ACCOUNTING
CONTINUING EDUCATION

Identifying and Addressing the Risk of Fraud in Nonprofit Organizations

(IAR4)

KAPLAN

Identifying and Addressing the Risk of Fraud in Nonprofit Organizations

(IAR4)

Marci Thomas, MHA, CPA, CGMA

KAPLAN®

Identifying and Addressing the Risk of Fraud in Nonprofit Organizations (IAR4)

Published in 2023 by Kaplan Financial Education.

ISBN: 978-1-0788-3428-5

CONTENTS

NOTES

UNIT 1

Introduction

LEARNING OBJECTIVES

When you have completed this unit, you will be able to accomplish the following:

- Identify the types of potential frauds that could occur in not-for-profit organizations.
- Understand the risk of fraud in not-for-profit organizations.

INTRODUCTION

The risk of fraud is not a recent one. It took center stage when massive corporate frauds came to light in the early 2000's and "Public Company Accounting Reform and Investor Protection Act" (Senate) and "Corporate and Auditing Accountability, Responsibility, and Transparency Act" (House of Representatives), otherwise known as the Sarbanes Oxley Act was enacted. The root cause of the high-profile frauds uncovered at Enron, WorldCom, Tyco International, Adelphia, and others was addressed in the Act highlighting the responsibilities of a public company's board of directors for oversight and adding criminal penalties for certain misconduct including retaliation against whistle blowers.

The requirement for most public companies (large and accelerated filers) to undergo an integrated audit of their financial statements and internal control may not have caused the same requirements for not-for-profit organizations, however, the trickle-down effect has been felt for all nonpublic organizations, given the new audit standards requiring additional focus by the auditor on the understanding of internal control, assessing the risk of fraud and significant unusual transactions.

Fraud is also present in not-for-profit organizations and other nonpublic organizations but since the impact of fraud does not affect as many people, it is not as visible. To those organizations affected, however, the impact can be devastating. Fraud has resulted in tarnished reputations, loss of donors and federal funding, not to mention misappropriated assets.

An area of fraud that has risen to the top of the radar screens of management and boards is cyber fraud (also referred to as cybercrime). This has become a significant issue due to the extent of occurrences and magnitude of losses on the parts of organizations of all sizes. The challenge is that perpetrators that commit these sorts of crimes against organizations continue to evolve their methods and techniques more quickly than the victims can adjust their defenses.

Price Waterhouse Coopers (PWC) releases a Global Economic Crime and Fraud Survey[1] (PWC Survey) in 2022, which provided some surprising results. Based on the results of the survey the reported rate of fraud at 49%, unchanged from its 2018 survey. This was unexpected due to supply chain issues, an uncertain economy and talent shortages.

Environmental, financial, and social pressures are creating a risk landscape that is more volatile than ever, complicating the challenge of preventing fraud and other economic crimes. While organizations respond to changing circumstances as quickly as they can to navigate change, perpetrators look for ways to exploit the situation.

Another surprise noted in the survey was that even though approximately 46% of organizations will encounter fraud at some level, misappropriation of assets, the largest category of fraud, was down. The survey suggested that this is because more employees are working remotely, with limited access to company assets. Digital security continues to be of heightened risk due to employees working remotely.

Lessons learned from the 2007–2009 economic downturn illustrate that the effects of a downturn do not show up immediately but often take 18–24 months to materialize. As organizations shift their priorities and strategies, perpetrators respond. We may see an uptick in the amount of fraud in the coming months.

The Association of Certified Fraud Examiners (ACFE) recognizes that it is difficult to project the total losses due to fraud. One problem is that the data is imperfect. No one really knows the number of losses due to fraud that are undetected or detected but not reported. The 2022 ACFE Report to the Nations (ACFE Report)[2] estimated the amount of fraud that they believe a typical entity loses each year at 5% of revenue. The loss is significant and an indication that more attention needs to be paid to preventing and detecting occupational fraud. Asset misappropriation was the most frequently reported fraud at 86%. Fraudulent financial reporting was much less prevalent at 9% with the remainder classified as "other."

Companies are spending more to combat fraud than ever. Forty-two percent of the respondents to the 2020 PWC Survey reported that their companies have increased their spending on fraud prevention and detection and 44% intend to continue to increase spending over the next two years. Many of the additional controls are technology based but respondents are also expanding their whistle blower programs and talking more to leadership and governance about the problem. It might be useful to ask the question, "Are companies reacting to frauds that have surfaced in their own organizations and others or are they being proactive and taking the time to assess the risk of fraud?"

Recent Changes to Professional Literature

Auditing standards dealing with assessing the risk of fraud became more robust in 1988 with SAS 53, *The Auditor's Responsibility to Detect and Report Errors and Irregularities.* This standard was significant because it removed the requirement in SAS 16 to plan the audit to search for

1 https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html Note that this survey includes organizations of all sizes.

2 https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf

errors or irregularities that would have a material effect on the financial statements. SAS 53 required the auditor to assess the risk of errors and irregularities and plan the audit to obtain reasonable assurance of identifying errors and irregularities that were material to the financial statements. SAS 82 (1997), *Consideration of Fraud in a Financial Statement Audit* changed the requirement so that the auditor was responsible for planning and performing the audit to obtain reasonable assurance that the financial statements were free material misstatement whether due to fraud or error. It also identified two specific types of fraud that could be present: misappropriation of assets and fraudulent financial reporting. SAS 99 (2002), also titled, *Consideration of Fraud in a Financial Statement Audit,* provided expanded procedures to use in a financial statement audit. SAS 122 (2011) clarified and codified the existing standards including *Consideration of Fraud in a Financial Statement Audit* into AU-C 240. This is where the fraud literature resides today.

Amendments were made to AU-C 240 with the issuance of the new suite of auditing standards (SAS 134-145). SAS 134 made significant modifications to the independent auditors' report. The paragraph dealing with the auditor's responsibilities reads as follows (in part):

> Our objectives are to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion. **Reasonable assurance is a high level of assurance but is not absolute assurance and therefore is not a guarantee that an audit conducted in accordance with GAAS will always detect a material misstatement when it exists. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.** Misstatements are considered material if there is a substantial likelihood that individually or in aggregate, they would influence the judgment made by a reasonable user based on the financial statements. In performing an audit in accordance with GAAS, we:
>
> Exercise **professional judgment and maintain professional skepticism** throughout the audit.
>
> - Identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, and design and perform audit procedures responsive to those risks. Such procedures include examining, on a test basis, evidence regarding the amounts and disclosures in the financial statements.
> - Obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of ABC Company's internal control. Accordingly, no such opinion is expressed.
> - Evaluate the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluate the overall presentation of the financial statements.
> - Conclude whether, in our judgment, there are conditions or events, considered in the aggregate, that raise substantial doubt about Example Company's ability to continue as a going concern for a reasonable period of time.
>
> We are required to communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit, significant audit findings, and certain internal control–related matters that we identified during the audit.

These modifications were made to highlight that the auditor has a responsibility to perform the audit in accordance with the standards but even with professional skepticism and prescribed audit procedures there is never absolute assurance that fraud will be detected.

SAS 134 also requires the auditor to communicate significant risks to those charged with governance in planning. This can be through a letter to governance or orally.

Where several of the other recently issued standards made minor changes to the standard, SAS 135, Omnibus Statement on Auditing Standards, had a bigger impact. It added guidance in the form of additional inquiries and audit procedures for the auditor to use related to significant unusual transactions and related parties. This will be discussed later in the discussion of the procedures that auditors are required to perform relative to assessing and responding to the risk of fraud.

SAS 143, Auditing Accounting Estimates and Related Disclosures, highlights the requirement for the auditor to perform a retrospective, or hindsight, review on accounting estimates. It also requires that the auditor evaluate whether management's judgments and decisions in making accounting estimates indicate a possible bias that may represent a material misstatement due to fraud. Indicators of possible management bias that may also be a fraud risk factor could cause the auditor to reassess whether the auditor's risk fraud risks, and related responses remain appropriate.

Association of Certified Fraud Examiners

AU-C 240 deals with what is referred to as occupational fraud and abuse. In 1988, a well renowned fraud expert, Dr. Joseph T. Wells, founded the Association of Certified Fraud Examiners. The organization's mission is to reduce the incidence of fraud and white-collar crime and to help its members develop ways to deter and detect fraud. This entity publishes its Report to the Nations every two years. The most recent report is dated 2022.

The Association of Certified Fraud Examiners (ACFE) estimates that organizational losses due to fraud account for 5% of annual revenues with projected estimated losses globally amounting to approximately $4.5 trillion each year. According to the ACFE, not-for-profit organizations reported 9% of fraud cases reported in the 2022 study and had a median loss of $60,000 and an average loss of $851,000. For many not-for-profit organizations, financial resources are extremely limited and a loss of any magnitude can be devastating.

Since the classification, nonprofit, includes educational institutions, healthcare companies, and religious, charitable, and social service organizations, the statistics in the preceding paragraph include all nonprofits in the study. The ACFE breaks the losses down by industry categories as follows:

Industry category	Mean (average)	Median (middle value)
Healthcare	$1,392,000	$100,000
Education	$1,022,000	$56,000
Social services, religious, and charitable organizations	$323,000	$78,000

Smaller not-for-profit organizations can be more vulnerable to fraud due to having fewer resources available to prevent and recover from a fraud loss. There is often less oversight and lack of segregation of duties is a common problem. Therefore, certain fraud schemes are more prevalent.

Types of Fraud

Auditing literature identifies two types of fraud in AU-C 240, *Consideration of Fraud in a Financial Statement Audit*. They are fraudulent financial reporting and asset misappropriation. The ACFE includes an additional category – corruption.

The most prevalent type of fraud according to the ACFE's 2022 Report is asset misappropriation (86%), followed by corruption (43%), and financial statement fraud (9%). The third category, corruption occurs in 50% of all cases.

Fraud category	Description	Occurrence	Median loss	Mean loss
Financial statement fraud (fraudulent financial reporting)	Perpetrator intentionally causes a material misstatement or omission in the financial statements	9%	$593,000	$1.2 million
Asset misappropriation	Employee stealing or misusing the employer's resources	86%	$100,000	$50 million
Corruption	Conflicts of interest, bribery, extortion	50% of all cases	$150,000	$2.6 million

Although fraudulent financial reporting is the least prevalent category, it is responsible for the biggest losses.

Risk in Not-for-Profits

Asset misappropriation is the number one occupational fraud category in terms of prevalence. Most often, misappropriation schemes are perpetrated by individuals for their own gain. This is a significant risk in not-for-profit organizations due to the lack of segregation of duties, the existence of unsolicited contributions, and the element of trust. However, these schemes, while the most prevalent, result in the lowest median loss per case. In contrast, fraudulent financial reporting, although less prevalent, results in the highest median loss per case. Additionally, accurate financial reporting is very important because donors, grantors, financial institutions, and others rely on financial statements to make decisions.

ACFE's 2022 *Report to the Nations* found that not-for-profit organizations, have fewer anti-fraud controls in place, leaving them more vulnerable to fraud. The top organizational weaknesses identified in the study follow:

- Lack of internal controls (in general) (35%)
- Lack of management review (19%)
- Override of existing internal controls (14%)

Understanding the most common weaknesses and fraud schemes can help a not-for-profit entity design controls to safeguard against its most significant threats. This will be discussed more fully in Section 3. As noted earlier, although the COVID-19 pandemic is no longer as

relevant of a factor, the pandemic made changes to organization's way of doing business that are not likely to change.

- Organizations still have a significant number of remote employees.
- Organizations have embraced more complex technology to do more work remotely. Electronic transmission of documents from the organization to vendors or customers, online payment capabilities and approvals within the electronic systems are just a few of the changes that organizations have made.

Many U.S.-based not-for-profits have seen extraordinary increases in funding in 2020 to address the COVID-19 crisis ($11.4 billion). A significant amount of the funding came from the federal government in the form of the Paycheck Protecction Program (PPP) loans, which were forgivable if the organization met certain criteria. In fact, approximately 60% of not-for-profits received those loans. Federal awards (including the PPP loan) related to COVID-19 amounted to $4.3 trillion. Where most of the federal funding was awarded to large for-profits and governments, not-for-profits also benefited by the federal programs. In addition, approximately $20 billion in philanthropic funding by institutional grant makers and high net worth donors was given to not-for-profits.

Even though in 2022 economic conditions due to COVID-19 have improved for many organizations, those that received PPP loans and other awards that subsidized them may find themselves with deficits for the next few years. Some not-for-profits have not changed their business models to match the times, and contributions from individuals, particularly at special events, have decreased. Inflation has impacted donors as well as the nonprofits themselves. This situation increases the risk of potential efforts to overstate or mischaracterize contributions.

Forward thinking not-for-profits are recognizing that the way they approach their constituents (donors, volunteers, and beneficiaries) may not yield the same results as in the past. Communication needs, donation mechanisms, and constituent preferences will continue to evolve as millennials take a larger role and members of the silent generation and baby boomers age out.

As a result:

Not-for-Profits May Need to:	**This Could Lead to:**
Have a certain level of donations or other revenue sources to obtain matching grants	Misclassification of funding
Pay operating expenses when cash is tight	Using donor-restricted net assets for unrestricted purposes
Show a level of contributions that may be needed to demonstrate they are a viable entity	Inflating contributions or revenue through receivables
Obtain additional financing to stay afloat	Altering the books and records to inflate assets or minimize liabilities
Meet debt covenants	Altering the books and records to improve ratios or other metrics
Cover certain operating expenses when unrestricted revenue sources have declined	Categorizing expenses as allowable for grant purposes when they are not or causing over allocation of payroll or other costs to grants

Some not-for-profits "borrowed" from restricted funding to pay operating expenses, believing that they would be able to pay it back. This has not happened for many of them, as the underlying problem of decreased funding remains.

Changes to Not-for-Profit Financial Statements

ASU 2016-14, *Financial Statements of Not-for-Profit Organizations*, is effective for fiscal years beginning after December 15, 2017, and interim periods thereafter for most not-for-profits. Those considered public organizations were required to implement it a year earlier. Among its many changes, changes in liquidity and availability and functional expense reporting should heighten the auditor's awareness as it relates to fraudulent financial reporting.

Functional Expense Presentation

All not-for-profit organizations are required to explain their policy for allocating expenses and present all expenses other than investment expenses in the functional expense statement or footnote. This focus on expenses by function may cause some organizations to push expenses into the program category that may be management and general or fundraising since Charity Navigator and other watchdog-type organizations want to see a very high percentage of expenses as devoted to program activities.

Liquidity and Availability Information

The new standard requires a footnote on liquidity and availability. A not-for-profit will be required to identify assets that are available for general expenditure within one year. This may be challenging for many since a significant portion of many organizations' assets may be restricted either by donors or regulator or are designated by the board. This could cause management to include assets that do not meet the liquidity requirements in that presentation.

NOTES

UNIT 2

AU-C 240 Revisited

LEARNING OBJECTIVES

When you have completed this unit, you will be able to accomplish the following:

- Identify and assess the risks of material misstatement of the financial statements due to fraud for not-for-profit organizations and smaller, less complex organizations.
- Describe and develop methods to obtain sufficient appropriate audit evidence regarding the assessed risks of material misstatement due to fraud, through designing and implementing appropriate inquiries and audit procedures.
- Develop an appropriate response to fraud or suspected fraud identified during the audit of a not-for-profit entity.

INTRODUCTION

AU-C 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with Generally Accepted Auditing Standards*, states, in part, that the auditor has a responsibility to:

> *obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, thereby enabling the auditor to express an opinion on whether the financial statements are presented fairly, in all material respects, in accordance with an applicable financial reporting framework.*

AU-C 240, *Consideration of Fraud in a Financial Statement Audit*, establishes standards and provides guidance to help auditors fulfill that responsibility with respect to fraud. When the standard was clarified, some additional considerations were identified in the explanatory material for governmental organizations and not-for-profit organizations as well as for smaller, less complex organizations. These things should be kept in mind when evaluating the type of entity and the procedures to perform, which are discussed in the following paragraphs.

The auditor's objectives under AU-C 240 are:

- to identify and assess the risks of material misstatement of the financial statements due to fraud
- to obtain sufficient appropriate audit evidence regarding the assessed risks of material misstatement due to fraud, through designing and implementing appropriate responses
- to respond appropriately to fraud or suspected fraud identified during the audit

Underlying the auditor's consideration of fraud is the use of professional skepticism. This has been highlighted in recently issued audit standards as well as in the new version of the independent auditor's report.

AU-C 200 cautions that the auditor should maintain professional skepticism throughout the audit and should recognize that there is a likelihood that a material misstatement due to fraud could exist even if management and those charged with governance have always appeared to be honest and above board. Unless the auditor has reason to believe the contrary, they may accept records and documents as authentic. However, the auditor should be alert and if conditions identified during the audit cause the auditor to believe that a document may not be authentic or that terms in a document have been modified but not disclosed to them, the situation should be investigated further.

The auditor should also be alert for responses to inquiries by management and governance that are inconsistent with the responses of employees. The auditor should challenge answers that appear to be vague or implausible.

Fraud Triangle

The fraud triangle is important to understand. AU-C 240 states that when there is incentive or pressure and inadequate internal controls (either a lack of controls or ineffective controls) along with the ability to rationalize the behavior, fraud is likely to occur.

The **fraud triangle** actually dates back to 1974 when Donald Cressey[3] published a hypothesis about what drives people to violate trust. This hypothesis is referred to as the fraud triangle. When perceived pressure, perceived opportunity, and rationalization intersect, fraud is likely to occur.

The triangle is not a comprehensive tool for detecting fraud. This is because two sides of the fraud triangle (pressure and rationalization) cannot be easily observed, and some important factors, like perpetrators' capabilities, are not included. But it offers a starting point for analysis, and the COSO Framework provides a way to identify internal controls that are important in preventing, detecting, and correcting misstatements due to fraud or error.

Considerations Specific to Not-for-Profit Organizations

When auditors perform work for these types of organizations, it is likely that they will have additional responsibilities relating to fraud. Government Auditing Standards identifies additional responsibilities for reporting when fraud is identified. The Uniform Guidance and AU-C 935 identify responsibilities related to the auditor's assessment of the risk of fraud and reporting should it be identified. In addition, a not-for-profit entity may have certain mandates or other requirements that are applicable to those to whom it provides funding.

3 http://www.acfe.com/fraud-triangle.aspx

Considerations Specific to Smaller, Less Complex Organizations

Auditing standards are intended to be scalable for smaller, less complex organizations. This does not mean that the auditor has the option of not performing the audit requirement. It means that the auditor may need to evaluate smaller, less complex organizations in a different way. Some ways that these organizations may be different follow:

- In smaller organizations, the focus of management's assessment may be on the risks of employee fraud or misappropriation of assets.
- Often, those charged with governance are also involved in managing the entity.
- A smaller entity may not have a written code of conduct but, instead, may have developed a culture that emphasizes the importance of integrity and ethical behavior through oral communication and by management example.
- In smaller organizations, management's authorization can compensate for otherwise deficient controls and reduce the risk of employee fraud. It is important to understand that domination of management by a single individual can be a potential deficiency in internal control because an opportunity exists for management override.

Audit Requirements

AU-C 240 requires the auditor to perform the following (several of these aspects will be discussed later).

