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)

James Hodge, CPA, CFE

KAPLAN

IDENTIFYING AND ADDRESSING THE RISK OF FRAUD IN NONPROFIT ORGANIZATIONS (IAR4)

Published in 2021 by Kaplan Financial Education.

ISBN: 978-1-0788-1510-9

TABLE OF CONTENTS

Unit 1

Introduction

LEARNING OBJECTIVES

- Identify the types of potential frauds that could occur in not-for-profit organizations.
- Gain an understanding of the impact of cyber fraud on not-for-profit organizations.
- Understand the risk of fraud in not-for-profit organizations.

INTRODUCTION

Occurrences of fraud in a not-for-profit entity can cost the entity not only the amount of the theft but also the entity's reputation. Once a fraud is made known, the public, including donors and other funding sources, can learn about it in a matter of hours with today's instant access to information.

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 entities reported 9% of fraud cases studied in 2019 and had a median loss of $75,000. For many not-for-profit entities, financial resources are extremely limited and a loss of $75,000 can be devastating. Additionally, not-for-profit entities can be more vulnerable to fraud due to having fewer resources available to prevent and recover from a fraud loss. The not-for-profit sector is susceptible because of less oversight and absence of certain internal controls to prevent certain schemes.

It is important to understand the type of frauds that are common for not-for-profit entities and to be able to appropriately identify and address the risks of occurrence. This is of significant importance since any fraud that occurs means that resources lost will not be used for charitable causes or social services. Additionally, reports of fraud within the sector can also discourage donations from donors if a donor believes there is significant risk that resources provided can be diverted and used inappropriately.

Not an Isolated Incident

In October 2013, the Washington Post published an article related to its analysis of Form 990 filings from 2008 to 2012. During that time, there were over 1,000 not-for-profit entities that checked the box indicating that they had discovered a significant diversion of assets. The losses were attributed to

theft, investment fraud, embezzlement, and other unauthorized use of funds.[1] The 10 largest diversions amounted to more than $500 million. Form 990, as redesigned for filings beginning in 2008, requires entities to report diversions of assets if the gross value of all diversions (not taking into account restitution, insurance, or similar recoveries) discovered during the entity's tax year exceeds the lesser of (1) 5% of the entity's gross receipts for its tax year, (2) 5% of the entity's total assets as of the end of its tax year, or (3) $250,000.

The Washington Post assembled the first public database of not-for-profits at http://www.washingtonpost.com/wp-srv/special/local/nonprofit-diversions-database/. This database provides the name of the entity, the amount of the diversion, and the Form 990 disclosure related to the diversion.

Not-for-profits are particularly vulnerable to fraud because of the following characteristics:

- Environment of trust, especially in financial personnel
- Excessive control by an executive director or owners (in the case of privately held entities)
- Existence of transactions that are easy to steal (contributions in a not-for-profit)
- Failure to devote sufficient resources to financial management
- Failure to include individuals with financial oversight expertise on the board (or in the case of a privately held entity, failure to have an independent board)

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 2020 *Report to the Nations*[2] is asset misappropriation (86%), followed by corruption (43%), and financial statement fraud (10%).

Although fraudulent financial reporting is the least prevalent category, it is responsible for the biggest losses. The median loss for fraudulent financial reporting was approximately $954,000 in the 2020 survey. The median loss for corruption was $200,000 and the median loss for asset misappropriation was $100,000.[3]

Cyber Fraud

One type of fraud that is not identified in the ACFE reports is cyber fraud. It may be because cyber fraud is generally thought to be acts from the outside perpetrated against an entity. It is mentioned

[1] https://www.washingtonpost.com/investigations/inside-the-hidden-world-of-thefts-scams-and-phantom-purchases-at-the-nations-nonprofits/2013/10/26/825a82ca-0c26-11e3-9941-6711ed662e71_story.html.

[2] The ACFE Report to the Nations is published every 2 years. It can be accessed at https://www.acfe.com/report-to-the-nations/2020/

[3] Ibid.

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 the hackers. Sometimes, what hackers want is payment. Organizations, particularly hospitals, are being blackmailed into paying ransom to hackers in order to regain access to data, or in the case of a Muncie, Indiana, not-for-profit, to return the data and not publish it.[4] There can also be legal and regulatory ramifications.

According to Verizon's *2019 Data Breach Investigations Report*, ransomware attacks are still going strong. They account for nearly 24% of incidents where malware was used. Ransomware has become so commonplace, that it is 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 entities. Ransomware can stop the processing of an entity until a ransom is paid to unlock the system. Most not-for-profit entities will pay the ransom to get back up and running again. By 2021, ransomware damage costs are estimated to hit $20 billion, 57 times the amount in 2015, according to Cybersecurity Ventures. 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 network 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.[5] 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.[6] 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*,[7] are:

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

---

[4] https://nonprofitquarterly.org/2017/06/08/nonprofit-cybersecurity-pay-attention/.

[5] 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

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

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

This illustrates that although cybercrime is a very real threat, many breaches could be prevented by better internal controls.

The ongoing COVID-19 pandemic has had an incredible impact on the way many not-for-profit entities operate, with large numbers of employees working remotely from home. This has 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.

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 entities. 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: 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.

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 (NTEN) 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.[8] Not-for-profit entities 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 entities 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 entities 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 entities 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 towards 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.[9] The guidance provides insight into how not-for-profit entities 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 entities 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

[8] https://www.nten.org/article/assessing-risk-protect-valuable-data/

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

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 software could be used in addition to next-generation anti-virus/anti-malware software. Many entities are using multi-factor 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 have the ability to do new things every day. 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 to the not-for-profit.

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 entities 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 2020 *Report to the Nations* found that not-for-profit entities have fewer anti-fraud controls in place, leaving them more vulnerable to fraud. The top three control weaknesses found in not-for-profit entities are the following:

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

The study also found that detection of fraudulent activity at not-for-profit entities were detected by the following:

- Tip or complaint (40%)
- Internal audit (17%)
- Management review (13%),
- Accident (7%)
- Examination of documents (6%)

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 is important now more than ever, given the changing landscape not-for-profit entities are navigating because of the COVID-19 pandemic.

While some U.S.-based not-for-profits have seen extraordinary increases in donations in 2020 to address the COVID-19 crisis ($11.4 billion) and racial inequalities in the country ($7.6 billion), a 2020 survey by the Nonprofit Finance Fund found that 75% of not-for-profit entities are seeing reduced earned revenues, 50% reduced contributions, and 27% reduced government revenue. To magnify this issue, many not-for-profit entities are simultaneously seeing a significant increase in the use of their services.[10] Some not-for-profits have not changed their business models to match the times, and contributions from individuals, particularly at special events, have decreased. 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 in order 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

[10] https://nff.org/covid-19-survey-results

Not-for-Profits May Need To:	This Could Lead To:
Cover certain operating expenses when unrestricted revenue sources have declined	Categorizing some expenses as allowable for grant purposes when they are not or causing over allocation to 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.

Focus on Transparency and Accountability

Since the enactment of the Sarbanes-Oxley Act in 2002, there has been a significant interest on the part of watchdog agencies in increasing the transparency and accountability for not-for-profit entities. The U.S. Senate Finance Committee, the Department of Justice, the OMB, GAO, and IRS are all heavily scrutinizing the actions of not-for-profits. The trickle down to not-for-profits advanced in 2008 with the revision to Form 990. The form asks over 50 questions throughout the core form and supporting schedules about business arrangements that the IRS may find troublesome as well as various policies, procedures, and processes designed to prevent or detect noncompliance with laws, regulations, and fraud. Many of these questions require detailed explanation. The answers to these questions serve to highlight the degree to which not-for-profits have appropriate governance. As noted earlier, there is also a question requiring not-for-profits to disclose whether they have experienced a significant diversion of assets during the year. A *diversion* of assets includes any unauthorized conversion or use of the entity's assets other than for the entity's authorized purposes, including but not limited to embezzlement or theft. Diversions can be by the entity's officers, directors, trustees, employees, volunteers, independent contractors, grantees (diverting grant funds), or any other person, even if not associated with the entity. A diversion of assets can, in some cases, result in inurement of the entity's net earnings. In the case of section 501(c)(3), 501(c)(4), and 501(c)(29) entities, it also can be an **excess benefit transaction** taxable under section 4958 and reportable on Schedule L (Form 990 or 990-EZ).

Small entities have a much harder time implementing anti-fraud programs and controls than larger ones because they generally have fewer resources with which to address the threat of fraud. Unfortunately, these entities can incur losses as large as bigger entities. In addition, when there are a limited number of employees over which to segregate duties, trust is an integral part of the environment. Trust is an inhibitor to effective internal control. In fact, trust in the wrong person can lead to disaster.

Changes to Not-for-Profit Financial Statements

ASU 2016-14, *Financial Statements of Not-for-Profit Entities*, is effective for fiscal years beginning after December 15, 2017 and interim periods thereafter for most not-for-profits. Those considered public entities were required to implement it a year earlier. Among its many changes, there are two changes that should heighten the auditor's awareness as it relates to fraudulent financial reporting. Those areas are explained in the following paragraphs.

Functional Expense Presentation

All not-for-profit entities will be 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 entities to push expenses into the program category that may be management and general or fundraising since Charity Navigator and other watchdog-type entities want to see a very high percentage of expenses as devoted to program activities.

Liquidity Information

The new standard requires a footnote on liquidity. 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 entities' assets are restricted either by donor 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

- Identify and assess the risks of material misstatement of the financial statements due to fraud for not-for-profit entities and smaller, less complex entities.
- 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 inquires 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 entities and not-for-profit entities as well as for smaller, less complex entities. 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 fraud triangle is important to understand. Our professional literature[11] says 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.

[11] AICPA Codification of Audit Standards, AU-C 240, Consideration of Fraud in a Financial Statement Audit.

The **fraud triangle** actually dates back to 1974 when Donald Cressey[12] 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 fraudsters' 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 Entities

When auditors perform work for these types of entities, 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.

Considerations Specific to Smaller, Less Complex Entities

Smaller entities may have other ways of addressing internal controls that do not involve written documents, although this is less likely in not-for-profits due to the questions being asked on IRS Form 990 and requirements of grantor agreements.

In some cases, 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 the tone set by management. Since the auditor is using this information to assess risk, she should be careful to determine whether an appropriate tone is really set before believing that this type of control is effective.

Often, in smaller not-for-profits there is domination of management by one person. This does not necessarily mean that there is failure by management to display and communicate an appropriate attitude regarding internal control and the financial reporting process, but the risk of management override is still there.

In some entities, the need for management authorization can mitigate controls that would be considered deficient, but the risk of management override still exists.

