CURRENT ISSUES IN AUDITING
Vol. 13, No. 1
Spring 2019
pp. C1–C9

American Accounting Association
DOI: 10.2308/ciia-52338

COMMENTARY

Comments of the Auditing Standards Committee of the Auditing Section of the American Accounting Association on International Auditing and Assurance Standards Board Exposure Draft, Proposed International Standard on Auditing 315 (Revised): *Identifying and Assessing the Risks of Material Misstatement* and Proposed Consequential and Conforming Amendments to Other ISAs

Participating Committee Members:

Veena Looknanan Brown, Paul J. Coram, Sean A. Dennis, Denise Dickins (chair), Christine E. Earley, Julia L. Higgs, Tammie J. Schaefer, Kay W. Tatum

SUMMARY: On July 16, 2018, the International Auditing and Assurance Standards Board (the Board or IAASB) issued a request for comment on its Exposure Draft, Proposed International Standard on Auditing 315 (Revised): *Identifying and Assessing the Risks of Material Misstatement* and Proposed Consequential and Conforming Amendments to Other ISAs (ED-315). Major enhancements proposed include explicit recognition of the auditor's use of automated tools and techniques, requiring an understanding of an auditee's use of information technology relevant to financial reporting, acknowledging the influence of an entity's complexity on the audit plan, and

---

The views expressed in this letter are those of the contributing members of the Committee and do not reflect an official position of the American Accounting Association. Although the comments reflect the consensus view of the Committee, they do not necessarily reflect the views of every member.

Editor's note: Accepted by Lisa Milici Gaynor.

Submitted: November 2018
Accepted: December 2018
Published Online: December 2018

increasing the emphasis on the need for professional skepticism. The comment period ended on November 2, 2018. This commentary summarizes the participating committee members' views on selected questions posed by the IAASB.

Data Availability: ED-315, including questions for respondents, is available at: https://www.ifac.org/publications-resources/exposure-draft-isa-315-revised-identifying-and-assessing-risks-material.

I. OVERALL COMMENTARY

We commend the Board on its actions to improve audit quality, which have resulted in the publication of ED-315 (including Application and Explanatory Material—AEM). Major enhancements proposed include explicit recognition of the auditor's use of automated tools and techniques, requiring an understanding of an auditee's use of information technology (IT) relevant to financial reporting, acknowledging the influence of an entity's complexity on the audit plan, and increasing the emphasis on the need for professional skepticism.

We believe the proposed enhancements substantially achieve the Board's intent, however, we have one overarching concern. As proposed, ISA 315 will be comprised of an Introduction, Specific Requirements, AEM, Appendices, and what appear to be separate Flowcharts. In preparing our responses to the questions posed by the Board, we individually had difficulty locating all applicable discussions and materials. Although accountability and knowledge have jointly been found to moderate the negative impacts of task complexity on auditors' performance (Tan and Kao 1999; Tan, Ng, and Mak 2002), to the extent possible, steps should be taken to reduce the volume and complexity of ISA 315. Our Question-specific Commentary provides a few suggestions to achieve this objective.

II. QUESTION-SPECIFIC COMMENTARY

Question 3: Do respondents agree with the approach taken to enhance ED-315 in relation to automated tools and techniques, including data analytics, through the use of examples to illustrate how these are used in an audit? Are there other areas within ED-315 where further guidance is needed in relation to automated tools and techniques, and what is the nature of the necessary guidance?

ED-315 elevates the importance of automated tools and techniques, including data analytics, by describing how they might be applied in performing risk assessment (among others, paragraphs A15, A18, A33, and A48). We support the "automated tools and techniques" terminology intended to clarify and make uniform the concept of Big Data and related ideas. Since research suggests there is confusion in the definition and use of the terms Big Data, business intelligence, business analytics, and data analytics (Vasarhelyi, Kogan, and Tuttle 2015; Appelbaum, Kogan, and Vasarhelyi 2017), we suggest "automated tools and techniques" be formally defined in ISA 315.

