTRODUCTION

Tran Nguen and Tick (2021) examined the hypothesis that charging higher audit fees causes external auditors to place greater emphasis and focus on businesses that have experienced cybersecurity attacks. Utilizing a sample of 100 businesses of various sizes, the authors' study highlighted a positive correlation between audit fees and breaches. An implication of this study is that the authors' hypothesis was supported.

Perols (2019) utilizes a two-essay approach to examine this topic. The first essay analyzes investor perceptions based on non-compulsory disclosures of cybersecurity risk management evaluations (Perols, 2019). It also explores whether this impact differs when an ensuing cybersecurity event occurs. The second essay looks into the impact of the different forms of cybersecurity assurance services on the decisions and perceptions of investors. This also explores whether this impact varies when a preceding cybersecurity event is disclosed.

This first essay highlights that an investor's positive impression of an auditor's competence is reversed by a negative indicator of an ensuing cybersecurity event (Perols, 2019). This may increase investor sensitivity to potential impairments of independence when examinations about cybersecurity risk management are jointly provisioned. It also may lead to decreased impressions of the audit quality.

Additionally, when examinations associated with cybersecurity risk management are jointly provisioned, investors are less willing to invest in the company.

The second essay highlights the increased willingness of investors to invest in and have greater impressions of management's credibility when non-compulsory disclosures include cybersecurity risk management evaluations, as opposed to a less extensive assurance service associated with cybersecurity (Perols, 2019). Cybersecurity risk management examinations are perceived by investors to provide a higher level of assurance quality pertaining to the organization's ability to prevent and recover from harmful cybersecurity events. Regulators have raised this key issue associated with risk management.

Authoritative guidance surrounding this topic is highlighted through the cybersecurity auditing standards (ISO/IEC 27007:2020) which the International Organization for Standardization has promulgated, the AICPA's Cybersecurity Risk Management Reporting Framework, and ISACA Standards, Guidelines, Tools and Techniques.

Researching the role of auditors in evaluating cybersecurity is important because it may be part of the profession's future. The topic of cybersecurity is becoming an ever more prominent issue in the business world, as we are seeing an increasing number of malicious incidents. There are certain areas of this issue that have been explored, especially an emphasis on the internal audit perspective and the effectiveness of assurance provided by internal auditors.

However, we are interested in researching the role of external auditors on this issue of cybersecurity. Although this topic has been previously investigated, we believe that our research will add to the literature and further support the debate on whether external auditors should be involved in cybersecurity testing. Additionally, this study contributes to the non-audit services literature regarding if cybersecurity testing should be treated like advisory services. We understand that there are inherent limitations of auditing and cybersecurity, but we wonder if there would be improvements if auditors provided opinions on their clients' cybersecurity. Management's perception of the auditor's opinions on the company's cybersecurity could encourage management to implement more preventative measures so cybersecurity would be improved.

In this paper, we discuss the implications and issues associated with whether to require external auditors to test companies' cybersecurity. We review the literature on standards and practices for evaluating United States companies' cybersecurity. In addition, we will review the current role of external auditors in this area. We also present comparisons and discuss the limitations of our research. Finally, we analyze the results and formulate our position.

Our research topic revolves around the question of who should be responsible for evaluating entities' cybersecurity (e.g., access and penetration tests performed regularly). The first question we consider is: Should auditors be responsible to test their clients for cybersecurity? Building on that question, we also consider the research question: If auditors are responsible for cybersecurity testing, should they charge additional fees?

We argue the two sides of the first question. The first side of this argument is that auditors should be responsible for evaluating clients' cybersecurity to a similar extent that they are responsible for evaluating internal controls since they should be able to adapt their auditing skills to this issue. Evaluating client cybersecurity should be included in the normal scope of an audit. Therefore, since auditors would be evaluating the cybersecurity, they should be obligated to express an opinion on client cybersecurity based on those findings.

