Fraud brainstorming
Planning to find fraud

Audit plans have to be designed to find fraud. Here’s help for your team on fraud brainstorming: delving into the details, thinking like a fraudster and using the knowledge of the processes to increase awareness of where frauds may be hiding.
to uncover the scam,” the indictment claimed. The scam represented possibly the largest potential loss to the National Credit Union Share Insurance Fund (NCUSIF). The frauds, which ran through a single credit union, resulted in more than $170 million in potential losses, involving bribery, money laundering, fraudulent loans, corruption, kickbacks and even a Ponzi scheme (Credit Union Journal, June 27, 2011).

When the big frauds hit, it doesn’t take long for others to ask “where were the auditors?” In this instance, the NCUSIF inspector general noted that “numerous red flags were present for many years,” including those spotted by examiners. The IG stated that examiners only performed “their required minimum procedures.” Board meeting minutes indicate that the audit reports identified no outstanding issues about the credit union operations.

The question beckons: Did the auditors properly prepare and plan to find fraud? Could effective fraud brainstorming have helped uncover these schemes much sooner? “If you don’t know what you’re looking for, how will you know when you’ve found it?”

This sums up the advantage of thinking about fraud before conducting an audit. An audit plan that’s not designed to find fraud may occasionally by chance find it. However, the fraud detection business shouldn’t be built on luck or hope but on proactive, planned and decisive measures.

In most of the published auditing standards and expectations for auditors, identifying fraud goes hand and hand with the key words “plan” or “planning.” The American Institute of CPAs, the Institute of Internal Auditors and the U.S. Government Auditing Standards all refer to proper audit planning and consideration of fraud schemes.

The “Statement on Auditing Standards No. 99: Consideration of Fraud,” also referred to as SAS 99, specifically requires fraud brainstorming sessions when reviewing financial statements. Unfortunately, merely having a sentence in the audit scope that states “the audit staff will remain vigilant for fraud during the course of the audit” isn’t enough.

In recent years, the phrase “the auditors failed to uncover the ongoing fraud scheme” has unfortunately been appearing more and more frequently. Satyam, Tyco, Olympus, Madoff and Healthsouth are just a few of the recent large frauds in which auditors and investigators missed the warning signs.

Finding fraud is difficult. We all know that. We’re constantly reminded at every audit, fraud and accounting conference we attend that fraud is inherently hidden. Deception, alteration, fabrication and the destruction of documents seems to be the norm for all fraudsters, yet qualified anti-fraud professionals still fall for and/or fail to identify their schemes. Did the fraud fighters properly plan and brainstorm for fraud?

Fraud brainstorming is more than sitting around a table for an hour talking about how fraud could occur. It involves delving into the details, thinking like a fraudster and using the knowledge of the processes to increase awareness of where frauds may be hiding.

When broken down into its parts, fraud brainstorming encompasses: assembling the right people; assessing the process(es), players, data and environment; developing fraud schemes and audit procedures based on these schemes; and developing fraud triggers.

By Ryan Hubbs, CFE, CIA, CCSA, PHR

Assembling the right people

For the most part, the audit team members will be the primary individuals involved in a fraud brainstorming session in advance of an audit so the objectives will remain relatively confidential. This also will minimize the possibility that the target group gets wind of the impending audit, especially steps designed to detect fraud. Therefore, carefully manage and safeguard the inclusion of others in this process.

CFEs in a fraud brainstorming session will bring investigative minds and skill sets to the session. On the other hand, don’t include management in the session. An auditor must assume that any employee in the target group could be committing fraud, including management. If they’re involved in the session, they could tip off the unknown fraudster. And be careful about including employees of the area being audited, such as an ethics or compliance specialist or human resources professional. Though they could be valuable additions, they could leak important information.

Assessing the process(es)

The audit staff clearly identify the process(es) that the brainstormers will review during the audit so they can identify the right fraud risks. Consider the following:

Process complexity

Assess the complexity of the process’ moving parts. The more complex a process, the greater the chance that fraud will slip through the cracks and crevices.

