



# The Role of the Internal Auditor:

## Assessing and Responding to Fraud Risk

April 2026



# About the Anti-Fraud Collaboration

The Anti-Fraud Collaboration, a partnership composed of the Center for Audit Quality (CAQ), Financial Executives International (FEI), The Institute of Internal Auditors (IIA), National Association of Corporate Directors (NACD), and Association of Certified Fraud Examiners (ACFE), is dedicated to advancing the discussion of critical anti-fraud efforts through the development of thought leadership, awareness programs, educational opportunities, and other related resources focused on enhancing the effectiveness of financial fraud risk management.



The CAQ champions the public interest in the capital markets by:

- ✦ Elevating the quality, credibility, and transparency of public company audits;
- ✦ Advancing critical issues affecting public company audits;
- ✦ Driving innovation in assurance; and
- ✦ Providing a collaborative forum for capital market stakeholders to address evolving needs and challenges.

As the voice of the public company audit profession, we work to instill trust in corporate reporting and the integrity of the auditing process, ultimately empowering investors, companies, and society as a whole. For more information, visit [www.thecaq.org](http://www.thecaq.org).



Financial Executives International (FEI) is the leading association and advocate for the views of corporate financial management. Its members hold policy-making positions as chief financial officers, chief accounting officers, controllers, treasurers, and tax executives at companies in every major industry. FEI enhances Member professional development through peer networking, career management services, conferences, research, and publications. Members participate in the activities of local Chapters in the U.S. FEI is located in Morristown, NJ. Visit [www.financialexecutives.org](http://www.financialexecutives.org) for more information.



The Institute of Internal Auditors (The IIA) is an international professional association that serves more than 260,000 global members and has awarded more than 200,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit [www.theiia.org](http://www.theiia.org).



The National Association of Corporate Directors (NACD) empowers more than 20,000 directors to lead with confidence in the boardroom. As the recognized authority on leading boardroom practices, NACD helps boards strengthen investor trust and public confidence by ensuring that today's directors are well-prepared for tomorrow's challenges. World-class boards join NACD to elevate performance, gain foresight, and instill confidence. Fostering collaboration among directors, investors, and corporate governance stakeholders, NACD has been setting the standard for responsible board leadership for 40 years. To learn more about NACD, visit [www.NACDonline.org](http://www.NACDonline.org).



The Association of Certified Fraud Examiners (ACFE) is the world's largest anti-fraud organization. By delivering best-in-class training, offering the CFE credential and fostering a dynamic, global community of anti-fraud professionals, the ACFE is reducing fraud and corruption worldwide. For more information, visit [www.acfe.com](http://www.acfe.com).

This publication is intended as general information and should not be relied on as being definite or all-inclusive. As with all other Anti-Fraud Collaboration (AFC) resources, this publication is not authoritative, and readers are urged to refer to relevant rules and standards. If legal advice or other expert assistance is required, the services of a competent professional should be sought. The AFC and its member organizations make no representations, warranties, or guarantees about, and assume no responsibility for, the content or application of the material contained herein. The AFC expressly disclaims all liability for any damages arising out of the use of, reference to, or reliance on this material. This publication does not represent an official position of the AFC or its member organizations, their respective boards, or their members.

© 2026 Anti-Fraud Collaboration. All Rights Reserved.

# Contents

4

**Executive Summary**

5

**Introduction**

6

**What Is Internal Audit's Responsibility for Assessing and Responding to Fraud Risk?**

8

**Why Is Professional Skepticism Important in Assessing and Responding to Fraud Risk?**

10

**How Can Internal Auditors Exercise and Maintain Their Professional Skepticism?**

12

**How Do Internal Auditors Consider Management's Fraud Risk Assessment?**

15

**Why Do Internal Auditors Perform Fraud Brainstorming?**

17

**How Do Internal Auditors Apply the Fraud Triangle?**

19

**Why Is Fraud Training Important for Internal Auditors?**

21

**How Do Internal Auditors Distinguish Fraud from Error?**

22

**Conclusion**

# Executive Summary

Fraud risk remains a persistent and evolving threat to organizations of all sizes and industries, driven by geopolitical uncertainty, increasing complexity in business models, rapid technological change, and heightened economic and regulatory pressures. As trusted providers of independent and objective assurance, internal auditors play a critical role in helping organizations assess, manage, and respond to fraud risk. This publication examines the internal auditor’s responsibilities in addressing fraud risk, as defined by the *Global Internal Audit Standards*, and highlights practical considerations for executing that role effectively.