Conversely, the other side of the argument would be that auditors should not be responsible for evaluating their clients' cybersecurity. Auditors are accountants and they are not qualified to effectively evaluate the technological aspects of cybersecurity because they lack competence in the area. Furthermore, there is an entirely different framework, the NIST Cybersecurity Framework, for evaluating cybersecurity that the auditor should not be required to know.

There are issues and implications related to both sides of the argument. If external auditors are required to evaluate their clients' cybersecurity, several issues come with implications. This addition of testing increases the scope of the audit and the required knowledge of the auditors. These issues cause a debate on whether audit fees should be increased due to the additional work. Additionally, the auditor's inherent limitations regarding cybersecurity would make this strategy more difficult and time-consuming.

Conversely, new issues arise if external auditors are not required to perform testing on companies' cybersecurity. There would be a question of who is responsible for testing cybersecurity if the evaluation does not fall in the scope of the external audit. Investors may be weary or even at risk if companies are not properly evaluated for cybersecurity.

The rest of our paper is structured as follows: in Section 2, we review the literature on standards and practices for testing cybersecurity and the current role of external auditors in this area. Section 3 presents the issues and implications related to the first side of the argument that external auditors should be required to test for cybersecurity. Section 4 presents the issues and implications of the opposing argument. Finally, we conclude the paper in Section 5 by providing our research-based opinion.

Literature Review

Prior Literature

According to Wertheim (2019), external auditors should be responsible for testing and understanding the cybersecurity risks of their clients. Wertheim's study focuses on governments as audit clients instead of privately held companies. Because governmental information can be sensitive, government entities must have strong cybersecurity practices. However, many governments do not have the knowledge or resources to test and strengthen their cybersecurity. Furthermore, because the external auditors are responsible for assessing risk, cybersecurity risks should be included in those assessments. This would ensure that the external auditors adequately understand their clients' risks. Additionally, the external auditors could apply their risk assessing strategies to cybersecurity.

Tran Nguen and Tick (2021) argue that external auditors should evaluate their clients for cybersecurity risks. However, the external auditors should be able to charge their clients audit fees for the additional testing services, instead of this testing just being included in the normal risk assessment portion of the audit. Cybersecurity risk assessment would expand the scope of the audit, which should lead to increased audit fees. The increase in audit fees may have an impact on the quality of the audit testing since the auditors may be more motivated to perform the additional work.

Perols (2019) finds that, when external auditors are responsible for cybersecurity testing, investors have lower perceptions of audit quality if cybersecurity testing is included in the normal scope of the audit. This may be because investors think auditors cut corners on parts of the audit when they have the added responsibility of cybersecurity testing. Auditors could be motivated to cut corners if they feel they are not being properly compensated for the additional effort required. Perols' findings seem to support Tran Nguen and Tick's viewpoint that cybersecurity testing should be an additional non-audit service external auditors perform. Separating cybersecurity testing from financial statement audits may improve investor confidence through better perceptions of the audit quality.

According to Lanz (2014), the audit committee should be responsible for managing and responding to cybersecurity breaches of the company. Therefore, external auditors are not responsible for testing for cybersecurity. Lanz argues this because the company is required to make disclosures about how the accounting information systems function and how cybersecurity breaches impact the financials. Since managing cybersecurity risk is similar to managing strategic risk, this is considered an internal issue to be managed by internal roles. However, Lanz notes that internal and external CPAs should be prepared to help the audit committee test and manage cybersecurity. This is based on the idea that CPAs should be able to adapt audit testing strategies to cybersecurity testing.

Authoritative and Nonauthoritative Guidance

The International Organization for Standardization promulgates standards used by professionals in various fields and industries. Multiple ISO standards apply to auditing management and information security management systems. ISO 19011:2018 provides guidelines for auditing management systems including managing an audit program and conducting management system audits, as well as evaluating the results from an audit. ISO/IEC 27007:2020 expands upon ISO 19011:2018, focuses on information security, cybersecurity and privacy protection, and provides guidelines for auditing information security

management systems. ISO/IEC 27007:2020 was authored closely with the International Electrotechnical Commission (IEC).