- Understand the entity and its environment.
- Make inquiries of management and others about their views on fraud, the risks of fraud and how they are addressed.
- Make inquiries of management and those charged with governance about related parties and significant unusual transactions.
- Consider any unusual relationships identified during planning such as through preliminary analytical review. The auditor should perform preliminary analytical procedures on revenue, as this is a specific area where the risk of fraud is increased. AU-C 240 requires procedures to be analytical and to be performed on revenue sometime during the audit.
- Consider fraud risk factors that correspond to the three legs of the fraud triangle: incentive/pressure, opportunity, and rationalization.
- Consider any other information gathered during the process of new client acceptance or client continuance.
- The information obtained is synthesized in a discussion with the audit team that explores how and where fraud could occur, identifies specific risks of fraud, and emphasizes professional skepticism.
- Presume that revenue recognition is a significant risk of fraud. If the auditor believes that it is not a risk of fraud, this must be justified and documented.
- Perform procedures related to management override of controls since it is deemed a risk of fraud.
- Remain alert during the audit process for circumstances that might indicate the possibility of fraud.
- Report suspicions of fraud as required by professional standards, government regulations, or legal requirements.

Fraud Risk Factors

It is useful to understand fraud risk factors before performing the fraud risk analysis so that the auditor is aware of where fraud could occur in a not-for-profit. AU-C 240 lists three fraud risk factors; incentive or pressure, opportunity, and rationalization which, as noted earlier, are part of the fraud risk triangle.

Incentive or pressure could be specific to an employee, such as a financial need or fear of the loss of a job due to failure to perform at a certain level. The pressure could also be organizational such as the need to report a certain level of income (increase in net assets) or meet other financial targets.

EXAMPLE

A social service organization is competing for grant funding with other similar organizations in its geographic area. The executive director is aware that grants management personnel look to GuideStar and Charity Navigator to determine which organizations to fund. The executive director understands that one of the criteria used by the funding sources is the ratio of program expenses to total expenses. The audit partner told the team to be aware of the risk of fraud in the classification of functional expenses.

EXAMPLE

During an economic downturn, the enrollment in an independent school was down. The CFO was concerned that the fixed expenses would not be covered. She spoke with the advancement department and learned that donations were still coming in for the endowment and that the development director had just been informed that a large bequest would be arriving shortly. The CFO considered how she might be able to justify reporting the restricted donations as unrestricted and recategorize the bequest so that it was without donor restriction. She considered that it would just be for one year until the economy improved. And it would certainly make the board of trustees happy to see that the entity had an increase in unrestricted net assets during these trying times.

EXAMPLE

The Board of Directors of a YMCA recently replaced its management team. Attendance at the center was at an all-time low and the new team was charged with getting the organization back on its feet. The new team was offered bonuses if they hit certain targets. Although the new management team worked hard to restore member confidence by investing in new equipment, improving the programming, and making improvements to the structure itself. Eleven months into the year, they were still $75,000 short of meeting their financial target. The advancement director decided to go back to existing donors and ask them to extend their yearly pledges by one year. The accounting staff were instructed to reverse the remainder of the old pledges and record the new pledges at the new number of years outstanding. The advancement director felt like the whole management team had earned the bonus and should be rewarded.

EXAMPLE

A not-for-profit child and adult day care facility received a significant amount of federal dollars. It also received individual donations and other small grants. Due to the demand for services the organization was stretched thin. The executive director considered the feasibility of relaxing eligibility requirements so that more people could be served, thereby increasing the revenue to the program. The CFO was concerned about the financial position of the organization as well and falsified the federal reports by adding fictitious people to the roster of individuals served.

EXAMPLE

A long-time employee working in accounts payable was aware that the CFO generally ran short of time and did not really review checks with her stamped signature prior to mailing as specified in the entity's internal control procedures. She didn't think much about it until her child became ill and required expensive medication. For the past few months, she charged the medication to her credit card but this month she hit her limit. Since she had access to the check stock as well as the signature stamp, she wrote a check to her credit card company, which was the same credit card company that the not-for-profit used. As expected, when she took the checks to the CFO to review, the CFO flipped through them quickly and told her to mail them.

EXAMPLE

An employee in the hospital's billing and coding department prided himself on his honesty and integrity. The federal government had recently decreased reimbursement to hospitals and implemented new quality, safety, and technology requirements that were expensive for hospitals to implement. The CFO made a presentation to the staff about these changes noting if revenue didn't grow in this fiscal year that there would be layoffs and the hospital might have to close. Even though the CFO never overtly told the employees to "up code," the implication was that their jobs were on the line when he said, "Billing and coding staff have a responsibility to the company to recover every dime of reimbursement possible from government programs."

Opportunity is generally present due to absent or ineffective internal controls, although it could also be due to management's ability to override controls that appear to be effective. It is management's responsibility to adopt sound accounting policies and to establish and maintain internal control that will, among other things, initiate, record, process, and report transactions consistent with management's assertions embodied in the financial statements.

EXAMPLE

An executive director was revered by the board of directors. She had a significant presence in the community and was the founder of the organization. She had influence not only over the board, who never questioned her actions, but over the staff who did whatever she requested without question. She refused to follow internal controls over significant procurements and awarded contracts to her relatives and friends. The treasurer retired from the board and a CPA in public practice was asked to join the board in that position. After several months, the treasurer brought the improper behavior with contracts and the executive director's refusal to implement recommendations by the independent auditor to the attention of the board chair, the chair told him that she would bring the situation up to the executive director. After three months, the treasurer concluded that that board was not interested in crossing the executive director and resigned citing the lack of oversight from the board as his reason.

EXAMPLE

A religious organization held several large events per year where cash was collected. Volunteers were recruited to collect and count the money. After one event, the pastor noted that the amounts collected were down and knew that the event was well attended. Not wanting to accuse the volunteers of syphoning off money, he consulted another church that held similar events to see if their experience related to event donations was the same. During the discussion, the pastor learned about internal controls over cash and implemented policies and procedures, talked to the volunteers, and installed surveillance devices in the count tents.

Rationalization is the ability to rationalize committing a fraudulent act, the third leg of the fraud triangle. A certain attitude, character, or set of ethical values can allow a person to knowingly and intentionally commit a dishonest act. AU-C 240 notes that even people who are otherwise honest individuals can commit fraud in an environment that puts sufficient pressure on them and that the greater the pressure, the more likely someone is to rationalize that it is acceptable to commit fraud.

EXAMPLE

An altruistic woman who valued childhood education was concerned about the quality of education in the city's economically disadvantaged neighborhoods. She applied and was approved to start a Charter School. She appointed herself as "head of school." Since the school was a startup, there were very few employees.

The school depended on federal and state funding. The government funding provided the basics to the school. As an educator, the head of school wanted to provide more including bus services and free meals to children who could not afford them. She intended to pay for these extra benefits through grants and contributions. Unfortunately, those funds did not materialize. When money became tight, and she could not meet payroll. She used payroll withholdings to pay salaries. She also claimed to have spent grant money for equipment but used it for payroll instead. She justified her actions to herself as "for the good of the children and the school." As head of school, no one questioned her instructions.

Circumstances That May Indicate the Possibility of Fraud

It is useful to consider circumstances that the auditor may encounter during the audit, which might indicate the possibility of fraud.

- Significant transfers or transactions between funds or programs, or both, without supporting documents
- Significant budget adjustments made without approval
- Large amounts of over-or-under spending
- Grant programs with an emphasis on spending money quickly
- Complaints received from potential suppliers about questionable practices related to awarding of contracts
- Program conditions, such as newly implemented programs without existing management and accountability structures
- Programs experiencing unusual growth due to conditions beyond the control of management
- Grant and donor funding conditions such as noncompliance with grant requirements, complaints from intended recipients or interest groups
- Lack of monitoring of grantee compliance with applicable law or regulation
- Client says they cannot locate documents or that the only documents they can provide are electronic or photocopied. In this time where electronic documents may be as prevalent as paper ones, the auditor should consider whether it is likely that paper documents exist and are simply not provided. The auditor would typically be aware of instances where only electronic documents exist from their understanding of the client's system.

- The auditor observes that certain documents appear to have been altered. Note that the auditor should remain alert for altered documents although the auditor is not responsible for identifying whether all documents obtained from the client are authentic.
- Electronic evidence is missing or unavailable.
- Client denies the auditor access to electronic files, operations staff, or certain facilities.
- Client is slow to provide information requested by the auditor. The auditor should consider whether this is due to disorganization or limited staff.
- Information provided by operations personnel is not able to be reconciled to the general ledger.
- Confirmations returned to the auditor show discrepancies and the client is not able to provide adequate explanations.
- There are numerous topside adjustments to the financial statements. Note that the auditor is required to understand internal controls over journal entries, particularly those made at the end of the year and those that are not posted to the general ledger.
- Transactions are not supported by evidence and are not approved.
- Accounting estimates appear to be consistently either low or high.
- Client reconciliations contain large unsupported differences.
- Excessive write-offs of receivables or other assets.
- Internal control deficiencies ignored by the client. There may be certain deficiencies, such as lack of segregation of duties, where management is unable to afford to hire additional people. The auditor should consider where deficiencies are due to circumstances and not an indicator of fraud.
- Employees can access systems and records that are inconsistent with their duties.
- Management tolerates or commits violations of their code of conduct.
- Answers given to the audit team in response to questions are inconsistent or implausible.
- Management gives the auditor unreasonable deadlines or fails to provide answers to complex or unusual and significant issues that arise at the end of the audit when there are tight deadlines.
- The auditor notes several changes to accounting estimates that appear unrelated to other activity in the general ledger or changes in circumstances.
- Client has implausible reasons for fluctuations or other issues noted in the auditor's analytical review procedures.

Presumption of the risk of fraud, AU-C 240 presumes that fraudulent financial reporting due to inappropriate revenue recognition is a risk of fraud. It can exist as premature revenue recognition, moving revenue from the current period to a later period, recording of fictitious revenue, and in a not-for-profit, misclassification of revenue in the wrong net asset class.

This presumption can be rebutted by the auditor. However, the auditor should have a compelling reason and thoroughly document the circumstances. It is also important to remember that not all sources of revenue may have a risk of fraud.

EXAMPLE

A not-for-profit was primarily funded by one large donor and had rental income from one building that used to house its operations until the organization outgrew it. The organization held a special event each year, but the revenue was not material. The donor was a long-time donor, and each year confirmed the donation. The rental agreement specified a fixed rent. The auditor concluded that revenue recognition was not a risk of fraud.

When the auditor identifies the revenue recognition as a risk of fraud, the auditor should treat it as a significant risk and obtain an understanding of the organization's controls, including the control activities, related to the risk. The auditor should evaluate whether those controls have been suitably designed and implemented to mitigate the fraud risks.

Inquiries of Management, Governance, and Others

Professional standards require the auditor to make inquiries of management, those charged with governance and others. Examples of others in the organization to whom the auditor may direct inquiries about the existence or suspicion of fraud include the following:

- Operating personnel not directly involved in the financial reporting process
- Employees with different levels of authority
- Employees involved in initiating, processing, or recording complex or unusual transactions
- Employees who supervise or monitor those employees
- In-house legal counsel
- Chief ethics officer or person in that role
- The person or persons charged with dealing with allegations of fraud

Required Fraud Inquiries

Management	Governance	Others
■ Whether management has knowledge of any fraud or suspected fraud affecting the organization. ■ Whether management is aware of allegations of fraud or suspected fraud affecting the organization; for example, received in communications from employees, former employees, analysts, regulators, or others. ■ The extent of management's understanding about the risks of fraud in the organization, including any specific fraud risks the organization has identified or account balances or classes of transactions for which a risk of fraud may be likely to exist. ■ The existence of programs and controls the organization has established to mitigate specific fraud risks the organization has identified or that otherwise help to prevent, deter, and detect fraud, and how management monitors those programs and controls. ■ The nature and extent to which organizations with multiple locations monitor them and whether there are operating locations for which the risk of fraud may be more likely to exist. ■ Whether and how management communicates to employees its views on business practices and ethical behavior. ■ Whether and how management has reported to the audit committee or others with equivalent authority and responsibility on how the organization's internal control serves to prevent, deter, or detect material misstatements due to fraud. ■ Whether the organization has entered into any significant unusual transactions and, if so, the nature, terms, and business purpose (or the lack thereof) of those transactions and whether such transactions involved related parties.	■ Its views on fraud and whether or how it exercises oversight. ■ Whether the members have any knowledge of fraud that has occurred. ■ Where and how fraud might occur. ■ Whether the organization has entered into any significant unusual transactions and, if so, the nature, terms, and business purpose (or the lack thereof) of those transactions and whether such transactions involved related parties.	■ Their views about the risk of fraud and how it might occur. ■ Whether they have seen or suspected fraud. ■ If internal auditors, whether they have performed any procedures to detect fraud and if there were findings, how management responded.

Significant Unusual Transactions

SAS 135 added certain inquiries to those previously specified in the standard for related parties and significant unusual transactions. Significant unusual transactions are those that are outside the normal course of business for the organization or that otherwise appear to be unusual due to their timing, size, or nature.

EXAMPLE

The auditor of a not-for-profit organization that sells religious books and other products in stores and online conducted a physical inventory observation as required by professional standards. When she obtained the inventory instructions from her client, she found that during the year the organization rented a warehouse in a remote location even though there was ample space in its other warehouses. With the decrease in sales, she was curious about the increase in the level of inventory recorded near year end. The auditor obtained the invoices from the entity that owned the warehouse. The cost seemed high per square foot in relation to the location. After some due diligence, she discovered that the warehouse was owned by a company owned by the board chair of the not-for-profit. This was deemed to be a significant unusual transaction.

The auditor of a not-for-profit health research collaborative was aware that the consolidated entity included four organizations that were headquartered overseas. During the year, there were wire transfers from the reporting entity to the overseas organizations and vice versa. There were also wires between the overseas organizations. The documentation for the wires stated that the transfers were related to payment of expenses paid by one entity on another's behalf. In addition, the intercompany accounts did not reconcile. The auditor was aware that the research was performed related to health disparities in developing countries. However, there did not appear to be a good business rationale for the transfers. This was deemed to be a significant unusual transaction.

EXAMPLE

A not-for-profit college had an endowment that was significant. Up until the current year the endowment had been invested solely in marketable securities. During the year under audit, half of the portfolio was liquidated, and the money was put into alternative investments. This was a significant unusual transaction given the entity and its environment and the auditor's knowledge of the conservative nature of those charged with governance.

SAS 135 requires the auditor to make additional inquiries of management about whether the organization has entered into any significant unusual transactions and, if so, the nature, terms, and business purpose (or the lack thereof) of those transactions and whether such transactions involved related parties.

Indicators that may suggest that significant unusual transactions may have been entered into to engage in fraudulent financial reporting or to conceal misappropriation of assets include the following:

- Form of such transactions appears overly complex (for example, the transaction involves multiple organizations within a consolidated group or multiple unrelated third parties).
- Management has not discussed the nature of and accounting for such transactions with those charged with governance of the organization, and inadequate documentation exists.
- Management is placing more emphasis on the need for a particular accounting treatment than on the economic substance of the transaction.

- Transactions involve nonconsolidated related parties, including special purpose organizations, have not been properly reviewed or approved by those charged with governance of the organization.
- Transactions involve related parties or relationships or transactions with related parties previously undisclosed to the auditor.
- Transactions involve other parties that do not have the substance or the financial strength to support the transaction without assistance from the organization under audit or any related party of the organization.
- Transactions lack commercial or economic substance or are part of a larger series of transactions. For example, a transaction that is entered into shortly prior to period end and is unwound shortly after period end.
- Transactions occur with a party that falls outside the definition of a related party with one party able to negotiate terms that may not be available for other, more clearly independent parties on an arm's-length basis.
- Transactions exist to enable the organization to achieve certain financial targets.

The examples discussed previously do not necessarily mean that fraudulent activity is present, only that the auditor should investigate and document the results of the investigation.

EXAMPLE

A not-for-profit skilled nursing company owned several nursing homes. The executive director's family also owned nursing homes privately. When performing preliminary analytical procedures, the auditor noted that there was a large note receivable on the books of the not-for-profit from a company owned by a relative of the executive director. The executive director defended the transaction stating that the board had approved it and the interest rate was fair and the interest on the receivable was fair compensation for the risk involved. The auditor confirmed that this was true. However, to assess the collectability of the receivable the auditor evaluated the financial capabilities of the related party to repay the note.

New procedures are introduced when transactions outside the normal course of business of the organization are identified:

- Evaluate the rationale and business purpose for those transactions as to whether they suggest that they were entered into to perpetrate fraudulent financial reporting or misappropriation of assets.
- Read the supporting documentation and evaluate whether the terms and other information about the transaction are consistent with explanations from inquiries and other audit evidence regarding the business purpose.
- Determine whether the transaction has been authorized and approved in accordance with the organization's policies and procedures.
- Evaluate whether significant unusual transactions identified have been properly accounted for and disclosed in the financial statements.

Remote Audits and Use of Electronic Communications

Remote audits appear to have increased the tendency that has been growing in audits to move away from face-to-face conversations with client personnel and governance in favor of questionnaires that are sent to the client's personnel and board member to complete. When this happens, the information and impressions that can be gained by a face-to-face conversation are lost. The American Institute of Certified Public Accountants (AICPA)

strongly encourages auditors to use face-to-face conversations and if that is not feasible to use technology such as Zoom or Teams to conduct conversations.

Some accounting firms have clients that have locations throughout the country. This makes it difficult to speak to as many people as they would like in person. To obtain better information in a timelier fashion and to aggregate the information in a more efficient manner, some firms have started using electronic surveys. There are several vehicles commercially available for low to no cost. One of these is Survey Monkey. The auditor selects questions (generally no more than 10), and they are inserted in the electronic form. Radio buttons (buttons to click on for the answer) are used for many questions although some are open ended. Survey Monkey has a feature where if a question is answered in a certain way, supplemental questions appear. Examples of questions for a board questionnaire follow. The words in parentheses indicate the radio button selections.

EXAMPLE

1. Are you aware of any known departures, during the last year, from approved policies or any unacceptable practices or conduct that might significantly affect the organization? (Yes, No)

1a. (If the answer is yes, the following question drops down.) Please describe the departure and any action taken to address the issue.

2. Do you believe that management handles all complaints from vendors, regulators, and external parties with comments with integrity and due professional care? (Yes, No)

2a. (If the answer is no, the following question drops down.) Please describe why.

3. Are you aware of any persistent comments or complaints from employees, vendors, regulators, or external parties in 2012? (Yes, No)

3a. (If the answer is yes, the following question drops down.) Please describe the most significant or persistent complaint or comment from employees, vendors, regulators, or other external parties in 20X8.

4. Are you aware of any conflict of interest that exists or existed between the organization and any member of the staff or volunteer? (Yes, No)

4a. (If the answer is yes, the following question drops down.) Please describe what happened and what was done to address it.

5. Are you aware of any fraud or abuse of the organization's resources (including credit card abuse) by either staff or volunteers during the past two years? (Yes, No)

5a. (If the answer is yes, the following question drops down.) Please describe what happened and what was done to address it.

6. Do you believe the organization has adequate processes for the investigation of potential frauds and for corrective action when necessary? (Yes, No)

7. How would you improve the organization's policies, processes, and procedures in this area?

8. Are you aware of any transactions with board members or management?

9. Are you aware of any significant unusual transactions?

10. For members of governance: Do you believe that the board has an adequate understanding of how fraud could occur?

10a. (If the answer is yes, the following question drops down.) Please describe the follow-up.