The publication explores how internal auditors contribute to fraud deterrence by evaluating the adequacy and effectiveness of fraud risk governance, management processes, and internal controls. It emphasizes the importance of professional skepticism as a foundational competency in identifying fraud risks, challenging assumptions, and assessing the reliability of information provided by management and other stakeholders. Through real-world examples, the publication illustrates how skepticism, data analysis, and persistence can uncover control deficiencies and fraudulent activity that might otherwise go undetected.

Key topics include how internal auditors evaluate management’s fraud risk assessment, incorporate fraud considerations into audit planning, and conduct fraud brainstorming to identify potential schemes and vulnerabilities. The publication also discusses the application of the fraud triangle—pressure, opportunity, and rationalization—as a framework for understanding how and why fraud occurs and highlights the areas where internal audit can most directly reduce fraud risk, particularly by strengthening controls that limit opportunity.

Finally, the publication underscores the importance of ongoing fraud training, collaboration with fraud specialists, and a strong organizational culture that encourages transparency and questioning. By maintaining professional skepticism, enhancing fraud awareness, and continuously developing their competencies, internal auditors can provide meaningful assurance and insight that helps organizations prevent, detect, and respond to fraud more effectively.

## FRAUD

Any intentional act characterized by deceit, concealment, dishonesty, misappropriation of assets or information, forgery, or violation of trust perpetrated by individuals or organizations to secure unjust or illegal personal or business advantage.

Source: *The Institute of Internal Auditors’ Global Internal Audit Standards*

U.S. publicly traded companies lost a median 1.06% of annual revenue to known frauds in 2024, consistent with levels in recent years.

Source: *The Impact of Fraud at U.S. Public Companies Benchmarking Report*, the Association of Certified Fraud Examiners (ACFE) and the Anti-Fraud Collaboration (AFC).

# Introduction

## OVERVIEW OF THE FRAUD LANDSCAPE

Fraud is one of the top six audit priorities for internal auditors across the globe, according to The Internal Audit Foundation's [2026 Global Risk in Focus](#). Some fraud risks are associated with sophisticated technologies, such as cybersecurity and digital disruption. At the same time, fraud can also be perpetrated using basic schemes involving forged signatures, checks, or documentation. In any case, the losses involved can be meaningful. In one year, 1,921 cases of fraud in 138 countries caused total losses of \$3.1 billion, based on the most recent [data](#) from the Association of Certified Fraud Examiners (ACFE).

According to The Institute of Internal Auditors' Global Practice Guide, [Internal Auditing and Fraud: Assessing Fraud Risk Governance and Management at the Organizational Level](#), "the internal audit function contributes to fraud deterrence by providing assurance on the adequacy and effectiveness of fraud risk governance and management and advises on opportunities for improvement." This publication examines several key factors involved with internal audit's role in assessing and responding to fraud risk.

## USE AND INTENDED AUDIENCE

This publication provides insights into practices, guides, and considerations that can help internal auditors maintain their professional skepticism and overall approach to assessing and responding to the risks of material misstatement resulting from fraud during the internal audit. It also provides clarity and understanding of the internal auditor's current role and responsibilities related to fraud, which may provide insights for those who are involved in evaluating and using financial reporting information as well as for policymakers and regulators. Although the term *professional skepticism* has a specific definition within the standards that regulators set for internal auditors, the perspectives in this publication are intended to inform all members of the financial reporting ecosystem.

Two-thirds of ACFE and AFC survey respondents believe fraud levels at U.S. public companies have risen in recent years, with more than 70% rating the current level of fraud as medium or high and two-thirds expecting continuing increases in fraud levels.

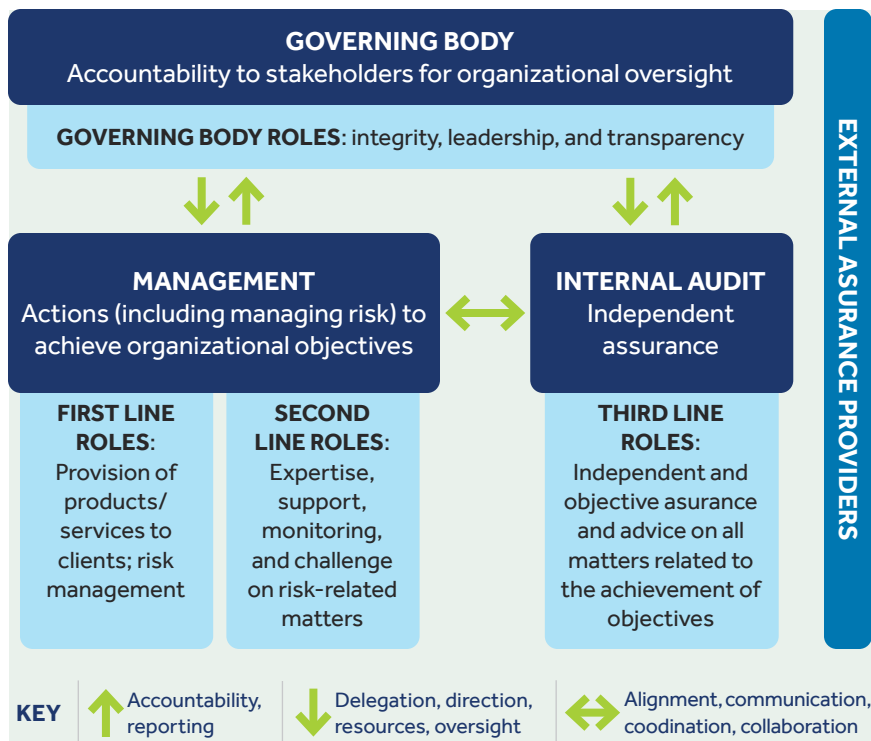
Source: [The Impact of Fraud at U.S. Public Companies Benchmarking Report](#), ACFE and AFC.