The Information Systems Audit and Control Association (ISACA) has promulgated standards that apply specifically to information technology (IT) audit and assurance which address the specialized nature of IT audit and assurance and the skills necessary to perform such engagements. These standards guide performing and reporting audits of IT. Certified Information Systems Auditor utilizes these standards when conducting audits and other assurance services associated with IT. The American Institute of Certified Public Accountants has published the Cybersecurity

Risk Management Reporting Framework. This Framework is utilized by organizations to aid in communication of relevant and useful information about the effectiveness of their cybersecurity risk management programs.

The Center for Audit Quality has published non-authoritative guidance regarding audit procedures related to cybersecurity that are performed in the audit of financial statements and internal control over financial reporting (ICFR). As part of the auditing process, auditors must develop an understanding of how their clients utilize information technology (IT) within their operations and the impact of these IT systems on the client's financial statements.

Expectations of Authoritative Sources

The following table summarizes the expectations of each applicable authoritative source. The following sources can be applied to either side of the argument. If external auditors included cybersecurity in ICFR audits, they would have to apply these standards to their practices. However, the sources are currently used by specific parties.

TABLE 1

Source:	**Provides Guidelines for/Assists with:**	**Current User of Standards:**
ISO/IEC	-auditing management systems -managing an audit program -evaluating the results from an audit	Third Party
ISACA	-performing and reporting audits of IT	Third Party Does not govern CPAs
AICPA	-utilized by organizations to aid in communication of relevant and useful information pertaining to the effectiveness of the organization's cybersecurity risk management programs	Both, External Auditor and Third Party

Argument 1: External Auditors Should Be Responsible for Cybersecurity Testing

With cyber-attacks on the rise, it is increasingly important for companies to ensure they have functional cybersecurity systems to protect their data. In order to ensure that these systems are effective, companies must undergo cybersecurity testing. However, this begs the question of who is responsible for this testing. The first side we argue is that external auditors should be responsible for the cybersecurity testing of their clients. This idea is based on a variety of factors.

External auditors are hired by clients to review and provide an opinion on the fair presentation of their financial reports. For public companies and governments, auditors are also required to provide an opinion on their clients' internal controls (IC) as part of the integrated ICFR audits. The integrated audits are optional for other non-public companies. Regardless of which type of audit, a key step in the planning phase of the audit process is assessing risks.

Because of this, auditors already have processes and strategies they need to assess risks and evaluate internal controls.

According to the Committee of Sponsoring Organizations of the Treadway Commission (COSO), risk assessment is one of the main components of internal controls. Furthermore, COSO has a pamphlet "Managing Cyber Risk in a Digital Age" that essentially states that cyber risk should be included as part of the normal risks. Cybersecurity is all but officially considered an internal control, so it should be treated as such. Therefore, cybersecurity should be included when external auditors assess their clients' risks and internal controls.

Cybersecurity should be considered another internal control of companies that auditors must evaluate during ICFR audits. Although auditors are not IT specialists, they are still required to develop an understanding of their clients' IT to be able to properly evaluate controls. Learning about their clients' cybersecurity could be part of this audit process of gaining understanding of clients' systems. Auditors should be able to adapt their internal control testing skills and strategies to evaluate cybersecurity. Even Lanz (2014), who opposes cybersecurity testing performed by external auditors, admits that CPAs know how to perform testing and can adapt their strategies despite not being IT specialists. As previously explained, Wertheim (2019) also shares the idea that cybersecurity is another internal control risk that external auditors can and should assess. Cybersecurity should be added to the regular evaluation process of ICFR audits because cybersecurity is an internal control.

However, including cybersecurity as an internal control that auditors must assess increases the normal scope of the audit; perhaps a potential reason for current increase in audit fees. Adding the evaluation of clients' cybersecurity increases the auditors' workload and increases the audit's difficulty and time consumption. As previously mentioned, Perols (2019) found that including cybersecurity in the scope of the audit decreased investor perceptions of audit quality. The investors believed the additional work could lead to auditors cutting corners in other places if they were not compensated for doing more work.