Requirements

AU-C 240 requires the auditor to perform the following:

- 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.

[12] http://www.acfe.com/fraud-triangle.aspx

- 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.

- Consider fraud risk factors, including the following:

  - **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.

  - **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.

  - **Rationalization** – The ability to rationalize committing a fraudulent act is 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.

- 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. Management override of controls and revenue recognition is presumed to be a significant risk of fraud. Once the risk has been determined, the auditor will design procedures to address the risk of fraud and incorporate them into the audit plan.

In recent years, some auditors have found it awkward to continue to ask the same questions over and over and have, in some cases, moved away from direct questions and gone to questionnaires that are given 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.

Example Fraud Inquiries

Management	Board/Audit Committee	Others
■ Whether management has knowledge of any fraud or suspected fraud affecting the entity. ■ Whether management is aware of allegations of fraud or suspected fraud affecting the entity; 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 entity, including any specific fraud risks the entity 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 entity has established to mitigate specific fraud risks the entity 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 entities with multiple locations monitor them and whether there are particular 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 entity's internal control serves to prevent, deter, or detect material misstatements due to fraud.	■ 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.	■ Their views about the risk of fraud and how it might occur. ■ Whether they have seen or suspect fraud. ■ If internal auditors, whether they have performed any procedures to detect fraud and if there were findings, how management responded.

Use of Electronic Surveys

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 Entity? (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 Entity 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 Entity'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 Entity has adequate processes for the investigation of potential frauds and for corrective action when necessary? (yes, no)

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

8. Do you have any questions or concerns which we should consider during our audit? (yes, no)

8a. (If the answer is yes, the following question drops down). Please describe any questions or concerns which we should consider during our audit.

Assessing Risk (AU-C 315)

In assessing risk, the auditor uses inquiry, observation, and the inspection of documents and performs preliminary analytical procedures to obtain sufficient information about the entity and its environment, which includes its internal control, to assess the risk of material misstatement.

The risk assessment procedures are designed to help the auditor evaluate risk in the entity and focus on these four broad categories.

1. Industry and Regulatory Factors:

   - Market and competition
   - Accounting principles and industry – specific practices
   - Regulatory framework
   - Legislation and regulations that affect operations
   - Taxation (unrelated business income)
   - Government policies including financial incentives (i.e., grants and other government aid programs, Medicare, Medicaid, UMIFA/UPMIFA)
   - Environmental requirements
   - General level of economic activity (i.e., recession, growth)
   - Interest rates and availability of financing
   - Inflation and currency revaluation
   - Impact of these factors on funding sources such as donors or foundations
   - Impact of these factors on demand for services offered by the not-for-profit

2. Nature of the Entity:

   - Business operations, including number of revenue sources (donors, fee for service, grants, endowment income, etc.)
   - Products or services and markets
   - Details of declining or expanding operations
   - Alliances, joint ventures, and outsourcing activities
   - Involvement in e-philanthropy or other e-commerce
   - Geographic dispersion
   - Key constituents and funding sources

- Research and development activities
- Employment considerations (i.e., nursing shortage, union activities)
- Transactions with related parties
- Investments
- Noncash donations
- Leases and loans
- Use of derivatives or alternative investments
- Accounting principles and industry specific practices
- Revenue recognition policies
- Industry specific significant categories (i.e., classification of net assets, contribution vs. exchange, beneficial interests, agency transactions, etc.)
- Accounting for unusual or complex transactions
- Financial statement presentation and disclosure

3. Objectives and Strategies and Related Business Risks:

   - New products/services
   - Use of information technology
   - Risk appetite of management and the board of directors
   - Effects of implementing a strategy that could lead to new accounting requirements (acquisition of another not-for-profit)

4. Measurement and Review of the Entity's Financial Performance:

   - Key ratios and operating statistics
   - Key performance indicators
   - Employee performance measures and incentive compensation policies
   - Trends
   - Use of forecasts, budgets, and variance analysis
   - Analyst reports and credit rating reports
   - Period to period analysis

Not-for-profit entities should monitor the **indicators** that demonstrate what matters most to their successful operations, as well as how funding sources and others see them. Auditors may want to be certain that the information is correct before using it in their risk assessment. Some of the metrics that could be monitored by not-for-profits are explained in the following paragraphs.

Operations Related Indicators

- Contributions (corporate, individual, etc., in total compared from period to period. Monthly information will assist in the AU-C 240 evaluation of the risk of improper revenue recognition since monthly variation is generally consistent from year to year, exclusive of special contributions such as from capital campaigns, bequests, etc.).

- Individual contribution per donor (contributions / number of donors). If the entity is part of a national entity, statistics from the national office on how the other branches are performing may be useful.

- Number of visitors to museums or events, revenue per visitor (visitor revenue / number of visitors).

- Membership statistics and revenue per member (membership revenue / number of members).

- People served and revenue per person served where the entity charges fees for service (fee for service revenue / number of people served).

- Revenue by source as a percentage of total revenue (revenue by source / total revenue – compared to prior years – illustrates dependence on funding sources).

- Cost per person served (program expense for a specific program / persons served).

- Salary costs per FTE (salary expense / full-time equivalent employees).

- Fundraising expense as a percentage of total expenses (fundraising expense / total expense).

- Management and general expense as a percentage of total expenses (management and general expense / total expense).

- Operating margin (unrestricted revenues over expenses / unrestricted revenues).

Liquidity Indicators

- Days of cash on hand (cash and cash equivalents + trading securities) / (operating expenses – depreciation and amortization).

- Current ratio (current assets / current liabilities).

- Accounts receivable (or pledges receivable) turnover shows average time to collect (accounts receivable / relevant revenue / 365).

- Liquid funds indicator (unrestricted net assets – fixed assets) / (cash expenses / 365) shows how many days liquid funds are on hand to pay expenses.

- Average payment period (current liabilities / operating expenses – depreciation expense / 365) shows how long the entity is taking to pay its payables and other current liabilities.

Debt Related (Where Applicable) Indicators

- Debt service coverage (excess of unrestricted revenues over expenses + interest expense + depreciation expense) / (interest expense + principal payments) shows the entity's ability to pay its debt.

- Times interest earned (excess of unrestricted revenues over expenses + interest expense) / (interest expense) shows the entity's ability to pay the interest on its debt.

- Debt to net assets (long term debt / unrestricted net assets) gives an indication of how leveraged the entity is.

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 efficiencies 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 entity for the current year.

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

- Market and competition – the entity was competing with larger entities for grants from foundations that were now moving toward focused funding (giving larger amounts to certain entities, typically larger ones).
- Accounting principles and industry – the state enacted a version of UPMIFA during the year and the entity has endowment investments. The entity 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 entity 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 entity was struggling to get sufficient contributions to remain an affiliate of the national entity. The national entity 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 entity's interest rate was recently raised and the limit on its line of credit lowered due to the perceived credit worthiness of the entity.

- Impact of these factors on funding sources such as donors or foundations – the entity'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 entity was measured by the national office were also down.

The auditor wanted to be prepared with a written list of questions so that she 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. 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*.

The auditor considered how to phrase the 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 entity 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 entity ■ Structure and governance ■ Measurement and review of the entity's financial performance ■ Entity's objectives, strategies, and business risks	Would you tell me about your relationship with the national entity and any communications you have had with them in the current year about merging your entity with another affiliate? Are there any actions that your entity 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? 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?	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 entities. 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
		What types of programs does your entity 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 entity, 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 entity level controls?	
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 entity)? 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		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	

Inquiry	Purpose	Specific Inquiries	Ask for These Documents So They Can Be Examined
such as grants accounting or development		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.
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?[13] 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 entity? Are you aware of any allegations of fraud?	
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	Given the possibility of being merged into an affiliate entity, 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	Committee meeting minutes, analyses performed relative to reviewing financial statements

[13] 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
	• Community developments • The extent of their participation in financial reporting • Document as knowledge of entity and environment, internal controls (at entity level), specific controls if any (i.e., any control activities they may perform).	you use to ensure accurate financial reporting? Would you describe the policies and procedures the entity has in place relative to conflicts of interest? Would you describe your interaction with management relative to judgments and estimates?	
	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? [14] As member of the board, do you discuss risks to the entity whether business risks, risks of error or fraud? Would you describe your thoughts relative to fraudulent financial reporting as it relates to the entity? Misappropriation of assets?	
	Obtain information about related parties and conflicts of interest in purchasing or other contractual arrangements.	Do you have any suspicions of fraud affecting the entity? As a member of the audit committee, would you describe your understanding of the entity's internal control and	

[14] 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
		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.	
Other people in positions performing entity level internal controls to help provide information about operations or the entity's risk. Be sure to consider those that would create estimates or perform nonroutine, nonsystematic transactions.	To get information about the entity 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 entity 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 entity and get away with it? Can you tell me how management might prepare incorrect or misleading financial statements?	We will be performing 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).
		Do you feel like you could bring any kind of instances of theft to the attention of either the board or audit committee?[15] Has theft or wrongdoing occurred this year or have you suspected wrongdoing (theft), preparation of misleading financial statements, or conflicts	For any entity level controls identified by management corroborate these with other people and obtain support where possible.

[15] 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.

Inquiry	Purpose	Specific Inquiries	Ask for These Documents So They Can Be Examined
		of interest on the part of others in the entity? 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?	
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.

Another good way to work in 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 actually, 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 entity 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.[16]

Anti-Fraud Provision	**Question**	**Response**
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 entity 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 entity seek knowledge of fraudulent activity? ■ Is there a message sent that there will be tests made to look for fraud? ■ Are there surprise audits? ■ Is software used to identify issues from data?	
Management's Tone from the Top	■ Does the entity 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?	

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

Anti-Fraud Provision	Question	Response
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 auditor assesses risk 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.

The person with final responsibility for the audit should be present, and key members of the team should be included. The discussion should include instruction 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. This is not always easy to do once the auditor gets comfortable with the client, so stressing this point continues to be important.

The auditor will also need to identify ways that management could override internal controls. Examples are:

- recording fictitious journal entries,

- intentionally biasing assumptions and judgments in management's estimates, and
- altering records and terms of significant or unusual transactions.

Integrating this discussion with the discussion of risk in general is also a good idea. An example follows.