Number of transactions

The more transactions, the easier fraudsters can hide their crimes. Pay close attention to those processes that generate significant numbers of transactions, and design fraud detection tests accordingly.
Number of dollars, both large and small
Auditors may be drawn to focus on the high-dollar transactions that are above a certain threshold. But a significant fraud scheme could be occurring just under established thresholds. In some instances, the smallest transaction could be the indicator of a large, ongoing fraud.

Manual vs. automated systems
Discover if a process is manual or automated. Manual processes may allow for employees’ manipulation. Understand the “touch points” in an automated system in which employees can enter, change and extract data.

New systems vs. legacy systems
New and legacy systems can pose separate unique risks and challenges when you’re trying to detect fraud. A new system may cause confusion, operator errors, manual workarounds and breakdowns of existing controls in peripheral systems. A potential fraudster waits for this sort of turmoil and opportunity.

Auditors who have been routinely auditing legacy systems for years with the same checklists and test steps may have become lax and overlook large frauds committed by longtime employees.

Process control by non-employees — outsourced or contractors
If contractors or non-employees have access to processes, audit staff should assess what frauds they could be committing. Lack of daily oversight and control and lack of their definitive reporting structures to the company could keep these non-employees out of sight and out of mind.

Previous process issues, gaps and errors
Consider and identify other issues involved in a process or group to help paint a more accurate picture of possible fraud schemes:

- What have been the previous audit findings and responses from management regarding this process or group?
  - Repeated findings?
  - Management pushback?
  - Lack of implementation of audit recommendations?
  - Has the process or group received any fines from state, local or federal agencies?
  - Has the process or group been involved in any lawsuits, complaints or injunctions?
  - Has the process or group been responsible for any issues that have affected the health or operation of the company?
  - Have there been investigations into this area, whether conducted by internal investigators, legal counsel or external agencies?

Process override or edit capabilities, direct and indirect
Many audit steps have historically worked to identify those situations that could arise from a direct override of process controls. But, the auditor, during the fraud brainstorming process, should also assess instances in which there could be “soft” or indirect overrides. A routine audit may simply look at a CFO’s access to the financial data and the ability to make unauthorized changes, such as a direct override capability. However, a finance manager who’ll make any changes to the accounting system based on the CFO’s direction, without question, could be a situation in which the CFO has an indirect override capability to alter the financials. Evaluating indirect override capability requires assessing the influence of the decision makers and the willingness to act without question.

Assessing the players
Auditors must apply the same critical eye to each employee, regardless of tenure, position or personal relationship.
Because fraudsters don’t wear special outfits or have the letter “F” sewn on their shirts, every employee must be thought of as having the possibility to commit fraud, so design every audit test step with this in mind. When assessing those employees who are involved in the daily business of managing the process, consider the following:

- Who are the employees, management and contractors involved in this process?
- What are their names?
- What are their backgrounds?
  - Do any of them have any previous disciplinary, ethics or non-compliance issues?
  - Have they ever been disciplined for untruthfulness, control deficiencies or fraud?
- How long have they been with the company?
- Before coming to this department, where did they work?
  - Does this previous work area interface with the current department or process?
  - If so, could they use their knowledge of this process and/or contacts in the previous area to commit a fraud?
- How much approval and decision-making authority have they been granted?

Assessing the data

By now, the fraud brainstorming process has identified the players or employees involved in the upcoming audit. The auditors must be aware that if one or more of those individuals are committing fraud, there’s a chance that they could manipulate, alter and/or destroy data before the auditors take possession of it for the audit. Auditors should question and assess the reliability of all data that’s used to support an audit; consider the following:

- Where's the data housed?
- Who has access to it?
- How is the data generated?
  - If manual,
  - Who creates the data?
  - What format is it in?
  - Where are the manual data/documents stored, and who has physical access to the data?
    - If automated,
    - Where is the data editable or capable of being manipulated?
    - Who can make changes to it?
    - Are backups kept, and are they accessible?
    - If a fraudster was going to manipulate, alter or destroy data prior to the audit, what fields or information would be the easiest and fastest to change?
    - How could we test if changes were made?
    - How does the audit team plan on getting access to the data it needs?

