THOMSON REUTERS
CHECKPOINT™

S. Davis & Associates, P.A.
Certified Public Accountants & Consultants

THE PPC
GOVERNMENTAL UPDATE

APRIL 2019, VOLUME 26, NO. 4

AICPA Publishes 2018/19 Audit Risk Alert for Yellow Book and Single Audits

The AICPA recently issued its audit risk alert *Government Auditing Standards and Single Audit Developments—2018/19*. AICPA audit risk alerts provide important considerations for planning and performing audits each year. This risk alert is prepared for auditors who perform Yellow Book and Uniform Guidance audits. AICPA audit risk alerts are considered *other auditing publications*. As such, they have no authoritative status; however, they may help auditors understand and apply auditing standards.

Government Auditing Standards

The GAO issued *Government Auditing Standards, 2018 Revision*, in July 2018. The revision supersedes the 2011 edition and is effective for financial audits, attestation engagements, and reviews of financial statements for fiscal periods ending on or after June 30, 2020, and performance audits beginning on or after July 1, 2019. Early implementation is *not* permitted. The risk alert summarizes key areas of the revision, including independence, competence, CPE, quality control, peer review, and waste. In addition, the guidance incorporates clarified and recodified attestation and review guidance, as well as revised guidance related to performance audits.

Uniform Guidance

The risk alert addresses the following Uniform Guidance audit topics:

- Uniform Guidance FAQs.
- Corrective action plan and schedule of prior audit findings submission on auditee letterhead.
- Examinations of single audit engagements as required by the Uniform Guidance's government-wide audit quality study.
- Ways auditors can enhance audit quality, including proper education and use of resources, an adequate quality control system, and the selection of peer reviewers with appropriate governmental engagement experience.

Compliance Supplement

The 2018 Compliance Supplement is discussed, with emphasis on the format diverging from prior years. The 2018

In this Issue:

This newsletter is also available online.
Please call (800) 431-9025, or order online:
https://tax.thomsonreuters.com/products/brands/checkpoint/ppc/

THOMSON REUTERS™

Compliance Supplement only provides guidance for areas that were updated and requires auditors to refer to the 2017 Compliance Supplement for areas that were unchanged.

Audit Quality

See a detailed discussion of this topic in the article titled, "Enhancing Audit Quality Initiative."

Ethics

The risk alert discusses an FAQ that was released in March 2018, "Long association of senior personnel of the engagement team," and familiarity threats that long association may present. It also summarizes the Interpretation, "Hosting Services," which is effective July 1, 2019, and provides examples of common hosting services.

Peer Review Matters

The risk alert includes a section on items for peer reviewers to consider in reviewing Yellow Book and single audit engagements. Matters discussed include Yellow Book independence, compliance audits performed when the entity is below the single audit threshold, single audit documentation, and high-risk type B program identification.

Practical Consideration:

You can access the risk alert on Checkpoint at **checkpoint.riag.com** if you subscribe to the AICPA materials. The risk alert can also be purchased from the AICPA at **www.aicpastore.com**.

Enhancing Audit Quality Initiative

As discussed in the previous article, the AICPA recently issued its audit risk alert *Government Auditing Standards and Single Audit Developments—2018/19*. Amongst other topics, the risk alert included an update on the AICPA's Enhancing Audit Quality (EAQ) initiative, which was launched in May 2014 in an effort to support quality improvement of firms by aligning all AICPA audit-related activities.

Practical Consideration:

The AICPA has published a report titled "Enhancing Audit Quality: 2018 Mid-Year Progress Report," available at **www.aicpa.org/interestareas/peerreview/eaq/eaq-annual-highlights-and-progress-reports.html**.

AICPA Peer Review Program Study

The risk alert informs practitioners that single audits have been identified as a risk area and designated as an area of focus for peer review. As part of the EAQ initiative, the AICPA Peer Review Program performed a study of potential quality factors in single audits and found there is a correlation between the number of single audits performed by a firm every year (regardless of the size of the firm) and the likeliness that a given single audit conformed to professional standards. A summary of the results is as follows:

- One single audit performed had conformity of 38%.
- Two to 10 single audits performed had conformity of 51%.
- Eleven or more single audits performed had conformity of 85%.

Notably, the study found that firms that were members of the Governmental Audit Quality Center (GAQC) had rates of conformity to professional standards that were two times greater than those of the nonmembers. In addition, GAQC member firms that performed 11 or more single audits each year had a conformity rate of 100%.

The study also found a similar correlation between a higher number of single audits performed by an engagement partner annually and a higher conformity rate.

Practical Consideration:

The GAQC is a voluntary membership center for CPA firms and state audit organizations that perform governmental audits, which promotes the importance of quality governmental audits and the value of such audits to their clients. GAQC members have access to communications, education, resources, and tools to support the performance of governmental and single audits. For more information, visit **www.aicpa.org/interestareas/governmentalauditquality.html**.

Single Audit Analysis

Also as part of the EAQ initiative, single audits were analyzed to identify pervasive areas of nonconformity, including the cause of the nonconformity. The risk alert lists examples of deficiencies that were found, along with common auditor misconceptions causing them.

The analysis found that both auditors and peer reviewers appeared to be making inappropriate connections between the single audit and the financial statement audit, such as:

- Believing it is appropriate to rely on internal control walk-throughs over financial reporting to eliminate the need for testing controls over compliance.
- Believing that by assessing control risk as "high", the need to test controls over compliance can be eliminated.
- Performing tests of details as part of their financial statement audit, while doing no work to assess compliance with direct and material requirements, and inappropriately classifying the procedures as "dual-purpose tests" (forgoing any compliance testing).

