WHAT IS WORKING IN AUDITING FOR FRAUD?

MOVING THE NEEDLE: FIGHTING FRAUD FROM THE INSIDE THROUGH AUDIT

As an internal auditor, you know the processes, the systems, the people and culture, the incentive programs, and the opportunities. You are already in the organization and looking, but to find fraud you must know what to look for. Traditional audit methods may not detect fraud because they are not designed to. This session will show specific steps and methods that you can incorporate immediately into your audit programs to start detecting existing fraud in your organizations tomorrow.

MARY BRESLIN, CFE, CIA
President
Empower Audit Training and Consulting

Mary Breslin has more than 20 years of experience in internal auditing, fraud examination, management, and accounting for companies such as ConocoPhillips, Barclays Capital, Costco Wholesale, Jefferson Wells, and Boart Longyear. She specializes in internal audit transformations, operational and financial auditing, fraud auditing and investigations, and corporate accounting.

In addition to audit, fraud, and accounting, she has significant international experience and has managed audit programs in more than 30 countries. Prior to becoming a full-time instructor, Breslin held the title of Vice President and Chief Audit Executive in a global financial services company, where she transformed a checklist audit function into a value add audit department which delivered measurable business results through the use of risk-based auditing, data analytics, continuous education, and skill development for her leadership team and staff.

Through her senior audit leadership roles, Breslin has implemented numerous baseline internal audit functions and year-one Sarbanes-Oxley programs, both domestically and abroad.

Additionally, Breslin has extensive fraud audit and investigation experience and has conducted major fraud investigations on multiple continents including large-scale federal cases domestically. She has developed and implemented fraud auditing programs in various industries focused on both accounting and operations.

“Association of Certified Fraud Examiners,” “Certified Fraud Examiner,” “CFE,” “ACFE,” and the ACFE Logo are trademarks owned by the Association of Certified Fraud Examiners, Inc. The contents of this paper may not be transmitted, republished, modified, reproduced, distributed, copied, or sold without the prior consent of the author.
Introduction
Internal Audit is uniquely positioned to help organizations fight fraud. If the average organization loses 5% of revenue to fraud, what if Audit could move the needle just one-half-of-one percent, from 5% to 4.5%, in your organization? How would that be for value-add?

Occupational Fraud
The Association of Certified Fraud Examiners defines “occupational fraud” as:

The use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization’s resources or assets.

The average organization loses 5% of revenue to fraud. Occupational fraud includes the intentional and wrongful obtainment of a benefit through:

- Theft or embezzlement
- False statements (documents, grants, applications)
- Corruption, kickback, conspiracies, collusion, bribes
- Misappropriation of assets (travel expenses, payroll, equipment)

Internal Auditors are uniquely positioned to help fight fraud from inside their organizations.

Why Internal Audit Is well Positioned to Fight Fraud
Internal auditors know the processes, the systems, the people and culture, the incentive programs and the opportunities. And are already in the organization… and looking. But to find fraud you must know what to look for. Traditional audit methods do not detect fraud, because they are not designed to. A standard audit catches less than 4% of existing frauds because audits are designed to test
effectiveness of controls and evaluate operating efficiency, not find fraud. And most controls are designed to prevent or detect errors, not fraud. Unfortunately, controls are frequently found to be working as intended during the most recent audit in many instances of fraud.

Auditors need to start embedding methods and techniques specifically designed to identify fraud into their programs. This session will show specific steps and methods that auditors can incorporate immediately into their audit programs to start detecting existing fraud in their organizations tomorrow.

- A look at why and how internal auditors can and should be identifying fraud within their organizations.
- Why fraud risk assessments are critical and how to perform them effectively.
- Learn specific tests and methods for identifying red flags and existing fraud that can be embedded into audit programs.
- How to analyze and evaluate internal incentive programs that could lead to fraud.

Some of the challenges auditors face when working to detect and prevent fraud include:

- Management Override
- Work Arounds
- Manual Processes
- Collusion
- Defining Fraud

One challenge is defining fraud for the organization. It is often easy to label an act “fraud” in hindsight, but many organizations and individuals struggle to call an act fraud when it is occurring. We frequently hear that acts and actions might be “bad business decisions” or “waste and abuse” but rarely do employees answer “yes” to the
question, “Are you aware of any fraud?” Defining fraud, knowing what to look for and what questions to ask are skills every auditor needs.

Collusion can render controls testing ineffective. Controls that are being circumvented through the collusion will appear to be working effectively even while a fraud is occurring. Traditional controls testing will not find fraud, and fraud specific techniques need to be used.

What if auditors could save their organizations just half of one percent of that 5%? What would your organization do with that money?

**Top Ten Things Auditors Should be Doing to Fight Internal Fraud**

1. **Learn the Fraud Basics**

   To fight fraud, you must understand fraud. Understand the fraud triangle and how it to use it to find and prevent fraud in your organization. In every instance of fraud, there was opportunity, there was pressure and there was rationalization. Spotting opportunity is easy for auditors – it’s what we do. Pressure is another area we can help.

   Pressure can be either real or perceived, but it is always real to the fraudster. It can also be either internal or external. Internal pressure is where we as auditors can help our organizations. We should be evaluating any pressures on employees that are created by the organization. Internal pressures can be negative or positive as well. Positive pressures could be through incentive programs such as commissions and bonus programs while negative pressures can be caused by mandatory targets in sales, collections, etc.
Rationalization is a bit more difficult for auditors, however understanding fraudster characteristics and combining that knowledge with other fraud knowledge can provide auditors with the insight on where to look for fraud.