Interestingly enough, a simple solution to this potential issue is to increase audit fees. Tran Nguen and Tick (2021) found that auditors perform higher quality work with increased audit fees. Frankly, many accountants join the field because of monetary motivation. Therefore, this solution is logical and is successful.

Unfortunately, audit clients may not initially be pleased with the increased audit fees, but auditor cybersecurity testing could save them much more money in the long run. Audit fees are normally just a small percentage of the client's revenue. Conversely, a single cyber attack usually costs between 50,000 and 500,000 U.S. dollars (Petrosyan, 2022). Additionally, public companies' stock value drops around 8.6% after a cyber breach (Bischoff). With around 2,220 cyber attacks daily (Fox), the potential loss from not having auditors evaluate

cybersecurity could easily outweigh the cost of additional audit fees. Therefore, companies should accept the additional audit fees that come with their auditors, including cybersecurity testing in the scope of ICFR audits.

Implications

The following table summarizes the implications of the first argument that external auditors should be responsible for cybersecurity testing.

TABLE 2
PROS AND CONS OF FIRST ARGUMENT

Pros	Cons
Auditors can adapt existing testing strategies	Auditors are not IT specialists
Cybersecurity testing can be included in normal scope of the audit	Increases scope of the audit
Increased fees motivate improved audit performance	Increases audit fees

Argument 2: External Auditors Are Not Responsible for Cybersecurity Testing

The second side we argue is that external auditors are not responsible for the cybersecurity testing of their clients. Ultimately, the responsibility of testing cybersecurity lies on management and not the auditor, this is comparable to internal controls where management, not the auditor, is responsible for testing. About both cybersecurity and internal control testing, the role of the auditor is to evaluate management's assertions. It is important to note that auditors are not cybersecurity professionals and although internal controls must be understood and evaluated in an ICFR audit, this is only a single piece of the cybersecurity in a company.

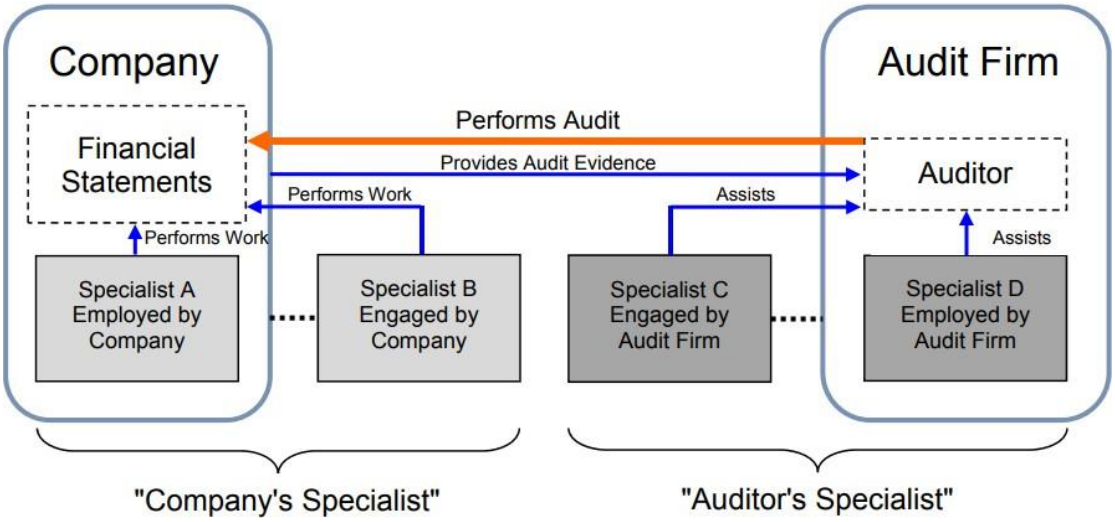
Adding cybersecurity testing to an ICFR audit expands the scope of the audit, meaning more resources must be utilized to complete the audit before the filing deadline. However, adding additional resources is not always possible as accounting firms are having difficulty attracting and retaining talent that would be utilized for staff engagements. Even if new associates cannot be hired, audits still must occur, meaning the existing engagement teams must take on the additional work. The amount of work to be completed does change even if engagement team members leave. Expanding the scope of an ICFR audit to include cybersecurity testing strains auditors even more due to the increased workload. According to RBT CPAs, "at the majority of accounting firms, it is not uncommon for an accountant's work schedule to go from 45-50 hours per week up to 65-70 hours (or more) per week [during busy season]" (RBT CPAs, 2020). Auditors already work long hours with their existing workloads, and with the addition of cybersecurity testing this adds additional strain and has the potential to have detrimental effects on the profession as the current working trends have pushed people to leave the profession altogether. This impacts the staffing levels on engagements, meaning there are less people to do more work.