# What Is Internal Audit’s Responsibility for Assessing and Responding to Fraud Risk?

Organizations face growing complexity in managing fraud risk, and internal auditors are expected to provide assurance that such risks are properly identified and managed. As such, internal audit has a critical role in assessing and responding to fraud risk as set forth in professional standards, especially *The Institute of Internal Auditors (IIA) Global Internal Audit Standards*.

Internal audit’s responsibilities are clearly recognized in the marketplace. Investors believe that internal auditors hold the primary responsibility for preventing and detecting fraud, according to a [Center for Audit Quality and KRC Research](#) survey . This aligns with the results of an [ACFE/AFC survey](#) in which internal audit topped the list of choices as most likely to “own” fraud at the public companies at which or with whom respondents work. Additionally, the ACFE found in a separate [study](#) that the presence of an internal audit department reduced fraud by a median of 43% and shortened fraud duration by 50%.

Internal audit’s role is established in the Three Lines Model.<sup>1</sup>



**Domain 1: Purpose of Internal Auditing** states that “internal auditing strengthens the organization’s ability to create, protect, and sustain value by providing the board and management with independent, risk-based, and objective assurance, advice, insight, and foresight.”

**Standard 11.1 Building Relationships and Communicating with Stakeholders** indicates under the Considerations for Implementation that discussions, along with surveys, interviews, and group workshops, are useful tools for obtaining input, especially on fraud and emerging risks.

*Global Internal Audit Standards*

<sup>1</sup> Refer to *The IIA’s Three Lines Model – An Update of the Three Lines of Defense*.

As the chart shows, as the provider of independent, objective assurance and consulting, internal audit's role is to identify and monitor fraud risks. As part of its audits and investigations, internal audit evaluates the potential for fraud and how the organization manages fraud risk.

As part of its audits and investigations, internal audit evaluates the potential for fraud and how the organization manages fraud risk.



# Why Is Professional Skepticism Important in Assessing and Responding to Fraud Risk?

For internal auditors to effectively assess and respond to fraud risk, it is important that they exercise professional skepticism. As the IIA standards note, professional skepticism enables internal auditors to make judgments based on facts, information, and logic. Skepticism removes the uncertainties related to complete trust or belief. It is the attitude of questioning or doubting the validity and truthfulness of claims, statements, documentation, and other information, thereby increasing the potential to discover fraud.

Conducting internal audits involves discussions with management and auditees about their processes and activities. Internal auditors use professional skepticism in the evaluation of the claims and explanations they receive in those discussions and make their own independent judgments to determine what is truly valid.

Exercising professional skepticism is important when it comes to fraud, says Eileen Iles, Principal, Financial Institutions Group, Doeren Mayhew Advisors, LLC, Chicago. Without it, internal auditors may miss not only red flags associated with fraud but also more subtle indicators that something is wrong, she says.

## REAL-WORLD EXAMPLE: PROFESSIONAL SKEPTICISM

In one case in which the facts didn't seem to add up, Iles's skepticism led to a determination that controls were deficient. In examining system-generated reports, the internal auditors found an unusual volume of corrections, adjustments, and reversals. Iles had to question whether the person involved was sloppy or if the corrections, adjustments, and reversals were intentional, possibly fraud. Throughout the process, the person responsible for the area being audited was insistent that there were no problems.

Because of the individual's behavior, the team began to wonder about their past experience and sought to learn more about their qualifications for the job. No resume was available, and their discussion of previous jobs was vague. The internal auditors finally turned to LinkedIn, where the person's experience was simply listed as "entrepreneur." It turned out that the individual had minimal experience related to their current role and position.