If this suggestion is adopted, we recommend that descriptions of applying automated tools and techniques be consistent throughout ED-315. For example, paragraph A15 says, "...through the use of technology, the auditor may perform procedures on large volumes of data..." We recommend this language be changed to, "...using automated tools and techniques, the auditor may perform procedures on large volumes of data..." Additionally, paragraph A33 states, "Analytical procedures can be performed using a number of tools or techniques, which may be automated. Applying automated analytical procedures to the data may be referred to as data

analytics." We suggest: "Analytical procedures can be performed using automated tools and techniques."

We also support the inclusion of example applications of automated tools and techniques. Beyond the generic examples included in ED-315 (e.g., recalculations, reperformance, reconciliations) and ability to examine 100 percent of the transactions in a population (paragraphs A155, A175, A213), it might be helpful to describe more explicitly how auditors might use automated tools and techniques to perform analytical procedures (e.g., trend analysis and ratio analysis) or search for outlier transactions. ISA 520—*Analytical Procedures* includes an example of how data analytics might be used to test rental income (¶A8), and Appelbaum, Kogan, and Vasarhelyi (2018) provide other examples of how data analytics might be incorporated into the audit process. These examples could be described or referenced in the AEM.

Automated tools and techniques may present both opportunities and obstacles for the audit. As described by Cao, Chychyla, and Stewart (2015), implementing Big Data analytics is not a trivial endeavor; it requires individuals with expertise in data analytics, as well as appropriate hardware and software resources. Relevant skills and human resource needs may constrain rather than facilitate Big Data usage by auditors (Alles 2015). Brown-Liburd, Issa, and Lombardi (2015) suggest that "more academic research is necessary to fully comprehend the effects of moving away from more traditional audit processes to fully leverage the benefits of Big Data and how the use of more advanced data analytics will impact auditor judgment." Based on the rationale that automated tools and techniques may not be available to all auditors or that, in the auditor's professional judgment, they may not be appropriate or necessary in the circumstances, ED-315 does not require auditors to use automated tools and techniques. We support this position.

Since audit partners have expressed concern that professional skepticism and critical thinking may be adversely impacted by automation and standardization (Alles 2015; Boland, Daugherty, and Dickins 2018), we suggest including cautionary language that automated tools and techniques are not a substitute for professional skepticism or critical thinking.

Question 4: Do the proposals support the appropriate exercise of professional skepticism throughout the risk identification and assessment process? Do you support the proposed change for the auditor to obtain "sufficient appropriate audit evidence" through the performance of risk assessment procedures to provide the basis for the identification and assessment of the risks of material misstatement, and do you believe this clarification will further encourage professional skepticism?

The proposed changes increase the extent to which professional skepticism is mentioned, encouraged, and discussed as an engagement team. As an emphasis on skepticism has been shown to cause auditors to more effectively and efficiently identify risk factors and choose relevant audit testing procedures (Carpenter and Reimers 2013; Dennis and Johnstone 2018), this should improve the risk assessment process. Additionally, the changes intended to promote a deeper understanding of the entity, its use of IT, and its operating environment, should increase the knowledge auditors possess, which is a key input into making skeptical judgments (e.g., Hammersley 2011; Hurtt, Brown-Liburd, Earley, and Krishnamoorthy 2013; Nelson 2009). The explicit guidance provided in paragraph A5 should be helpful in assessing the risk of fraud associated with management's personality-driven fraudulent tendencies as auditors tend to have difficulty appropriately applying professional skepticism when assessing subjective components of fraudulent behavior (Cohen, Dalton, and Harp 2017).

Question 5: Do the proposals made related to the auditor's understanding of the entity's system of internal control assist with understanding the nature and extent of the work effort required and the relationship of the work effort to the identification and assessment of the risks of material misstatement? Specifically,

(a): Have the requirements related to the auditor's understanding of each component of the entity's system of internal control been appropriately enhanced or clarified? Is it clear why the understanding is obtained and how this informs the risk identification and assessment process?