11. For members of governance: Does the board discuss the risk of fraud on a periodic basis with management?

11a. (If the answer is yes, the following question drops down.) Please describe any questions or concerns, which we should consider during our audit.

12. For members of governance: Does the board follow-up when internal control deficiencies are noted by external auditors or regulatory authorities? (Yes, No)

13. Do you have any questions or concerns, which we should consider during our audit? (Yes, No)

Integrating AU-C 240 and 315 Inquiries

Integrating the inquiry, observation, and inspection required by the two standards will give auditors a better basis for discussion and improve their understanding of the risk of material misstatement whether caused by fraud or error. In addition, combining the two will save time. Therefore, it is more efficient and much more effective to perform the procedures required by AU-C 240 and 315 at the same time.

EXAMPLE

The auditor of Social Services for the Elderly wanted to gain efficiency by combining the questions he intended to ask the Executive Director, the Finance Director, and the Chair of the Audit Committee about risk with the questions about fraud. He had the following observations about the organization for the current year.

Knowledge of the (1) Nature of the Organization; (2) Objectives, Strategies, and Business Risks; (3) Industry & Regulatory Environment; and (4) Measurement of the Organization's Financial Performance

- Market and competition – the organization was competing with larger organizations for grants from foundations that were now moving toward focused funding (giving larger amounts to certain organizations, typically larger ones).
- Accounting principles and industry – the state enacted a version of UPMIFA during the year and the organization has endowment investments. The organization did not keep very good records by donor, so obtaining the information to make the reclassification of amounts that were unrestricted to the donor restricted net asset class that were not appropriated for expenditure might be a challenge.
- New projects that might give rise to unrelated business income – the organization started a thrift store and was selling products online to try to raise money for operations since contributions and grants were down.
- General level of economic activity (i.e., recession) – the organization was struggling to get sufficient contributions to remain an affiliate of the national organization. The national organization planned to cull the number of affiliates and merge the struggling into the healthiest affiliates. This could potentially cost the executives their jobs.
- Interest rates and availability of financing – the organization's interest rate was recently raised and the limit on its line of credit lowered due to the perceived credit worthiness of the organization.
- Impact of these factors on funding sources such as donors or foundations – the organization's funding sources were also experiencing difficulties and were not able to

provide the level of support as they had in the past. State grants were not available in the current year.

- Impact of these factors on demand for services offered by the not-for-profit – as with most not-for-profits, the need for services increases in a down economy.
- Preliminary analytical procedures showed that contributions were down, investment income was down, and the metrics by which the organization was measured by the national office were also down.
- Compliance with laws and regulations
- Significant unusual transactions and whether they are with related parties

EXAMPLE

An audit manager was preparing training for staff people in their first and second years with the firm. She noticed that when she listened to staff members interviewing clients that they were not always prepared for the interview. Many times this resulted in having to return to the same client personnel to ask follow-up questions. She created a handout for the training so that staff members could use it as a starting point for the questions they wanted to ask. This way they would be able to spend the time listening and observing the interviewee's nonverbal responses instead of trying to make up questions on the fly. Since she knew that the best interview material comes from asking open-ended questions as opposed to closed-end questions that can be answered with a short phrase or the words *yes* or *no*, she planned role plays for the training so that staff members could practice asking open-ended questions using phrases such as:

- Please explain the process …
- Please tell me about the internal accounting controls over …
- Please help me understand …
- Why do …
- What are some possible explanations as to why …
- Would other _____ be affected by _____? Why or why not?
- Explain several reasons why …
- Give me some suggestions on how …
- If someone wanted to steal, how would they …
- What do you think about …
- How does …
- Tell me anything else you believe would help me to understand …

Integrated Questionnaire

Inquiry	Purpose	Specific Inquiries	Ask for These Documents So They Can Be Examined
Executives [CEO (or exec assistant), CFO (or finance director)], and any others that are important such as grants accounting or development	To get information about the organization and its environment, information about the risk of fraud (AU-C 240 inquiries) and entity level internal controls. This is a good place to also get information to help construct expectations for Substantive Analytical Procedures (SAP). Also be sure to obtain information about related parties and conflicts of interest in purchasing or other contractual arrangements. If this is a new client, the auditor will also ask questions designed to obtain an understanding of the: ■ Nature of the organization ■ Structure and governance ■ Measurement and review of the organization's financial performance ■ Organization's objectives, strategies, and business risks	Would you tell me about your relationship with the national organization and any communications you have had with them in the current year about merging your organization with another affiliate? Are there any actions that your organization could take to ensure that you are one of the surviving affiliates? Would you describe how contributions and grants have been affected by the economy? How are you handling the increase in demand for services when contributions and grants are down? How have you addressed the possibility of unrelated business income from your new ventures? Do you know of any employees that handle cash that may be adversely affected by the economy – for example, spouses laid off? How have you addressed the risk of theft?	Internal communications to employees such as intranet, information in the break room, on-boarding materials for new hires, codes of ethics with or without acknowledgements, documents used in monitoring, communications from regulatory agencies, and communications with national organizations. Ask for documents that management states they must support the entity level controls identified.

Inquiry	Purpose	Specific Inquiries	Ask for These Documents So They Can Be Examined
		Have you looked at how UPMIFA is going to impact your financial statements? What impact do you believe this could have on funding sources that use them to make decisions? How are you handling the lack of liquidity now that the interest rate on the line of credit was raised and the limit lowered? How do you communicate the importance of ethical behavior and business practices to your employees? What types of programs does your organization have in place to prevent or detect either fraudulent financial reporting or misappropriation of assets? Would you describe the process you use to assess risk in the organization, including the risk of fraud? Would you describe the monitoring activities that you use to prevent or detect misstatements (use the checklists previously provided to management) relative to organization level controls?	

Inquiry	Purpose	Specific Inquiries	Ask for These Documents So They Can Be Examined
Executives [CEO (or exec assistant), CFO (or finance director)], and any others that are important such as grants accounting or development	Be sure to obtain information on any commitments and contingencies and identify all significant estimates and concentrations.	Go over the document where the client has identified internal controls at the entity level. Would you describe your closing process, including the review of financial information (i.e., financial statements or other summary form prepared by the organization)? Can you tell me who reconciles detail to the general ledger?	
Executives [CEO (or exec assistant), CFO (or finance director)], and any others that are important, such as grants accounting or development		Please describe the reasons for the unusual relationships noted in preliminary analytical procedures.	The auditor should do more than just take management's word for this. He should ask for support.
Executives [CEO (or exec assistant), CFO (or finance director)], and any others that are important such as grants accounting or development		Would you describe the process by which journal entries are prepared and approved? (i.e., direct interface from subsidiary to G L, to record activity from service providers, to adjust account balances, to record nonroutine/ nonsystematic transactions or judgments and estimates)?	
		Have there been any communications from regulatory agencies during the year? Please tell me about any changes to internal control that were made as a result.	Ask to see the written communications and consider obtaining a copy for the audit file.

Inquiry	Purpose	Specific Inquiries	Ask for These Documents So They Can Be Examined
Executives [CEO (or exec assistant), CFO (or finance director)], and any others that are important such as grants accounting or development		Would you tell me the different ways you believe that employees could commit fraudulent financial reporting? How about misappropriation of assets?[4] Do you discuss the risk of fraud with members of the board (or audit committee)? Has fraud occurred this year or have you suspected fraud in the organization? Are you aware of any allegations of fraud?	

4 Although these questions are directed at the executives, in some organizations, the executives may not be knowledgeable about auditing terminology, especially as it relates to internal control and fraud. Another way to ask this question is: If someone wanted to steal from the organization, how could they do it and get away with it? If someone wanted to present false and misleading financial statements, how could they do it so that no one would notice?

Inquiry	Purpose	Specific Inquiries	Ask for These Documents So They Can Be Examined
Board (Board of Trustees, Board of Directors, Audit Committee)	To understand: ■ The environment in which the financial statements are prepared ■ The board's attitude toward fraud (i.e., whether they believe it would happen, their knowledge, etc. See AU-C 240) ■ New concerns they may have from a business perspective ■ Community developments ■ The extent of their participation in financial reporting ■ Document as knowledge of organization and environment, internal controls (at entity level), specific controls if any (i.e., any control activities they may perform).	Given the possibility of being merged into an affiliate organization, was there any attempt to keep that from happening by altering the books and records? Have you seen any changes in the behavior of management or other personnel that would suggest that they are under financial pressures? Would you describe your involvement as a board member in reviewing financial information? As an audit committee member, would you describe the methods you use to ensure accurate financial reporting? Would you describe the policies and procedures the organization has in place relative to conflicts of interest? Would you describe your interaction with management relative to judgments and estimates?	Committee meeting minutes, analyses performed relative to reviewing financial statements

Inquiry	Purpose	Specific Inquiries	Ask for These Documents So They Can Be Examined
	If the auditor is intending to use the budget when performing SAPs, this information could be used to support the quality of the information for his expectation. Document in the file as support for substantive testing (SAP) when there is any kind of tangible evidence available about the budget, large purchases, etc. Obtain any other evidence available to help construct expectations for substantive analytical procedures.	Would you discuss concerns you may have relative to management override? [5] As member of the board, do you discuss risks to the organization whether business risks, risks of error or fraud? Would you describe your thoughts relative to fraudulent financial reporting as it relates to the organization? Misappropriation of assets?	

5 Although these questions are directed at executives, they may not always have sufficient understanding of auditing and internal control terminology and will not understand the question in these terms. Another way to ask the question might be: Can you think of any ways that the system could be circumvented by members of management?

Inquiry	Purpose	Specific Inquiries	Ask for These Documents So They Can Be Examined
	Obtain information about related parties and conflicts of interest in purchasing or other contractual arrangements.	Do you have any suspicions of fraud affecting the organization? As a member of the audit committee, would you describe your understanding of the organization's internal control and management's attitude toward internal control? Do you feel that the board/audit committee serves as a good monitoring control? How? For any entity level controls identified by management, corroborate these with the board.	

Inquiry	Purpose	Specific Inquiries	Ask for These Documents So They Can Be Examined
Other people in positions performing entity level internal controls to help provide information about operations or the organization's risk. Be sure to consider those that would create estimates or perform nonroutine, nonsystematic transactions.	To get information about the organization and its environment, information about the risk of fraud (AU-C 240 inquiries) and entity level internal controls. This is a good place to also get information to help construct expectations for SAPs.	Would you discuss how management communicates the importance of ethical behavior and business practices to the employees? What types of programs does your organization have in place to prevent or detect either fraudulent financial reporting (preparing misleading financial statements) or misappropriation of assets (stealing)? Have you ever been asked to change the accounting records without normal documentation? Would you tell me the different ways you believe one would be able to steal from the organization and get away with it? Can you tell me how management might prepare incorrect or misleading financial statements?	We will be performing a substantive analytical review for revenue and expenses. Obtain a list of donors from the development director, along with average donation levels. Ask for evidence of large donations noted in the board minutes (use as a detail test).

Inquiry	Purpose	Specific Inquiries	Ask for These Documents So They Can Be Examined
		Do you feel like you could bring any kind of instances of theft to the attention of either the board or audit committee?[6] Has theft or wrongdoing occurred this year or have you suspected wrongdoing (theft), preparation of misleading financial statements, or conflicts of interest on the part of others in the organization? Have you ever been asked to make journal entries with no or little support or alter documentation? Are you aware of any allegations of theft or wrongdoing on the part of management or employees?	For any entity level controls identified by management corroborate these with other people and obtain support where possible.
Management and IT supervisory personnel	To determine the level of diligence that is used in granting and terminating access to portions of the IT system.	Has the organization ever performed an access audit? Please describe the process followed when: ■ Granting employees or management access to a portion of the system ■ Terminating access to employees who no longer need it or have been terminated How could segregation of duties be enhanced?	For any entity level controls identified by management, corroborate these with other people and obtain support where possible. Where the controls are not in place, consider the AU-C 265 impact.

6 It is a good idea to avoid using the word *fraud* with lower-level employees. Simply express the types of frauds that could occur as examples.

Another good way to incorporate questions related to fraud is for the staff to ask them in the ordinary course of their audit work.

EXAMPLE

An audit staff member was instructed by her senior to make inquiries of the accounts payable clerk during her normal work with accounts payable. She was also instructed to continue to ask questions until she understood what the clerk was saying, and it made sense. The audit staff asked a question of the clerk and the answer she got from the clerk made it appear that the balance in the account they were discussing had decreased from the prior year, when, it increased by a significant amount. Since that did not make sense, the audit staff member tried asking the question a different way and asked the clerk to explain what she meant by showing an example. After about 15 minutes of discussion, the clerk became scared and began to stammer. She finally confessed to a fraud she was perpetrating by receiving vendor refunds for overpaid amounts and pocketing them. The staff person's questions and refusal to leave with vague answers paid dividends in this instance.

Additional Questions That Could Be Important

In June 2010, Joseph T. Wells gave some advice to auditors. It is timeless and still very appropriate today. The controls discussed below are ones that set the tone for the organization rather than try to detect fraud at the transaction level.

It could be used by auditors to determine the anti-fraud controls in place but could also be used by management and the board to assess their anti-fraud programs and controls.[7]

Anti-Fraud Provision	Question
Training	Do employees receive training that helps to educate them about: ■ What constitutes fraud? ■ Have costs of fraud such as job loss, publicity issues, etc., been discussed with employees? Have employees been told where to go for help if they see something? Is there a zero-tolerance policy for fraud and has it been communicated?
Reporting	Does the organization have an effective way for employees to report fraud? ■ Are there anonymous reporting mechanisms? ■ Do employees understand that those issues reported will be investigated?
Perception of Detection	Does the organization seek knowledge of fraudulent activity? ■ Does management send a message that there will be tests made to look for fraud? ■ Are there surprise audits? ■ Is software used to identify issues from data?

7 Adapted from Joseph T. Well's article in the *Journal of Accountancy*, June 2010.

Anti-Fraud Provision	Question
Management's Tone from the Top	■ Does the organization value honesty and integrity? ■ Are employees surveyed to determine whether they believe that management acts with integrity? ■ Have fraud prevention goals been set for management and are they evaluated on them as an element of compensation? ■ Is there an appropriate oversight process by the board or others charged with governance?
Anti-Fraud Controls	Are any of the following performed? ■ Risk assessments to determine management's vulnerabilities ■ Proper segregation of duties ■ Physical safeguards ■ Job rotation ■ Mandatory vacations ■ Proper authorization of transactions
Hiring Policies	Are the following incorporated? ■ Past employment verification ■ Credit check ■ Criminal and civil background check ■ Education verification ■ Reference check ■ Drug screening
Employee Assistance	■ Are there any programs in place to help struggling employees – financial issues, drug issues, mental health issues? ■ Is there an open-door policy so that employees can speak freely? ■ Are anonymous surveys conducted to assess employee morale?

Synthesizing the Information Obtained

Once the information has been collected, the audit team synthesizes the information in an audit team discussion and determines where the risk of material misstatement is likely to occur in the financial statements. The person with final responsibility for the audit should be present, and key members of the team should be included. The discussion should include instructions about maintaining an attitude of professional skepticism and this state of mind should continue throughout the audit, including evaluating the risks of misstatement of fraud near or at the completion of fieldwork.

The team meeting will generally combine the topic of risk in general (AU-C 315) and the topic of fraud risk specifically (AU-C 240). If the audit includes a financial statement and single audit (or program specific audit), the auditor could include a discussion of fraud as it relates to federal awards. This could also be discussed at a later date. The important point is to ensure that the audit team does not simply cross reference the work as it relates to consideration of fraud in the single audit at the major program level to the work performed in connection with the financial statement audit unless fraud related to the major programs was specifically discussed.

The audit team should discuss and identify:

- known external and internal factors affecting the organization that may create incentive or pressure for management or others to commit fraud
- internal factors that provide the opportunity for fraud to be perpetrated
- the likelihood of a culture or environment at the client that enables management or others to rationalize committing fraud
- the ways that management could override internal controls
  - recording fictitious journal entries,
  - intentionally biasing assumptions and judgments in management's estimates, and
  - altering records and terms of significant or unusual transactions.
- consideration of circumstances that might be indicative of revenue or expense management or manipulation of other financial measures and the practices that might be followed by management committing fraudulent financial reporting
- how the audit team might respond to the susceptibility of the organization's financial statements to material misstatement due to fraud

In addition, the audit team should consider areas where there may have been significant changes in risks, including:

- Regulatory changes and increased regulatory scrutiny, which may have changed the way the organization's products or services may be produced or delivered
- Legal or regulatory changes, which may impact how the organization safeguards the privacy of data and maintains information system security
- Risks resulting from national and international political uncertainty, including how these risks might limit growth opportunities or funding
- New cyber threats with the potential to significantly disrupt operations
- What changes to the organization's business model and core operations, needed to meet changes in its external environment, might find internal resistance to change
- Financial issues due to COVID-19 may have been partially or fully mitigated by federal and state funding. An important issue may be what happens now that there is less funding available if the organization has not recovered to its prepandemic levels and is unable to meet its obligations.

The fraud risk assessment by the team cannot only be done once. It is important for team members to communicate when any risks of material misstatement due to fraud are noted during the audit.

Assessing Fraud Risk

The auditor assesses risk at the overall account level and by account balance/class of transaction and assertion. In addition, auditors will identify where they believe there is significant risk and design audit procedures to be responsive to those risks. Note that all "fraud" risks are also "significant" risks; however, not all "significant" risks are "fraud" risks.

Once the team has identified a list of ways that fraud could possibly occur, the list must be narrowed down to risks that could have the risk of **material** misstatement and a likelihood of occurring. To narrow the field, the internal controls that could mitigate the risk of fraud either at the company or transaction level (or both) should be considered.

Auditors should take care to ensure that there are no loose ends in this process. If a risk is identified on one workpaper, there needs to be linkage to specific audit procedures that address the risk or there needs to be a comment made that the risk is not significant. Some auditors prefer to show all the preliminary risks identified and then trim them down to the significant ones. Others prefer to only list the ones that are significant. Either way is acceptable if the auditor deals with all the risks identified.

EXAMPLE

The audit team of Social Services for the Elderly held an audit team meeting and identified the following risks of material misstatement due to of fraud:

1. Management override of controls
2. **Overstated receivables and revenue from a pledge drive held shortly before the end of the year.**
   The risk is that the pledges may not all be collectible, and that management has not allowed for the effect of the economy on collections to show more revenue. This is possible because it is an estimate (valuation). It is also possible that since many of the pledges were taken over the phone, that there are fictitious pledges included in with the actual pledges (existence)
3. **Inappropriate releases from restriction for operating purposes (classification)**
4. Failure to record all expenses in the current period due to the need to show an increase in net assets
5. Management appears to be very concerned about remaining an affiliate of the national organization (completeness)

EXAMPLE

1. Welcome and introduction of team members
2. Importance of professional skepticism
3. Prior year experiences with misstatements or issues with the client
4. Preliminary calculation of materiality (financial statement and account level, if different) and how materiality will be used to determine extent of testing
5. Unusual accounting procedures used by the client
6. Consideration of the organization and its environment:
   - Industry, regulatory, and other external factors
   - Nature of organization
   - Objectives, strategies, and business risks
   - Measurement and review of financial performance
   - Internal control, including focus on client's level of information technology and important control systems
   - Application of accounting principles considering individual facts and circumstances
7. Definition of conditions of fraud (incentive/pressure, opportunity, rationalization/attitude)
8. Definition of significant risk
9. Management override is deemed to be a risk of fraud. The team should discuss in what ways this might occur.