**Standard 4.3 Professional Skepticism** requires that "internal auditors must exercise professional skepticism when planning and performing internal audit services." To exercise professional skepticism, internal auditors must:

- ▶ "Maintain an attitude that includes inquisitiveness.
- ▶ Critically assess the reliability of information.
- ▶ Be straightforward and honest when raising concerns and asking questions about inconsistent information.
- ▶ Seek additional evidence to make a judgment about information and statements that might be incomplete, inconsistent, false, or misleading."

*Global Internal Audit Standards*

Given their growing doubts, the internal auditors continued to investigate. They decided to test a larger sample of the records involved and discovered intentional wrongdoing. They found that the individual had intentionally structured transactions to benefit themselves, their relatives, and other individuals. The individual had access to systems that allowed them to execute transactions, set up accounts, perform changes, and approve transactions. This lack of separation of duties was key to allowing this individual to structure transactions in their favor. Iles notes that a stronger vetting process during hiring and a control structure with appropriate monitoring and segregation of duties could have prevented the problem.

Fraud awareness is a crucial foundation of professional skepticism. It can lead to earlier discovery of fraud and minimize the financial impact, according to Anne DeTraglia, an internal audit and risk executive. “If employees are working in an environment in which they believe fraud cannot occur, then they aren’t paying attention to red flags that point to fraud,” she says.

During the walkthroughs and in interviewing first-line management or operations staff, internal auditors should trace specific transactions or processes to identify what controls they are subject to and to spot potential risks and weaknesses within a company’s operations, says Naohiro Mouri, Chair of the Audit and Advisory Committee at the United Nations Office for Project Services. Throughout this process, internal auditors scrutinize the information they are given to look for anomalies or unusual results, he says.

### **REAL-WORLD EXAMPLE: PROFESSIONAL SKEPTICISM**

In examining a reconciliation as part of an audit, Iles’s team noticed several reconciling items. These were unexpected because reconciling items for the account typically cleared within one to three days. Iles’s team also noticed that several of the items were missing dates and descriptions. When her team asked for more information, the auditee did not respond to numerous requests. “When they’re not responding, that’s a red flag,” says Iles.

Finally, the auditee responded, indicating that the reconciling items were related to expired transactions and, hence, were no longer collectible. Further investigation by the internal auditors revealed that the items in question totaled over \$2 million and had been on the reconciliation for more than seven years. The individuals involved had been consistently masking the uncollected receivables by recording journal entries to the general ledger account so that the reconciling items appeared to be different items each period rather than the same items.

Fraud awareness is a crucial foundation of professional skepticism. It can lead to earlier discovery of fraud and minimize the financial impact.

# How Can Internal Auditors Exercise and Maintain Their Professional Skepticism?

Among other things, maintaining professional skepticism includes being aware of the many surprising factors that can challenge skepticism and make it more difficult for internal auditors to retain arms-length independence. It can be difficult to maintain professional skepticism in many cases because the person or team being audited is knowledgeable about their area and in a position of authority. It may seem natural to assume that what they say is correct. Iles recommends a “trust but verify” stance, in which the necessary reliance on the information supplied by the team being audited doesn’t cloud the internal auditor’s ability to make an objective evaluation.

Internal auditors should also consider the impact that culture can have on professional skepticism and fraud, DeTraglia says. Internal auditors may be aware that employees can feel pressure to commit fraud in a high-stress environment or when there is pressure to not make mistakes. That can be the case when employees are expected to meet high sales targets or revenue goals, for example. Difficult work environments are another warning sign, she notes, including superiors who are abusive to their people, fail to share information with their teams, or refuse to take vacations because they have secrets to hide.

Although organizational loyalty and trust are considered positive attributes, they can discourage employees from spotting fraud or asking questions when something doesn’t seem right. In one company, DeTraglia found that the level of loyalty and trust was such that everyone, from the CEO on down, shared their passwords with their assistants. Unfortunately, several assistants were let go every year because they used those passwords to make inappropriate purchases on their supervisors’ accounts.

Another key consideration is differentiating between skepticism and cynicism. Cynicism about perceived problems in the work environment may cause employees and even internal auditors to miss warning signs or fail to recognize fraud, according to DeTraglia, because they have decided that cutting corners is part of the culture in their organization. Another danger is when internal auditors slip into what Iles refers to as “checklist mode.” This may occur when an internal audit team focuses on getting procedures done without being alert to potential problems or asking sufficient questions. In these cases, they may miss identifying areas that merit further examination.

**Standard 14.1 Gathering information for Analyses and Evaluation** states that “internal auditors use professional skepticism to evaluate whether information is reliable.”