ED-315 adds a significant amount to the requirements for evaluating components of an entity's system of internal control, increases clarity in evaluating controls, and provides guidance in the evaluation of controls, all of which will be useful to the auditor in understanding and evaluating an entity's system of internal control relevant to financial reporting. The guidance is also useful in applying an approach consistent with the Committee of Sponsoring Organizations of the Treadway Commission's *Internal Control—Integrated Framework* (COSO 2013) as it highlights the importance of management's integrity, ethical values, and operating philosophy (i.e., the control environment).

(b): Have the requirements related to the auditor's identification of controls relevant to the audit been appropriately enhanced and clarified? Is it clear how controls relevant to the audit are identified, particularly for audits of smaller and less complex entities?

ED-315, paragraphs 39–40 clearly inform the auditor on how to determine controls relevant to the audit. The amendments and explanations are important as extant research results and inspection reports of the Public Company Accounting Oversight Board (PCAOB) show that auditors tend to fall short of understanding the internal control process well enough to fully identify and assess where controls are missing (Brazel and Agoglia 2007; Bierstaker and Thibodeau 2006; PCAOB 2009, 2012, 2013). ED-315 describes various ways to determine relevant controls which is important as controls may differ between smaller, less complex audits and larger, more complex engagements. In some cases, the AEM could be written more clearly and succinctly. For example, the 3rd sentence of paragraph A166 states, "controls are required to be relevant to the audit. . ." It is clearer and more succinct to say, "controls are relevant to the audit. . ."—which is also consistent with the language used throughout this section of ED-315.

Extant research and the PCAOB have documented concerns about the quality of integrated audits (i.e., how well auditors integrate the audits of internal controls and the financial statements–PCAOB 2012; 2013; Rice and Weber 2012). However, research on how auditors identify controls relevant to an audit is scant. Although it is unclear how successful the proposed revisions will be in practice, the amendments and guidance are needed as studies show that an auditor's inability to properly identify and assess internal controls during an integrated audit is associated with lower financial statement quality (Bhaskar, Schroeder, and Shepardson 2019).

(c): Do you support the introduction of the new IT-related concepts and definitions? Are the enhanced requirements and application material related to the auditor's understanding of the IT environment, the identification of the risks arising from IT and the identification of general IT controls sufficient to support the auditor's consideration of the effects of the entity's use of IT on the identification and assessment of the risks of material misstatement?

We believe the introduction of new IT-related concepts and definitions will improve the quality and relevance of audits. Academic research consistently shows the importance of strong IT controls in the achievement of organizational objectives. For example, Klamm and Watson (2009) suggest that weak IT controls have a pervasive negative impact on a company's financial reporting process. Correspondingly, Stoel and Muhanna (2011) find that companies reporting IT-related internal control weaknesses report lower earnings and have lower earnings multiples than companies that do not report these weaknesses. Other research suggests that the effects of strong versus weak IT controls extend to management forecasts (e.g., Dorantes, Li, Peters, and Richardson 2013; Li, Peters, Richardson, and Watson 2012).

While we generally believe that the enhanced requirements proposed by ED-315 will support the auditor's consideration of IT in assessing risks of material misstatement, we think there is room to improve clarity. The guidance in paragraphs A144 through A150 and A180 through A193 (all of which are cross-referenced to ED-315 paragraph 35d) seems disorganized and lacks focus. Each of these paragraphs appears to address one or more specific topics; however, it is difficult to identify the specific topics without reading entire paragraphs. This may make the guidance difficult for auditors to use. We encourage the use of additional headings in this section of the AEM that better organize and more precisely identify the specific topics addressed within each paragraph. Clarity may also be enhanced by grouping portions of the AEM by topic rather than mapping chronologically to ED-315 paragraphs.

Relatedly, we encourage the use of cross-references within the AEM, when applicable. As one example, paragraph A181 appears to refer to criteria that paragraph A149 discusses in further detail. Without a reference to paragraph A149, the wording in paragraph A181 seems vague. Cross-references that identify other related guidance are likely to be highly useful to auditors.

