



Agenda Item 9

Auditor Transparency Research and Peer Review Survey Outreach

Greg Jenkins, ASB Member

Research Team Members

Fraud and Going Concern

- Joe Brazel, NC State University
- Tina Carpenter, University of Georgia
- Christine Gimbar, DePaul University
- Keith Jones, University of Kansas

Peer Review

- Eric Negangard, University of Virginia
- Mark Sheldon, John Carroll University

Research Update

- Completed surveys - Completed
 - Survey of financial statement users and preparers
 - Survey of peer reviewers
- Interviews - Ongoing
 - Financial statement users and preparers
- Synthesis of academic literature - Completed

Three-pronged
Approach

Survey of Peer Reviewers

- Survey sought peer reviewers' perspectives on
 - Fraud-related audit procedures
 - Scalability of U.S. GAAS
 - Auditor's use of IT
- Respondents
 - 139 responses
 - Average public accounting experience – 33 years
 - Average peer review experience – 16 years
 - On average, respondents completed 15 peer reviews in the past 3 years

Overview and
Demographics

Fraud-related Procedures

- Required discussion and fraud brainstorming session
 - Discussion among engagement team was sufficiently documented – 95%
 - Important matters were communicated to those who did not attend – 94%
 - Engagement team considered management's fraud risk assessment – 93%
- Documentation on the use of information technology (IT) in the consideration of fraud is limited
 - 42% of engagements include documentation on use of IT
 - Journal entry testing and general ledger analysis were most common

Journal Entry Testing

| | Performed | | Documented | |
|---|-----------|-----|------------|-----|
| | Yes | No | Yes | No |
| Obtain an understanding of the entity's financial reporting process and controls over journal entries and other adjustments and the suitability of design and implementation of such controls | 95% | 5% | 91% | 9% |
| Obtain an understanding of the entity's controls surrounding journal entries, including nonstandard journal entries used to record nonrecurring, unusual transactions, or adjustments | 89% | 11% | 86% | 14% |
| Make inquiries of individuals involved in the financial reporting process about inappropriate or unusual activity relating to the processing of journal entries and other adjustments | 91% | 9% | 90% | 10% |
| Consider fraud risk indicators, the nature and complexity of accounts and unusual entries processed | 95% | 5% | 91% | 9% |
| Select journal entries and other adjustments made at the end of a reporting period | 89% | 11% | 87% | 13% |
| Consider the need to test journal entries and other adjustments throughout the period | 86% | 14% | 86% | 14% |

Fraud-related Challenges

| | Average Rank |
|--|--------------|
| Using data analytics to identify fraud risks | 3.22 |
| Using technology to conduct testing of journal entries | 3.81 |
| Possessing the necessary specialized skills (e.g., skills related to information technology, forensic training, etc.) to identify and assess fraud risks | 3.99 |
| Identifying fraud risks | 4.14 |
| Conducting an effective fraud brainstorming | 4.43 |
| Assessing fraud risks | 4.65 |
| Developing audit responses to identified fraud risks | 4.68 |
| Communicating with management and/or those charged with governance regarding fraud-related matters | 7.08 |

Scalability of U.S. GAAS

- In their capacity as auditors, respondents slightly agree with the statement that “U.S. GAAS is scalable”
- Respondents generally agree that auditors are reluctant to exercise professional judgment in scaling U.S. GAAS because of concerns that they will be second-guessed by a peer reviewer
- More experienced peer reviewers and those who recently reviewed smaller firms (i.e., firms with 10 or fewer professionals) perceive auditors to be more reluctant to scale U.S. GAAS

Which standards do engagement teams have difficulty scaling?

| | % Who Selected |
|---|----------------|
| AU-C 315, <i>Understanding the Entity and its Environment and Assessing the Risks of Material Misstatement</i> | 45% |
| AU-C 530, <i>Audit Sampling</i> | 45% |
| AU-C 330, <i>Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained</i> | 41% |
| AU-C 230, <i>Audit Documentation</i> | 35% |
| AU-C 300, <i>Planning an Audit</i> | 27% |
| AU-C 240, <i>Consideration of Fraud in a Financial Statement Audit</i> | 19% |
| AU-C 540A, <i>Auditing Accounting Estimates, Including Fair Value Accounting Estimates, and Related Disclosures</i> | 17% |
| AU-C 265, <i>Communicating Internal Control Related Matters Identified in an Audit</i> | 9% |
| AU-C 260, <i>The Auditor's Communication with Those Charged with Governance</i> | 6% |
| AU-C 505, <i>External Confirmations</i> | 2% |

Auditors' Use of IT

- Respondents generally believe IT is not used efficiently or effectively
- Explanations for inefficiency
 - Lack of training, understanding, and trust in IT
 - Inadequate understanding of client's system
 - Over-reliance on substantive testing when entire populations could be tested using IT
- Explanations for ineffectiveness
 - Lack of training
 - Reluctance to change audit approach to employ IT
 - Relative cost of IT
- 45% believe auditors are reluctant to use IT in the audit because of concerns related to a peer reviewer second-guessing their judgment

Areas of Observed IT Use

| | % Who Selected |
|-----------------------------------|----------------|
| Substantive analytical procedures | 37% |
| Journal entry testing | 36% |
| Tests of details | 32% |
| Confirmations | 29% |
| Risk assessment | 27% |
| Planning | 24% |
| Wrap-up analytical procedures | 23% |
| Client acceptance/continuance | 9% |