**Standard 14.1 Considerations for Implementation** says, “In applying professional skepticism, internal auditors should critically assess whether the information is factual, current, and obtained directly (such as by observation) or from a source independent of those responsible for an activity under review.”


*Global Internal Audit Standards*

### **REAL-WORLD EXAMPLE: PROFESSIONAL SKEPTICISM**

When looking for fraud, it's always a good idea to follow the money. Internal auditors don't have to understand the details of every transaction, but they should look for ways in which the process could have been circumvented, Mouri says. When internal auditors understand the business well, they should be able to see when facts and figures aren't adding up.

In examining traders in a bank, for example, internal auditors might challenge results that are consistently positive. "Good traders win probably 60% to 70% of the time, but they lose 30% to 40% of the time," Mouri says. If the results show few or no losses, questions should be asked, including why risk managers did not spot unusual results.

When internal auditors understand the business well, they should be able to see when facts and figures aren't adding up.



# How Do Internal Auditors Consider Management's Fraud Risk Assessment?

Understanding management's fraud risk assessment, including anti-fraud processes and controls and the operation and results of monitoring activities, can be helpful to internal auditors in considering where and how fraud could occur, Iles says.

The *Internal Auditing and Fraud Global Practice Guide* provides questions aligned with the Committee of Sponsoring Organizations of the Treadway Commission ("COSO") *Fraud Risk Management Guide* for internal auditors to consider when assessing an organization's fraud risk management program. The questions focus on the following elements:

- ▶ Control environment
- ▶ Risk assessment
- ▶ Control activities
- ▶ information and communication
- ▶ Monitoring activities

According to Global Internal Audit Standard 9.4 Internal Audit Plan, Considerations for Implementation, "The internal audit function should only rely on management's information about risks if it has concluded that the organization's risk management processes are effective." Internal auditors should apply their critical thinking and professional skepticism in evaluating the adequacy and accuracy of management's fraud risk assessment.

Management will often acknowledge the existence of risk, but it may take a higher-level view of risk than internal audit would, according to Iles. It may, for example, insist that risk in one area is low because fraud has never been discovered there before. "That doesn't mean that it can't happen," she says. Management may point to controls that address the level of risk as management perceives it and, as a result, incorrectly perceive that fraud risk has been addressed. Internal audit results of testing anti-fraud processes and controls are good feedback for management to incorporate in its assessment of fraud risk.

Management may use data analysis in performing their fraud risk assessment. It can also be a powerful tool to help internal auditors validate management's risk assessment and scope their audits. Often, fraud risk assessments are performed via interviews and workshops.

**Standard 9.4 Internal Audit Plan** requires that the chief audit executive base the internal audit plan on a documented assessment of the organization's strategies, objectives, and risks.

**Standard 13.2 Engagement Risk Assessment** states "internal auditors must identify the criteria that management uses to measure whether the activity is achieving its objectives."

*Global Internal Audit Standards*

Risk levels may be set based on subjective information. Data analysis could help identify potential hidden fraud schemes not identified or discussed through interviews or workshops. Data analysis may also detect trends, anomalies, and outliers of the population of transactions, indicating manual overrides, policy exceptions not reported, and ineffective separation of duties. Further, data analysis may assist internal audit in planning their audits once risks have been identified.

### **REAL-WORLD EXAMPLE: DATA ANALYSIS**

Consider an example of a bank that has a significant portfolio of commercial loans, which typically have inherently higher risk than consumer loans. Internal audit can use data analysis to identify the percentage of loans held in the bank's portfolio and determine which commercial loan products have greater risk, breaking the numbers down in a way that management may not have done, according to Iles. Risk assessment should convey and quantify the relative risk exposure, such as structure and collateral of the loan, borrower credit, geography, and loan type, to name a few. The portfolio size may not be as important as the risks related to the loans in that portfolio, in other words. This is an opportunity for internal audit to enhance its risk-based audits in a way that is meaningful and valuable, Iles said.

In another situation, a retail business may have a small amount of credit that is highly delinquent, a situation that could impair its cash flow, hurt its credit standing, and damage supplier relationships. By analyzing the relevant data, internal audit may find that a relatively smaller debt portfolio with a higher likelihood of default could have an outsized impact on the business, she says.

Internal auditors examine a wide range of data to understand the overall risk environment and the adequacy of existing controls. The internal auditor's job, Iles notes, is to challenge the risk assessment and the assumptions used in making that assessment based on the work done during the audit. That includes examining controls, fraud awareness, and mitigation steps across the organization, as well as the organization's inherent risk. If controls aren't effective, it will be impossible to reduce inherent risk, Iles says. When effective controls are applied to inherent risks, what's left are the residual risks.