Paragraphs A145 and A148 include lists of items for auditors to consider in identifying and assessing risks. While we find these lists to be instructive, auditors may end up using them as checklists in the field. Research suggests that such decision aids may have deleterious effects on auditors' performance (e.g., Pincus 1989; Hackenbrack 1992; Asare and Wright 2004; Hammersley 2011; Wood 2012; Dennis and Johnstone 2016; Boland et al. 2018). We encourage wording that more strongly encourages auditors to consider other potential risks/matters.

We also encourage specific discussion around the consideration of IT processes and risks that are centralized (e.g., system access and change management controls that are common across all a company's applications managed by a central IT group) versus those that are decentralized. When a company manages these IT process-related risks at the entity-level, should auditors identify these risks at the entity-level or at the specific application level (or both)? If auditors can identify IT process-related risks at the entity-level, would they still need to test these controls on every application that is relevant to the audit? Or is it acceptable for auditors to identify IT process-related risks at the entity level and test these entity-level controls using only a sample of applications relevant to the audit? We encourage the Board to provide guidance to address these potential situations.

Conspicuously absent in the requirements of ED-315 is the explicit consideration of cybersecurity which may directly impact data and process integrity and the risk of material misstatement. Cybersecurity has been on the agenda of the PCAOB's Standing Advisory Group (SAG) for some time, suggesting an expectation that the auditor has a role in considering cybersecurity in an audit (PCAOB 2018); and speaking at a meeting of the SAG in 2016, Chairman Schilder of the IAASB said, "We also have an innovation working group led by the IAASB Deputy Chair, Chuck Landes, where topics like corporate governance and cybersecurity are being explored at an early phase" IAASB (2016). Further, although an auditor does not yet appear to

have been named as a defendant, in 2017 the first four cybersecurity-related U.S. securities class action lawsuits were filed (PricewaterhouseCoopers 2018). Litigation increases risk to the auditor. These things underscore the importance of explicitly addressing cybersecurity risk in the ISA 315. In 2011, the Securities and Exchange Commission (SEC) issued guidance on how IT related incidents related to cybersecurity could result in a material misstatement (SEC 2011). At a minimum, ISA 315 should discuss the types of misstatements identified by the SEC that could result from cybersecurity incidents.

In 2017, the American Institute of Certified Public Accountants (AICPA) released a framework (Trust Services Criteria–the Framework) for assessing cybersecurity risk (AICPA 2017). The Framework was developed to be part of a System and Organizational Controls (SOC) for cybersecurity service but could also be applied to assessing risks of material misstatement related to an entity's IT functions. It may be appropriate to include or reference elements of the Framework in the AEM to aid in the evaluation of the risk of material misstatement applicable to cybersecurity.

Question 6: Will the proposed enhanced framework for the identification and assessment of the risks of material misstatement result in a more robust risk assessment? Specifically:

(a) Do you support separate assessment of inherent and control risk at the assertion level, and the revised requirements and guidance appropriate to support the separate assessments?

We generally support the revised guidance requiring separate assessments of inherent and control risk at the assertion level (paragraphs 45–50 of ED-315). However, it is important to note that research has consistently shown that auditors tend to spontaneously combine the two assessments. Vandervelde, Tubbs, Schepanski, and Messier (2009) note that auditors appear to use what they refer to as a "range model," where risk factors are weighted and combined in a way that places more weight on factors that are perceived as having the highest risk and less on factors perceived as low risk. Messier and Austen (2000) find there is a "knowledge-based dependence" between inherent and control risk assessment; and Miller, Cipriano, and Ramsay (2012) report that even when auditors are instructed to perform separate inherent and control risk assessments, they tend to evaluate inherent risk with a presumption that controls are effective and revise their combined risk assessments upward only when explicitly informed that controls are not effective. Thus, even though ED-315 provides guidance to assess each of these components in separate sections or paragraphs, it may be difficult or impossible for auditors to not combine these two risk assessments in the absence of specific guidance to the contrary. More explicitly identifying the order in which the assessments should occur might reduce auditors' tendency to combine their assessments of inherent and control risk.