10. Whether the audit should incorporate an element of unpredictability
11. Since the risk of management override of controls is higher when management has relationships with related parties that involve control or significant influence the team should discuss where this might occur because these relationships may present management with greater incentives and opportunities to perpetrate fraud.
12. Revenue recognition and where it could be a specific risk of fraud. If the team believes it is not, this must be justified.
13. Significant estimates and possibility for management bias
14. Significant unusual transactions and nature, terms, and business purpose (or the lack thereof) and whether such transactions involve related parties
15. Brainstorming:
    - Identification of risks (both fraud and error)
    - Consideration of magnitude and likelihood of material misstatement of risks identified
    - Determination of areas where substantive tests alone may not be sufficient
    - Determination of areas where control reliance would be efficient, effective, or required
    - Consideration that financial statement level risks may also give rise to risks at the assertion level
    - Conclusion on risks of fraud and areas that may be significant risks
16. Audit responses to the risks identified (both fraud and significant risks identified)
    - Overall (e.g., assign supervisory personnel)
    - Specific procedures
17. How matters will be brought to the team's attention during the audit.

Addressing the Risk of Fraud

Once the risks of fraud have been identified, auditors should link those specific risks to the changes that they will make to the audit plan. Auditors may have overall responses such as assigning more experienced staff to the engagement or more supervisory review. Auditors will also specifically link audit procedures to the risks identified by altering the nature, timing, and extent of procedures to be performed.

EXAMPLE

Account Balance	Risk of Material Misstatement Due to Fraud	Linkage to Audit Procedures
Overstated receivables and revenue from pledge drive held shortly before the end of the year	The risk is that the pledges may not all be collectible, and that management has not allowed for the effect of the economy on collections to show more revenue. This is possible because it is an estimate (valuation). It is also possible that since many of the pledges were taken over the phone, that there are fictitious pledges included in with the actual pledges (existence).	Focus additional effort on subsequent receipts of uncollected pledges. Where subsequent receipts are not available, examine thank you letters. Use more experienced personnel to perform the work on the allowance for uncollectible pledges.
Net assets	Inappropriate release from restriction due to need to show net assets without donor restrictions so they could be spent for operations.	Alter the extent of testing of net assets released from restriction.
Expenses	Failure to record all expenses in the current period due to the need to show an increase in net assets. Management appears to be very concerned about remaining an affiliate of the national organization (completeness).	Extend the period for the search for unrecorded liabilities and test more selections of checks written after year end. Also perform analytical procedures to test the expense levels from one period to the next. Have more experienced personnel perform the work and ask the questions about expenses patterns that appear odd.

Additional Procedures Required by AU-C 240

Management Override

Journal Entries

One way fraudulent financial reporting can occur is through the manipulation of the financial reporting process by recording unauthorized or inappropriate journal entries. This may occur manually or within the computerized information system.

Even if specific risks of material misstatement due to fraud are not identified by the auditor, there is always the possibility that management override of controls could occur. Therefore, the auditor is required to design and perform procedures to test the journal entries recorded in the general ledger and other adjustments made in the preparation of the financial statements, including entries posted directly to financial statement drafts. The auditor may understand and test other journal entries throughout the period.

The auditor should understand the organization's processes and internal controls related to journal entries and other adjustments. The auditor should:

- make inquiries of individuals involved in the financial reporting process about inappropriate or unusual activity relating to the processing of journal entries and other adjustments
- consider fraud risk indicators, the nature and complexity of accounts, and unusual entries processed
- select and test journal entries and other adjustments made at the end of a reporting period
- consider the need to test journal entries and other adjustments throughout the period

EXAMPLE

An audit senior had a new staff member who he felt was ready for additional responsibility. He discussed the possibility that management override that could be perpetrated by inappropriate journal entries. The senior told the staff member to be sure to pay particular attention to entries that are processed outside of the normal course of business since they pose an increased risk of error or fraud. Then he walked through the following audit steps for the staff member to perform.

- Obtain an understanding of the organization's financial reporting process and the controls over journal entries and other adjustments.
- Understand the type of journal entries that occur during the year, especially at the end of a reporting period.
- Understand the procedures used to enter transaction totals into the general ledger.
- Understand procedures used to initiate, record, and process journal entries in the general ledger.
- Determine what support is required to make a journal entry if journal entries must be approved and if so, at what level.
- Understand consolidating and eliminating entries and reclassification entries.
- Identify and select journal entries and other adjustments for testing. Before selecting the entries, perform tests to ensure that the population of journal entries is complete.

The senior noted that since other than journal entries made in the closing process, the auditor uses professional judgment to decide which entries to test, the staff person should consider the following and then run the testing plan by the senior. The senior asked the staff member to consider:

- Assessment of the risk of material misstatement due to fraud
- Complexity of the client's financial reporting process
- Effectiveness of controls that have been implemented over journal entries and other adjustments
- Types of evidence that can be examined. For example, whether the journal entries are in paper form or if it will take someone familiar with the IT system to extract the information.
- Accounts that are not regularly used
- Post-closing entries that have little or no explanation or description
- Entries made by personnel who generally don't make journal entries, such as a controller or CFO
- Entries that contain round numbers or a consistent ending number
- Entries made before or during the preparation of the financial statements that do not have account numbers

When testing journal entries, it is important to **document** the entries tested. Some possible attributes for testing might be:

- Entry was approved by someone with the appropriate level of authority
- Entry was for a bona fide business purpose
- Entry appeared to have no bias
- Entry had the appropriate level of supporting documentation
- Entry did not give the appearance of fraud

Accounting Estimates

The auditor should also review accounting estimates for bias and if found, evaluate whether the issues identified represent a risk of material misstatement due to fraud. The auditor may find that individual estimates are reasonable but bias that suggests that a risk of fraud is present. In this event, the auditor should also evaluate estimates collectively and then perform a review of management judgments and assumptions related to significant accounting estimates in the prior year financial statements. The auditor would select estimates that are based on highly sensitive assumptions or contain significant management judgments.

Related Parties

AU-C 240 requires the auditor to obtain an understanding of the entity's related party relationships and transactions. This is important because, as described in AU-C 240, fraud may be more easily committed through related parties.

SAS 135 states that the auditor should make inquiries of management and others within the organization as follows:

- The identity of the organization's related parties, including changes from the prior period
- The nature of the relationships (including ownership structure) between the organization and these related parties
- The business purpose of entering into a transaction with a related party versus an unrelated party
- Whether the organization entered into, modified, or terminated any transactions with these related parties during the period and, if so, the type and business purpose of the transactions

Domination of management by a single person or small group of persons without compensating controls is a fraud risk factor. This situation is often found with related parties. Indicators of dominant influence exerted by a related party include the following:

- The related party has vetoed significant business decisions taken by management or those charged with governance.
- Significant transactions are referred to the related party for final approval.
- Little or no debate occurs among management and those charged with governance regarding business proposals initiated by the related party.
- Transactions involving the related party (or a close family member of the related party) are rarely independently reviewed and approved.
- Sometimes dominant influence exists if the related party founded the organization and continues to play a significant role in managing the entity either unofficially or as a board member.

Evidence of the related party's excessive participation in, or preoccupation with, the selection of accounting policies or the determination of significant estimates may suggest a likelihood of fraudulent financial reporting.

EXAMPLE

A charity had a significant donor whose donations represented approximately 25% of the organization's revenue. The donor was passionate about the cause and insinuated that her donations would cease if the organization did not "strongly" consider her ideas. These ideas were not always in keeping with the mission of the charity. In addition, she suggested specific vendors to use in her suggested programs and expected that her wishes would be carried out.

As it relates to the auditor's evaluation fraud, the discussions with the audit team could include specific consideration of how related parties may be involved in fraud. The team should consider:

- Organizations formed to accomplish specific purposes and that are controlled by management might be used to facilitate obtaining financial results.
- Transactions between the organization and a known business partner of a key member of management could be arranged to facilitate misappropriation of the organization's assets.
- It is possible that a related party transaction may look like one sort of transaction when it is really another. For example, a transaction with a related party may be disguised as one with an unrelated party to circumvent laws, regulations or bylaws that limit or restrict the organization's ability to engage in transactions with related parties.

EXAMPLE

A not-for-profit downtown development organization makes programmatic loans. The program director approved a loan to an entity owned by his brother's wife, characterizing it as a program loan, even though this was a direct conflict of interest according to the organization's bylaws. An alert auditor obtained the loan documents in routine test work and identified the conflict while process of asking questions of the program staff. AU-C 550 requires the auditor to ask questions to try to identify related parties not previously identified to them. This is due to the risk of fraud.

When the auditor encounters related party transactions, they should evaluate the transaction considering their understanding of the organization and its environment as well as other information obtained during the audit, whether the business purpose of significant unusual transactions suggests that they were undertaken for purposes of fraudulent financial reporting or to conceal misappropriation of assets.

The auditor should consider performing the following:

- Read the underlying documentation and evaluate whether the terms and other information about the transaction are consistent with explanations from inquiries and other audit evidence about the business purpose of the transaction.
- Determine whether the transaction has been authorized and approved in accordance with the organization's established policies and procedures.
- Evaluate whether significant unusual transactions with related parties have been properly accounted for and disclosed in the financial statements.

Responding to Suspected Fraud

When the auditor has identified suspected fraud, whether material or not, they should bring this to the attention of management so it can be investigated. It is important to do this in a timely way because early detection helps the entity prevent future occurrences.

If management (especially senior management) is involved, the auditor has a more serious issue.

Unless all of those charged with governance are involved in managing the organization, if the auditor has identified or suspects fraud involving management, employees who have significant roles in internal control or others, when the fraud results in a material misstatement in the financial statements, the auditor should communicate these matters to those charged with governance on a timely basis. If the auditor suspects fraud involving management, the auditor should communicate these suspicions to those charged with governance and discuss with them the nature, timing, and extent of audit procedures necessary to complete the audit. The auditor should communicate with those charged with governance any other matters related to fraud that are, in the auditor's professional judgment, relevant to their responsibilities.

Near the End of the Audit

Near the end of the audit, the auditor should look at the accumulated results of auditing procedures, including the final analytical review, to determine if any evidence came to light that would affect the assessment of the risks of material misstatement due to fraud made earlier in the audit or indicate might a previously unrecognized risk of material misstatement due to fraud.

If analytical procedures related to revenue have not been performed along with the final analytical review, they should be performed at this time so see if any previous conclusions related to revenue recognition appear appropriate.

The auditor should also evaluate any misstatements noted during the audit where adjustments were proposed by the auditor for the risk of fraud. The auditor should consider how these misstatements might impact the audit, specifically in the areas of materiality, management and employee integrity, and the reliability of management representations. Instances of fraud are unlikely to be an isolated occurrence.

Reevaluating the Risk Assessment

If suspected fraud is noted, the auditor should reevaluate the previous risk assessment considering whether circumstances or conditions indicate possible collusion involving employees, management, or third parties. This situation may impact the reliability of evidence and the auditor may find it is appropriate to perform additional work. If the auditor concludes that, or is unable to conclude whether, the financial statements are materially misstated because of fraud, the auditor should evaluate the implications for the audit.

If, because of suspected fraud, the auditor believes they should not continue performing the audit, they should:

- Determine the professional and legal responsibilities applicable in the circumstances.
- Determine if a requirement exists for the auditor to report to regulatory authorities.
- Consider whether withdrawal is possible under applicable law or regulation.

If the auditor decides to withdraw, they should discuss the situation with the appropriate level of management and those charged with governance discussing the reasons for the withdrawal.

AU-C 240 reminds us that although the auditor may suspect or, in rare cases, identify the occurrence of fraud, the auditor does not make legal determinations of whether fraud has occurred. This is left to the legal system. Auditors should present the evidence obtained and refrain from characterizing actions as fraudulent. It may be prudent for the auditor to consult their own legal counsel and their insurance carrier.

Communications to Management, Governance, Regulators, and Enforcement Authorities

When the auditor identifies instances or suspected instances of fraud that are material, the auditor identifies the associated control deficiency and communicates the deficiency in writing in accordance with AU-C 265 to management and those charged with governance as a material weakness. Significant deficiencies are reported for deficiencies that are not deemed to be material but merit the attention of those charged with governance. Clearly insignificant instances should be communicated to management and may be communicated to those charged with governance either orally or in writing.

Government Auditing Standards and Single Audits

Many not-for-profits have financial statement audits under Government Auditing Standards (Yellow Book). Some are required to have Single Audits under the Uniform Guidance. The Yellow Book and Uniform Guidance impose additional requirements on the auditor with regard to fraud.

If the auditor has identified or suspects a fraud, it may be necessary to report to a party outside the organization. Generally, the auditor's professional duty to maintain the confidentiality of client information is paramount but could be overridden by the auditor's legal responsibilities.

The Yellow Book requires the auditor to issue a report on internal control and compliance with provisions of laws and regulations. The internal control report identifies material weaknesses and significant deficiencies as noted above. The compliance report identifies instances of noncompliance with provisions of laws and regulations, contracts, and grant agreements. Therefore, auditors should include the relevant information about noncompliance and fraud when:

- noncompliance with provisions of laws, regulations, contracts, or grant agreements that has a material effect on the financial statements
- fraud that is material, either quantitatively or qualitatively, to the financial statements

Sometimes the effect on the financial statements is less than material but warrants the attention of those charged with governance or the auditor has obtained evidence of suspected instances of fraud that has an effect that is less than material but warrant the attention of those charged with governance. This is reported to audited entity officials in writing and may be in a separate communication.

When necessary, auditors may need to consult with authorities or legal counsel about whether publicly reporting such information would compromise investigative or legal proceedings. Auditors may limit their public reporting to matters that would not compromise those proceedings and report only on information that is already a part of the public record.

Auditors should report identified or suspected noncompliance with provisions of laws, regulations, contracts, and grant agreements and instances of fraud directly to parties outside the audited entity when either of these situations are present:

- Audited entity management fails to satisfy legal or regulatory requirements to report the information to external parties specified in law or regulation.
- When audited entity management fails to take timely and appropriate steps to respond to fraud or noncompliance with provisions of laws, regulations, contracts, and grant agreements that is likely to have a material effect and involves funding received directly or indirectly from a government agency:
  - Auditors should first report management's failure to take timely and appropriate steps to those charged with governance.
  - If the audited entity still does not take timely and appropriate steps as soon as practicable, then the auditors should report the audited entity's failure to take timely and appropriate steps directly to the funding agency.

Documentation

The auditor should document the following as it relates to fraud:

- Their understanding of the organization and its environment and the assessment of the risks of material misstatement including those risks of fraud (AU-C 315)
- Significant decisions reached during the discussion among the engagement team regarding the susceptibility of the organization's financial statements to material misstatement due to fraud
- The identified and assessed risks of material misstatement due to fraud at the financial statement level and at the assertion level
- Audit responses to the assessed risks of material misstatement including:
- Overall responses to the assessed risks of material misstatement due to fraud at the financial statement level and the nature, timing, and extent of audit procedures, and the linkage of those procedures with the assessed risks of material misstatement due to fraud at the assertion level
- Results of the audit procedures, including those designed to address the risk of management override of controls
- Any communications about fraud made to management, those charged with governance, regulators, and others
- If the auditor has concluded the presumption that there is a risk of material misstatement due to fraud related to revenue recognition is overcome in the circumstances of the engagement, the auditor should discuss the reasons for that conclusion.

Practice Aids

The consideration of fraud is very important. It is true that the auditor is not performing the audit to search for fraud. However, when fraud occurs and the appropriate procedures, according to professional guidance, were not performed, then the auditor comes under more scrutiny. Practice aids can be helpful, but auditors need to be sure they perform all the procedures set forth in AUC 240.

Fraud Procedures Summary Form – Completed for Sample Client

Fraud Evaluation Element	Where This Is Addressed	Sign Off
Discussion among engagement personnel in planning the audit regarding the susceptibility of the organization's financial statements to material misstatement due to fraud.	See the team discussion workpaper XX.	TTH
Inquiries of management and others within the organization about the risks of fraud (this should include direct face to face discussions as well as any questionnaires deemed appropriate).	Discussions were held with Jenny Jones during the audit about the nature of fraud, anti-fraud procedures in place, how fraud could be committed and observed her attitude about fraud. We also noted the commitment of herself and the executive director to appropriate reporting as we were working with them this year. This is evident in their treatment of the amounts due to Medicare and the allowance for bad debts. We believe that Jenny sets the appropriate tone for the staff and that the appropriate level of controls is present even if not documented in writing. Jenny shows openness to our suggestions, as does the executive director.	TTH
Consideration of preliminary analytical procedures **including procedures specifically related to revenue**.	Revenue recognition was already identified as a risk of fraud, so analytical procedures were performed at a more detailed level in workpaper XX.	TTH
Other procedures performed to obtain information necessary to identify and assess the risks of material misstatement due to fraud.	We were alerted to unusual fluctuations in account balances in preliminary analytical procedures but found that those balances supported our expectations (i.e., patients and therefore revenue decreased in the current year).	TTH
Specific risks of material misstatement due to fraud that were identified and description of the auditor's overall and specific responses.	The specific risks of fraud identified were revenue recognition and evaluation of the allowance. These were documented at workpaper XX and in the team meeting memo.	TTH
The auditor's reasons supporting a conclusion that improper revenue recognition is **not a risk or material misstatement due to fraud**.	We believe that revenue recognition in accounts receivable / revenue is a significant risk. The other types of revenue are not deemed to be a significant risk of fraud due to its magnitude.	TTH

Fraud Evaluation Element	Where This Is Addressed	Sign Off
Results of procedures performed to further address the risk of **management override of controls**, including identification of JEs tested.	1. Journal entry testing was performed. We obtained an understanding of the internal controls over journal entries and inspected all entries made during the closing process. Additionally, we selected 10 entries spanning all types of entries and reviewed for lack of support or unusual transactions. None were noted. See workpaper XX. 2. Retrospective Review of Estimates (to ensure no management bias) – see workpaper XX. 3. Introduced an element of unpredictability; see workpaper XX, for example, lower known $ scope for sample selection in high-risk area of repairs and maintenance 4. Review business purpose of significant unusual transactions and transactions with related parties. – see workpaper XX.	TTH
Other conditions and analytical relationships that caused the auditor to believe that additional auditing procedures or other responses were required and any further responses that the auditor deemed appropriate.	There were none.	TTH
Nature of the communications about fraud made to management and those charged with governance.	None were made.	TTH

NOTES

UNIT 3

Common Characteristics of Fraud Schemes

LEARNING OBJECTIVES

When you have completed this unit, you will be able to accomplish the following:

- Describe common characteristics of major fraud schemes and scenarios.
- Understand the potential red flags for fraud and the concealment of fraud to understand the importance of a strengthened control environment.
- Identify components of an organization's system of internal control that support its ability to prevent and detect fraud.

CHARACTERISTICS OF FRAUD SCHEMES AND RISKS OF FRAUD

Risks of Fraud

In 2004, the Senate Finance Committee encouraged the Independent Sector to commission a report on ways that charitable organizations could strengthen their governance, transparency, and accountability. The Independent Sector produced two reports recommending approximately 150 actions that charities, the IRS, and Congress could take to improve governance and ethical conduct. It later issued another report called *Principles for Good Governance and Ethical Practice,* which describes 33 practices that should be adopted by board members and not-for-profit leadership. The Good Governance publication was updated and rereleased in 2018. The principles are categorized as:

- Legal Compliance and Public Disclosure
- Effective Governance
- Strong Financial Oversight
- Responsible Fundraising

Not-for-profits are notorious for failure to prosecute those that perpetrate fraud against the organization. A frequent explanation is that the negative publicity could cost the organization

donors. This also may explain why so few of the frauds in the *Report to the Nations* are specific to not-for-profits even though the number of employees and size are like the privately held companies who reported most of the frauds.