The fraud tree is the basis for understanding fraud schemes. To understand where their organization is most likely to be susceptible to fraud requires understanding the known fraud schemes and combining that knowledge with systems, process, people and cultural knowledge for the organization. That is the basis for a fraud risk assessment.

2. Conduct Fraud Risk Assessments
Fraud Risk Assessments enable an organization, and an audit team to focus their fraud detection and prevention methods on the areas their organization is most likely to be susceptible to fraud. Fraud risk, just like all risk, that an organization is susceptible to is unique to each organization. An organization’s culture, business and industry, systems, process and people all combine to create a uniquely individual environment with risks specific to that environment. Without conducting a fraud risk assessment, you may be monitoring, auditing, and looking for fraud in the wrong places.

While it is best practice for an organization to conduct an entity-wide fraud risk assessment separately and distinctly from their Enterprise Risk Management Assessment (ERM) auditors can and should conduct their own fraud risk assessment on both and entity-wide and/or and engagement level.
3. **Know the Red Flags**

Conducting a fraud risk assessment includes not just understanding where your organization is susceptible to fraud but also brainstorming how those frauds might occur and what they would look like as a fraud scenario in your organization. Different frauds have different red flags and different approaches for detection. Learn what red flags you should be looking for if those scenarios occurred. For different fraud schemes, we may look for:

- The attributes of the actual fraud.
- Concealment of the fraud.
- Conversion of the fraudulent activity to benefit of the fraudster.
- Or what’s missing that would normally be found in a normal transaction or activity.

4. **Reconcile the Cash**

It should be obvious that the cash needs to be reconciled in every organization but it can be quite surprising how often reconciliations are either not performed or, not performed timely. Reconciliations not performed in a timely manner create an opportunity for fraud. It is much more difficult to resolve variances and outstanding items on a reconciliation if the issue is months, or worse, years old. A stunning 60% of internal frauds involve cash.

5. **Use Data Analytics**

The 16.5% of frauds that are being identified through internal audit groups that are actively looking for fraud are primarily detecting fraud through data analytics. Finding fraud manually can be about as easy as winning the lottery. Let a computer do the work. Automation and continuous fraud auditing can look at all transactions, something an auditor cannot do manually.
In addition to detecting and therefore stopping existing fraud, detection programs can be some of the strongest prevention programs. Knowing someone is actively looking for fraud in an area will be a very strong deterrence. Stopping a fraud before it occurs is the best fraud program there is.

Many audit departments start with some common analytics focused on common fraud areas such as accounts payable, vendor management, payroll and accounts receivables. These areas are good starting points for many reasons, including leveraging existing scripts in many data analytics tools and many experienced and knowledgeable data analysts and audit teams who share experiences and knowledge.

Once a fraud has been detected, data analytics can be an exceptional tool for the investigation to quantify impact. Identifying every instance related to a fraud strengthens the investigation and the case.

6. **Control Vendor Lists**

Preventing vendor related fraud by locking down the vendor master and who has access to the vendor master, is much easier than detecting vendor related fraud. This is an area where continuous auditing and monitoring are a real advantage. Monitoring all changes to vendor addresses, banking info, length of inactive time and invoice patterns will detect many frauds but will make it clear to everyone with access that the vendor master is being monitored. And that acts as a deterrent.

7. **Understand Fraudster Characteristics**

Unfortunately, fraudster characteristics include a wide array of behaviors that range from one end of the spectrum to the other. Fraudsters can be the most loyal...
and trusted employee who everyone loves or the exact opposite, someone who openly loathes the organization and complains incessantly. And everyone in between.

However, understanding the most commonly found fraudster characteristics and combining that knowledge with other red flags will help identify areas we should be looking into. Some of the more common traits can be a flashy lifestyle the individual can’t help but show off, or one who never takes time off, or people incredibly protective over their work, or unusual relationships with vendors or customers.

8. Vacation Policies
Employees who are very protective over their work, or never take days off are ensuring no one ever looks at their work. Fraudsters have to manage and control their fraud and having other employees have access, help, or fill in is too risky. When a company has a vacation policy that mandates a required amount of time off, it eliminates the ability to have complete control over who sees or has access to their work. Most of the time.

9. Do Your Homework
Nothing can damage an auditor’s credibility more quickly or deeply than announcing they have found a fraud, and be wrong. Auditors must be certain in their understanding of the difference between errors and actual fraud. People are still performing most activities and in an organization and they make mistakes.

A fear many auditors have is that of teaching individuals to commit fraud by pointing out opportunities for fraud and the potential related fraud scenarios. This does require a balanced approach and may warrant expedited action plans to close the gap.
10. Fraud Response Plan and Know Your Role

As auditors begin to actively detect and prevent fraud in their organization they need to establish a predetermined plan of action and identify:

- Who does what?
- Who is notified?
- Who is involved?
- When are others notified?

There are many things that can negatively impact a fraud investigation and fraud case and some are:

- Involving too many people in the beginning;
- Not involving the right people or departments;
- Not having the right skill set to do the forensic accounting;
- Not have the right skill set to conduct interviews or interrogations;
- Contaminating evidence; or
- Not being prepared for the authorities.

The role of internal audit during a fraud investigation varies from organization to organization. Understand what the expectation is in your organization and never overstep your authority or ability.