In some cases, internal audit may suspect that management itself is involved in fraud. In that situation, internal audit must gather concrete evidence to support that belief, Mouri says. He recommends bringing the evidence to the company's general counsel to consider its validity and any legal implications.


Although management may have a strong grasp of daily operations, perform an effective risk assessment, and appropriately identify potential weaknesses or risk areas, internal auditors can dig deeper, Iles notes. If

Internal auditors examine a wide range of data to understand the overall risk environment and the adequacy of existing controls.

the department is involved in payroll processing, for example, internal audit needs to understand who's involved in the processes, including everything from who approves employees' time entries to how payroll is processed and checks are cut to the controls over direct deposits. This detailed understanding might allow the internal audit review to identify a bad actor who has been able to falsely inflate their hours because there is insufficient oversight of time entry or when a wrongdoer has changed information on a manual or digital payroll file and diverted payroll funds to an account they have created.

"There's a lot of detail involved at every step of the process, and each step could be a weakness or an opportunity," Iles says. For that reason, it's important to dig into details, whether files are manual or automated.

There's a lot of detail involved at every step of the process, and each step could be a weakness or an opportunity.



# Why Do Internal Auditors Perform Fraud Brainstorming?

In addition to considering management's risk assessment when evaluating when and how fraud can occur, internal auditors also perform fraud brainstorming. Fraud brainstorming is an exercise that asks "What's the worst that could happen?" according to Mouri. Fraud brainstorming begins in the audit planning session. Internal audit team members consider the ways in which fraud could occur based on the team's understanding of the organization and examples of fraud at other organizations. The process considers how someone could intentionally misstate, steal, or conceal.

As an example of considering fraud schemes that have been perpetrated at other organizations, Mouri recommends examining any area where payments are involved. As noted, fraud risks in these areas include weak controls over access to accounts and lack of segregation of duties. Internal auditors should also consider people who are authorized to make decisions and whether they might be subject to the three points of the Fraud Triangle: pressure, opportunity and rationalization

Effective fraud brainstorming involves active participation from members of management and internal audit of all levels of experience, Iles says. Internal auditors should assume that fraud can occur at any organization and can be perpetrated by individuals across the organization.

The best fraud brainstorming occurs when business partners are included in the process, according to DeTraglia. As part of internal audit's annual risk assessment, her team conducts fraud workshops that include brainstorming. "You learn so much about the business in these workshops," she says. "It's incredibly enlightening." The learning includes not only potential fraud schemes but also much about culture, including the business function's fraud awareness and its attitudes toward fraud.

According to DeTraglia, asking the business partners how fraud would occur is not sufficient. "Control owners typically don't believe a fraud is occurring in their function," she says. Instead, internal auditors can uncover valuable information by asking:

- ▶ Have you ever seen this control process done differently?
- ▶ How would you do it differently?
- ▶ Could you do it differently?

These questions can reveal ways to strengthen controls and perhaps also identify ways that a bad actor might subvert them.

**Standard 13.2 Engagement Risk Assessment** states, "Internal auditors must identify the risk to review by:


- ▶ "Identifying the potentially significant risks to the objectives of the activity under review.
- ▶ Considering specific risks related to fraud.
- ▶ Evaluating the significance of the risks and prioritizing them for review.

Internal auditors must identify the criteria that management uses to measure whether the activity is achieving its objectives."

*Global Internal Audit Standards*

Mouri pointed out that generative AI can be a powerful tool to use in developing potential risk scenarios as part of fraud brainstorming. Generative AI can provide information and comparisons with past fraud occurrences in a particular industry or business and potential fraud vulnerabilities in the business. Users can then probe deeper for more ideas or insights, he notes. This can be especially useful to newer auditors.

Generative AI  
can provide  
information and  
comparisons  
with past fraud  
occurrences in a  
particular industry  
or business and  
potential fraud  
vulnerabilities in  
the business.



# How Do Internal Auditors Apply the Fraud Triangle?

Internal auditors might apply the fraud triangle during fraud brainstorming sessions and throughout other internal audit procedures. When assessing and responding to fraud risks, internal auditors can leverage the fraud triangle to consider specific risks of material misstatement from fraud and to design audit responses tailored to those risks.