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 entity and its environment:
    - Industry, regulatory, and other external factors
    - Nature of entity
    - 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. Possibility of management override
10. Revenue recognition and where it could be a specific risk of fraud
11. Significant estimates and possibility for management bias
12. Unusual and infrequent transactions
13. 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
14. Audit responses to the risks identified (both fraud and significant risks identified)

- Overall
- Specific procedures

15. How matters will be brought to the team's attention during the audit.

In addition, the audit team should consider areas where there may have been significant changes in risks, including:[17]

1. Regulatory changes and increased regulatory scrutiny which may have changed the manner in which the entity's products or services may be produced or delivered

2. Legal or regulatory changes which may impact how the entity safeguards the privacy of data and maintains information system security

3. Risks resulting from national and international political uncertainty, including how these risks might limit growth opportunities

4. New cyber threats with the potential to significantly disrupt operations

5. What changes to the entity's business model and core operations, needed to meet changes in its external environment, might find internal resistance to change

In contrast to public and privately held for-profit entities, all five of these risk areas were rated as having "significant impact" by not-for-profits responding to a Protiviti survey.

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 as long as the auditor deals with all of the risks identified.

EXAMPLE

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

- **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 in order 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).

[17] http://www.protiviti.com/en-US/Documents/Surveys/NC-State-Protiviti-Survey-Top-Risks-2014.pdf.

- **Inappropriate releases from restriction for operating purposes (classification).**
- **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 entity (completeness).

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 in order 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 unrestricted net assets 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 entity (completeness).	Extend the period of time 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

Testing Journal Entries

Fraudulent financial reporting may involve the manipulation of the financial reporting process by recording unauthorized or inappropriate journal entries. This may occur manually or within the computerized information system. Accordingly, it is **not sufficient to look only at nonstandard journal entries**.

The process of understanding the flow of transactions and testing journal entries can be summarized as follows:

1. Obtain an understanding of the entity's financial reporting process and the controls over journal entries and other adjustments.

    a. Understand the type of journal entries that occur during the year, especially at the end of a reporting period

    b. Understand the procedures used to enter transaction totals into the general ledger

    c. Understand procedures used to initiate, record, and process journal entries in the general ledger

    d. Determine what support is required to make a journal entry if they must be approved and at what level

    e. Consider the use of IT, the applications involved, automatic interfaces, and postings from sub-ledgers

    f. Understand consolidating and eliminating entries and reclassification entries

    g. 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

2. Identify and select journal entries and other adjustments for testing. The auditor should perform tests to ensure that the population of journal entries is complete. Data extraction software can be useful. In addition, some software enables the user to run reports on all journal entries.

    The auditor should use professional judgment in determining how to test journal entries and how they should be tested. As a part of that process, the auditor should consider:

    a. Assessment of the risk of material misstatement due to fraud

    b. The complexity of the client's financial reporting process

    c. The effectiveness of controls that have been implemented over journal entries and other adjustments

    d. The types of evidence that can be examined; that is, whether the journal entries are in paper form or if it will take someone familiar with computer processes to extract the information

    e. The characteristics of fraudulent entries or adjustments

3. The auditor should consider the following when determining which entries to examine:

    a. Accounts that are not regularly used

    b. Post-closing entries that have little or no explanation or description

    c. Entries made by personnel who generally don't make journal entries such as a controller or CFO

    d. Entries which contain round numbers or a consistent ending number

    e. Entries made before or during the preparation of the financial statements that do not have account numbers

In computer significant environments, the auditor may need to treat the closing process as a separate system. Currently, many auditors do not test the closing process but perform substantive tests of the disclosures and amounts that flow from the general ledger to the financial statements. The auditor may also need a better understanding of the "flow" of transactions from a client's accounting sub-ledgers to the general ledger and then to the financial statements.

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

The auditor will also need to evaluate significant estimates for management's bias and examine the rationale for any unusual transactions.

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 of the procedures set forth in AU-C 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 entity's financial statements to material misstatement due to fraud.	See the team discussion workpaper XX.	TTH
Inquiries of management and others within the entity 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 from 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 the revenue recognition and evaluation of the allowance. These were documented at workpaper XX and also 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 the area of accounts receivable / revenue is a significant risk. The other types of revenue are not deemed to be a significant risk of fraud due to 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.	Journal entry testing was performed. We selected 10 entries spanning all types of entries and reviewed for lack of support or unusual transactions. None were noted. 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

Case Study for Discussion

A social service agency dealing with at-risk youth experienced a fraud. Since it was a small agency (approximately $5 million in revenue), it had one person responsible for accounting. Even the CFO was a part-time employee. As in many small entities, the bookkeeper was a trusted individual that had worked with the agency for many years. Since there was no money available for additional accounting personnel, the board made a decision to become more involved with the financial affairs of the entity. The bookkeeper was required to obtain additional approval by the CFO for every payment made. The CFO was the first signature on the check. To further safeguard assets, a board member also reviewed the documentation for each invoice and was the second signature on all checks.

The board was engaged. The financial package, which consisted of a comparison of budget to actual and current period to prior period, was discussed in depth at board meetings.

However, the bookkeeper was really not to be trusted at all. She was actually stealing approximately $200,000 a year from the entity. At the time the fraud was discovered, investigators believed it had been going on for at least seven years. The bookkeeper set up a fictitious management company. She terminated contracts between the entity and its legitimate vendors and set up contracts between her fictitious company and those same vendors. Then her company contracted with the social service entity. The theft was the markup she put on the amounts her company paid to legitimate vendors.

This was discovered by accident at a board meeting when the board was discussing the monthly operating results. Outside counsel was listening to the discussion and suggested that the amount that the entity was paying for those services was too high and that they should go out to bid. During that process the theft was discovered. However, the authorities are uncertain that the magnitude will ever really be known since investigators only went back seven years.

The auditors believed that the mitigating controls were appropriate and had not issued a management letter comment for several years.

Questions for Discussion

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?

2. The audit firm made all of the inquiries of management and the board related to fraud. In addition, they performed analytical procedures on the line items where the fictitious amounts were located and their analysis was a five-year trend comparison. No unusual fluctuations were noted. They vouched 10 of the fictitious invoices. What is the auditor's responsibility as it relates to the evaluation of fraud and what could they have done differently?

3. Do you believe that a management letter comment or a communication containing a significant deficiency or material weakness should have been issued by the auditors?

4. Assuming that the board was sincere, what other procedures could be put in place to reduce the risk of fraud in a very small entity?

Unit

3

Pressure on Not-for-Profits to Strengthen Controls

LEARNING OBJECTIVES

- Describe common characteristics of major fraud schemes and scenarios.
- Understand the potential red flags for fraud and the concealment of fraud in an effort to understand the importance of a strengthened control environment.
- Construct and design a system of internal control for not-for-profit entities by leveraging the COSO framework.

PRESSURE ON NOT-FOR-PROFITS TO STRENGTHEN CONTROLS

Risks of Fraud

In 2004, the Senate Finance Committee encouraged the Independent Sector to commission a report on ways that charitable entities 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 IRS has also played a role in the effort toward transparency, accountability, and fraud prevention with its new Form 990. This form asks a number of questions and requires disclosure on certain policies and procedures that would support the Independent Sector's goals. Not-for-profits are not legally required to answer these questions *yes* but failure to do so could send up a red flag to the IRS to more closely scrutinize the not-for-profit's activities. Perhaps worse could be the reaction of donors and funding sources who download the 990s from Guidestar's website. They may not look favorably on not-for-profits that do not answer the questions or have *no* answers to questions asking whether they have certain policies and procedures in place.

The 33 principles provide excellent guidance to not-for-profits in setting the tone from the top (control environment), communication, and monitoring.

Principle	Important Policy
Compliance with Laws and Regulations	N/A
Code of Ethics	Code of Ethics
Conflicts of Interest	Conflicts of Interest
Whistleblower Policy	Whistleblower Policy
Protection of Business Records	General Policies Should Include
Document Retention and Destruction Policy	Document Retention and Destruction Policy
Protection of Assets	Human Resource Policies Should Include
Availability of Information to the Public	N/A
Board Responsibilities	N/A
Board Meetings	Board Meeting Attendance Policy
Board Diversity	Policy on Diversity
Board Independence	Important Policy
CEO Evaluation and Compensation	Executive Compensation Policy
Separation (independence) of CEO, Board Chair, and Treasurer Roles	Executive Compensation Policy
Board Education and Communication	N/A
Evaluation of Board Performance	N/A
Board Member Term Limits	Term Limits Policy, Consecutive Terms Policy
Review of Governing Documents	N/A
Review of Mission and Goals	N/A
Board Compensation	Board Compensation Policy
Financial Statements and Reporting	N/A
Annual Budget, Financial Performance, and Investments	N/A
Loans to Directors, Officers, and Trustees	Loan Policy
Resource Allocation for Programs and Administration	N/A
Travel and Other Expense Policies	Payment or Reimbursement of Expenses and Travel Policy
Expense Reimbursement for Nonbusiness Travel Companions	Payment or Reimbursement of Expenses and Travel Policy
Accuracy and Truthfulness of Fundraising Materials	N/A
Compliance with Donor Intent	Investment Policy, use of Reserves Policy

Principle	Important Policy
Acknowledgement of Tax-Deductible Contributions	Loan Policy
Gift Acceptance Policy	Gift Acceptance Policy
Oversight of Fundraisers	N/A
Fundraiser Compensation	
Donor Privacy	Donor Privacy Policy

Not-for-profits are notorious for failure to prosecute those that perpetrate fraud against the entity. A frequent explanation is that the negative publicity could cost the entity donors. Although this may be true, as noted earlier, the revised Form 990 makes it very difficult to hide misappropriation of assets. 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 similar to the privately held companies who reported the majority of the frauds.

Characteristics of Fraud Schemes

The ACFE's *Report to the Nations* for 2020[18] noted that entities with less than 100 employees tend to have greater instances of fraud. Approximately 26% of frauds noted in the study were perpetrated against entities with less than 100 employees.

Number of Employees	Frequency	Median Loss
< 100	26%	$150,000
100–999	23%	$120,000
1,000–9,999	27%	$100,000
10,000+	25%	$140,000

Unfortunately, the typical time between when a fraud begins and when it is detected is 14 months for all entities.

[18] The ACFE *Report to the Nation* for 2020 can be accessed at https://www.acfe.com/report-to-the-nations/2020/.

Scheme	Duration of Scheme Before Identification (months)
Payroll	24
Check tampering	24
Register disbursements	24
Financial statement fraud	24
Expense reimbursement	24
Billing	24
Cash larceny	21
Corruption	18
Skimming	16
Cash on hand	15
Noncash	13

Fraudsters may not limit themselves to one type of scheme. Approximately 35% of fraudsters committed more than one type of fraud. Fraudsters 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%.

The most prevalent asset misappropriation sub-schemes are noted in the report that follows.