The risk alert explains that the items noted above are misconceptions because the Uniform Guidance requires auditors to perform procedures to obtain an understanding of internal control over federal programs sufficient to plan the audit and support a low assessed level of control risk of noncompliance for major programs. Furthermore, testing of both internal control over compliance and compliance with direct and material compliance requirements is required for each major program in a Uniform Guidance compliance audit.

These misconceptions indicate that some auditors do not understand that a Uniform Guidance compliance audit is an audit of compliance with its own requirements that is separate from the financial statement audit. The risk alert went on to describe additional deficiencies that were found in the areas of planning, internal control testing, and compliance testing, and identified misconceptions that relate to those deficiencies.

Practical Consideration:

To see more deficiencies and related misconceptions in these areas, you can access the 2018/19 edition of the GSA/SA Audit Risk Alert on Checkpoint at **checkpoint.riag.com** if you subscribe to the AICPA materials. The audit risk alert can also be purchased from the AICPA at **www.aicpastore.com**.

Fraud in Governments

Yes, fraud happens in all types of entities, including governments, and it happens more often than most people think. As auditors, we may not work with governments that have experienced fraud, but it's good to be knowledgeable about fraud that does occur within governmental entities. So, let's explore how often fraud occurs, how much money is lost, and the ways it is perpetrated.

The Association of Certified Fraud Examiners (ACFE) issues an annual report on fraud specific to governments, *2018 Report to the Nations, Government Edition,* which discusses this exact topic. In 2017, 364 cases of fraud within governmental entities were reported in the ACFE's survey, which accounted for 16% of all fraud cases reported. The median loss for these governmental cases was $118,000.

Fraud by Type

The ACFE categorizes fraud into three groups: asset misappropriation, corruption, and financial statement fraud, as follows:

- Misappropriation of assets is the theft or misuse of assets, such as cash, company vehicles, inventory, etc. 88% of the cases reported included asset misappropriation, with a median loss of $100,000.
- Corruption is the wrongful use of influence in business dealings, such as bribery, kickbacks, collusion, conflict of interest, etc. Corruption was reported in 47% of the cases, with a median loss of $400,000.
- Financial statement fraud is the intentional misstatement of financial statements to deceive the users, such as misstating or omitting financial statement amounts or disclosures. Only 6% of cases included financial statement fraud, with a median loss of $315,000.

While exacting the lowest median loss, misappropriation of assets is by far the most common fraud. The types of fraud occurring within misappropriation of assets is broken down into further categories as follows: noncash (20%), billing (15%), cash on hand (13%), skimming (13%), cash larceny (12%), expense reimbursement (11%), payroll (10%), check and payment tampering (9%), and register disbursements (1%). (Note the percentages in this section add up to more than 100% because cases may include more than one type.)

How Is Fraud Detected?

The most frequent method by which fraud is detected is through tips; 45% of frauds are discovered this way, which is more than the next closest six methods combined. Organizations with hotlines detected fraud through tips in 66% of the cases while only 34% of cases were detected through tips in organizations

The PPC Governmental Update is published monthly by Thomson Reuters/Tax & Accounting, P.O. Box 115008, Carrollton, Texas 75011-5008, (800) 431-9025.

Tax & Accounting - Checkpoint
P.O. Box 115008
Carrollton, Texas 75011-5008
UNITED STATES OF AMERICA

ADDRESS SERVICE REQUESTED

PRSRT STD
U.S. POSTAGE
PAID
Thomson

without a hotline. These statistics are clear indications that implementing a hotline is a strong control in the detection of fraud.

The other common methods of detecting fraud included: internal audit (15%), management review (9%), external audit (6%), law enforcement (5%), other (5%), document examination (4%), and account reconciliation (4%).

Practical Consideration:

Consider sharing this information with your government clients and suggesting they implement a hotline if they don't already have one. Of course, they must not only implement the hotline but publicize it widely.

Control Weaknesses

Governments of all sizes experience fraud. Whether the government employs less than 100 employees or over 10,000, the occurrence of fraud is approximately 20–30%. However, weaknesses in controls are a common contributor to instances of fraud in all sizes of governments. According to the report, the top three control weaknesses that contributed to fraud were: a lack of internal controls (30%), override of the existing controls (18%), and a lack of management review (17%).

Fraudster Profile

Who commits fraud? The typical fraudster is more likely to be male (68%) and can be aged anywhere from 22 to 66, with the median age being 45 and losses rising with age. Additional information related to perpetrators:

- Employees committing fraud worked in operations (18%), accounting (13%), and executive or upper management (13%), and the median loss increased significantly with higher levels of authority.
- In 86% of cases, the fraudster displayed *at least* one of the following behavioral flags:
  - Living beyond means.
  - Financial difficulties.
  - Unusually close relationship with customer or vendor.
  - Exhibiting control issues and unwilling to share responsibilities.
  - "Wheeler-dealer" attitude.
- Surprisingly, 95% did not have a prior fraud conviction, meaning their background checks had come back clean.
- Perpetrators that act alone are far less damaging than those who collude with others. The median loss for lone fraudsters was $40,000, while it was $280,000 for those acting with others.

Practical Consideration:

The ACFE report provides further details concerning fraud in governments. The report is available on the ACFE's website at **www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2018/RTTN-Government-Edition.pdf**.

What's Next

The information published by the ACFE is a useful reminder to auditors of a couple key things. First, governments are exempt from taxes but not fraud. Secondly, internal controls matter! You encourage your clients to have them for a reason, and it's not just to make our jobs easier. Share this information with your clients and their governing bodies. Hopefully, it encourages them, as stewards of public funds and resources, to implement internal controls to protect those resources.