The fraud triangle describes the factors that accompany a fraud:

- ▶ **Incentive or pressure**, such as debt that the person must repay or another significant financial need. Pressure may also be associated with the demands of a job or the culture of a department. Among other steps, Mouri examines areas where people are expected to bring in profits, such as at a trading desk or on a sales team. “There is constant pressure to make money every day,” he says. These employees may, for example, set up fake transactions to meet profit goals. “We always look at sales and cancellations,” he says. “When someone’s sales numbers keep going up, we ask how they are doing it.”
- ▶ **Opportunity**, or a weakness in the control system that enables fraud. As an example, opportunity can occur if there is inadequate segregation of duties, Mouri says. If no one is reviewing how money is being spent, those authorizing payments have the chance to make improper outlays. Weak controls may make it possible for an employee to steal from general ledger accounts, take home office supplies or equipment, or engage in fictitious reporting on financial documents.
- ▶ **Rationalization**, or some imagined justification for fraud, such as perceived unfairness from the boss or company. An employee may believe they have been unjustly denied a promotion or raise, for example, or they may decide it is fair to steal because the company or its owners can afford it.

Among the three points of the triangle, opportunity is likely the one that internal auditors can most directly affect, Iles notes. They do so by ensuring that the right controls are in place and that they are properly implemented so that opportunity is less likely to occur. If existing controls aren’t adequate, internal auditors recommend new ones and offer advice to improve implementation of existing controls. Iles typically begins her audit planning process with interviews. It’s not possible to audit what you do not understand or are not aware of. Understanding the processes allows internal audit to be prepared to audit the right risks, test the right controls, and deliver real value.


It can be more difficult to identify whether someone is under the kind of pressure that will lead them to commit fraud, but process walkthroughs

**Standard 4.2 Due Professional Care** states that “internal auditors must exercise due professional care by assessing the nature, circumstances, and requirements of the services to be provided, including ... probability of ... fraud.”

*Global Internal Audit Standards*

can help. In these walkthroughs, the internal auditor may hear that the department or company has set lofty goals, such as opening a significant number of accounts or bringing in a certain level of customers in a short time. The fact that the team may feel pressure under these circumstances doesn't indicate the presence of fraud, but it is important information to keep in mind, Iles says. Internal audit may audit new accounts to determine whether related information is valid, accurate, and complete and preventative internal controls, such as separation of duties and system user access, are effectively designed and operating.

Internal audit  
may audit  
new accounts  
to determine  
whether related  
information is  
valid, accurate,  
and complete  
and preventative  
internal controls,  
such as  
separation of  
duties and system  
user access,  
are effectively  
designed and  
operating.



# Why Is Fraud Training Important for Internal Auditors?

As fraud schemes continue to evolve, it is important that all internal auditors, including less experienced ones, be trained in their role in assessing and responding to fraud risks and how they can execute this role, including identifying behavioral red flags associated with fraud, more effectively. Internal auditors are not expected to have the expertise of a person whose primary responsibility is to investigate fraud, but they still must keep current on new and emerging fraud risks in the face of constant innovation from bad actors, Mouri says. They must know the business well enough to spot results or actions that seem out of line. Their training should include insights on how fraudsters cheat or steal and, in particular, new methods fraudsters use to develop more effective schemes.

Dedicated fraud training should be part of an internal audit team's annual plan, according to DeTraglia. Her team has fraud awareness training at least twice a year. At her team's "Audit University," and during their annual fraud risk assessment, internal auditors meet with their business partners and try to imagine possible fraud schemes. She reminds the business partners that, when considering situations in which risks exceed the appetite, "fraud has no materiality." In other words, most fraud cases start out small and grow over time. Convicted fraudsters typically don't begin by stealing large sums. Instead, they begin slowly, realize that they can get away with fraud, then repeat it over time. Ultimately, it explodes into large sums. As a result, there is no such thing as an immaterial or de minimis fraud because all frauds have the potential to grow, she says.

Internal audit team leaders should also create an environment that encourages asking questions related to fraud because it can elevate less experienced auditors' fraud awareness and empower them to raise concerns.

## BEHAVIORAL RED FLAGS ASSOCIATED WITH FRAUD

In ACFE surveys, respondents consistently identify six red flags as the most common indicators of people involved in fraud:

- ▶ Living beyond one's means: Having signs of affluence that are not consistent with their known income.
- ▶ Financial difficulties: Someone with financial problems may be more likely to commit fraud.
- ▶ Unusually close association with a vendor or customer: This may indicate a conflict of interest or collusion.

**Standard 3.1 Competency** notes that "internal auditors should develop competencies related to ... pervasive risks, such as fraud."

**Standard 3.2 Continuing Professional Development** says "internal auditors must maintain and continually develop their competencies to improve the effectiveness and quality of internal audit services. Internal auditors must pursue continuing professional development including education and training."

**Standard 11.5 Communicating the Acceptance of Risks** states, in Considerations for Implementation, "when risks exceed the risk appetite, impacts may include ... conflicts of interest, fraud, or other illegal acts."