Scheme	Description	Median Loss
Billing	A disbursement scheme in which a person causes an entity to issue a payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases.	$100,000
Noncash misappropriations	An employee steals or misuses noncash assets of the entity.	$78,000
Expense reimbursement	A disbursement scheme in which an employee makes a claim for reimbursement for fictitious expenses or inflated expenses.	$33,000
Skimming	A scheme in which cash is stolen before it is recorded in the books and records of the entity.	$47,000
Cash on hand misappropriation	A scheme in which an employee steals cash kept on hand at the entity.	$26,000
Check or payment tampering	A disbursement scheme in which an employee steals the entity's funds by intercepting, forging, or altering a check or electronic payment drawn on one of the entity's bank accounts.	$110,000

Scheme	Description	Median Loss
Payroll scheme	A disbursement scheme in which an employee causes his employing entity to issue a payment for an improper amount or for a fictitious employee.	$62,000
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).	$83,000
Register disbursements	A disbursement scheme in which an employee makes incorrect entries on a cash register to hide the removal of cash.	$20,000

The following table shows the schemes broken down by industry sector.

Scheme	% Cases Reported Education	% Cases Reported Health Care
Financial Statement Fraud	67%	14%
Corruption	30%	40%
Billing	30%	33%
Expense reimbursement	22%	22%
Noncash misappropriations	17%	24%
Skimming	22%	10%
Check and payment tampering	18%	14%
Payroll	13%	15%
Cash on hand	13%	10%
Cash larceny	9%	10%

Concealment of Fraud

Participants in the study were asked how the fraudsters 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 fraudsters 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	40%
Altered physical documents	36%
Altered electronic documents or files	27%
Created fraudulent electronic documents or files	26%

A common question that comes up is, to whom and at what level should communication of known or suspected fraud be addressed? Whistleblowers reported suspicions to their direct supervisor 28% of the time. The next highest were *other* at 15%and fraud investigation team at 14%.

Committee of Sponsoring Organizations (COSO) Internal Control Integrated Framework

In response to the Foreign Corrupt Practices Act, the COSO sets forth a framework that can be used to design a system of internal controls. By selecting and implementing controls from this framework, an entity 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 possibility that there will be lapses in internal control due to human nature, and there is 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 controls that are most associated with fraud prevention and detection are those at the activity level. However, the entity level controls are as important and maybe, in some instances, even more important. In 2004, the International Federation of Accountants and the Chartered Institute of Management Accountants performed an analysis of some of the largest recent corporate failures. As noted in the following chart, failure of entity level controls was the root cause. When management

has the incentive or pressure to commit fraudulent financial reporting and a weak or colluding board supplies the opportunity, activity level controls are not effective.

	Failure Due to Lack of Ethics/Tone at the Top	**Failure Due to Role of CEO**	**Failure Due to Role of Board of Directors**	**Lack of Internal Control Compliance/ Risk Management Functions**	**Failure Due to Aggressive Earnings Management**
Ahold	+	++		++	++
Enron	++	++	++	++	++
WorldCom	++	++	++	++	++
Xerox	++	++		++	++
AHERF*	++	++	++	++	
Baptist Foundation of Arizona*	++	++	++	++	

* These entities were not mentioned in the study but are included here to emphasize that public companies are not the only place where large high-profile frauds occur.

\+ Issue had moderate significance of the entity

++ Issue had major significance in the downfall of the entity

In the 2020 *Report to the Nations*, the certified fraud examiners identified the following as the most prevalent control weaknesses:

Weakness	**Percentage**
Lack of internal controls	32%
Override of existing internal controls	18%
Lack of management review	18%
Poor tone at the top	10%
Lack of competent personnel in oversight roles	6%
Other	6%
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%

This is why 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 entity 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 control activities should address the risk of fraud at the transactional level and thus help to prevent or detect fraudulent financial reporting and misappropriation of assets.

After launching its integrated framework in 1992, the COSO issued publications to address specific needs of users. In 2006, it issued a publication for smaller entities, and in 2009, it issued another publication on effective monitoring.[19] As will be discussed later, the COSO issued its integrated framework in early 2013. The revised framework includes information from these two publications.

The two examples below highlight why it is important to focus on the entity level controls.

See entity level anti-fraud programs and controls in Appendix A. See examples of internal controls that accomplish the 17 principles of the revised COSO framework in Appendix B.

Case Study

The American Legacy Foundation (Legacy) was founded from a big settlement that resolved health claims against cigarette companies. The entity had approximately $1 billion in assets and expended approximately $50 million every year. The entity has a high-profile board in including two Attorneys General (Iowa and Idaho), two governors (Utah and Missouri), and a senator.

The perpetrator was Deen Sanwoola, a computer specialist who was hired to build the entity's IT department. The entity did not have adequate internal financial controls. Sanwoola was in charge of purchasing IT equipment. He also was the person that approved the invoice and received the goods. The IT department spent significant sums on computers, monitors, and software.

Subsequent investigations showed that Legacy spent far more on computer equipment than it was worth. Sanwoola is alleged to have generated as many as 255 invoices for equipment sold to Legacy, 75% of which was deemed fraudulent.

Sanwoola left in 2007 to go back to Nigeria. Six months later an inventory of computer equipment was conducted, and an executive reported that the equipment could not be found. The CFO dismissed the complaint without investigation. The CFO was receiving $568,000 in current and deferred compensation (2012). About three years later, the same executive raised an alarm and took it to the board, bypassing the CFO.

Legacy hired forensic auditors and conducted an investigation. Investigators found a template in the computer system which had been used to generate fictitious invoices from a Maryland IT supply company. The investigation concluded that of the $4.5 million in checks and credit card charges made with that company, $3.4 million were fraudulent.

[19] COSO Guidance on Monitoring Internal Control Systems, http://www.coso.org/documents/coso_guidance_on_monitoring_intro_online1_002.pdf.

The following was reported in the entity's 2012 Form 990 to describe the diversion of assets:

> In fiscal year 2011, Legacy became aware of an unauthorized diversion of assets in excess of $250,000 committed by a former employee. This fraud did not meet other materiality tests for financial reporting (5% of total assets or 5% of yearly revenues). Legacy leadership notified both its board of directors and law enforcement, with whom the entity has cooperated fully in the ongoing investigation. A subsequent insurance claim was filed by Legacy and in fiscal year 2012 the case was settled.

The allegedly fictitious invoices came from a company called Xclusiv which was out of business at the time of the investigation. One of the board members of Xclusiv, Mack Adedokun, knew of Sanwoola but told investigators that Xclusiv was a barbershop. The other Xclusiv director, Abdul Yusuf, said that computers were sold to Legacy but was not sure how many or who arranged the deal. He also said that he had no idea how documents bearing his name and social security number were on Legacy's computer. He thought it might have been identity theft. Property records showed that Sanwoola bought a home from someone with Yusuf's name.

Form 990 does not require the dollar figure of the diversion to be disclosed, but Legacy admitted that the full loss came to $3,391,648.

It took Legacy more than 3 years to report the missing computers and its records were not deemed reliable. Accordingly, the FBI closed the investigation. The entity was unable to recover its losses either in criminal or civil court because of the delay and condition of the records.

Case Study

The Baptist Foundation of Arizona was created in 1948 to raise money to help build churches and make donations to Southern Baptist related charities. People who invested money in the Foundation were promised a high rate of return on their investment. In the 1980s, the Foundation had new management and under that leadership began to lose money. The losses resulted primarily from a series of bad real estate investments.

The Foundation did not admit to those losses. Instead, it created a company called ALO. It sold the bad investments to ALO and effectively moved them off the books of the Foundation. The two entities were not consolidated, although ALO was created, controlled, and financed by the Foundation. The financial statements of the Foundation did not show the investments or the debt. Accordingly, it was easier to continue to sell securities to investors. The new proceeds were used to make the interest payments to the old investors.

An accountant for the Foundation tried to call the scheme to the attention of the Foundation's auditors in 1997 to no avail. Later, an investment advisor whose client was concerned about his investment obtained ALO's financial statements and realized that the entity was effectively bankrupt. The Foundation had a $50 million receivable from ALO on its books.

Between the time of the first warning and the bankruptcy, the Foundation took in another $200 million from investors. Reports say that during the life of the Foundation, only a very small portion of its earnings was ever received by the churches and charities that were supposed to benefit. Instead, it spent millions of dollars on salaries, automobiles, and other benefits for insiders.[20]

[20] 60 Minutes 7/31/02 and Christianity Today 10/25/99, BLB & G website, http://www.blbglaw.com/cases/00099.

The Foundation went bankrupt in 1999. It was the largest not-for-profit bankruptcy in the history of the United States. At the time the bankruptcy was filed, the Foundation had $650 million in liabilities and only $290 million in assets. Approximately $570 million of those liabilities were owed to over 11,000 investors. A Trust was set up to liquidate the assets and wind up the affairs of the Foundation. The Trust sought compensatory damages from Andersen who eventually agreed to pay $217 million to settle the claims against it.

Interestingly enough, the Baptist Foundation and a very similar fraud case – Enron were audited by the same firm. The root cause? Lack of ethical values on the part of the executives and lack of monitoring by the board.

Behavioral Red Flags

Much has been written about behavioral red flags. Perpetrators tend to demonstrate certain characteristics. The following is from the ACFE 2020 *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 behavior when involved in a fraud scheme.

Red Flag	**Percentage**
Living beyond means	42%
Financial difficulties	26%
Unusually close association with vendor or customer	19%
No behavioral red flags	15%
Control issues, unwilling to share duties	15%
Irritability, suspiciousness, or defensiveness	13%
"Wheeler-dealer" attitude	13%
Divorce/ family problems	12%
Addiction problems	9%
Complaints about inadequate pay	8%
Refusal to take vacations	7%
Excessive pressure from within the entity	7%
Past employment-related problems	6%
Social isolation	6%
Complaints about lack of authority	5%
Past legal problems	5%
Excessive family/peer pressure for success	4%
Instability in life circumstances	4%
Other	4%

Identifying the behavioral signs exhibited by fraudsters can help not-for-profit entities successfully detect fraud and reduce their losses. Eighty-five percent of all fraudsters in the 2020 ACFE report demonstrated at least one behavioral red flag while committing their crime and 49% exhibited multiple red flags. The ACFE report states that 86% of fraudsters in the cases in their study were not previously punished or terminated, 8% were previously terminated, and 8% were previously punished.

Where AU-C 240 defines fraud as asset misappropriation and fraudulent financial reporting, the ACFE adds one more category—conflicts of interest/corruption. The revised 2013 COSO Integrated Framework provides suggestions of controls that address that category of fraud.

Elements of Internal Control

The elements of the COSO framework are incorporated into the AICPA's statements on auditing standards. AU-C 315 describes them the way that they were laid out in the integrated framework years ago. The COSO framework is still the most widely recognized framework for internal controls here in the United States.