Characteristics of Fraud Schemes

The ACFE's *Report to the Nations* for 2022[8] noted that organizations with less than 100 employees tend to have greater instances of fraud. Approximately 22% of frauds noted in the study were perpetrated against organizations with less than 100 employees. However, of note is that the median loss for that group was $150,000.

Number of Employees	Percentage of Cases	Median Loss
< 100	22%	$150,000
100–999	24%	$100,000
1,000–9,999	29%	$100,000
10,000+	25%	$138,000

As discussed earlier, the Report to the Nations notes three different types of fraud schemes: fraudulent financial reporting, misappropriation of assets and corruption. Most of the frauds that are reported in the Report to the Nations involved misappropriation of assets, followed by corruption and fraudulent financial reporting.

The median fraudulent financial reporting scheme resulted in a loss of $593,000, which is significantly higher than the other categories. The most prevalent ways that fraudulent financial reporting occurs is:

- Timing differences
- Fictitious revenue
- Concealed liabilities/expenses
- Improper valuation
- Improper disclosure

The median asset appropriation scheme resulted in a loss of $100,000. The most prevalent asset misappropriation sub-schemes and median loss are noted in the table that follows.

Scheme	Description	Median Loss
Billing	A disbursement scheme in which a person causes an organization to issue a payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases.	$100,000
Noncash misappropriation	An employee steals or misuses noncash assets of the organization.	$78,000
Expense reimbursement	A disbursement scheme in which an employee makes a claim for reimbursement for fictitious expenses or inflated expenses.	$40,000
Skimming	A scheme in which cash is stolen before it is recorded in the books and records of the organization.	$50,000

8 The ACFE *Report to the Nation* for 2022 can be accessed at https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf

Scheme	Description	Median Loss
Cash on hand misappropriation	A scheme in which an employee steals cash kept on hand at the organization.	$15,000
Check or payment tampering	A disbursement scheme in which an employee steals the organization's funds by intercepting, forging, or altering a check or electronic payment drawn on one of the organization's bank accounts.	$100,000
Payroll scheme	A disbursement scheme in which an employee causes his employing organization to issue a payment for an improper amount or for a fictitious employee.	$45,000
Cash larceny	A scheme in which cash receipts are stolen after they have been recorded in the books and records (cash is recorded but the checks are stolen before they go to the bank).	$50,000
Register disbursements	A disbursement scheme in which an employee makes incorrect entries on a cash register to hide the removal of cash.	$10,000

Corruption may take the form of conflicts of interest, purchasing schemes, sales schemes, bribery, kickbacks, bid rigging, and illegal gratuities.

Perpetrators may not limit themselves to one type of scheme. Approximately 35% of perpetrators committed more than one type of fraud. Perpetrators tend to be opportunistic and steal whenever the opportunity presents itself. The most prevalent combination is asset misappropriation and corruption. This accounts for why many of the charts in the ACFE *Report to the Nations* sum to more than 100%.

Type of Fraud Scheme	Prevalence
Misappropriation of assets by itself	47%
Misappropriation of assets and corruption	32%
Corruption by itself	12%
Asset misappropriation, corruption, and fraudulent financial reporting	6%
Fraudulent financial reporting by itself	1%
Corruption and fraudulent financial reporting	1%
Asset misappropriation and fraudulent financial reporting	1%

Unfortunately, the typical time between when a fraud begins and when it is detected is 12 months for all organizations. This is good news because the 2022 Report also noted that the longer the fraud goes without detection the higher the loss as noted in the charts that follow.

Scheme	Duration of Scheme Before Identification (months)
Payroll	18
Check tampering	18
Financial statement fraud	18
Expense reimbursement	18
Billing	18

Scheme	Duration of Scheme Before Identification (months)
Cash larceny	14
Corruption	12
Cash on hand	12
Noncash	12
Register disbursements	12

The following table illustrates the median loss by duration of fraud scheme.

Duration	Median Loss
Less than 6 months	$47,000
7–12 months	$100,000
13–18 months	$125,000
19–24 months	$110,000
25–36 months	$300,000
37–48 months	$698,000
49–60 months	$800,000

The Report revealed differences in scheme velocity (amount per month stolen) based on the number of perpetrators involved in a case, as well as the position held by the primary perpetrator. Schemes with three or more perpetrators escalate faster than those with just one or two perpetrators.

In addition, schemes committed by an owner/executive have a velocity nearly three times that of schemes committed by employees and manager-level individuals. These findings emphasize how those in the highest positions can damage the company much more quickly than those in lower-level positions.

Perpetrator	Amount	Duration	Velocity
1	$57,000	12	$4,800
2	$145,000	12	$12,100
3	$219,000	12	$18,300
Employee	$50,000	8	$6,300
Manager	$125,000	16	$7,800
Owner/Executive	$337,000	18	$18,700

Concealment of Fraud

Participants in the study were asked how the perpetrators concealed the schemes. Methods of concealment were very similar no matter the type of fraud perpetrated. The most common concealment method was to alter source documents. The vast majority of perpetrators took

steps to conceal their fraud. Twelve percent of the perpetrators did not bother to try to conceal their activities.

Method	Percentage Concealed in this Manner
Create fraudulent physical documents	39%
Altered physical documents	32%
Created fraudulent electronic documents or files	28%
Altered electronic documents or files	25%
Destroyed or withheld documents	23%

Behavioral Red Flags

Perpetrators tend to demonstrate certain characteristics. The following is from the ACFE 2022 *Report to the Nations*. It provides information about the red flag and the percentage of cases reported in the survey where an employee, a manager, or an executive demonstrated the identified behavior when involved in a fraud scheme. Identifying the behavioral signs exhibited by perpetrators can help not-for-profit organizations successfully detect fraud and reduce their losses.

Red Flag	Percentage
Living beyond means	39%
Financial difficulties	25%
Unusually close association with vendor or customer	20%
No behavioral red flags	15%
Control issues, unwilling to share duties	13%
Irritability, suspiciousness, or defensiveness	12%
Bullying or intimidation	12%
Divorce/ family problems	11%
"Wheeler-dealer" attitude	10%
Excessive pressure from within the organization	8%
Addiction problems	7%
Complaints about inadequate pay	7%
Refusal to take vacations	7%
Social isolation	6%
Past legal problems	5%
Complaints about lack of authority	5%
Other employment related problems	4%
Excessive family/peer pressure for success	4%
Excessive tardiness or absenteeism	3%
Instability in life circumstances	4%
Excessive internet browsing	2%

The following are factors that could relate to the perpetrator's job performance or job security. These indicators might be noticed in human resource records. Each of these factors could

potentially cause financial stress or resentment toward an employer, which might impact a person's decision to commit fraud.

The *Report to the Nations* indicated that 50% of perpetrators exhibited at least one HR-related red flag prior to or during the time of their frauds. The three most common were fear of job loss, poor performance evaluations, and having been denied a raise or promotion.

Red Flag	Percentage
Poor performance evaluation	15%
Denied a raise or promotion	12%
Cut in benefits	7%
Cut in pay	6%
Job loss	6%
Involuntary cut in hours	4%
Demotion	4%

Committee of Sponsoring Organizations (COSO) Internal Control Integrated Framework

The COSO sets forth a framework of 17 principles that can be used to design a system of internal controls. By selecting and implementing controls from this framework, an organization can prevent, detect, and correct fraud or error. Of course, a system of internal control will never provide absolute assurance that fraud or error will be detected. There is always the likelihood that even with the best of controls there will be lapses in their effectiveness due to human nature. There is also the possibility of collusion.

There are five elements of internal control:

1. Control environment (principles 1–5)
2. Risk assessment (principles 6–9)
3. Control activities (principles 10–12)
4. Information & communication (principles13 –15)
5. Monitoring (principles 16–17)

The AICPA does not mandate the use of the COSO Framework. There are other frameworks such as the government's Green Book that sets forth a similar framework. Another popular framework is the control objectives for information and related technology (COBIT) framework. The COBIT framework is the most popular IT control framework with the IT auditor community. ISACA (Information Systems Audit and Control Association) created the COBIT framework and designed it for IT governance and management. Therefore, it is not a complete framework.

SAS 142, *Audit Evidence,* and SAS 145, an amendment to AU-C 315, the current auditor risk assessment standard, discuss changes in the characteristic of audit evidence due to more advance information technology at the auditee and changes in how the auditor gains an understanding of internal control, which includes a more robust understanding of the organization's systems and technology controls. SAS 145 makes a change to the terminology that categorizes the 5 levels of internal control. Controls that were previously categorized as entity controls are now referred to as primarily indirect controls. Control activities and application controls that address the risk of fraud or error at the transaction level are referred to as direct controls.

Anti-fraud controls can be primarily indirect as well as direct. The controls that are most associated with fraud prevention and detection are primarily direct controls. However, the primarily indirect controls are as important and maybe, in some instances, even more important. Several years ago, the International Federation of Accountants and the Chartered Institute of Management Accountants performed an analysis of large corporate failures. The study found that the failure of the primarily indirect controls, specifically a lack of ethics, a weak board, lack of a compliance/risk management function, and the role of the CEO, was the main causes of the large frauds. When management has the incentive or pressure to commit fraudulent financial reporting and a weak or colluding board supplies the opportunity, primarily direct controls are not effective.

In the 2022 *Report to the Nations*, the certified fraud examiners identified the following as the most prevalent control weaknesses. Note that most of these controls are primarily indirect controls.

Weakness	**Percentage**
Lack of internal controls	29%
Override of existing internal controls	20%
Lack of management review	16%
Poor tone at the top	10%
Lack of competent personnel in oversight roles	8%
Other	7%
Lack of independent checks/audits	5%
Lack of fraud education for employees	3%
Lack of clear lines of authority	2%
Lack of reporting mechanism	<1%

Therefore, it is important to implement a selection of controls that will set the tone from the top, provide for the assessment of risk, provide adequate information, communicate to the necessary levels of the organization, and with external parties such as regulators or auditors, and provide the appropriate level of monitoring that will set the foundation for transactional control activities. The primarily direct controls should address the risk of fraud at the transactional level and thus help to prevent or detect fraudulent financial reporting and misappropriation of assets.

EXAMPLE: Executive Director Embezzles Funds—October 2022

Control Deficiencies: Lack of management integrity and tone from the top, lack of board oversight, lack of segregation of duties, and controls over cash disbursements.

A former executive director of a children's not-for-profit organization based in New York City, was charged with embezzling funds from the organization from 2018 to 2021. The perpetrator is said to have embezzled nearly $100,000 from the organization that provides inclusive arts programming for students of all development profiles, including autistic children.

He began embezzling funds from the organization's bank account for unauthorized personal expenses in 2018. Beginning in 2019, the organization began receiving overdraft notices from the bank. The perpetrator claimed this was caused by the bank's loss of donor checks. The following year, the organization switched banks, and he continued his embezzlement. A subsequent audit revealed that he stole approximately $98,000.

While serving as the executive director, he married a fellow employee and stole her father's credit cards and on which she was an authorized user making unauthorized transactions, that later found to total more than $143,000. When caught, he said that the credit card was used to cover operational expenses for the not-for-profit organization.

With uninhibited access to the not-for-profit's systems, he impersonated the organization's treasurer by email to negotiate repayments by the organization to his wife's father. During the three-year fraud, he made hundreds of unauthorized personal transactions using the not-for-profit organization's bank accounts, such as payments for pet grooming, food delivery, restaurants, groceries, alcohol, clothing, shoes, transportation, ESPN Plus and Netflix subscriptions, Amazon orders, and wedding photography services. He also withdrew thousands of dollars in cash from the not-for-profit organization's accounts.

EXAMPLE: Collusion Results in $250 Million in Federal Award Fraud

Control Deficiencies: Lack of management integrity and tone from the top, lack of internal controls over grant programs, lack of board oversight

In September 2022, federal authorities charged 47 people with conspiracy and other counts in what is believed to be one of the largest fraud schemes to take advantage of the COVID-19 pandemic by stealing $250 million from a federal program that provides meals to low-income children.

Feeding Our Future, a not-for-profit organization, created other organizations that claimed to be offering food to tens of thousands of children across Minnesota, submitting requests for reimbursement for those meals through the U.S. Department of Agriculture's child nutrition programs. Prosecutors say few meals were really served. The perpetrators used the money to buy luxury cars, property, and jewelry.

The organization's founder and executive director was indicted although she claimed to have no knowledge of the fraud. Investigators stated that she and others in her organization submitted fraudulent claims for reimbursement and received kickbacks.

Federal officials noted that the government was billed for more than 125 million fake meals, with some defendants making up names for children by using an online random name generator. He displayed one form for reimbursement that claimed a site served exactly 2,500 meals each day Monday through Friday. It was interesting to note that during that time no children were ever reported as sick or were otherwise missing from the program. At this time, the government has so far recovered $50 million in money and property and expects to recover more.

In Minnesota, the funds are administered by the state Department of Education, and meals have historically been provided to children through educational programs, such as schools or day care centers. The sites that serve the food are sponsored by public or nonprofit groups, such as Feeding Our Future. The sponsoring agency retains 10% to 15% of the reimbursement funds as an administrative fee in exchange for submitting claims, sponsoring the sites, and disbursing the funds.

During the pandemic, some of the standard requirements for sites to participate in the federal food nutrition programs were waived. The USDA allowed for-profit restaurants to participate and allowed food to be distributed outside educational programs. The documents stated that the perpetrators exploited these rule changes for personal gain. Feeding Our Future sponsored the opening of nearly 200 federal child nutrition program sites throughout the state.

In one instance, the court documents described a small storefront restaurant that typically served only a few dozen people a day. Two defendants offered the owner $40,000 a month to use his restaurant, then billed the government for approximately 1.6 million meals through 11 months of 2021. They listed the names of around 2,000 children—nearly half of the local school district's total enrollment. Only 33 names matched actual students.

Feeding Our Future received nearly $18 million in federal child nutrition program funds as administrative fees in 2021 alone, and the executive director and other employees received additional kickbacks, which were often disguised as "consulting fees" paid to shell companies.

Primarily Indirect Internal Controls

As noted at the beginning of this program it is management's responsibility to implement a system of internal controls to prevent, detect, and correct errors or fraud.

Control Environment

Principles 1 through 5 fall within the **control environment** element. These include an organization level commitment to integrity and ethical values, independence, and oversight of internal control by the board of directors, and an organization level commitment to attract and retain competent staff.

Commitment to ethical values can be demonstrated in many ways. One way is to provide employees with a mechanism to report suspicious behavior.

Reporting Mechanisms

The chart below sheds some light on how frauds are detected. Although there are many ways that fraud is detected, it is most likely to be detected by a tip, most frequently from an employee. Tips also come from customers, vendors, competitors, or anonymous tipsters. The following are the most prevalent ways that fraud is detected. The 2022 *Report to the Nations* identifies formal reporting mechanisms as a technique that can have a substantial impact on reporting. As noted below, employees are a major source of tips.

Some people have an erroneous belief that the independent audit is the way fraud gets detected. As noted in the chart below that was only true 4% of the time. The most prevalent ways that fraud is detected are noted as follows.

Medicaid

Detection Method	Median Duration	Median Loss	Detection Method	Percentage
By accident	23 months	$100,000	Passive detection	5%
External audit	20 months	$219,000	Potentially active or passive detection	4%
Notified by law enforcement	18 months	$500,000	Passive detection	2%
Confession	14 months	$159,000	Passive detection	1%

Detection Method	Median Duration	Median Loss	Detection Method	Percentage
Automated system monitoring/IT controls	6 months	$50,000	Passive detection	4%
Surveillance	6 months	$60,000	Active detection	3%
Account reconciliation	8 months	$74,000	Active detection	5%
Management review	12 months	$105,000	Active detection	12%
Internal audit	12 months	$108,000	Active detection	16%
Tip	12 months	$117,000	Potentially active or passive detection	42%
Document examination	12 months	$200,000	Active detection	6%

The bolded detection mechanisms noted are internal controls. It is easy to see that implementing strong internal controls can be very important in preventing or detecting fraud.

Even though a tip from an employee or third party is not a control itself, since most of the frauds are detected by tips, it is important for management to ensure that a reporting mechanism is in place. As shown, employees are a major source of tips.

Source of Tip	Percentage
Employee	55%
Customer	18%
Anonymous	16%
Vendor	10%
Other	5%
Competitor	3%
Shareholder/owner	3%

The 2022 *Report to the Nations* stated that 70% of victim organizations had hotlines. Hotlines, however, have changed forms from previous reports. In previous studies, telephone hotlines were the most common mechanism whistleblowers used. However, in 2022 telephone hotline use has declined substantially, while email and web-based/online reporting hotlines have dramatically increased. These findings demonstrate that whistleblowers' preferred methods of reporting fraud are diverse and evolving, particularly regarding online and electronic forms. Accordingly, organizations should maintain multiple channels for reporting fraud. Fraud loss is two times higher without a hotline.

Reporting Mechanism	2022 Percentage	2016 Percentage
Email	40%	34%
Web-based/online form	33%	24%
Telephone hotline	27%	40%
Mailed letter or form	12%	17%
Other	9%	12%

Often people ask to whom and at what level the communication of fraud or suspected fraud should be addressed. Whistleblowers reported suspicions to their direct supervisor 30% of the time.

Suspicions Reported to	**Percentage**
Direct supervisor	30%
Executive	15%
Internal audit	12%
Fraud investigation team	12%
Other	9%
Board or audit committee	9%
Coworker	8%
Law enforcement or regulator	8%
Owner	8%
Human resources	5%
In-house counsel	3%
External audit	1%

Another important control in the control environment is to run background checks on individuals before they are hired. Some of the types of investigatory procedures may work better than others. For example, although an organization may run criminal background checks, often they come up empty. One reason for this is the reluctance of organizations to report activity to authorities or prosecute.

Background Check Run on Perpetrator	**Percentage**
Employment history	45%
None	43%
Criminal checks	40%
Reference checks	30%
Education verification	30%
Credit checks	21%
Drug screening	11%
Other	2%

People frequently wonder why cases are not reported to law enforcement officials. The most common reasons are the belief that internal discipline is sufficient followed by the fear of bad publicity. This information is from the 2020 Report.

Reason That Fraud Is Not Reported	**Percentage**
Internal discipline sufficient	46%
Fear of bad publicity	32%
Private settlement	27%
Too costly	17%
Lack of evidence	10%
Civil suit	6%
Perpetrator disappeared	1%

The ACFE notes that organizations are taking note of the need for anti-fraud controls. Most of the anti-fraud controls identified in the survey are primarily indirect controls related to the control environment. The most common controls and the percentage of organizations in the survey are shown in the following table.