Assessing the environment

One of the most overlooked aspects of conducting an audit is the environmental factors that could have an impact on the area and, especially, the individuals who are to be audited. This assessment can be easily correlated to the “pressure” side of the fraud triangle. What are those internal and external pressures or environmental factors that could cause wrongdoing, fraud or unethical behavior to materialize in this department or process?

- From an external environment assessment:
  - What frauds have been identified in other companies within this type of process?
  - What differences or similarities does our process have with them?
  - Are there any significant forces or pressures driving external goals or metrics within this process?
- Wall Street?
- Rating agencies?
- Significant investors or shareholders?
  - Are there pressures to meet or exceed the targets of competitors?
  - Are there any external financial, political, legal or operational issues that could force the manipulation of data with the process to be audited?
- Lawsuits.
- Recalls.
- Loss of market share.
- From an internal environment assessment:
  - What is the expectation of management and the tone at the top?
  - Get it done at all cost?
  - Whatever it takes?
  - How are internal goals and metrics set and formulated?
  - Are employees given incentives for doing the wrong behaviors?
  - Are the incentives unrealistic and by their very design entice individuals to commit fraud?
  - Are there strong internal financial pressures?
    - To meet budget?
    - Are layoffs possible if this doesn’t get done correctly?
  - Are there enough resources to get the job done?
  - Is one person doing the job of three, five, 10?
  - What is the morale level of the individuals?
    - Everyone loves coming to work?
    - Everyone can’t wait for 5 p.m. to get here fast enough?
  - Assessing the environment as part of the fraud brainstorming process could also be very helpful for the audit staff in determining the truthfulness and cooperation of the audited individuals.

Developing fraud schemes

The ability of the audit team to uncover
fraud in the audit will rely heavily on its ability to develop possible fraud schemes and corresponding audit tests that can detect these schemes. In 2006, research was published by Carpenter et al (2006) that found that when fraud is present, a group that interactively brainstormstorms outperforms auditors brainstorming individually and those that don't brainstorm, which provides further evidence of the benefit of interactive brainstorming sessions [See “Financial Statement Fraud: Insights from the Academic Literature,” by Chris E. Hogan, Zabihollah Rezaee, Richard A. (Dick) Riley Jr. and Uma Velury, Auditing: A Journal of Practice & Theory, November 2008].

When developing fraud schemes, consider the following:

- Start at the beginning of the process and work through until the end. Some fraud schemes may rely on multiple steps of manipulation or alteration in the process.
- The audit staff’s knowledge of internal controls shouldn’t be interjected here. At this point in the fraud brainstorming and audit process no one has a clue as to what is actually occurring daily in the audit area. No schemes or risks are impossible. Capture the schemes, and don't rule anything out.
- Audit members should build upon other member’s ideas. Many fraud schemes can have multiple moving parts.
- Don’t overlook collusion.
- Give specific attention to how many times the possible fraud scheme could go unchecked or be committed without detection.
- Assess single and cumulative dollar losses.
- Detail step by step how the fraudster would commit the scheme, including manipulating, altering or destroying data.
- Detail what specific players would be involved in each scheme.
- Detail how the fraudster would convert his or her fraud into a direct incentive, cash, stock, payoff, etc.
- No matter how much time is devoted to this section, the audit staff can’t contemplate or detect all fraud schemes. Devote a reasonable amount of time and resources to come up with as many schemes as possible, and then move on to designing those specific test steps that will help detect possible fraud.