In addition, although the changes proposed by ED-315 are generally expected to aid in promoting professional skepticism, it is possible that increasing the focus on separating assessments of inherent and control risk could have a negative impact. Rasso (2015) finds that more broad, abstract interpretations of audit evidence result in heightened skepticism. Combined assessments such as those described by Vandervelde et al. (2009) allow individuals to connect individual pieces of information or evidence and develop more complete mental representations of the "big picture" (e.g., Christ 1993). It is important that the Board monitor the adoption of ISA 315 (Revised) for implementation issues and unintended consequences.

(b) Do you support the introduction of the concepts and definitions of "inherent risk factors" to help identify risks of material misstatement and assess

inherent risk? Is there sufficient guidance to explain how these risk factors are used in the auditor's risk assessment process?

We support the concepts and definitions of inherent risk factors, noting that the factors are consistent with those described in Miller et al. (2012). Research has demonstrated that auditors tend to assess inherent risk similarly for all assertions related to an account (Waller 1993; Elder and Allen 2003), implying that auditors tend to consider inherent risk at the account balance level, rather than the assertion level. We believe it would be helpful to provide examples of how qualitative inherent risk factors map to relevant financial statement assertions to promote an assessment of inherent risk at the assertion level. For example, paragraph A5 includes a specific example of how complexity impacts supplier rebates. It would be helpful to add a sentence describing that complexity in the calculation of supplier rebates impacts the completeness assertion of an entity's supplier rebate liability account. It would also be helpful to include additional specific examples of how the other listed qualitative inherent risk factors (i.e., subjectivity, change, uncertainty, susceptibility to bias or fraud) impact specific assertions. As an example, the subjectivity of the estimation of uncollectible customer balances impacts the valuation assertion of an entity's allowance for doubtful accounts.

REFERENCES

Alles, M. G. 2015. Drivers of the use and facilitators and obstacles of the evolution of big data by the audit profession. *Accounting Horizons* 29 (2): 439–449. https://doi.org/10.2308/acch-51067

American Institute of Certified Public Accountants (AICPA). 2017. *Trust Services Criteria*. Available at: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf

Appelbaum, D., A. Kogan, and M. A. Vasarhelyi. 2017. Big Data and analytics in the modern audit engagement: Research needs. *Auditing: A Journal of Practice & Theory* 36 (4): 1–27. https://doi.org/10.2308/ajpt-51684

Appelbaum, D., A. Kogan, and M. A. Vasarhelyi. 2018. Analytical procedures in external auditing: A comprehensive literature survey and framework for external audit analytics. *Journal of Accounting Literature* 40: 83–101. https://doi.org/10.1016/j.acclit.2018.01.001

Asare, S. K., and A. M. Wright. 2004. The effectiveness of alternative risk assessment and program planning tools in a fraud setting. *Contemporary Accounting Research* 21 (2): 325–352. https://doi.org/10.1506/L20L-7FUM-FPCB-7BE2

Bhaskar, L. S., J. H. Schroeder, and M. L. Shepardson. 2019. Integration of internal control and financial statement audits: Are two audits better than one? *The Accounting Review* 94 (2). https://doi.org/10.2308/accr-52197

Bierstaker, J. L., and J. C. Thibodeau. 2006. The effect of format and experience on internal control evaluation. *Managerial Auditing Journal* 21 (9): 877–891. https://doi.org/10.1108/02686900610704984

Boland, C., B. Daugherty, and D. Dickins. 2018. Evidence of the relationship between PCAOB inspection outcomes and the use of structured audit technologies. *Auditing: A Journal of Practice & Theory* (forthcoming). https://doi.org/10.2308/ajpt-52214

Brazel, J. F., and C. P. Agoglia. 2007. An examination of auditor planning judgments in a complex accounting information system environment. *Contemporary Accounting Research* 24 (4): 1059–1083. https://doi.org/10.1506/car.24.4.1

Brown-Liburd, H., H. Issa, and D. Lombardi. 2015. Behavioral implications of Big Data's impact on audit judgment and decision making and future research directions. *Accounting Horizons* 29 (2): 451–468. https://doi.org/10.2308/acch-51023