Anti-Fraud Control	Percentage Implemented	COSO Category
External audit (note that the external audit is not a control even though it is listed in the ACFE survey)	82%	N/A
Code of conduct	82%	Control environment
Internal audit department (if the internal auditors focus on the area of financial reporting)	77%	Monitoring
Management Certification of Financial Statements	74%	Monitoring
External audit of internal controls over financial reporting (if performed as a control and not a required integrated audit)	71%	Monitoring
Hotline	70%	Control environment
Management review (could be monitoring if management is reviewing internal control effectiveness). Or could be a control activity.	69%	Monitoring or Control activity
Independent audit committee	67%	Control environment
Fraud training for employees	61%	Control environment
Anti-fraud policy	60%	Control environment
Fraud training for management and executives	59%	Control environment
Employee support programs	56%	Control environment
Dedicated fraud department, function, or team	48%	Control environment/ Monitoring
Formal fraud risk assessment	46%	Risk assessment
Proactive data monitoring/analysis	45%	Control activity
Surprise audits	42%	Monitoring
Job rotation/mandatory vacation	25%	Control environment
Rewards for whistle blowers	15%	Control environment

The increase in the implementation of controls over the last 10 years has been significant.

Anti-Fraud Control	2012	2022	Increase
Hotline/reporting mechanism	54%	70%	16%
Fraud training for employees	47%	61%	13%
Anti-fraud policy	47%	60%	13%
Fraud training for managers/executives	47%	59%	12%
Formal fraud risk assessments	36%	46%	11%

Risk Assessment

The **risk assessment** element comprises principles 6 through 9. These cover clarity of objectives, identification, and management of risks, potential for fraud, and identification and

assessment of changes that could impact the internal control system. Principle 8, dealing with fraud risk, is of particular importance. **The organization considers the potential for fraud in assessing risks to the achievement of objectives.**

Management and the board should consider the potential for fraud in financial reporting, non-financial reporting, misappropriation, and illegal acts. They should be particularly aware of potential issues in the areas of:

- Lack of segregation of duties
- Management bias
- Estimates
- Common frauds in their industry
- Geographic regions
- Incentives
- IT
- Complex or unusual transactions
- Management override

The not-for-profit should assess the risk of fraud. The fraud risk assessment should identify where the organization is vulnerable to fraud.

EXAMPLE

The management of a not-for-profit healthcare clinic received a notice from the state Medicaid department stating that they were being investigated for suspicious billing patterns. During the past 9 months a coding pattern emerged that indicated a possibility of upcoding to receive a higher reimbursement. The CFO was concerned and began an investigation of the issue. Based on discussions with the personnel involved in billing the CFO learned that employees were encouraged to make aggressive interpretations of physician documentation when possible. The CFO considered why the billing manager might give those instructions since the instruction did not come from senior management. Since this issue involved fraudulent financial reporting and not employee theft the CFO concluded that the new performance bonus arrangement for the year could have caused the manager to give the employees those directives.

Management and the board should consider incentives/pressures internally and externally, the effectiveness of the organization's internal controls and reasons why employees might rationalize inappropriate behavior.

Management and the board should be aware that fraud risk increases with complex or unstable organization structure, high turnover, poor controls, or deficient controls over information technology. Perpetrators often rationalize by considering theft as *borrowing*, believing they are *owed* and not caring about consequences.

Information and Communication

Principles 13 through 15 fall within the **information and communication** element. Information and communication can be primarily indirect controls or in the case of IT applications, direct controls. The proper functioning of the IT system and adequate communication between management and employees, management and the board,

management and regulators or other outside parties, and management and the board with the external auditor. The COSO objectives for information and communication are as follows:

- The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.
  - Management identifies information requirements, identifying and defining those requirements at the relevant level and with specificity. This is an ongoing and iterative process.
  - Management ensures that the information system processes relevant data, capturing and processing large volumes of data from internal and external sources into meaningful, actionable information to meet defined information requirements.
  - Management ensures that information systems maintain quality throughout processing
- The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

Monitoring

Principles 16 through 17 fall within the **monitoring** element. Monitoring is an important level of internal control. In this category, management and the board evaluate the quality of the organization's internal control including anti-fraud controls. Some internal controls that can play a role in preventing or detecting instances of fraud are as follows:

- The board receives and reviews periodic reports describing the nature, status, and disposition of alleged or suspected fraud and misconduct.
- An internal audit plan (if the not-for-profit is large enough) that addresses fraud risk and a mechanism to ensure that the internal auditor can express any concerns about management's commitment to appropriate internal controls or report suspicions or allegations of fraud.
- The involvement of other experts—legal, accounting, and other professional advisers—as needed.
- A review of accounting principles, policies, and estimates used by management in determining significant estimates.
- The review of significant nonroutine transactions entered into by management.
- The functional reporting by internal and external auditors to the board and audit committee.

The 2022 ACFE Report shows that frauds are being caught faster and causing smaller losses. The median losses from 2012–2022 decreased 16%. The median duration of fraud decreased 33% during the same time.

Primarily Direct Controls

Principles 10 through 12 fall within the **control activities** element. They are considered primarily direct controls because they support the mitigation of risks to the achievement of objectives to acceptable levels. They should be tailored to the entity's specific characteristics and information technology as well as the complexity of the entity. The broad categories that these controls fall in to follow:

- Management integrates internal control with the risk assessments that are performed. Control activities support all the components of internal control but are particularly

aligned with the risk assessment component. Along with assessing risks, including the risk of fraud, management identifies and puts into effect actions needed to carry out specific risk responses.

- Management evaluates a mix of control activity types to prevent, detect, and correct the risk of error and fraud. Control activity types considered are:
  - Authorizations and approvals
  - Verifications
  - Physical controls
  - Controls over standing data (e.g., master files)
  - Reconciliations
  - Supervisory controls
- Management considers a mix of control activities that are preventive and detective. In doing so, management considers the precision needed from the control as well as what the control is designed to accomplish.
- Management selects and develops a mix of controls that operate more broadly and at higher levels. These are usually business performance or analytical reviews involving comparisons of different sets of operating or financial data. These relationships are analyzed, investigated, and corrective action is taken.
- Management addresses segregation of duties, which is intended to reduce the risk of error or inappropriate or fraudulent actions. Segregation generally separates responsibility for authorizing, approving, and recording transactions, and handling the related asset. In small organizations, ideal segregation may not be practical, cost effective, or feasible, and alternative control activities must be designed.
- Management designs procedures that specify when a control and any corrective actions should be performed to help ensure that controls are executed in a timely manner.
- Management ensures that corrective action is taken in response to issues identified. Matters identified for follow-up should be investigated and corrective action taken if needed.
- In performing a control, management evaluates the competency of personnel performing the control. A well-designed control cannot be performed unless the entity uses competent personnel with sufficient authority.
- Management periodically reassesses policies and procedures and related controls for continued relevance and effectiveness.

Unit 4 discusses examples of specific frauds and recommended controls to prevent or detect them.

Cyber Fraud

One type of fraud that is not identified in the ACFE reports is cyber fraud. This is because the ACFE reports on occupational fraud (fraud internal to the organization) and cyber fraud is generally thought to be acts from the outside perpetrated against the organization entity. It is mentioned here because there are some things auditors should consider when addressing internal controls related to the prevention and detection of cyber fraud.

Ten years ago, this issue plagued larger companies but did not register very high on the not-for-profit risk scale. Today, data breaches can cause significant financial and reputational damage to a not-for-profit. Not-for-profits collect personally identifiable information such

as health information, social security numbers, employee and volunteer records, and billing information, and this information, even with a good internal control system, is subject to breach. The impact on the entity and its employees can be damaging. Stolen data can be sold or used by hackers. Sometimes, what hackers want is payment. Organizations, particularly hospitals, are being blackmailed into paying ransom to hackers to regain access to data, or in the case of a Muncie, Indiana, not-for-profit, to return the data and not publish it.[9] There can also be legal and regulatory ramifications.

According to Verizon's *2021 Data Breach Investigations Report*, ransomware attacks are still going strong. They account for nearly 61.2% of incidents where malware was used. Ransomware attacks have become so common that they are less frequently mentioned in the media unless there is a high-profile target in the mix. However, it is still a serious threat to all industries, including not-for-profit organizations. Ransomware can stop the processing of an entity until a ransom is paid to unlock the system. Most not-for-profit organizations will pay the ransom to get back up and running again. Ransomware is predicted to cost its victims more around $265 billion annually by 2031, according to Cybersecurity Ventures, with a new attack every two seconds as ransomware perpetrators progressively refine their malware payloads and related extortion activities. The dollar figure is based on 30% year-over-year growth in damage costs over the next 10 years. This rise makes ransomware the fastest growing type of cybercrime. The cost was $325 million in 2015 and $11.5 billion in 2019.

Cybersecurity and data security are related but deal with different aspects of information technology management. Cybersecurity focuses on protecting networks and infrastructure from attacks. Data security focuses on securing personal information. There are a variety of laws regulating both types of issues.

According to Venable, a national law firm, cybercrimes affect approximately 1 million victims daily and cost over $450 billion a year globally. This is a 200% increase in cost from 2010 to 2015.[10] Allianz Group, a leading global corporate insurance carrier, noted that in 2020, cyber incidents rank as the most important business risk in its annual risk barometer. Compare this with 2013, where cyber incidents were ranked 15th in its annual risk barometer.[11] This increased risk is driven by organizations' increasing reliance on data and IT systems. Overall, cyber incidents are becoming more sophisticated and targeted as criminals seek higher rewards with extortion demands. The Ponemon Institute identified that the three main causes of data breach from its study, *2020 Cost of Data Breach Report*,[12] are:

- Malicious attack (52%)
- System glitch (25%)
- Human error (23%)

This illustrates that cybersecurity threats are escalating, unnerving the boards of directors, managers, investors, and other stakeholders of organizations of all sizes—whether public or private.

Organizations are under pressure to demonstrate that they are managing threats, and that they have effective processes and controls in place to detect, respond to, mitigate, and recover from

9 https://nonprofitquarterly.org/2017/06/08/nonprofit-cybersecurity-pay-attention/.

10 https://www.venable.com/files/Event/8f068f95-0d0d-47c1-8045-df53e73a1445/Presentation/EventAttachment/c3d6a15c-9bd9-429d-a4ba-b9c18afc604b/Top-Ten-Cybersecurity-Tips-for-Nonprofits-Managing-Your-Technical-and-Legal-Risks-handouts-02-02-2.pdf

11 https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2020-cyberincidents.html

12 https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf

cybersecurity events. Where appropriate, organizations can consider obtaining a SOC for Cybersecurity.[13]

The COVID-19 pandemic has had a significant impact on the way many not-for-profit organizations operate, with large numbers of employees working remotely from home. This situation caused an increased demand for video conferencing, cloud applications, and network resources. Seventy-six percent of organizations that participated in the Ponemon Institute study indicated that remote work made responding to a potential data breach a much more difficult ordeal. The study found that remote work during the COVID-19 pandemic increased the time to identify and contain a potential data breach. By having a remote workforce, the total average cost of a data breach increased by nearly $137,000.

Although many people believed that once the risks of the various strains of COVID-19 were reduced, most employees would return to the bricks and mortar workplace. Some have but other organizations have decided that employees do not need to be onsite to be productive and intend to reduce space requirements when their leases expire. Some are subleasing excess space to other organizations. This suggests that organizations should continue to train employees related to the cyber risks that exist now and, in the future, and enforce their policies and procedures related to accessing the organization's systems remotely.

The degree of complexity of data security solutions and the skilled employees it takes to monitor and manage them is a barrier to implementation. The cost is also a factor for many organizations. The following table outlines several threats that not-for-profits face.

Threat	**Defined**
Hackers/ hacktivists	Hackers are people who use computers to gain unauthorized access to data. They can be criminal groups, cyber criminals, or script kiddies—people who use existing computer scripts or code to hack into computers because they don't have the expertise to write their own. A hacktivist is a hacker with a political agenda.
Insiders	Insiders look for deficiencies in internal controls to gain unauthorized access to data, or if they are authorized to have access, use the data for gain.
Spyware/malware	Spyware is a type of software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive. Malware is software that is intended to damage or disable computers and computer systems.
Ransomware	Ransomware is a type of malicious software from crypto virology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.
Social engineering	Social engineering is psychological manipulation of people into performing actions or divulging confidential information. Examples include: Posing as IT personnel to get employees to divulge their passwords; learning the company lingo to convince employees they are legitimate; or pretending to be law enforcement, IRS, or other types of agents. These threats can be in person, via email, on the phone, or through other electronic means.

13 AICPA. "SOC for Cybersecurity: Information for Organizations." AICPA. Accessed November 16, 2021. https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/cybersecurityfororganizations

A risk assessment is an important step in identifying all the areas where the network is vulnerable, starting with an inventory of digital assets. The Nonprofit Technology Network suggests that the first step in assessing a not-for-profit entity's data risks is to take inventory of all the data the not-for-profit collects and identify where it is stored.[14] Not-for-profit organizations should answer these questions:

- What data do we collect?
- What do we do with it?
- Where do we store it?
- Who do we share it with?
- Who is responsible for it?
- What do we do when we are done with it?
- Do organizations and individuals on which we collect data know we possess it?
- Do they know what we do with it?
- Does it identify them personally?
- What do we do if they want their data back?

As part of its data inventory assessment, not-for-profit organizations should consider the cost associated with maintaining all the data it maintains as well as the associated benefits of maintaining such data. Many not-for-profits may find that there is data kept that may not be needed. In such instances, not-for-profit organizations should decrease or limit the data they amass and modernize their storage process (as well as their process for destroying data). One helpful approach is to divide data identified into the following three categories: (1) data that cannot be lost, (2) data that cannot be exposed, and (3) nonessential data. In some instances, some data identified may be classified as both data that cannot be lost *and* exposed. This would indicate that these items are the not-for-profit's highest priority to protect. This is the first step toward mitigating risks.

Not-for-profits will continue to confront new and evolving cyber risks that they will need to mitigate. To help address these challenges, not-for-profits should consider utilizing the guidance *Managing Cyber Risks in a Digital Age*, released by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in collaboration with Deloitte Risk & Financial Advisory in December 2019.[15] The guidance provides insight into how not-for-profit organizations can leverage the five components and 20 principles of the Enterprise Risk Management (ERM) Framework to identify and manage cyber risks. The guidance notes that the fast-evolving cyber threat landscape makes it imperative for organizations to increase their cyber proficiencies and capabilities so that they may effectively assess how well these risks are being addressed.

As part of its assessment, not-for-profit organizations should consider its need for insurance. Cybersecurity insurance is available, and while it may not mitigate reputational risk, it can be very helpful in paying for the remediation that will need to be performed after an attack. It is important to develop policies and procedures and then provide security awareness training to users. The entity should also develop an incident response plan to help contain any breach that occurs.

It is important to evaluate the entity's firewalls and spam filtering system. In addition, it is important to perform operating system updates. Intrusion prevention and detection

14 https://www.nten.org/article/assessing-risk-protect-valuable-data/

15 To access this guidance, visit: https://www.coso.org/Documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-Digital-Age.pdf

software could be used in addition to next-generation anti-virus/anti-malware software. Many organizations are using multifactor authentication. Some fixes are as easy as forcing staff to use different and changing passwords and ensuring that the training that should be given to all employees on cybersecurity is thoroughly understood so it can be implemented. This includes verifying when transactions involve cash as noted in the illustrations that follow.

EXAMPLE

A hacker infiltrated the IT system of a not-for-profit entity and was able to read email and interoffice communications on the entity's server. The Controller and the CFO were having a series of discussions over email and through interoffice communications about a wire transfer that was to occur when the amount became known. One day the Controller got an email from the CFO instructing him to transfer $200,000 to the vendor as they had previously discussed. The email sounded like it came from the CFO (the hacker had learned the entity lingo and acronyms). The Controller made the transfer to the vendor with the routing number and account specified in the email. It was not until later that day when he saw the CFO that he learned that the email was not real.

Note that hackers create new schemes once people become aware and don't fall for their old ones. In a similar instance, a vendor asked a not-for-profit to change the payment routing instructions. The employee hovered the cursor over the email address to ensure it was from a bona fide employee at the vendor. Noting no discrepancy but still wanting to confirm that the instructions were authorized, the employee called the vendor. There she learned that no such instructions had been sent.

Strong internal control can help to prevent or detect fraud on the part of employees. It can also help to identify areas where the organization is at risk of fraud from external parties. There have been numerous articles written recently about **cyber fraud**. With more and more organizations dealing in some way with e-commerce, this has become a more significant threat. The AICPA issued a special report that discussed the top five cybercrimes.[16] Four of those are of particular concern to not-for-profits:

1. **Corporate Account Takeover**. In this fraud, the perpetrator illicitly acquires login information for the victim's online bank access and hacks into the victim's computer, enabling him to bypass additional bank security protocols, and transfers money to an account he controls, often in a foreign country. Cyber criminals prefer to target small- to mid-size organizations because of their weaker cyber security. The commencement of the global pandemic and its subsequent uncertainty have further bolstered perpetrators. Federal agencies such as the Federal Trade Commission (FTC), Department of Justice (DOJ), and the Federal Bureau of Investigation (FBI) have all advised that perpetrators are aggressively targeting organizations with COVID-19–related frauds. Not-for-profit organizations are likely to face the increased threat of account takeovers in 2022 and beyond as perpetrators continue to look for ways to con all different types of organizations.
2. **Identity Theft**. This occurs when a cybercriminal steals personally identifiable information. There is often no direct financial benefit to the criminal; rather, this crime empowers the perpetrator to other crimes such as opening a line of credit, purchasing goods or services, renting, or buying a house or apartment, receiving medical care, or obtaining employment, all using the name and credit of the victim. Any entity can potentially be a victim. For example, in May 2020, Blackbaud, a leading cloud software company used by many not-for-profit organizations, fell victim to a ransomware attack. The perpetrators copied a subset of data before being locked out. Information compromised in the breach included telephone numbers, email addresses, dates of birth, mailing addresses, donation

16 The Top 5 Cybercrimes – AICPA, 2013.

dates, donation amounts, and other donor profile information. Blackbaud ultimately paid the ransom and received confirmation from the hackers that the information compromised was destroyed. For a not-for-profit that has sensitive information from donors such as credit card numbers or bank account information, this highlights the need to have controls to prevent their theft.

3. **Theft of Sensitive Data**. This is like identity theft but involves additional types of data as well. For example, a cybercriminal might copy an organization's customer or donor files onto a flash drive and sell them to a competitor.
4. **Theft of Intellectual Property**. Any intellectual property, such as copyrighted, patented, or proprietary data, may become the target of cybercriminals. According to a *New York Times* article quoted by the AICPA, this form of cybercrime is complicated by state-sponsored hacking, especially China.

Small organizations face unique challenges in combatting fraud, from limited financial resources and smaller staff sizes that require many individuals to perform numerous functions, to the large amount of trust needed to keep operations running and the business growing. Unfortunately, that means that many of the protective anti-fraud controls that larger organizations rely on are simply not enacted within small businesses. The study showed the implementation rates of anti-fraud controls at small businesses (i.e., organizations with fewer than 100 employees) compared to their larger counterparts. Across all 18 controls, small organizations had notably lower levels of implementation; even the most common controls—external audits of financial statements and a formal code of conduct—were only in place at 53% of small businesses in our study, compared to approximately 90% of larger organizations.

UNIT 4

Fraud Schemes and Controls

LEARNING OBJECTIVES

When you have completed this unit, you will be able to accomplish the following:

- Apply knowledge obtained to identify, detect, and prevent fraud schemes.
- Construct effective internal controls that prevent and/or detect potential fraud schemes.
- Critique an organization's control design and determine potential control deficiencies and possible improvements in an organization's controls.