### Developing audit procedures based on identified fraud schemes

To transition from developing fraud schemes to developing audit procedures, the audit team should ask: “Knowing what we now know, how are we going to test for these possible fraud schemes?” The type, scope and size of the audit will play a significant factor in how you develop and implement fraud audit steps, as will the availability of adequate audit resources. Sample sizes and audit methodologies may also differ from organization to organization, as will various audit standards among internal, external and governmental agencies. When planning the audit procedures, pay attention to the following:

- Do not openly refer to the audit test steps designed to detect fraud as the “audit test steps for detecting fraud.” This may make employees nervous or may tip off a potential fraudster. Fraud test steps should simply be referred to as “routine” audit test steps and downplayed as much as possible to those being audited.
- Consider how the audit team can get to audit data without alerting potential fraudsters. Is there a way for the team to request data from a separate or parallel means and cross check and compare the two?
- Design test steps to assess if a fraudster has manipulated, altered, fabricated or destroyed supporting data.
- Be open to requesting or accessing non-traditional data sources such as employee computer records, emails, phone records or Internet history. These records could be extremely valuable when conducting audits involving contractors, vendors and suppliers or when those being audited have to interface with others outside of their own groups.
- Fraudsters lie, and since no one identifies his or her self as a fraudster, the audit team must take all statements, attestations and affirmations with a grain of salt. “Trust but verify” must be built into every audit test step.
- Design fraud detection audit tests with built-in mechanisms that will expand scope and sample size or require additional testing if certain indicators or red flags present themselves. This also requires pre-planning by the audit staff as to what could be a triggering event.
- Develop audit test steps that evaluate the chronological timeline of data, transactions and information. Can things happen in the order in which they are being presented? Are there holes, gaps or anomalies in the timeline?

### Development of fraud triggers

The final step in the fraud brainstorming process is the development of fraud detection red flags. Design them so that after you identify them, they will trigger additional tests for fraud. Audits, as well as audit staff, must be able to change and adapt as a situation changes. Those audit teams that stay the course to a pre-planned audit program and fail to recognize the danger or warning signs along the way, may pass up the chance to uncover fraud. Some red flags to consider beforehand are:
• When asked to provide information for the audit, the individual is reluctant or hesitant to share information.

• When asked to provide data or documentation, the individual fails to respond, may be argumentative or creates an unusual delay in responding to the audit request.

• When asked to provide data or documentation, the individual provides the information faster than the data could have been retrieved. This could mean the individual had prepared in advance of the request.

• Inconsistencies exist between the statements made by several employees. This could indicate that one or more people could be actively deceiving the audit team.

• A "command and control" figure, who emerges early in the audit, mandates that all requests, data, support, interviews and questions are routed through him or her first. This individual could be a manager, executive or some other authority figure who has oversight over the process being audited or may be on the periphery. This individual could be the fraudster using his or her authority to filter information to the audit team.

• Data, documentation or information appears to have been manipulated, altered, fabricated or destroyed. The audit team must stop and regroup and determine if they missed a potential fraud scheme, or if the current audit tests need to be refined or enhanced.

It’s simple but difficult

Take any process in the world that’s designed to identify hidden items, and you’ll see an extraordinary amount of pre-planning. From oil exploration to mining for precious metals, the amount of upfront planning can help dictate the ultimate success of the project. The same holds true for uncovering fraud. The fraud brainstorming framework is relatively simple; the difficult part is implementing it. The widespread implementation of fraud brainstorming techniques may not only help uncover more frauds but also lead to more headlines that state "the auditors were able to uncover the long-running fraud scheme." — FM

Ryan C. Hubbs, CFE, CIA, PHR, CCSA, is senior manager of anti-fraud and investigation services at Matson Driscoll & Damico LLP in Houston, Texas. He is a member of the ACFE faculty. His email address is: rhubbs@mdd.com.

The material in this article and much more will be included in the revamped ACFE Auditing for Internal Fraud course. See ACFE.com/AIF. — ed.