However, over time, business practices have evolved so that controls that may have been effective in the past are no longer as effective. One of the main reasons for this is the extent that technology has evolved. Another factor is the extent of complex regulations that many entities are required to follow. The framework has been updated to reflect these changes as well as the globalization. It has also been updated to reflect the larger and more significant role of the board of directors and the expectations for competencies and accountability and expectations related to the prevention of fraud including corruption. The updated framework[21] uses a principles-based approach with 17 principles. Appendix B contains a list of those principles along with the controls that support them.

The five elements of internal control (control activities, control environment, risk assessment process, information, and communication and monitoring) remain the same. The 17 principles are organized within those elements.

A consistent theme throughout the new framework is the emphasis on management and the board's evaluation of risks and the creation of an integrated set of internal controls to effectively mitigate the risks identified.

Anti-fraud controls are an important part of a system of internal control. The 2013 COSO Framework emphasizes this throughout each element of internal controls. The existence of anti-fraud controls can help prevent or detect fraud.

Entities will often find it useful to benchmark their anti-fraud controls against their peers, both in terms of what mechanisms are being employed and the effectiveness of those approaches.

The chart below illustrates the frequency with which small entities (< 100 employees) and large entities (100+ employees) enact anti-fraud controls for all entities in the ACFE *Report to the Nations* for 2020.[22]

---

[21] The revised framework was issued in May 2013.

[22] The ACFE *Report to the Nations* (2020) will be referenced throughout this manual. The survey population came from entities that had experienced frauds.

Anti-Fraud Control	Small Entities	Large Entities
External audit of financial statements*	56%	92%
Code of conduct	48%	91%
Management certification of financial statements	39%	85%
Management review	35%	76%
External audit of internal control over financial reporting	33%	80%
Internal audit department	31%	88%
Employee support programs	23%	65%
Independent audit committee	21%	76%
Hotline	20%	79%
Anti-fraud policy	20%	67%
Fraud training for employees	19%	67%
Fraud training for managers/executives	19%	67%
Proactive data monitoring/analysis	15%	46%
Surprise audit	14%	47%
Dedicated fraud department or team	11%	55%
Formal fraud risk assessment	9%	52%
Job rotation/mandatory vacation	9%	27%
Rewards for whistleblowers	4%	16%

* Note that financial statement auditors are not considered to be a part of the internal control structure themselves, but the board and management may view them as a good monitoring control since they get recommendations from them and issues may be identified.

The ACFE also looked at the change in control implementation rates from 2010 to 2020. The implementation rates that increased more than 5% over the last decade were:

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%

These controls are among those most frequently linked with a strong anti-fraud program. The rise in implementation of the above controls over the last decade indicates that an increasing number of entities are taking the threat of fraud seriously and employing procedures designed to help them diminish fraud threats.

Control Environment

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

Fraud 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 2020 *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.

Detection Method	Median Duration	Median Loss	Control Type	Percent
Tip	14 months	$145,000	Potentially active or passive detection[23]	43%
Management review	17 months	$100,000	Active detection	12%
Account reconciliation	7 months	$81,000	Active detection	4%
Document examination	18 months	$101,000	Active detection	3%
By accident	24 months	$200,000	Passive detection	5%
Internal audit	12 months	$100,000	Active detection	15%

[23] The ACFE identifies this as a potentially active or passive detection control in the Report to the Nations.

Detection Method	Median Duration	Median Loss	Control Type	Percent
External audit	24 months	$150,000	Potentially active or passive detection[24]	4%
Notified by law enforcement	24 months	$900,000	Passive detection	2%
Confession	17 months	$225,000	Passive detection	1%
IT controls	6 months	$80,000	Active detection	2%
Surveillance	7 months	$44,000	Active detection	3%

It is easy to see that implementing strong internal controls can be very important in preventing or detecting fraud. To make this information more useful, it is important to know how tips are received and from whom, since a formal reporting mechanism program can really enhance an entity's internal controls. The 2020 *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.

Source of Tip	Percentage
Employee	50%
Customer	22%
Anonymous	15%
Vendor	11%
Other	6%
Competitor	2%
Shareholder/owner	2%

The ACFE asked which mechanisms were used by survey participants.

Reporting Mechanism	Percentage
Telephone hotline	33%
Email	33%
Web-based/online form	32%
Mailed letter or form	12%
Other	9%
Fax	1%

[24] The ACFE identifies this as a potentially active or passive detection control in the Report to the Nations.

Another question that comes up is whom and at what level should the communication of fraud or suspected fraud be addressed to. Whistleblowers reported suspicions to their direct supervisor 28% of the time. The next highest were *other* at 15% and other at 14%. Other responses are noted below.

Suspicions Reported To:	**Percentage**
Direct supervisor	28%
Other	15%
Fraud investigation team	14%
Internal audit	12%
Executive	11%
Coworker	10%
Law enforcement or regulator	7%
Owner	7%
Board or audit committee	6%
Human resources	6%
In-house counsel	4%
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 entity may run criminal background checks, often they come up empty. One reason for this is the reluctance of entities to report activity to authorities or prosecute.

The participants in the study were entities where a fraud occurred. Unfortunately, many of these entities performed one or more of the background checks identified below and the fraud occurred anyway. This is one reason why an entity cannot pin all its assurance on the operation of one or two controls.

Background Check Run on Perpetrator	**Percentage**
Employment history	81%
Criminal checks	75%
Reference checks	56%
Education verification	50%
Credit checks	38%
Drug screening	28%
Other	4%

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.

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%

Principle 3 details guidelines for the authority and responsibilities of each entity level, from the board of directors to personnel and third-party service providers. Principle 5 provides details on how individuals are held accountable for their internal control responsibilities.

The COSO continues to issue white papers. One of them, Enhancing Board Oversight, Avoiding Judgment Traps and Biases,[25] is helpful for not-for-profits since boards tend to consist of members that tend to be of similar backgrounds and hold similar views.

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 concern. **The entity considers the potential for fraud in assessing risks to the achievement of objectives.**

Management and the board consider the potential for fraud in financial reporting, non-financial reporting, misappropriation, and illegal acts. They stay particularly aware of potential issues in the areas of management bias, estimates, common frauds in their industry, geographic regions, incentives, IT, complex or unusual transactions, and management override. They look for performance incentives that may be too strong and become pressured to commit fraud. They look for fraud opportunities, remaining aware that fraud risk increases with complex or unstable entity structure, high turnover, poor controls, or poor IT systems. Fraudsters often rationalize by considering it *borrowing*, believing they are *owed* and not caring about consequences.

Control Activities

Control activities comprises principles 10 and 11. These deal with selection of appropriate control activities including segregation of duties. Technology is one of the most important focuses of the

[25] https://www.coso.org/documents/COSO-EnhancingBoardOversight_r8_Web-ready%20(2).pdf.

revised framework and it is discussed at length, including the importance of security management processes (who has what access to the system).

Internal control can prevent or detect fraud on the part of employees. It can also help to identify areas where the entity is at risk of fraud from external parties. There have been numerous articles written recently about **cyber fraud**. With most entities dealing at least in some way with e-commerce, this has become a big threat. In a 2013 report, the AICPA discussed the top five cybercrimes.[26] Four of those are of particular concern to not-for-profits:

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 entities because of their weaker cyber security. The commencement of the global pandemic and its subsequent uncertainty have further bolstered fraudsters. Federal agencies such as the FTC, DOJ, and the FBI have all advised that fraudsters are aggressively targeting entities with COVID-19 related frauds. It is a near certainty that not-for-profit entities will face the increase threat of account takeovers in 2020 and beyond than ever before as fraudsters continue to look for ways to con entities.

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 entities, 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 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.

Theft of Sensitive Data. This is similar to identity theft but involves additional types of data as well. For example, a cybercriminal might copy an entity's customer or donor files onto a flash drive and sell them to a competitor.

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.

EXAMPLE

On January 15, 2001, Amy Elaine Phillips, 27 years old, was hired as an administrative assistant 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.

---

[26] The Top 5 CyberCrimes – AICPA, 2013.

Beginning in 2004, Amy 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. But in 2007, her bank informed her they would no longer accept deposits into her account of checks on which she was not the payee.

Undeterred, Amy 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, Amy 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, from 2007 to early 2009 Amy was able to steal additional amounts totaling more than $657,000, for a total theft of $717,999.

Unsurprisingly, Amy did not pay any income tax on her ill-gotten gains. On October 11, 2011, Amy pleaded guilty to theft of program funds and tax evasion. In 2012 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.

Source: https://www.justice.gov/archive/usao/mow/news2012/phillips.sen.html

---

EXAMPLE

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 which he stole and spent on personal expenses including 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 fund-raising, 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 in order 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.

Source: https://www.justice.gov/archive/usao/mow/news2012/taylor.sen.html

EXAMPLE

Use of Debit Cards

Vernell Reynolds, a former Miami Florida police officer, was head of the Miami Community Police Benevolent Association which was founded in 1946. The group devotes efforts to charity work to benefit the inner city.

Beginning in late 2008 and for nearly 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 reports that she embezzled to fund her gambling habit.

In early 2012, she pled guilty in federal court to fraud and tax charges. Separately, Florida state prosecutors charged her in 2011 with defrauding the not-for-profit Step up Students of nearly $7,000. The charges claimed that while earning more than $140,000 annually, 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 Students.

Source: http://miami.cbslocal.com/2012/08/22/former-miami-cop-convicted-of-fraud-to-be-sentenced/

NOTES

Unit

4

Case Studies – Fraud Schemes

LEARNING OBJECTIVES

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

CASE STUDIES – FRAUD SCHEMES

Case Study 1

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 entity. 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 entity was in such dire straits, a member of the Board of Directors for the entity 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.

1. Name the fraud schemes perpetrated by Ms. Distefano.

2. What, if anything, do you believe that Turning Pointe did right in this case?

3. What are some of the "fraud symptoms" that might have alerted the Board of Directors to fraudulent activity?

4. What controls should Turning Pointe put in place to prevent this from happening to them again?

Case Study 2

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 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 entity.

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.

1. What are the internal control deficiencies noted in this case?

2. What might have been done to prevent this fraud from occurring?

Case Study 3

Avelyn Reynolds was the trusted executive assistant to the Chief Operating Officer (COO) at Support Childhood Education (SCE), a prestigious non-profit entity in Milwaukee. 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 entity.

As the COO's assistant, she had an entity 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 fraudsters, she started small but steadily increased the size of her thefts. She began using the entity credit card for personal purchases, forging the COO's signature. The entity 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.

1. What are the internal control deficiencies noted in this case?

2. What might have been done to prevent this fraud from occurring?

Case Study 4

Ian Turner, who worked for a Florida not-for-profit, was able to steal $112,000 during a two-year period through payroll fraud.[27] His incentive was that he needed the money to pay for his expensive HIV drugs.