ANTI-FRAUD CONTROLS REDUCE LOSSES AND TIME TO DETECT

The *Report to the Nations* concluded that the presence of anti-fraud controls is associated with lower fraud losses and quicker detection. According to the study, 81% of victim organizations modified their anti-fraud controls following the fraud. Specifically, 75% increased management review procedures and 64% increased the use of proactive data monitoring and analysis. Job rotation and mandatory vacation policies and surprise audits were very effective contributing to a 50% decrease in the loss. They are among the **least** used anti-fraud controls. There is significant room for improvement here.

Management of not-for-profits should consider evaluating the improvement that control implementation can make relative to fraud loss.

Anti-Fraud Control	**Percentage of cases**	**Percentage reduction in loss if control is in place**	**Difference in time to detect when control is implemented**
External audit of financial statements*	82%	33%	18 mos. to 12 mos.
Code of conduct	82%	40%	18 mos. to 12 mos.

Anti-Fraud Control	Percentage of cases	Percentage reduction in loss if control is in place	Difference in time to detect when control is implemented
Management certification of financial statements	74%	29%	18 mos. to 12 mos.
Management review	69%	33%	18 mos. to 12 mos.
External audit of internal control over financial reporting	71%	33%	18 mos. to 12 mos.
Internal audit department	77%	33%	18 mos. to 12 mos.
Employee support programs	56%	25%	No change
Independent audit committee	25%	54%	18 mos. to 12 mos.
Hotline	70%	50%	18 mos. to 12 mos.
Anti-fraud policy	60%	45%	18 mos. to 12 mos.
Fraud training for employees	61%	45%	18 mos. to 12 mos.
Fraud training for managers/ executives	59%	39%	18 mos. to 12 mos.
Proactive data monitoring/ analysis	45%	47%	18 mos. to 8 mos.
Surprise audit	42%	50%	18 mos. to 9 mos.
Dedicated fraud department or team	48%	33%	18 mos. to 10 mos.
Formal fraud risk assessment	46%	45%	18 mos. to 10 mos.
Job rotation/mandatory vacation	25%	54%	16 mos. to 8 mos.
Rewards for whistleblowers	15%	5%	13 mos. to 8 mos.

* Note: The auditor is not considered an internal control although the study illustrates it that way.

It appears that more organizations are implementing anti-fraud controls. The increase from 2010 and 2020 shows a significant change.

Control	2010	2020	Increase
Hotline	51%	64%	13%
Anti-fraud policy	43%	56%	13%
Fraud training for employees	44%	55%	11%
Fraud training for managers/executives	46%	55%	9%

Fraud Schemes and Anti-Fraud Controls in Smaller Organizations

Smaller organizations experience fraud in different ways than larger ones. Smaller organizations are defined as those with fewer than 100 employees. Larger organizations have 100 or more employees. Fraudulent financial reporting occurred in 5% of smaller

organizations and 10% of larger ones. Corruption occurred in 24% of smaller organizations and 54% of larger ones.

The most prevalent types of asset misappropriation schemes by size of organization follow.

Scheme	Description	Median Loss (all organizations)	Percentage of Smaller Organizations	Percentage of Larger Organizations
Billing	A disbursement scheme in which a person causes an organization to issue a payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases.	$100,000	13%	19%
Expense reimbursement	A disbursement scheme in which an employee makes a claim for reimbursement for fictitious expenses or inflated expenses.	$40,000	7%	11%
Skimming	A scheme in which cash is stolen before it is recorded in the books and records of the organization.	$50,000	9%	8%
Check or payment tampering	A disbursement scheme in which an employee steals the organization's funds by intercepting, forging, or altering a check or electronic payment drawn on one of the organization's bank accounts.	$100,000	10%	8%
Payroll scheme	A disbursement scheme in which an employee causes his employing organization to issue a payment for an improper amount or for a fictitious employee.	$45,000	8%	8%

Scheme	Description	Median Loss (all organizations)	Percentage of Smaller Organizations	Percentage of Larger Organizations
Cash larceny	A scheme in which cash receipts are stolen after they have been recorded in the books and records (cash is recorded but the checks are stolen before they go to the bank).	$50,000	7%	7%
Register disbursements	A disbursement scheme in which an employee makes incorrect entries on a cash register to hide the removal of cash.	$10,000	1%	3%
Cash on hand misappropriation	A scheme in which an employee steals cash kept on hand at the organization.	$15,000	7%	9%
Noncash	Scheme where noncash assets such as equipment and supplies are stolen.	$78,000	9%	19%

Small organizations face more challenges than larger ones. Limited financial resources and smaller staff sizes often resulting in lack of segregation of duties are the most significant. Unfortunately, that means that many of the protective anti-fraud controls that larger organizations rely on are not implemented in smaller organizations, within small businesses. The following chart shows the implementation rates of anti-fraud controls at organizations with fewer than 100 employees compared to their larger counterparts. Smaller organizations had lower levels of implementation in all 18 controls.

Fraud in Charitable, Educational, Social Service, and Health Care Organizations

EXAMPLE: Billing Schemes—Juvenile Justice Organization Defrauded of $1.8 Million

A small juvenile justice organization was short staffed. One woman, who held the position of Secretary to the Board, had the ability to initiate transactions, process transactions, approve transactions, and write checks. She reconciled the bank statements and performed analytics for the board package. Unbeknownst to the CFO and board she created a fictitious company. Her scheme lasted over seven years.

The secretary paid legitimate vendors from her fictitious company and then billed the Juvenile Justice organization. Her bills to the Juvenile Justice organization were inflated so she was making a 25% markup on legitimate expenses. To help ensure there were no

questions about the expenses she kept the account balances constant. The CFO and the board did not see any significant fluctuations month to month and the auditors never questioned balances that did not have more than a 10% variance.

This was a recurring engagement for the audit firm. This was their third year performing the audit. The year they were engaged the board asked them to remove the material weakness dealing with lack of segregation of duties from the AU-C 265 letter. They agreed on the condition that a board review the checks each month before they were released and that the full board review the monthly analytics.

The auditors were notified of the issue when the legislative auditor wrote to them asking to review the workpapers. The fraud was identified by an attorney that was sitting in on a board meeting. During the presentation of financial results for the month he observed that the balance of certain accounts appeared high. He suggested that the organization go out to bid. The CFO handled the search for a new vendor and in the process discovered the fictitious company.

The secretary was prosecuted but was unable to repay the $1.8 million.

Analysis: Lack of segregation of duties was the primary issue in this case. The fraud had been going on so long the new auditors did not question the vendor as one that was unusual. The expenses were in a category that fluctuated with volume. Since the volume of juveniles served changed from year to year, an analytic using financial and nonfinancial information might have detected an unusual pattern. The board appeared to be involved. However, they were not trained in evaluating the risk of fraud and although they asked questions at board meetings, they did not perform a risk analysis. The board was not sufficiently trained to review expense analytics. The board member reviewing the checks prior to mailing saw the fictitious invoices as documentation and never questioned the vendor.

The organization should evaluate how it may be possible to better segregate duties. The CFO may need to take on more accounting responsibilities. The organization should implement a vendor approval system. Analytics using financial and nonfinancial information will help to identify rate variances. The CFO and the board should assess the risk of fraud on a regular basis and implement anti-fraud controls.

EXAMPLE: Check or Payment Tampering, Embezzlement, Skimming, Billing Schemes, and Cash Larceny

Louise Distefano embezzled $209,000 from Turning Pointe Therapeutic Riding Center in Westerly, Rhode Island. She was charged after the not-for-profit reported that money was missing from the organization. Turning Pointe offers riding lessons for people with disabilities at a farm and was in danger of closing because of financial issues. In trying to understand why the organization was in such dire straits, a member of the Board of Directors for the organization performed an analysis and determined that money had not been deposited. Distefano was the bookkeeper. Under questioning, Distefano told the police that she stole cash but claimed to have repaid part of it. Bank of America disclosed that 317 checks, totaling $165,886 and written to Turning Pointe, were deposited in her checking account.

Distefano opened an account at The Washington Trust Company and deposited a $25,000 grant check from the Lattner Family Foundation into it. She used that account to write approximately 40 checks to herself for expenditures for daily supplies. She also deposited approximately $10,000 of checks written to Turning Pointe for boarding (horses) into her checking account. She also wrote checks to her former employer, a heating and air conditioning company, from the Turning Pointe checking account, which she deposited into her own checking account.

Distefano said that she was able to perpetrate the fraud because there was very little oversight of her work. If Turning Pointe had checked, they would have discovered that she had been charged for larceny in connection with a fraud against an elementary school.

Analysis: Distefano committed the following fraud schemes:

Skimming or Cash Larceny—It was hard to tell whether the checks were logged and recorded and then stolen or whether they were stolen before they ever hit the books and records. Regardless, Distefano opened an unauthorized bank account and deposited the grant check and deposited the smaller checks into her own personal account.

Billing—Distefano wrote checks to a vendor where services were not rendered (air conditioning company) and wrote checks for personal bills out of the unauthorized bank account.

Expense Reimbursement—Distefano wrote checks to herself reimbursing for supplies that she never purchased on behalf of the entity.

Board Discovery—Although it took a while, a board member finally looked at the poor financial position of the entity. When he discovered the money was missing, he called in the authorities and terminated Distefano. Many not-for-profits try to handle the issues privately and don't prosecute.

Some of the fraud symptoms that might have alerted the Board of Directors to fraudulent activity were:

- Cash sales (boarding revenue) differing from normal or expected patterns
- Cash deposits differing form normal or expected patterns
- Lack of segregation of duties
- Unusual reconciling items on bank reconciliations
- Differences between daily list of receipts and deposits on bank statements
- Increased use of petty cash fund
- Lack of vacation on part of bookkeeper
- Increase in expenses
- Unusual vendors noted

The board should have reviewed financial statements regularly and asked questions. Where there is a lack of segregation of duties, and in this case, where there is a lack of financial executives, it is very important that someone assume the review role, even if it is a board member.

Background checks and perhaps even credit checks should have been performed.

Code of conduct/conflict of interest statements for the board and employees—this may or may not have set the tone since there was one employee who had access to virtually all assets and a lack of monitoring. If she felt like she was being held accountable, it may have had a deterring factor, or she may have quit.

Monitoring in the form of reviewing bank reconciliations, subsidiary ledgers, budget to actual, etc. Setting an expectation for boarding revenue and comparing it to actual, monitoring the compliance with the grant document, including ensuring the funds were received and deposited.

EXAMPLE: Procurement Fraud, Kickbacks

Ralph Clark was hired by the Woodruff Arts Center in Atlanta as an HVAC mechanic. The next year he was made acting director of facilities. Five years later Clark pleaded guilty to embezzling more than $1.1 million from the Woodruff Arts Center.

As director of facilities, Clark was authorized to approve vendor contracts up to $50,000. He embezzled the money by submitting invoices from his wife's business, Lowe's Services, for goods and services that were never provided or were performed by Clark himself. He would then pick up the checks for the payments and deposit them into accounts that he controlled. Clark also demanded that another maintenance vendor inflate invoices to the Center by 30% and remit the extra 30% to him.

In February 2014, Clark was sentenced to two years and six months in prison plus three years supervised release and ordered to repay $1 million embezzled from the Center.

Analysis: Fraud involving vendor contracts, sometimes with kickbacks generally happens when internal controls over procurement are lax and large procurements are made. It appears that the organization did not require competitive bidding and monitor to ensure contracts were awarded fairly or have a new vendor approval process. Where with the small juvenile justice organization one might not expect to see this sort of control, in a large organization such as Woodruff Arts Center this control would be expected. This is also a case of collusion. If the vendor was coerced into the kickback scheme as a condition of selection, some type of hotline would have provided them the opportunity to report. With some kickback schemes there is complete agreement between the procurement official and the vendor making it harder to detect. The organization should perform background checks for new employees with significant spending authorization authority, verify new vendors to confirm they exist and can provide the goods/services contracted for, and establish an anonymous communication channel for complaints.

EXAMPLE: Expense Reimbursement—Inappropriate Credit Card Use, Corruption, and Forgery

In 2007, Sean Patrick Taylor was hired to manage the day-to-day operations of the Epilepsy Foundation of Kansas and Western Missouri (EFK) in Kansas City, Missouri. EFK provides medical assistance, other aid, and programs for persons with epilepsy, and it works to raise public awareness of the many challenges posed by epilepsy. In April 2009, Taylor was pressured to resign from EFK after being confronted about his embezzlement of foundation funds.

Much of the money he embezzled was donations that he stole and spent on personal expenses, including out at casinos and restaurants. Taylor admitted he embezzled at least $78,227 from EFK from April 2007 to August 2009. It is important to note that this occurred months after he no longer worked at EFK. In his guilty plea, Taylor admitted charging personal purchases on EFK's account at Staples on six occasions after his employment was terminated.

During his employment, he also convinced EFK's board to hire Impact Consulting (IC) for lobbying and fundraising, but somehow forgot to mention that he was IC's founder and sole employee. EFK eventually paid IC a total of at least $11,000, but never received any services. Taylor also used the EFK credit card for his personal use, opened an unauthorized credit card account, and obtained cash advances on these cards totaling at least $7,532.

About a month after being forced out of EFK, Taylor was hired to manage the day-to-day operations of Westport Cooperative Services (WCS), also in Kansas City, where he resumed his career of embezzlement.

WCS operated a Meals on Wheels program, a foster grandparents' program, and a back-to-school program. Meals on Wheels provided meals to 40 individuals, mostly senior citizens, five days per week. Foster grandparents paired roughly 80 low-income senior citizens with children in preschool through junior high. Back-to-school provided uniforms, school supplies, and shoe vouchers to 400–500 low-income children. WCS was a bidder to become a permanent sponsor of the foster grandparents' program, which would have been funded by a $1.3 million, three-year grant.

Taylor admitted to embezzling at least $46,810 from WCS from August 2009 to May 2010. He forged signatures of two board members to open an unauthorized bank account under the name of WCS, and then deposited WCS contribution cash and checks totaling at least $43,402 into this account. He also fraudulently authorized additional vacation pay for himself. As a direct result of Taylor's theft, WCS was forced to end its Meals on Wheels program and lost its foster grandparents' bid.

In 2012, Taylor pleaded guilty in federal court to fraud. In his plea, Taylor admitted to embezzling a total of more than $100,000 from EFK and WCS from April 2007 to May 2010. But the government believes he stole $133,161. While this two-act scheme was going on, Taylor lost more than $72,000 playing slot machines at Prairie Band Casino, which expressed its gratitude by providing him with more than $5,200 in complementary benefits including travel and lodging.

Analysis: Lack of segregation of duties, inadequate controls over cash receipts, lack of board oversight. Lack of management oversight, lack of new vendor evaluation.

EXAMPLE: Expense Reimbursement—Use of Debit Cards

Vernell Reynolds, a former Miami, Florida, police officer, was head of the Miami Community Police Benevolent Association. The group devotes efforts to charity work to benefit the inner city.

For approximately two years, Vernell used an association-issued debit card to access its credit union accounts to make unauthorized cash withdrawals, personal purchases, and money transfers to her personal credit union account, totaling more than $210,000. Many of the withdrawals were made at the Seminole's casino in Hollywood, Florida. *The Miami Herald* reported that she embezzled to fund her gambling habit.

Four years later, she pled guilty in federal court to fraud and tax charges. Separately, Florida state prosecutors charged her with defrauding the not-for-profit, Step Up for Students, of nearly $7,000. The charges claimed that while earning more than $140,000 a year, she sent her son to private schools on scholarships meant for low-income children by falsifying tax returns, a birth certificate, and other documents to make it appear her lower-income sister was the boy's guardian, thus fraudulently obtaining nearly $7,000 in scholarships from Step Up for Students.

Analysis: Lack of control over use of debit cards and other cash payment mechanisms

EXAMPLE: Expense Fraud

Avelyn Reynolds was the trusted executive assistant to the Chief Operating Officer (COO) at Support Childhood Education (SCE), a prestigious nonprofit organization. She had good relationships with the COO and other colleagues and had an excellent work ethic.

During her second year at SCE, she got divorced and became embroiled in a lawsuit. Her financial and emotional stress soared, and she began to feel underpaid and to think of ways to get what she deserved from the organization.

As the COO's assistant, she had an organization credit card, maintained the petty cash, and had the ability to initiate payments by the bank and payment requests to accounts payable, create purchase orders, approve her own timecard, and authorize payments to families awarded assistance from SCE.

Like many perpetrators, she started small but steadily increased the size of her thefts. She began using the organization's credit card for personal purchases, and forging the COO's signature. The organization paid her phone bills far above her authorized amount, assuming the charges were the COO's. Her children had different last names, so it was easy for her to authorize thousands of dollars in payments to them as if they had been legitimately awarded educational assistance. Unidentified donation checks came to her to be identified, and she developed a scheme to divert them to her own bank account. She approved several hours per week of unauthorized overtime for herself and stole $400 in petty cash.

In all, she stole more than $100,000 in less than 10 months. Among other things, she spent the money on laptops, smartphone bills, vacations, a $30,000 recreational vehicle, and a nose job.

The fraud was uncovered only after she slipped up. Accounting questioned a duplicate check request to a child in need—her daughter. The COO found a credit card slip under her desk on which she had forged his name.

Because some of the checks to her children were mailed across state lines, the FBI was called in and she was charged with mail fraud. She was fired but never made restitution or served jail time. She had previously been convicted of fraud, but this was not determined until after this fraud occurred since background checks were not performed by SCE.

Analysis: There are several control deficiencies that need to be corrected in this case.

- Lack of tone from the top (background checks, management, and board fraud risk assessment)
- Lack of segregation of duties
- Lack of manager review of account changes for suspicious transactions
- Failure to check award recipients against the human resources database for conflicts
- Self-approval of timesheets
- Lack of monitoring of credit card charges and phone bills
- Lack of controls over cash receipts, especially when there was no donor correspondence

EXAMPLE: Cash Larceny

A 27-year-old woman was hired as an administrative employee for the College of Nursing, a division of St. John's Mercy Health Care Systems (now called Mercy Hospital) in Missouri, which was run jointly with Southwest Baptist University. She was responsible for the upkeep of the facilities, College of Nursing staff payroll, budgetary issues, and general administrative duties for the dean and program director of the College of Nursing.

Three years later, she began intercepting checks intended for St. John's and the College of Nursing and depositing them directly into her personal bank account. She stole nearly $61,000 using this scheme. Four years after that, her bank informed her they would no longer accept deposits into her account of checks on which she was not the payee.

Undeterred, she came up with a new plan. She had access to the Student Nurses Association bank account at the St. John's Employees Credit Union, which was a private savings account owned and funded by the students of the College of Nursing. After her own bank shut off her ability to deposit her stolen checks into her own bank account, she began to deposit them into the Student Nurses Association bank account. She would then withdraw the funds from that account on the same day. Using this new scheme, in just two years she was able to steal additional amounts totaling more than $657,000, for a total theft of $717,999.

As is the most likely case in frauds of this nature, the perpetrator paid no income tax on her ill-gotten gains. Later that year she pleaded guilty to theft of program funds and tax evasion. She was sentenced to 30 months in federal prison without the possibility of parole and was ordered to pay $717,999 in restitution to Mercy Hospital, as well as $115,117 plus interest to the IRS.

Analysis: Lack of segregation of duties is the primary enabler of this fraud. The perpetrator was inventive and determined but more supervision over the cash handling function could have detected this fraud.

EXAMPLE: Internal Controls That Can Help to Prevent Cash Schemes

Other controls that could help prevent cash schemes in small- to midsize organizations are listed in the following tables.