ISACA, which previously was known as the Information Systems Audit and Control Association, "is an independent, nonprofit, global association that engages in the development, adoption and use of globally accepted information system (IS) knowledge and practices" (Tech Target, 2013). ISACA is integral in this area as it "provides guidance, benchmarks and governance tools for enterprises that use information systems" (Tech Target, 2013). ISACA currently offers multiple certifications and credentialing programs, which include Certified Information Systems Auditor (CISA), Certification in Risk and Information Systems Control (CRISC), Certified Information Security Manager (CISM), IT Risk Fundamentals Certificate, IT Audit Fundamentals Certificate, Cybersecurity Audit Certificate, and Certificate of Cloud Auditing Knowledge (ISACA, 2023). Professionals who hold these credentials and certifications are better suited to conduct audits of cybersecurity as they hold the competencies needed to holistically understand this area. These professionals also can better handle the ever-evolving issues and problems surrounding cybersecurity.

With external auditors not being responsible for cybersecurity testing this allows them to focus on their core competencies. However, this does not mean that auditors cannot utilize the results of the cybersecurity testing by a third-party professional. Additionally, the public perceives quality associated with the work of auditors and public accounting firms. Although cybersecurity professionals and auditors are professionally qualified and competent to complete their jobs, their roles, responsibilities, and quality of work are not as well known to the general public as auditors are. This lack of understanding by the general public can negatively impact the perception of the quality of work conducted by these professionals. If a company still wants its cybersecurity to be tested, it would have to utilize an external third party or if the firm offers these services in a different practice such as risk assurance if they are wary of the quality of work produced by the external third party. However, if the company wants the auditor to complete the testing this can be achieved through the auditor utilizing a specialist. Per the Public Company Accounting Oversight Board's (PCAOB) 2018 release of Amendments to Auditing Standards for Auditors Use of the Work of Specialists. Page 13 of the release, *Figure 2: Potential Ways Auditors Use Specialists in an Audit* highlights the different types of specialists (PCAOB, 2018, p.13). In the figure below, Specialist C, who is engaged by the audit firm, and Specialist D, who the audit firm employs are considered Auditor's Specialist (PCAOB, 2018, p.13). An auditor could engage a third party, such as a cybersecurity professional to conduct the testing and Figure 2, this would be a Specialist C. Similarly, an audit firm could employ professionals who work in another area of the firm to conduct the testing, per figure 2, these professionals would be considered

Specialist D. Upon completion of the testing by the specialist, an auditor would then subsequently review the work of this professional which would help ensure quality. Although the auditor would still have to assume responsibility for the professional, this would relieve the auditor of having a responsibility to conduct the actual testing. The perception of the quality of work by the general public would likely not be impaired as the general public would perceive the work to have been completed by the auditor rather than the third party.

FIGURE 1
POTENTIAL WAYS AUDITORS USE SPECIALISTS IN AN AUDIT



(PCAOB, 2018, p.13).