Turner was a payroll clerk whose responsibilities were posting time and attendance information to the computer system and preparing the payroll disbursement summaries. 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 co-worker 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. Interestingly enough, the

[27] Wells, Joseph T., *Keep Ghosts off the Payroll*, Journal of Accountancy, 2002.

fictitious report was prepared with a different type face than the real reports, but that was not noticed by the supervisor.

His 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.

This fraud was caught when 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. They saw that they all 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

Since Turner was the only one who benefitted from the scheme (no other accounts received these fictitious deposits), it was determined that Turner acted alone. He pleaded guilty and was sentenced to 15 years' probation and ordered to make restitution.

The auditors noted that there were several clues 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

What are some internal controls that might prevent or detect payroll fraud?

Case Study 5

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 a number of 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 the 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 entity. Donations continued to rise each year. Liersch relied on his control and knowledge of the entity's workings to hide fraud. He also lied to the Board of Directors.

What is amazing about this case is the commendations that Liersch received for his work with Goodwill and his work in Guatemala, extending even to a commendation from President Ronald Reagan. He 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.

What could have been done to prevent or detect this fraud?

Case Study 6

In 2004, Ralph Clark was hired by the Woodruff Arts Center in Atlanta as an HVAC mechanic. In late 2005, he was made acting director of facilities, with that promotion made permanent in June 2006.

In 2013, Clark pleaded guilty to embezzling more than $1.1 million from the 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.

1. What are the internal control deficiencies noted in this case?

2. What might have been done to prevent this fraud from occurring?

Case Study 7

The Elie Wiesel Foundation for Humanity was established in the 1980s to foster dialogue and support programs that promote acceptance, understanding, and equality across the globe. While

distinct in its origins with Holocaust survivor, author, and Nobel-laureate Elie Wiesel, the foundation is in many ways indistinct from other foundations that selflessly aspire to create social change, and in doing so, touch the hearts and lives of millions.

In late 2008, the following appeared on the Wiesel Foundation website:

> *To Our Friends:*
>
> *We are deeply saddened and distressed that we, along with many others, have been the victims of what may be one of the largest investment frauds in history. We are writing to inform you that the Elie Wiesel Foundation for Humanity had $15.2 million under management with Bernard Madoff Investment Securities. This represented substantially all of the Foundation's assets.*
>
> *The values we stand for are more needed than ever. We want to assure you that the Foundation remains committed to carrying on the lifelong work of our founder, Elie Wiesel. We shall not be deterred from our mission to combat indifference, intolerance, and injustice around the world.*
>
> *At this difficult time, the Foundation wishes to express its profound gratitude for all your support.*
>
> *The Elie Wiesel Foundation for Humanity*

The Elie Wiesel Foundation was not the only not-for-profit that experienced losses. Individual and institutional investors lost over $50 billion due to the fraud and deceit perpetrated by Bernie Madoff. The loss to foundations, in turn, caused losses to the not-for-profits that receive grants or contributions from them.

How could something like this happen? What types of due diligence was performed when investing so much in one investment? There were many red flags, but boards just weren't watching. The Elie Wiesel Foundation was not alone. The Madoff scandal touched 150 not-for-profit entities, and 105 of them lost 30% or more of their assets.[28] Some of the other entities affected by Madoff's duplicity are Yeshiva University, Picower Foundation, Chais Family Foundation, Betty and Norman Levy Foundation, Gift of Life Foundation, and the Chais Family Foundation.

Madoff was a successful and well-respected man who had extensive financial expertise. At one time, he was the nonexecutive chairman of the NASDAQ market. He was also very popular in the Jewish community and promoted a kind of club atmosphere around his investment services. Hedge funds have fewer regulations than other types of investment vehicles and that helped him to go undetected. But although issues with his scheme were identified, the SEC investigated and let him go with minor adjustments.

Madoff's Ponzi Scheme promised large returns while subsequent investments pay the returns while money is siphoned off into the pockets of the perpetrator. Investors in Madoff's scheme clearly didn't realize that when out of the ordinary returns are produced year after year, even in down markets, it may be too good to be true. Madoff also counted on private foundations, which held a significant portion of the funds, and which only required 5% of its noncharitable use assets to be paid out, the largest of which is its investments. He knew that foundation managers would not be asking for large distributions from his funds. And in fact, that is how the scheme unraveled. When markets declined and some investors needed to liquidate their shares, Madoff was unable to keep up. The money simply wasn't there.

---

[28] NCRP Report: Foundations Hit by Madoff Scheme Lacked Adequate Board Size and Diversity, Issued June 25, 2009.

What types of controls should not-for-profits have to prevent these types of losses in the future?

NOTES

Unit

5

Appendix A: Entity Level Anti-Fraud Programs and Controls

LEARNING OBJECTIVE

- Summarize entity level anti-fraud programs and controls that can enhance the control environment, risk assessment, information and communication, and monitoring controls of an entity.

APPENDIX A: ENTITY LEVEL ANTI-FRAUD PROGRAMS AND CONTROLS

Control Environment

- Code of Conduct/Ethics
- Ethics Hotline/Whistleblower Program
- Hiring and Promotion Guidelines—background and credit checks
- Oversight by the Audit Committee and Board
- Investigation/Remediation

Fraud Risk Assessment

- Management's identification of fraud risks and implementation of anti-fraud measures
- Board assesses the potential for management override of controls or other inappropriate influence over the financial reporting process

Information and Communication

- Appropriate internal controls to prevent unauthorized changes to programs or master files

- Communication between management and staff, management and the board, management and the auditors, the auditors and the board, and if there are internal auditors, communication between them and the board
- Ethics hotline (or equivalent for smaller entities)
- Open-door policy
- Collaborative board

Monitoring

- Board receives and reviews periodic reports describing the nature, status, and eventual 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
- Involvement of other experts—legal, accounting and other professional advisers—as needed
- Review of accounting principles, policies, and estimates used by management in determining significant estimates
- Review of significant non-routine transactions entered into by management
- Functional reporting by internal and external auditors to the board and audit committee

Unit

6

Appendix B: 2013 COSO Framework

LEARNING OBJECTIVE

- Gain an understanding of the 2013 COSO framework of internal control to include the 5 components of internal control and its associated 17 principles.

APPENDIX B: 2013 COSO FRAMEWORK

The 2013 COSO revision added some valuable insights into types of controls that could be implemented to accomplish the 17 principles. Following is a discussion of the revised framework's principles along with examples by internal control element.

CONTROL ENVIRONMENT

Principle 1. The organization demonstrates a commitment to integrity and ethical values. There are several points of focus.

Setting the Tone at the Top

The board and management demonstrate the importance of integrity and ethical values to support the functioning of internal control. Together, they set their expectations that values, philosophy, and operating style will be followed. Some of the documents and procedures where this is evident could be the following:

- Mission and values statements
- Standards or codes of conduct
- Policies and practices
- Operating principles
- Directives, guidelines, and other supporting communications

- Actions and decisions of management at various levels and of the board of directors
- Attitudes and responses to deviations from expected standards of conduct
- Informal and routine actions and communication of leaders at all levels of the entity

Establishing Standards of Conduct

The board's expectations of management for integrity and ethical values are defined in standards of conduct and understood at all levels. These standards of conduct guide the entity by:

- establishing what is right and wrong,
- providing guidance for considering associated risks in navigating gray areas, and
- reflecting legal and regulatory expectations by stakeholders.

Management is ultimately accountable for activities delegated to outsourced service providers. To ensure compliance with the entity's standards of conduct, they must be subject to oversight.

Evaluates Adherence to Standards of Conduct and Addresses Deviations in a Timely Manner

- Management should have processes in place to evaluate conformity of individuals and teams to the standards of conduct. Some red flags that may indicate a lack of adherence to standards are the following:
  - Tone at top does not effectively convey expectations
  - Board does not provide impartial oversight of management
  - Decentralization without adequate oversight
  - Coercion by superiors, peers, or external parties
  - Performance goals that create pressure to cut corners
  - Inadequate channels for employee feedback
  - Failure to remedy non-existent or ineffective controls
  - Inadequate complaint response process
  - Weak internal audit function
  - Inconsistent, insignificant, or unpublicized misconduct penalties
- Deviations from the standards of conduct are identified and remedied timely and consistently, using a process that includes the following:

- Defining a set of indicators to identify issues and trends related to the standards of conduct
- Establishing continual and periodic compliance procedures to confirm that expectations and requirements are being met
- Identifying, analyzing, and reporting business conduct issues and trends to senior management and the board
- Evaluating the strength of leadership in the demonstration of integrity and ethical values for performance reviews, compensation, and promotions
- Compiling allegations centrally and have them independently evaluated
- Investigating allegations using defined investigation protocols
- Implementing corrections timely and consistently
- Periodically reviewing issues; searching for causes in order to modify policy, communications, training, or controls

Principle 2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. There are several points of focus.

Establishes Oversight Responsibilities

- The board identifies and accepts its oversight responsibilities
- Public companies in many jurisdictions are required to have board committees in specific areas such as nominating/governance, compensation, audit, investment, finance, human resources, operations, legal

Applies Relevant Expertise

- The board defines, maintains, and evaluates the skills needed among its members. Specialized skills needed among board members may include:
  - Internal control mindset
  - Market and entity knowledge
  - Financial expertise
  - Legal and regulatory expertise
  - Social and environmental expertise
  - Incentives and compensation

- Relevant systems and technology

Operates Independently

- The board has sufficient members who are independent and objective

Provides Oversight for the System of Internal Control

- The board maintains oversight of management's design, implementation and conduct of internal control. This includes control environment, risk assessment, control activities, information and communication, and monitoring activities

Principle 3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. There are several points of focus.

Consideration of All Structures of the Entity & Establishment of Reporting Lines of Responsibility

Entities are often structured along various dimensions such as management operating model, legal entity structures, geographic markets, and relationships with outsourced service providers. Many variables must be considered when establishing organizational structures, including:

- Nature, size, and geographic distribution of the entity's business
- Risks related to the entity's objectives and business processes
- Nature of the assignment of authority
- Definition of reporting lines
- Financial, tax, regulatory, and other reporting requirements

Management and governance consider these variables and the risk when establishing or changing the organizational structure.

Defines, Assigns, and Limits Authorities and Responsibilities

- The board of directors delegates authority and defines and assigns responsibility. Key roles and responsibilities assigned typically include the following:
  - Board stays informed and challenges senior management for guidance on significant decisions
  - Senior management establishes directives, guidance, and control to enable staff to understand and carry out their duties
  - Management executes senior management's directives

  - Personnel understand standards and objectives for their area
  - Management and responsible personnel oversee outsourced service providers
- Authority empowers, but limitations of authority are needed so that:
  - delegation occurs only as required,
  - inappropriate risks are not accepted,
  - duties are segregated to reduce risk of inappropriate conduct,
  - technology is leveraged as appropriate to facilitate definition and limitation of roles and responsibilities, and
  - third-party service providers clearly understand the extent of their decision-making authority.