Cao, M., R. Chychyla, and T. Stewart. 2015. Big Data analytics in financial statement audits. *Accounting Horizons* 29 (2): 423–429. https://doi.org/10.2308/acch-51068

Carpenter, T. D., and J. L. Reimers. 2013. Professional skepticism: The effects of a partner's influence and the level of fraud indicators on auditors' fraud judgments and actions. *Behavioral Research in Accounting* 25 (2): 45–69. https://doi.org/10.2308/bria-50468

Christ, M. Y. 1993. Evidence on the nature of audit planning problem representations: An examination of auditor free recalls. *The Accounting Review* 68 (2): 304–322.

Cohen, J. R., D. W. Dalton, and N. L. Harp. 2017. Neutral and presumptive doubt perspectives of professional skepticism and auditor job outcomes. *Accounting, Organizations and Society* 62: 1–20. https://doi.org/10.1016/j.aos.2017.08.003

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2013. *Internal Control—Integrated Framework*. New York, NY: COSO.

Dennis, S. A., and K. M. Johnstone. 2016. A field survey of contemporary brainstorming practices. *Accounting Horizons* 30 (4): 449–472. https://doi.org/10.2308/acch-51503

Dennis, S. A., and K. M. Johnstone. 2018. A natural field experiment examining the joint role of audit partner leadership and subordinates' knowledge in fraud brainstorming. *Accounting, Organizations and Society* 66: 14–28. https://doi.org/10.1016/j.aos.2018.02.001

Dorantes, C. A., C. Li, G. F. Peters, and V. J. Richardson. 2013. The effect of enterprise systems implementation on the firm information environment. *Contemporary Accounting Research* 30 (4): 1427–1461. https://doi.org/10.1111/1911-3846.12001

Elder, R. J., and R. D. Allen. 2003. A longitudinal field investigation of auditor risk assessments and sample size decisions. *The Accounting Review* 78 (4): 983–1002. https://doi.org/10.2308/accr.2003.78.4.983

Hackenbrack, K. 1992. Implications of seemingly irrelevant evidence in audit judgment. *Journal of Accounting Research* 30 (1): 126–136. https://doi.org/10.2307/2491095

Hammersley, J. S. 2011. A review and model of auditor judgments in fraud-related planning tasks. *Auditing: A Journal of Practice & Theory* 30 (4): 101–128. https://doi.org/10.2308/ajpt-10145

Hurtt, K., H. L. Brown-Liburd, C. E. Earley, and G. Krishnamoorthy. 2013. Research on auditor professional skepticism: Literature synthesis and opportunities for future research. *Auditing: A Journal of Practice & Theory* 32 (Supplement): 45–97. https://doi.org/10.2308/ajpt-50361

International Auditing and Assurance Standards Board (IAASB). 2016. *IAASB Chairman Prof. Arnold Schilder Presentation to the U.S. PCAOB Standing Advisory Group on Matters of Mutual Interest to the IAASB and PCAOB and Ongoing Coordination between the Two*. Available at: https://www.ifac.org/news-events/2016-05/iaasbs-work-enhance-audit-quality

Klamm, B. K., and M. W. Watson. 2009. SOX 404 reported internal control weaknesses: A test of COSO framework components and information technology. *Journal of Information Systems* 23 (2): 1–23. https://doi.org/10.2308/jis.2009.23.2.1

Li, C., G. F. Peters, V. J. Richardson, and M. W. Watson. 2012. The consequences of information technology control weaknesses on management information systems: The case of Sarbanes-Oxley internal control reports. *MIS Quarterly* 36 (1): 179–203. https://doi.org/10.2307/41410413

Messier, W. F., Jr., and L. A. Austen. 2000. Inherent risk and control risk assessments: Evidence on the effect of pervasive and specific risk factors. *Auditing: A Journal of Practice & Theory* 19 (2): 119–131. https://doi.org/10.2308/aud.2000.19.2.119

Miller, T. C., M. Cipriano, and R. J. Ramsay. 2012. Do auditors assess inherent risk as if there are no controls? *Managerial Auditing Journal* 27 (5): 448–461. https://doi.org/10.1108/02686901211227931