Auditors should not have direct responsibility for testing the cybersecurity of a client, rather the direct testing should be accomplished by a third party, primarily an auditor's specialist. In recent years, accounting firms have been finding it difficult to attract and retain talent, this talent is utilized to staff engagements. Holding the auditor responsible for cybersecurity testing as well would further the already intense workloads and long hours worked. Additionally, this area does not align with the core competencies of an auditor. Cybersecurity professionals such as Certified Information Systems Auditor (CISA) and other individuals holding IT Audit Fundamentals Certificate, Cybersecurity Audit Certificate, and Certificate of Cloud Auditing Knowledge (ISACA, 2023) who specialize in conducting cybersecurity audits have the core competencies to complete audits in this area.

IMPLICATIONS

The following table summarizes the implications of the second argument that external auditors are not responsible and that cybersecurity testing should be performed by an alternative third party.

TABLE 3
PROS AND CONS OF SECOND ARGUMENT

Pros	Cons
Cybersecurity professionals have more knowledge of cybersecurity and its intricacies compared to auditors	Decreased perception in the quality of work done by the third party
Helps prevent increases to an already extensive workload	Company must seek out an additional third party
IT professionals are better able to handle the ever evolving issues and problems	
Allow auditors to focus on core competencies	

CONCLUSION

Comparing Both Arguments

The following table summarizes the advantages of each argument.

TABLE 4
SUMMARIZING ADVANTAGES EACH ARGUMENT

External Auditor	Alternative Third Party
Auditors can adapt existing testing strategies	Cybersecurity professionals have more knowledge of cybersecurity and its intricacies compared to auditors
Cybersecurity testing can be included in normal scope of the audit	Helps prevent increases to an already extensive workload
Increased fees motivate improved audit performance	IT professionals are better able to handle the ever evolving issues and problems
	Allow auditors to focus on core competencies

LIMITATIONS

Our research paper has certain limitations. We could not base our ideas on actual data because of availability issues. Not much data exists about this topic because of the lack of cybersecurity audits. If we had access to data, it would have been interesting to compare the opinion of cybersecurity evaluators to how the companies withstood cyber-attacks. However, our paper is more theoretical and based on prior research and our own theories.

IMPLICATIONS AND RECOMMENDATIONS

Ideas presented in this paper can be utilized to further research in this topic. This topic can be furthered through factoring in the implications of continuous reporting. While continuous reporting is not applicable nor feasible in all areas of a company, cybersecurity is an area that heavily relies on real time information which must be acted on swiftly to mitigate damage, thus making continuous reporting applicable and feasible in this area. Additionally, continuous reporting would play a key role within cybersecurity testing as it allows professionals conducting the testing to see if any “holes” exist within the cybersecurity environment based on the information they receive. While external auditors are qualified to conduct audits and testing by utilizing professional judgment and oversight, they are not the most qualified professionals to conduct testing of cybersecurity. The testing responsibility likely will fall on IT professionals who exhibit competencies with this area. The frequency of cybersecurity testing would be determined by a professional

who is engaged to conduct the testing. Companies that present increased cybersecurity risk may need to test on a quarterly or even monthly basis, while companies that present a decreased level of cybersecurity risk may only need to test annually. This is where continuous reporting plays a key role. The professional testing cybersecurity of a company could utilize many forms of simulated cyber-attacks or even partner with a social engineer to test the system. Continuous reporting would provide real time feedback to the professionals where suggestions would then be made to mitigate risks.

Based on the ideas presented, we conclude that cybersecurity testing should be performed by alternative third parties instead of external auditors. Auditors are not IT specialists, so they should not be responsible for one. However, auditors have evaluation strategies that can be somewhat adapted to cybersecurity testing, IT and cybersecurity are not their core competencies. Even with increased audit fees, auditors do not want the scope of audits to increase to include evaluating areas they are not knowledgeable about. Companies truly concerned about cybersecurity should want an IT specialist who is more knowledgeable and qualified about cybersecurity to be the ones responsible for evaluating it. These specialists would better certify the company is protected from cyber-attacks. In a world riddled with cybercrime, we should leave the cybersecurity testing to IT specialists, not accountants.