Principle 4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. There are several points of focus.

Management and the Board Establish Policies and Practices

Policies and practices are the entity-level guidance and behavior that reflect the expectations and requirements of stakeholders. They provide the following:

- Requirements and rationale
- Skills and conduct necessary to support internal control
- Defined accountability for performance of key business functions
- Basis for evaluating shortcomings and defining remedial actions
- Means to react dynamically to change

Evaluates Competence and Addresses Shortcomings

Entities define competence requirements needed to support achievement of objectives, considering, for example:

- Knowledge, skills, and experience needed
- Nature and degree of judgment needed for a specific position
- Cost-benefit analysis of different skill and experience levels

Attracts, Develops, and Retains Individuals

Management at different levels establishes structures and processes to attract, train, mentor, evaluate, and retain employees who fit the entity's culture and have the needed skills.

Plans and Prepares for Succession

Management develops contingency plans for assigning responsibilities important to internal control. The board, along with executive management, develops succession plans for key executives, trains and coaches succession candidates for each target role.

Principle 5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives. There are several points of focus.

Enforces Accountability through Structures, Authorities, and Responsibilities

The tone at the top helps to establish and enforce accountability, morale, and a common purpose through:

- clarity of expectations,
- guidance through philosophy and operating style,
- control and information flow,
- anonymous or confidential communication channels for reporting ethical violations,
- employee commitment toward collective objectives, and
- management's response to deviation from standards.

Establish and Evaluate Performance Measures, Incentives, and Rewards

Good performance measures, incentives, and rewards support an effective system of internal control. Key success measures include the following:

- Clear objectives—consider all levels of personnel and the multiple dimensions of expected conduct and performance
- Defined implications—communicate objectives, review relevant market events, and communicate consequences of failure
- Meaningful metrics—define metrics, measure expected vs. actual and assess the expected impact
- Adjustment to changes—regularly adjust performance measures based on continual risk/reward evaluation

Management and the Board Consider Excessive Pressures

Excessive pressures can cause undesirable side effects. Excessive pressures are most commonly associated with the following:

- Unrealistic targets, especially short-term
- Conflict with objectives of different stakeholders
- Imbalance between rewards for short-term vs. long-term objectives

Evaluates Performance and Rewards or Disciplines Individuals

At each level, adherence to standards of conduct and expected levels of competence are evaluated, and rewards allocated or disciplinary action exercised as appropriate.

RISK ASSESSMENT

Principle 6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. There are several points of focus.

Operations Objectives

- Reflects management's choices
- Considers tolerances for risk
- Includes operations and financial performance goals
- Forms a basis for committing of resources

External Financial Reporting Objectives

- Complies with applicable accounting standards
- Considers materiality
- Reflects entity activities accurately and clearly

External Non-Financial Reporting Objectives

- Complies with externally established standards and frameworks
- Considers the required level of precision
- Reflects entity activities accurately and clearly

Internal Reporting Objectives

- Reflects management and the board's choices
- Considers the required level of precision
- Reflects entity activities

Compliance Objectives

- Reflects external laws and regulations and provisions of contracts and grants, if applicable
- Considers tolerances for risk

Principle 7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. There are several points of focus.

Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels

Entity-level risk identification is at a high level and does not include assessing transaction-level risks. Process-level risk identification is more detailed and includes transaction-level risks. Management also assesses risks from outsourced service providers, key suppliers, and channel partners.

Analyzes Internal and External Factors

Management realizes that risk is dynamic and considers the rate of change in risks. If a rate of change increases, management will accelerate the frequency of risk assessment.

Management evaluates the external factors affecting entity-level risk including the following:

- Economic
- Natural environment
- Regulatory
- Foreign operations
- Social
- Technological

Management evaluates the internal factors affecting entity-level risk including the following:

- Infrastructure and use of capital resources
- Management structure
- Personnel, including quality, training, and motivation

- Access to assets, including possibilities for misappropriation
- Technology, including possibility of IT disruption

Management solicits input from employees as to transaction-level risks (also see control activities).

Involves Appropriate Levels of Management

Effective risk assessment mechanisms match an appropriate level of management expertise to each risk.

Estimates Significance of Risks Identified

- Management assesses the significance of risks using criteria such as the:
  - likelihood of risk occurring and impact,
  - velocity or speed to impact upon occurrence of the risk, or
  - persistence or duration of time of impact after occurrence of risk.
- Management determines how to respond to risks. Risk responses fall within the following categories:
  - Acceptance—no action taken
  - Avoidance—exiting the risky activities
  - Reduction—action taken to reduce likelihood, impact, or both
  - Sharing—transferring part of the risk, for example, insurance, joint venture, hedging, or outsourcing
- In relation to risk responses, management should consider the following:
  - Which response aligns with entity's risk tolerance
  - Segregation of duties needed to get intended significance reduction
  - Cost/benefit of response options

Principle 8. The organization considers the potential for fraud in assessing risks to the achievement of objectives. There are several points of focus.

Management and the Board Have an Awareness of How Fraud Can Occur and Considers Various Types of Fraud

- They consider the potential for fraud in the following areas:

- Fraudulent financial reporting
- Fraudulent non-financial reporting
- Misappropriation of assets
- Illegal acts

- As part of the risk assessment process, management identifies various fraud possibilities, considering the following:
  - Management bias
  - Degree of estimates and judgments in external reporting
  - Fraud schemes and scenarios common in the industry
  - Geographic regions
  - Incentives
  - Technology and management's ability to manipulate information
  - Unusual or complex transactions
  - Vulnerability to management override

Management Assesses Incentives and Pressures

Management reviews the entity's incentives structure to identify incentives that may be too strong and become pressure to commit fraud. This review is performed in the context of opportunities, attitudes, and rationalizations that may allow or support fraud related to each incentive.

Management Assesses Opportunities for Fraud to Occur

Opportunity refers to the ability to acquire, use, or dispose of assets, which may be accompanied by altering the entity's records.

The likelihood of loss of assets or fraudulent external reporting increases when there is:

- a complex or unstable organizational structure,
- high employee turnover, especially in accounting, operations, risk management, internal audit, or technology,
- ineffectively designed or poorly executed controls, or
- ineffective technology systems.

Management Assesses Attitudes and Rationalizations

Attitudes and rationalizations by individuals engaging in or justifying inappropriate actions may include the following:

- Considers it borrowing, or intends to repay
- Believes entity owes him something because of some form of job dissatisfaction
- Does not understand or care about consequences
- Does not understand or care about accepted ideas of decency and trust

Principle 9. The organization identifies and assesses changes that could significantly impact the system of internal control. There are several points of focus.

Management Assesses Changes in the External Environment

- Management considers changes that have taken place or will occur shortly in the following:
  - Regulatory environment
  - Economic environment
  - Physical environment

Management Assesses Changes in the Business Model

- Management considers changes in the business model, such as:
  - new or dramatically altered business lines,
  - altered service delivery system,
  - significant acquisitions and divestitures,
  - foreign operations, especially expansion or acquisition,
  - rapid growth, and
  - new technology.

Management Assesses Changes in Leadership

- Management considers significant personnel changes:
  - A new member of senior management may not understand the entity's culture or may reflect a different philosophy or focus on performance to the exclusion of control-related activities.

CONTROL ACTIVITIES

Principle 10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. There are several points of focus.

Management Integrates Control with Risk Assessments Performed

Control activities support all the components of internal control but are particularly aligned with the Risk Assessment component. Along with assessing risks, management identifies and puts into effect actions needed to carry out specific risk responses.

Management Considers Entity-Specific Factors

Since each entity has its own set of objectives and implementation approaches, there will be differences in objectives, risk, risk responses, and related control activities.

- Management considers the many entity-specific factors that can impact the control activities needed such as the following:
  - Environment and complexity
  - Nature and scope of operations, both physically and logically
  - Degree of regulation
  - Multinational operation
  - Diversity of operations
  - Sophistication of enterprise resource planning (ERP) system
  - Centralization/decentralization
  - Degree of innovation

Management Determines Relevant Business Processes

Business processes often cover many objectives and sub-objectives, each with its own set of risks and risk responses. A common way to consolidate these business process risks into a more manageable form is to group them according to information processing objectives:

- Completeness—transactions that occur are recorded
- Accuracy—transactions are timely recorded at the correct amount in the correct account
- Validity—recorded transactions represent economic events that actually occurred

While these objectives are most often associated with financial processes and transactions, the goals of completeness, accuracy, and validity apply to any activity in any entity.

Management Evaluates a Mix of Control Activity Types

- Management considers a variety of transaction control activities for its control portfolio including the following:
  - 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 Considers at What Level Activities Are Applied

In addition to transaction-level controls, 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

Segregation of duties 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 entities, ideal segregation may not be practical, cost effective, or feasible, and alternative control activities must be designed.

Principle 11. The organization selects and develops general control activities over technology to support the achievement of objectives. There are several points of focus.

Management Determines Dependency Between the Use of Technology in Business Processes and Technology General Controls and Implements Effective General Controls

The reliability of technology within business processes, including automated controls, depends on the selection, development, and deployment of general control activities over technology. These general controls help ensure that automated processing controls work properly initially, and that they continue to function properly after implementation. General controls apply to technology

infrastructure, security management, and technology acquisition, development, and maintenance. They also apply to all technology, both IT and technology used in production processes.

Management Establishes Relevant Technology Infrastructure Control Activities

Technology infrastructure may include computers, networks, power supply and backup systems, software, and robotics. This infrastructure is often complex and rapidly changing. These complexities present risks that need to be understood and addressed, and management should track changes and assess and respond to new risks.

Management Establishes Relevant Security Management Process Control Activities

Security management includes sub-processes and controls over who and what has access to an entity's technology, including who has the ability to execute transactions. Security threats can come from both internal and external sources. Evaluating and responding to external threats will be more important when there is reliance on telecom networks and the internet. Internal threats may come from former or disgruntled employees, who pose unique risks. User access to technology is generally controlled by authentication controls. These controls are very important and are often the most abused by employees who may share access codes (generally passwords) and IT personnel who do not immediately shut off an employee's unneeded access to systems resulting from job change or termination.

Management Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities

Technology controls vary depending on risks; large or complex projects have greater risks, and control rigor should be sized accordingly. Use of packaged software can reduce some risks versus in-house software development. Another alternative is outsourcing, which, however, presents its own unique risks and often requires additional controls.