Internal Controls That Could Help Prevent Cash Schemes (Small- to Midsize Organizations)

Control	Stealing Deposits	Stealing Cash on Hand	Skimming Part of Contribution or Sale	Kiting	Lapping
Use prenumbered deposit slips	✓		✓		
Make all deposits intact daily	✓		✓		
Keep undeposited amounts in a safe	✓		✓		
Consider a lockbox for large volumes of cash receipts	✓	✓	✓		
Use multipart deposit slips and compare the amount on the in-house copy to the amount deposited on the bank statement	✓		✓		
Perform analytical review on the quantity of cash received from week-to-week and month-to-month or for events	✓	✓	✓		✓
Reconcile receivables ledger to the general ledger balance with supervisory review					✓
Bond employees who handle cash receipts and make deposits	✓	✓			✓

Internal Controls That Could Help Prevent Cash Schemes (Small- to Midsize Organizations)					
Have supervisory personnel review the pledges or other receivables for collectability, as well as any write-offs before they occur					✓
Post a toll-free number where donors, customers, or clients can make complaints	✓		✓		✓
Separate the responsibility for logging the cash receipt, posting the cash receipt, and depositing the cash receipt (to revenue or against receivables)	✓		✓		✓
Have employee that is independent of billing, posting receipts, and cash handle any complaints from donors, clients, or customers	✓		✓		
Have independent supervisory personnel perform tests at the end of the period to determine if any interbank transfers have been properly recorded				✓	
For events or times where there is a large amount of cash collected, have two people count cash as a check on one another	✓	✓	✓		

Internal Controls That Could Help Prevent Fraudulent Disbursements (Small- to Midsize Organizations)						
Control	Kickbacks	Fictitious or Inflated Invoices	Excess Purchasing Schemes	Duplicate Payment Schemes	Stealing Checks	Stealing Cash by Using Wire Transfers
Use competitive bidding	✓		✓			
Review recent purchases to see whether one vendor is winning most bids	✓					
Notify vendors of conflict-of-interest policy	✓					

Internal Controls That Could Help Prevent Fraudulent Disbursements (Small- to Midsize Organizations)						
Control	Kickbacks	Fictitious or Inflated Invoices	Excess Purchasing Schemes	Duplicate Payment Schemes	Stealing Checks	Stealing Cash by Using Wire Transfers
Scan general ledger for unusual levels of purchases		✓	✓	✓		
Use data extraction software to search for vendors with same addresses as employees, vendors with P.O. boxes, duplicate payments		✓	✓	✓		
Use programmed controls to prevent unauthorized access to check writing and AP systems		✓	✓		✓	
Use prenumbered requisition, purchase orders, receiving reports, and ensure sequence is accounted for		✓	✓	✓	✓	
Reconcile subsidiary ledgers to G/L		✓				
Perform analytical review on expenses by category		✓	✓	✓	✓	✓
Scan G/L for unusual activity		✓	✓			
Lock up check stock		✓			✓	
Set up positive pay with bank		✓		✓	✓	
Use multipart/ prenumbered checks		✓				
Investigate void or reissued checks		✓				
Recompute vendor invoices for accuracy		✓				

Internal Controls That Could Help Prevent Fraudulent Disbursements (Small- to Midsize Organizations)						
Control	Kickbacks	Fictitious or Inflated Invoices	Excess Purchasing Schemes	Duplicate Payment Schemes	Stealing Checks	Stealing Cash by Using Wire Transfers
Match vendor invoices with requisitions and receiving documents		✓				
Require varying levels of approval for higher purchases		✓				
Enforce mandatory vacations	✓	✓	✓	✓	✓	✓
Use approved vendor list and have management approve changes to master file		✓		✓		
Compare budget to actual disbursements		✓	✓	✓		
Require original invoices and receiving reports				✓		
Use passwords for those initiating and those authorizing wire transfers						✓
Require bank to call back to verify wire transfers over a certain amount						✓
Compare petty cash reimbursements to other reimbursements to prevent double dipping by employees				✓		
Bond employees	✓	✓	✓	✓	✓	✓

Internal Controls That Could Help Prevent Fraudulent Disbursements (Small- to Midsize Organizations)						
Control	Kickbacks	Fictitious or Inflated Invoices	Excess Purchasing Schemes	Duplicate Payment Schemes	Stealing Checks	Stealing Cash by Using Wire Transfers
Bank statement sent to senior management or someone who does not have responsibility for cash receipts and disbursement records	✓					
Reconciliation of bank statement by someone who doesn't prepare or sign checks or initiate wire transfers		✓			✓	✓
Have an independent person review bank reconciliation		✓			✓	✓
Separate duties for person who authorizes invoices for payment and person who receives vendor refunds				✓		
Separate duties between those who initiate, process, authorize, record, and handle check stock and check writing		✓	✓	✓	✓	
Separate duties between those initiating and approving wire transfers						✓
Separate purchasing from requisitions and receiving	✓					

EXAMPLE: Payroll Fraud

Ian Turner was a payroll clerk whose responsibilities were posting time and attendance information to the computer system and preparing the payroll disbursement summaries. He was able to steal $112,000 during a two-year period through payroll fraud.

There was segregation of duties at the not-for-profit. A payroll supervisor approved all disbursements and verified the payroll was deposited directly into the employees' bank accounts. Turner had to be creative.

He stole the password of his coworker who added and deleted records to the master payroll file by watching her key in that information. This helped him add fictitious employees to the system. He was smart enough to figure out that the payroll deductions were set for employee numbers within a certain range so when he created the fictitious employees, he made sure that the employee number was outside that range so no deductions would be made for them. He arranged for their wages to be deposited into his bank account. He knew from prior experience that the bank did not match employee names to the depositor's account.

Since payroll was approved by the supervisor, he prepared a fictitious payroll summary. No one checked his work because his performance had been superior in the past. The fictitious report was prepared with a different type face than the real reports, but that was not noticed by the supervisor.

Turner's one concern was that he had to create file copies of the paychecks for the fictitious employees. The check copies printed in the accounting department were yellow. He was only able to print the copies for the fictitious employees in white. And no one noticed until an auditor selected one of the fictitious transactions in his sample. He noted the white copy when the rest were yellow. The employee was not in the payroll register when the auditor went to trace it through the system. This caused the auditor to dig a little further and he found out that there were others. The auditor noted that all the suspicious payroll amounts were being deposited into the same bank account.

The auditor thought there might be collusion going on, so the auditor performed the following steps:

- Obtained original copies of payroll registers, payroll check summaries, direct-deposit records, personnel files, time sheets, and bank documents
- Interviewed the accounting department employees and the supervisor

The auditors noted that there were several red flags as they were performing the extra procedures:

- The passwords were not changed frequently (this would have required Turner to obtain a new password every 90 days or whatever the length of time would be).
- The fictitious employees had the social security number of a deceased person. Turner got these from death records open to the public. He made up names to go along with them.
- The employee ID numbers were higher than those of legitimate employees and Turner left a gap between the ID numbers in case there were new employees legitimately added to the records.
- The new payroll expense was lower than the funds issued because it did not include amounts paid to the fictitious employees.
- The fictitious employees did not have personnel files or tax withholdings.
- The paycheck summaries did not have the same type face as the system.
- Multiple direct deposits were made to the same bank account but under different names.

When caught, Turner stated that he needed the money to pay for his expensive HIV drugs. Since he was the only one who benefitted from the scheme (no other accounts received these fictitious deposits), it was determined that he acted alone. Turner pleaded guilty and was sentenced to 15 years' probation and ordered to make restitution.

Analysis: Although the not-for-profit had good segregation of duties, this control alone is not enough.

Adding the following internal controls might have prevented or detected the fraud.

- Inspect paychecks and see if there are any without deductions.
- Tie out the payroll summary to expense.
- From time to time, do a hand delivery and require positive identification.
- Analyze payroll expense (it was not clear from the information available on this fraud where the debits were posted since it was not to payroll expense).
- Change passwords every 90 days.

EXAMPLE: Internal Controls Over Payroll

Other ways to prevent payroll fraud are shown in the following table.

Internal Controls That Could Help Prevent Payroll Schemes (Small- to Midsize Organizations)

Control	Fictitious Employees	Inflated Payroll	Terminated Employees on Payroll	Expense Report Fraud	Stealing Checks	Payroll Tax Schemes
Use a payroll service and have senior management review payroll documentation analytically	✓	✓	✓		✓	
Payroll service handles payroll tax payments to IRS						✓
Supervisory approval for additions and terminations	✓		✓			
Supervisory review to changes in the master payroll file	✓		✓			
Surprise delivery of paychecks if not direct deposited	✓					
Mandatory vacations for personnel and payroll employees	✓	✓	✓		✓	
Supervisory approval of time sheets or timecards		✓				
Lock personnel files	✓					

Internal Controls That Could Help Prevent Payroll Schemes (Small- to Midsize Organizations)						
Control	Fictitious Employees	Inflated Payroll	Terminated Employees on Payroll	Expense Report Fraud	Stealing Checks	Payroll Tax Schemes
Lock up payroll check stock					✓	
Reconcile payroll with the general ledger			✓			✓
Reconcile total W-2 wages to the general ledger and payroll register			✓			✓
Require employees to sign W-4 forms and other appropriate withholding documents						✓
Use direct deposit	✓		✓		✓	
Separate duties of check stock custody and check signing	✓		✓		✓	
Separate duties for preparing payroll and personnel					✓	
Use a separate imprest account (cash account) for payroll and deposit only the amount needed		✓			✓	
Senior management performs analytical review of payroll and payroll liabilities	✓	✓	✓		✓	✓
Supervisory employee reviews reimbursable expenses against budget				✓		
Establish travel, hotel, and meal guidelines and limits				✓		
Require review and approval of all expense reports before they are paid. Check that signers should not approve their own reports				✓		

Internal Controls That Could Help Prevent Payroll Schemes (Small- to Midsize Organizations)						
Control	Fictitious Employees	Inflated Payroll	Terminated Employees on Payroll	Expense Report Fraud	Stealing Checks	Payroll Tax Schemes
Require that original receipts be submitted for each item over a certain dollar threshold				✓		
Review mileage reimbursements for reasonableness in accordance with expectations				✓		

EXAMPLE: THEFT OF NONFINANCIAL ASSETS

Andrew Liersch was the president of Goodwill Industries. His fraudulent activities cost Goodwill Industries of Santa Clara County (13 stores) approximately $26 million spanning approximately 18 years. He involved the core store managers in the fraud and paid them $1,000 a week for selling the most valuable items in back-door sales. They also had duplicate registers and that cash was siphoned off in the scheme. There were other employees involved who received payoffs in varying amounts. When sold, investigators believe that Liersch's proceeds were deposited into several bank accounts, some in Switzerland, Scotland, and Austria. This fraud took investigators six years to unravel.

The fraud came to light when one of the conspirators was going through a contentious divorce. Her husband called to report the fraud. The original mastermind of the scheme was Carol Marrs, Goodwill's director of stores. She originally was skimming valuable items and selling them at garage sales. When Liersch came on board, he took the fraud to a whole new level. Marrs committed suicide after investigators searched her home. They found approximately $1 million in accounts allegedly set up with her share of the profits from the fraud scheme.

Goodwill officials believed that the fraud was undetected for so long because Liersch kept producing superior results for the organization. Donations continued to rise each year. Liersch relied on his control and knowledge of the organization's workings to hide fraud. He also lied to the Board of Directors.

It is interesting that when Liersch pled guilty that he was not punished at the same level as the theft he committed. It may be that commendations that Liersch received for his previous work with Goodwill and his work in Guatemala, extending even to a commendation from President Ronald Reagan softened the sentencing. Liersch was seen as a great humanitarian.

Liersch eventually pleaded guilty to a charge of tax evasion to avoid being charged with stealing from Goodwill Industries. The plea agreement dismissed the embezzlement charges and did not require prison time. Liersch was ordered to pay $540,000 in restitution.

Analysis: Executive management was corrupt so there was no tone from the top to set an expectation that fraud would not be tolerated. As discussed earlier, the *Report to the Nations* noted that 58% of the frauds in the study were committed by two or more perpetrators acting in collusion. Median losses tend to rise significantly when more than one person conspires to commit fraud. One reason for the larger losses in collusion

schemes is that multiple perpetrators working together may be able to circumvent controls based on separated duties and independent verification of transactions. In this case, the collusion was so massive that only a change of heart by one of the participants in the scheme or observation by an outside party would have detected the fraud. The *Report to the Nations* showed that frauds with or without collusion appear to have the same duration.

The board clearly was not sufficiently involved and since the perpetrator made significant contributions to the organization in other ways, red flags may have been overlooked. If available, a hotline of some kind might have been used by employees, donors, or others to report suspicious activity.

Clearly the controls over receipt of goods in donation were deficient. Controls that may help to prevent or detect fraud when there is inventory present are:

- reconciling donation acknowledgments provided for goods to the level of goods received or sold
- segregation of larger, more expensive donated items to ensure their placement for sale
- using physical access controls for all assets and inventory and restricting access to inventory
- monitoring employees who have access for unusual patterns of entry and departure
- using electronic surveillance equipment such as video cameras

The following controls could be used when inventory is purchased.

- Using sequentially prenumbered documents for inventory control
- Segregating duties such as requisition of inventory, purchase of inventory, receipt of inventory, custody of inventory, and physical counts of inventory
- Performing periodic surprise inventory and asset counts and reconciling the counts to the amounts recorded in the books and records
- Using analytical review to monitor for unusual trends such as persistent or rising inventory shortages
- Having policies on the use of company assets. Management must lead the way and set the example.
- Reconciling inventory counts to general ledger

EXAMPLE: FRAUDULENT FINANCIAL REPORTING

Francine Gordon was a model employee at Small Town Federal Credit Union (STFCU). She had been controller for 15 years and managed the IT system, running it herself when the data-processing clerk was sick or on vacation. Her great value to STFCU overcame her dictatorial manner and moody temper. A small institution, STFCU had little segregation of duties. Gordon created financial statements, prepared budgets and forecasts, reconciled STFCU's bank statement, supervised the IT department, and managed the investment portfolio. Gordon was single with no children, had few friends, had a family who lived far away, and was not close with colleagues. She regularly awarded 90% of STFCU's investment business to one of three approved brokers; one whose skillset ran more toward client flattery than investment expertise.

STFCU decided to hire a CPA for internal audit and financial accounting. Six months after he started, regulators were performing their annual on-site review and found a $130,000 reconciling item by Gordon in the bank reconciliation. Gordon gave the CPA a confusing explanation, which he passed on to the regulators, and the regulators accepted it. Two months later, the CPA found the same $130,000 item had not been cleared and was still in the reconciliation. When the CPA asked Gordon about it again,

she became flustered, said she was busy, and promised to get back to him by the end of the week. She left the organization.

Upon further investigation, STFCU determined that Gordon purchased inappropriate and complex investments from her favorite broker for STFCU. It also appears that the broker received the highest commissions for these types of investments. One such investment was a mortgage-backed investment purchased three years earlier at a significant premium. Not really understanding the investment, Gordon also did not know how to properly account for it, she provided inadequate amortization of the premium. When mortgage rates dropped, consumers refinanced, and STFCU received large early principal repayments. This should have caused a large increase in amortization or expensing of the premium but doing so would have caused STFCU to show a loss. So, Gordon continued to amortize the premium straight-line, and disguised the difference with the reconciling item of $130,000.

Analysis: Lack of segregation of duties gave Gordon the opportunity to commit this fraud. It is also instructive as a demonstration that fraud does not always occur for financial reasons. In this case, Gordon's motivation was to save face by not admitting she had chosen an imprudent investment. She also set a poor tone by being dictatorial and causing people to be afraid to question her. The internal auditor should have been able to report directly to the audit committee if the item was not cleared and he expected wrongdoing. Even if the regulator passed on questioning the item further, it is the organization's responsibility to maintain the appropriate level of internal control.

Gordon rarely took vacation, and when she did it was usually for less than a week. All employees should be required to take an annual vacation of at least a week. In addition, organizations should cross-train all employees in duties.

All reconciling items should have an explanation and be verified by someone independent of the entry's creator. A recurring reconciling item for the same amount should be investigated particularly closely. The reporting relationship between the internal auditor and the board/audit/finance committee chair should be established. Otherwise, a strong executive such as Gordon will be able to override controls.

Frequently Asked Question Related to Fraud

1. How does an auditor know if the board and management are really experienced enough so that their oversight really mitigates a lack of segregation of duties?

   It is very difficult to know if management and the board are experienced enough that their oversight can mitigate the risk of fraud. The auditor should ask questions to determine the level of their review by asking what documents, support, reports, etc., are reviewed, how often, what questions are asked in the review, and determine the general thought process behind the review. Credentials are not necessarily enough. For example, CPAs on a board may not have the time or inclination to analytically review at a detailed enough level. And since documentary evidence can be falsified such as in the case of a fictitious invoice, understanding the reviewer's thought process is very important.

2. What is the auditor's responsibility as it relates to the evaluation of fraud**?**

   The auditor has the responsibility to plan and perform the audit to obtain reasonable assurance that the financial statements are free from material misstatement whether due to fraud or error. This means that the auditor should exercise professional skepticism and follow through on the risk assessment process, as outlined in professional standards. Simply rolling forward checklists assuming that the circumstances of a particular organization are always the same year after year is not appropriate. Professional skepticism is important. The auditor should be alert for management bias and red flags during the audit that may

warrant further investigation. An understanding of the business purpose behind relationships is an important consideration. In cases where there is a lack of segregation of duties there is always heightened risk. Surprise procedures such as investigating vendors to ensure they are legitimate or performing analytics using financial and nonfinancial information to tease out a volume variance can be helpful.

3. Do you believe that a management letter comment or a communication containing a significant deficiency or material weakness should be issued by the auditors in cases where there is lack of segregation of duties?

   Lack of segregation of duties is a deficiency. Although there may be mitigating controls, it is important for the auditor to challenge how well management and the board are exercising their reviews to determine whether it should be reported as a management letter comment, a significant deficiency, or a material weakness. Understanding that there are always limitations to internal controls and that human beings are fallible, it is a good idea to remind management and the board that segregation of duties along with management review is an important goal for the entity. The comment may be softened by applauding the entity for what it is trying to achieve with limited resources but reminding them that there is still a risk when segregation of duties is not present.

Take Advantage of Diversified Learning Solutions

We are a leading provider of continuing professional education (CPE) courses to Fortune 500 companies across the globe, CPA firms of all sizes, and state CPA societies across the country, as well as CPA associations and other financial organizations. Our efficient and flexible approach offers an array of customized cutting-edge content to meet your needs and satisfy the priorities of your business. Select from live classes, live webinars, conferences, or online training, including Nano courses, based on your preferred method of learning.

Meet your CPE requirements, increase productivity, and stay up-to-date with relevant industry trends and mandatory regulations with collaborative live or online learning.

Live Training Topics	Online Training Topics
Accounting and Auditing	**Accounting and Auditing**
Employee Benefit Plans	**Business Law**
Ethics	**Business Management and Organization**
Information Technology	**Economics**
Governmental and Not-For-Profit	**Ethics**
Non-Technical (including Professional Development)	**Finance**
Tax	**Information Technology**
	Management Services and Decision Making
	Personal and Professional Development
	Tax

"We have enjoyed [your] programs and have found the content to be an excellent learning tool, not only for current accounting and management issues, but also how these issues apply to our company and affect how our business is managed."

—Debbie Y.

KAPLAN®