*Global Internal Audit Standards*

- ▶ Excessive control issues or unwillingness to share duties: A lack of transparency at work and reluctance to delegate can be indicators that someone is trying to hide fraudulent activity.
- ▶ Irritability, suspiciousness, or defensiveness: Someone who has become more aggressive or defensive may be feeling the strain of concealing fraudulent behavior.
- ▶ A general “wheeler-dealer” attitude involving shrewd or unscrupulous behavior: People who seem more open to cutting corners or ignoring the rules may be more likely to engage in fraud.

Source: [ACFE](#).

### LEVERAGING FRAUD EXPERTISE

“The internal auditor should not be expected to have the expertise of a person whose primary responsibility is to investigate fraud. Such investigations are best carried out by those experienced to undertake such assignments. Internal audit should use its expertise to analyze data sets to identify trends and patterns that might suggest fraud and funding abuse. Where the experience is not available within the internal audit team, the organization should consider recruiting or engaging resources with sufficient knowledge or expertise....”

“Operationally, internal audit should have sufficient knowledge of fraud to:

- ▶ Identify red flags indicating fraud may have been committed.
- ▶ Understand the characteristics of fraud and the techniques used to commit fraud, and the various fraud schemes and scenarios.
- ▶ Evaluate the indicators of fraud and decide whether further action is necessary or whether an investigation should be recommended.
- ▶ Evaluate the effectiveness of controls to prevent or detect fraud.”

Source: IIA Position Paper *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*.

Internal audit should use its expertise to analyze data sets to identify trends and patterns that might suggest fraud and funding abuse.

# How Do Internal Auditors Distinguish Fraud from Error?

Providing adequate fraud training for internal auditors is vital not only for the aforementioned reasons but also so that they can distinguish fraud from error in practice. According to *Internal Auditing and Fraud*, unlike in cases of negligence, “perpetrators of fraud intentionally seek to take advantage of circumstances by exploiting weaknesses in controls, either because they are under duress or for personal gain.”

Intent is the crucial differentiator between error and fraud, DeTraglia notes. Frequency is another key factor. “Did it occur once or are we seeing a pattern?” she asks. Frequency concerns also include how long the employee has been in a role because their experience over time may have helped them determine how best to engage in and conceal fraud. This is particularly true if others in the organization don’t understand how to perform the fraudster’s role or don’t closely supervise their actions.

Reluctance to address an error is another red flag, according to Iles. “Usually, when people make errors, they’re quick to want to fix them,” she says. “And they typically have a logical explanation for the oversight.” Those engaged in fraud may attempt to justify or excuse the error to draw attention away from it.

**Standard 14.3 Evaluation of Findings** states that “internal auditors must evaluate each potential engagement finding to determine its significance. When evaluating potential engagement findings, internal auditors must collaborate with management to identify the root causes when possible, determine the potential effects, and evaluate the significance of the issue.”

*Global Internal Audit Standards*

# Conclusion



Even when organizations and their internal auditors can uncover fraud, they should remain consistently vigilant to minimize damage from undiscovered fraud. Unfortunately, concealment is a key element of any fraud. As a result, notes the ACFE, known frauds are not necessarily indicative of the level of wrongdoing within an organization. An uncertain economic and political climate and the disruptions caused by new and emerging technologies have created an environment that can make it easier and perhaps more tempting to commit and hide fraud.

With those considerations in mind, internal auditors should be alert to the possibility of fraud and understand their role in identifying not only fraud but the circumstances that can allow it to occur. By exercising their professional skepticism and through consistent fraud training, internal auditors can provide insightful and effective guidance to the business functions and organizations with which they work.

When asked to rate the likelihood and significance of six categories of fraud, respondents believed:

- ▶ Frauds considered most likely to occur included external frauds, such as cyberfraud—which was also considered the most significant fraud risk overall—as well as customer payment fraud and fraud by vendors and sellers.
- ▶ Least likely risks cited were internal frauds (i.e., those perpetrated by individuals inside the organization), such as financial statement fraud, bribery and corruption, and asset misappropriation/embezzlement. Note that although financial statement fraud was considered least likely to happen, the impact of such frauds that did occur was expected to be significant.

Source: *The Impact of Fraud at U.S. Public Companies Benchmarking Report*, the ACFE and the AFC.

An uncertain economic and political climate and the disruptions caused by new and emerging technologies have created an environment that can make it easier and perhaps more tempting to commit and hide fraud.





The Institute of  
**Internal Auditors**

[www.theiia.org](http://www.theiia.org)

**CAQ**

[www.thecaq.org](http://www.thecaq.org)

 **AFC**

[www.antifraudcollaboration.org](http://www.antifraudcollaboration.org)

**We welcome  
your feedback!**

Questions or comments?  
Visit [antifraudcollaboration.org/contact](http://antifraudcollaboration.org/contact)