REFERENCES

AICPA. (2017, November). *Overview of cybersecurity risk management reporting framework*. Retrieved from https://cybersecuritysummit.com/wp-content/uploads/2017/11/AICPA.pdf

Bischoff, P. (2021, February 9). *How data breaches affect stock market share prices.* Comparitech. Retrieved from https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/

Center for Audit Quality. (2019, March). *Understanding cybersecurity and the external audit.* Retrieved from https://www.thecaq.org/wp-content/uploads/2019/03/cybersecurity_and_external_audit_final.pdf

Chimwanda, E. (2022, April 8). *Essentials for an effective cybersecurity audit*. ISACA. Retrieved from https://www.isaca.org/resources/news-and-trends/industry-news/2022/essentials-for-an-effective-cybersecurity-audit

Deloitte & Touche LLP, E. Galligan, M., Herrygers, S., & Rau, K. (2019, November). *Managing cybersecurity risk in a digital age.* COSO. Retrieved from https://www.coso.org/Shared%20Documents/COSO-Deloitte-Managing-Cyber-Risk-in- a-Digital-Age.pdf

Fox, J. (2022, December 27). *Top cybersecurity statistics to know for 2023.* Cobalt. Retrieved from https://www.cobalt.io/blog/cybersecurity-statistics-2023#:~:text=How%20many%20people%20get%20hacked,over%20800%2C000%20attacks%20each%20year

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal, 34*(7), 808–834. https://doi.org/10.1108/MAJ-09-2018-2004

International Organization for Standardization, & International Electrotechnical Commission. (2020). *Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing* (ISO/IEC 27007:2020). Retrieved from https://www.iso.org/home.html

International Organization for Standardization. (2018). *Guidelines for auditing management systems* (ISO 19011:2018). ISO. Retrieved from https://www.iso.org/home.html

ISACA. (2023). *Credentialing.* Retrieved from https://www.isaca.org/credentialing

Lanz, J. (2014). Cybersecurity governance: The role of the audit committee and the CPA: Certified public accountant. *The CPA Journal, 84*(11), 6–10. Retrieved from http://bryant.idm.oclc.org/login?url=https://www.proquest.com/scholarly-journals/cybersecurity-governance-role-audit-committee-cpa/docview/1656058898/se-2

Perols, R.R. (2019). *Two essays on the impact of cybersecurity risk management examinations on investor perceptions and decisions* (Order No. 13814758). Accounting, Tax & Banking Collection. (2246444889). Retrieved from http://bryant.idm.oclc.org/login?url=https://www.proquest.com/dissertations-theses/two-essays-on-impact-cybersecurity-risk/docview/2246444889/se-2

Petrosyan, A. (2022, October 13). *Financial loss of cyber attacks on U.S. companies 2022*. Statista. Retrieved from https://www.statista.com/statistics/1334399/us-common-results-of-cyber-attacks/#:~:text=According%20to%20a%202022%20report,50%2C000%20and%2099%2C999%20U.S.%20dollars

Public Company Accounting Oversight Board (PCAOB). (2018, December 20). *PCAOB Release No. 2018-006: Amendments to Auditing Standards for Auditor's Use of the Work of Specialists*. Retrieved from https://pcaobus.org/Rulemaking/Docket044/2018-006-specialists-final-rule.pdf

RBT CPAs. (2020). *Hours, hours, and less hours.* Retrieved from https://www.rbtcpas.com/articles/hours-hours-and-less-hours/

Tech Target. (2013). *ISACA.* Retrieved from https://www.techtarget.com/searchcio/definition/ISACA#:~:text=ISACA%20is%20an%20independent%2C%20nonprofit,goes%20by%20its%20acronym%20only

Tran Nguen, B.N., & Tick, A. (2021). Cyber-security risks assessment by external auditors. *Interdisciplinary Description of Complex Systems, 19*(3), 375–390. https://doi.org/10.7906/indecs.19.3.3

Wertheim, S. (2019). Auditing for cybersecurity risk: Certified public accountant. *The CPA Journal, 89*(6), 68–71. Retrieved from http://bryant.idm.oclc.org/login?url=https://www.proquest.com/scholarly-journals/auditing-cybersecurity-risk/docview/2239577276/se-2