Effects of U.S. GAAS on Use of IT

- 76% believe U.S. GAAS neither encourages nor discourages use of IT
- U.S. GAAS currently encourages use of IT by
 - Allowing for judgment
 - Discussing electronic evidence and how to rely on it
 - Calling for sufficient audit evidence combined with the idea that IT can provide more reliable evidence
- U.S. GAAS could better encourage use of IT by
 - Including more clarity and guidance around the implementation and use of IT
 - Including examples of how IT might be used to meet certain requirements
 - Having a requirement to specifically consider and document how IT was used on the audit

Update on Interviews

- 13 interviews have been completed
 - Former regulators
 - Valuation specialists
 - Forensic specialists
 - Corporate management
 - Auditors
- Observations based on completed interviews
- Additional interviews are targeted for Q4

Synthesis of Academic Literature

- Synthesis of fraud-related academic studies between 2017-2022
- The focus of the synthesis was to learn about the latest findings on the
 - identification
 - assessment
 - response to fraud risks

Fraud Risk Identification – Key Takeaways

- Audit teams whose partners emphasize brainstorming as a training opportunity and share personal experiences on engagements involving fraud identify and discuss an increased number of fraud risk factors during fraud brainstorming sessions.
- Audit staff and seniors are more apt to share relevant fraud risk factors when an engagement partner establishes a supportive, non-threatening group dynamic that encourages idea sharing.
- High trait skepticism of the audit partner can drive fraud brainstorming quality (e.g., greater contribution of specialists, more extensive discussion, and more time spent preparing for the meeting).
- Unless supervisors consistently reward appropriate skepticism with positive performance evaluations (regardless of whether a misstatement is ultimately identified), auditors are unlikely to pursue fraud red flags.

Partner Influence

Fraud Risk Identification – Key Takeaways

- Structured technology can inhibit both the number and quality of ideas generated during a brainstorming session (i.e., reduce creative thinking).
- Fraud interviews
 - Performing fraud interviews with two auditors can induce deceptive clients to talk more and enhances feelings of nervousness, making them more likely to “leak” fraud-related information.
 - Individuals are more likely to report fraudulent activities when they are reminded about statutory whistleblower protections and the interview occurs in the afternoon, when auditees’ self-regulation is depleted, making them less likely to resist impulses to keep fraud information to themselves.

Fraud Risk Assessment – Key Takeaways

- Generating more explanations for account fluctuations can be counterproductive because doing so increases the perceived difficulty of the audit task and can lead to anchoring on client explanations.
- Planning analytics based on industry data, nonfinancial measures and cash flows data are more effective in assessing fraud risks than those based on prior year balances and relations within the client's financial data.

Analytical Procedures

Fraud Risk Assessment – Key Takeaways

- Auditors make more appropriate fraud risk assessments when they consult with forensic specialists with a greater understanding of the client's business and engagement objectives.
- Auditors who take a forensic specialist's perspective assess fraud risk higher in higher and lower fraud risk environments. These auditors also propose more audit plan changes in a high fraud risk environment than auditors who do not take a forensic specialist's perspective. The proposed changes are largely consistent with recommended responses from a panel of audit and forensic experts.

Forensic Specialists

Fraud Risk Assessment – Key Takeaways

- Auditors who decompose fraud risk assessments into separate assessments of the *likelihood* and *magnitude* of risk develop lower fraud risk assessments when fraud risk is high than auditors who take a holistic approach.
- Auditors judge misstatements as less likely to be intentional and are less likely to follow up when a misstatement results from omission rather than commission. This is important because some managers are more likely to commit fraud by omitting a transaction than falsifying a transaction.

Arriving at a Risk Assessment

Fraud Risk Assessment – Key Takeaways

- Auditors interpret verbal and nonverbal expressions of high CFO narcissism as indicative of increased fraud risk. Although, verbal cues of narcissism have a greater influence on auditors than nonverbal cues.
- Morally disengaged auditors (i.e., disassociating the risk of fraud from its moral and ethical implications) assess fraud risk as lower for clients with narcissistic CFOs. This suggests that moral disengagement reduces professional skepticism.
- More narcissistic auditors generally underestimated fraud risk relative to less narcissistic auditors.

Effects of Narcissism

Fraud Risk Response – Key Takeaways

- Auditors who informally advise other team members engage in more deliberative thinking and identify more effective responses to fraud.
- Forensic specialist involvement often results in incremental audit findings (e.g., identification of material misstatements, financial reporting fraud, misappropriation of assets, and internal control deficiencies).
- An auditor's evaluation of whether evidence is indicative of fraud is most effective when the auditor thinks openly and reflectively about the evidence.
- Higher trait skepticism leads auditors to perform additional inquiries and other audit procedures in response to fraud risks.

Fraud Risk Response – Key Takeaways

- Empowering auditors (i.e., feeling as though they can overcome constraints and are supported to navigate their own work) improves the development of effective responses to evidence indicative of fraud without making auditors inefficient when fraud is not present.
- While auditors receiving audit firm communication that resembles practice fail to detect a seeded fraud, when innovative communication that contains game-like elements is provided, auditors' responses are effective at addressing heightened fraud risk.



Association
of International
Certified Professional
Accountants®

Thank you