Nelson, M. W. 2009. A model and literature review of professional skepticism in auditing. *Auditing: A Journal of Practice & Theory* 28 (2): 1–34. https://doi.org/10.2308/aud.2009.28.2.1

Pincus, K. 1989. The efficacy of a red flags questionnaire for assessing the possibility of fraud. *Accounting, Organizations and Society* 14 (1/2): 153–163. https://doi.org/10.1016/0361-3682(89)90039-1

PricewaterhouseCoopers (PwC). 2018. *Securities Litigation Study: Seeing through the Smoke*. Available at: https://www.pwc.com/us/en/services/forensics/library/securities-litigation-studies.html

Public Company Accounting Oversight Board (PCAOB). 2009. *Report on the First-Year Implementation of Auditing Standard No. 5, an Audit of Internal Control over Financial Reporting That Is Integrated with an Audit of Financial Statements. PCAOB Release No. 2009-006 (September 24)*. Washington, DC: PCAOB.

Public Company Accounting Oversight Board (PCAOB). 2012. *Observations from 2010 Inspections of Domestic Annually Inspected Firms Regarding Deficiencies in Audits of Internal Control over Financial Reporting. Release No. 2012-006 (December 10)*. Washington, DC: PCAOB.

Public Company Accounting Oversight Board (PCAOB). 2013. *Considerations for Audits of Internal Control over Financial Reporting. Staff Audit Practice Alert No. 11 (October 24)*. Washington, DC: PCAOB.

Public Company Accounting Oversight Board (PCAOB). 2018. *Standing Advisory Group Meeting: Panel Discussion—Cybersecurity*. Available at: https://pcaobus.org/News/Events/Pages/SAG-meeting-June-2018.aspx

Rasso, J. T. 2015. Construal instructions and professional skepticism in evaluating complex estimates. *Accounting, Organizations and Society* 46: 44–55. https://doi.org/10.1016/j.aos.2015.03.003

Rice, S., and D. Weber. 2012. How effective is internal control reporting under SOX 404? Determinants of the (non-) disclosure of existing material weakness. *Journal of Accounting Research* 50 (3): 811–843. https://doi.org/10.1111/j.1475-679X.2011.00434.x

Securities and Exchange Commission (SEC). 2011. *Corporate Finance Disclosure Guidance: Topic No. 2: Cybersecurity*. Available at: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Stoel, M., and W. Muhanna. 2011. IT internal control weaknesses and firm performance: An organizational liability lens. *International Journal of Accounting Information Systems* 12 (4): 280–304. https://doi.org/10.1016/j.accinf.2011.06.001

Tan, H.-T., and A. Kao. 1999. Accountability effects on auditors' performance: The influence of knowledge, problem-solving ability, and task complexity. *Journal of Accounting Research* 37 (1): 209–223. https://doi.org/10.2307/2491404

Tan, H.-T., T. B.-P. Ng, and B. W.-Y. Mak. 2002. The effects of task complexity on auditors' performance: The impact of accountability and knowledge. *Auditing: A Journal of Practice & Theory* 21 (2): 81–95. https://doi.org/10.2308/aud.2002.21.2.81

Vandervelde, S. D., R. M. Tubbs, A. Schepanski, and W. F. Messier, Jr. 2009. Experimental tests of a descriptive theory of combined auditee risk assessment. *Auditing: A Journal of Practice & Theory* 28 (2): 145–169. https://doi.org/10.2308/aud.2009.28.2.145

Vasarhelyi, M. A., A. Kogan, and B. M. Tuttle. 2015. Big Data in accounting: An overview. *Accounting Horizons* 29 (2): 381–396. https://doi.org/10.2308/acch-51071

Waller, W. 1993. Auditors' assessments of inherent and control risk in field settings. *The Accounting Review* 6 (4): 783–802.

Wood, L. 2012. The impact of decision aid use on the dilution effect when assessing fraud. *Journal of Finance and Accountancy* 9: 23–42.