Principle 12. The organization deploys control activities through policies that establish what is expected and in procedures that put policies into action. There are several points of focus.

Management Establishes Policies and Procedures to Support Deployment of Management's Directives

A policy is a management statement of what should be done. A procedure consists of actions that implement a policy. Policies may be written or unwritten. Unwritten may be effective and cost-effective in a small entity if the policy is long-standing and well-understood, but can be easier to circumvent, can reduce accountability, and be costly, especially with high employee turnover.

Management Establishes Responsibility and Accountability for Executing Policies and Procedures

A policy must establish clear responsibility and accountability, with clarity on the responsibilities of personnel performing the control. Policies must be deployed thoughtfully and conscientiously, and the related procedures timely performed diligently and consistently by competent personnel.

Management Specifies That Controls Must Be Performed in a Timely Manner

Management designs procedures that specify when a control and any corrective actions should be performed.

Management Ensures That Corrective Action Is Taken in Response Issues Identified

In performing a control, matters identified for follow-up should be investigated and corrective action taken if needed.

Management Ensures That Controls Are Performed by Competent Personnel

A well-designed control cannot be performed unless the entity uses competent personnel with sufficient authority.

Management Reassesses Policies and Procedures

Management periodically reassesses policies and procedures and related controls for continued relevance and effectiveness.

INFORMATION AND COMMUNICATION

Principle 13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control. There are several points of focus.

Management Identifies Information Requirements

Obtaining relevant information requires management to identify and define information requirements at the relevant level and with requisite specificity. This is an ongoing and iterative process.

Management Captures Internal and External Sources of Data

Information is received from a variety of sources and in a variety of forms, for example:

- Internal data:
  - Organizational changes
  - On-time and quality production experience
  - Actions in response to energy consumption metrics
  - Hours incurred on time-based projects
  - Units shipped in a month
  - Factors impacting customer attrition
  - Complaint on manager's behavior
- Internal data sources:
  - Email
  - Inspections of production processing
  - Committee minutes, notes
  - Personnel time reports
  - Manufacturing systems reports
  - Customer surveys
  - Whistle-blower hotline
- External data:

- Products drop-shipped
- Competitor information
- Market and industry metrics
- New or expanded requirements
- Opinions about the entity
- Customer preferences
- Claim of misuse of funds, bribery

- External data sources:
  - Data from outsourced providers
  - Industry research reports
  - Peer company earnings reports
  - Regulatory bodies
  - Social media, blogs
  - Trade shows
  - Whistle-blower hotline

Management Ensures That the Systems Processes Relevant Data into Information

Information systems capture and process large volumes of data from internal and external sources into meaningful, actionable information to meet defined information requirements.

Management Ensures That Systems Maintain Quality throughout Processing

Maintaining quality of information is necessary to an effective internal control system. The quality of information depends on whether it is:

- Accessible—easy to obtain by those who need it
- Correct—accurate and complete
- Current—most recent
- Protected—access to sensitive data restricted to authorized personnel
- Retained—properly and securely stored

- Sufficient—enough information, right level of detail, extraneous eliminated
- Timely—available when needed
- Valid—represents events that actually occurred
- Verifiable—supported by evidence from the source

Management Considers Costs and Benefits of Internal Controls

The nature, quantity, and precision of information communicated are commensurate with and support the achievement of objectives.

Principle 14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. There are several points of focus.

Management Communicates Internal Control Information

Communication of information conveyed across the entity include:

- Policies and procedures that support personnel in performing their internal control responsibilities
- Specified objectives
- Importance, relevance, and benefits of effective internal control
- Roles and responsibilities of management and other personnel in performing controls
- Expectations of the entity to communicate within the entity any significant internal control matters including weakness, deterioration, or non-adherence

Management Communicates with the Board of Directors

Communication between management and the board provides the board with information needed to exercise its oversight responsibility for internal control. Frequency and detail must be sufficient to enable the board to timely respond to indications of ineffective internal control.

Management Provides Separate Communication Lines

For information to flow up, down, and across the entity, there must be open channels of communication and a clear willingness to report and listen. In some circumstances, separate lines of communication are needed, such as whistle-blower and ethics hotlines and anonymous or confidential reporting via information systems.

Management Selects Relevant Method of Communication

Clarity of information and effectiveness with which it is communicated are important to ensure messages are received as intended. Communication can take such forms as:

- Dashboards
- Email
- Live or online training
- Memos
- One-on-one discussions
- Performance evaluations
- Policies and procedures
- Presentations
- Social media postings
- Text messages
- Webcast and other videos
- Website or collaboration site postings
- When choosing a communication medium, management considers that when messages are transmitted orally, tone of voice and nonverbal cues are very important. In addition, cultural, ethnic, and generational differences can affect how messages are received.
  - Management is aware that communications relevant to internal control may require long-term retention or employee review and acknowledgement (e.g., code of conduct, corporate security).
  - Management is aware that time-sensitive communications may be more cost-effectively delivered through informal media such as email, text messaging, or social media.
  - Management is aware that communications solely through formal means (e.g., official memos) may not reach their intended audience and may not receive return communications from those more comfortable with email, text messages, social postings, etc.

Principle 15. The organization communicates with external parties regarding matters affecting the functioning of internal control. There are several points of focus.

Management Ensures That the Level of Communication to External Parties Is Appropriate

Management develops and implements controls that facilitate external communication. Outbound communication should be viewed distinctly from external reporting. Communication to external parties allows them to readily understand events, activities, or other circumstances that may affect how they interact with the entity.

Management Enables Inbound Communications

Communications from external parties may provide important information on the functioning of the entity's internal control system. These can include:

- Outsourced independent internal control assessment
- Auditor's internal control assessment
- Customer feedback, especially complaints
- New or changed laws, regulations, etc.
- Regulatory compliance review results
- Vendor questions, especially payment complaints
- Social media postings, especially on entity-sponsored site

Management Enables Communications from External Parties to the Board of Directors

Relevant information resulting from assessments conducted by external parties is communicated to the board.

Management Provides Separate Communication Lines

Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.

Management Selects Relevant Method of Communication

The medium by which management communicates externally affects its ability to obtain information needed as well as to ensure that key messages about the entity are received and understood. It should take into account the audience, nature of the communication, timeliness, and any legal or regulatory requirements.

MONITORING

Principle 16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. There are several points of focus.

Management Considers a Mix of Ongoing and Separate Evaluations

Management selects, develops, and performs a mix of monitoring activities, usually including both ongoing and separate evaluations, to ascertain whether each of the five components of internal control is present and functioning.

Management Considers Rate of Change

Management considers the rate that an entity or its industry is expected to change. In a quickly changing industry, an entity may need more frequent separate evaluations and may reconsider its ongoing/separate mix.

Management Establishes Baseline Understanding of the System of Internal Controls

Understanding the design and current state of a system of internal control provides useful baseline information for establishing ongoing and separate evaluations. If an entity lacks a baseline understanding in higher risk areas, it may need a separate evaluation to establish the baseline for those areas.

Management Uses Knowledgeable Personnel for Monitoring Tasks

Since separate evaluations are conducted periodically by independent managers, employees, or external reviewers to provide feedback with greater objectivity, evaluators need to be knowledgeable about the entity's activities and how the monitoring activities function and understand what is being evaluated.

There are a variety of approaches available to perform separate evaluations, including the following:

- Internal audit evaluations
- Other objective evaluations
- Cross-operating unit or functional evaluations
- Benchmarking/peer evaluations
- Self-assessments

Management Integrates Ongoing Evaluations with Business Processes

Ongoing evaluations are built into the business processes and adjust to changing conditions.

Management Adjusts Scope and Frequency of Separate Evaluations Depending on Risk and Makes Objective Evaluations to Provide Good Feedback

Principle 17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate. There are several points of focus.

Management and the Board Assess Results of Monitoring Procedures

Management and the board regularly assess internal control for deficiencies; information comes from a variety of sources, including the following:

- Ongoing evaluations
- Separate evaluations
- Other internal control components
- External parties such as customers, vendors, external auditors, and regulators

Management Communicates Deficiencies in Internal Control

Communicating internal control deficiencies to the right parties to take corrective actions is critical for entities to achieve objectives. In some cases, external reporting of a deficiency may be required by laws, regulations, or standards.

Management Monitors Corrective Actions

- After internal control deficiencies are evaluated and communicated to those parties responsible for taking corrective action, management tracks whether remediation efforts are timely conducted.
- When deficiencies are not corrected on a timely basis, management revisits the selection and deployment of monitoring activities, until corrective actions have remediated the internal control deficiency.

Unit

7

Answers to Questions for Case Study Discussion

ANSWERS TO QUESTIONS FOR CASE STUDY DISCUSSION

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. 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. **The audit firm made all of the inquiries of management and the board related to fraud. In addition, they performed analytical procedures on the line items where the fictitious amounts were located and their analysis was a five-year trend comparison. No unusual fluctuations were noted. They vouched 10 of the fictitious invoices. What is the auditor's responsibility as it relates to the evaluation of fraud and what could they have done differently?**

   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. The auditor should ensure that analytical procedures are based on plausible relationships that are reasonably expected to exist. So just evaluating items that fluctuated significantly is not sufficient. Items that are expected to fluctuate but do not are also an indicator of risk. The auditor is not a document specialist and cannot be expected to pick up forgery.

   An understanding of the business purpose behind relationships is an important consideration. The auditor might have asked, "Why does an entity serve as a conduit for other service providers?" or "Has the government entity gone out to bid for significant vendors that have been serving the entity for a number of years?" There may be a good answer, but the questions

should be asked. The auditor should also consider surprise procedures. An example might be to choose a sample of vendors to examine and determine if they are registered with the secretary of state or if they have websites or street addresses that can be verified.

3. **Do you believe that a management letter comment or a communication containing a significant deficiency or material weakness should have been issued by the auditors?**

   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.

4. **Assuming that the board was sincere, what other procedures could be put in place to reduce the risk of fraud in a very small entity?**

   A possible control to mitigate the risk of improper payments is to have management and the board periodically review vendor relationships and determine if they are legitimate. Another important step would be to evaluate the price that the entity is paying for its goods/services and evaluate competitors to determine if the amounts are reasonable.

Answers to Case Study 1 Questions

1. **Name the fraud schemes perpetrated by Distefano.**

   - **Skimming or Cash Larceny—**It is 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—**She 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—**She wrote checks to herself reimbursing for supplies that she never purchased on behalf of the entity.

2. **What, if anything, do you believe that Turning Pointe did right in this case?**

   Although it took a while, a board member finally took a look 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.

3. **What are some of the fraud symptoms that might have alerted the Board of Directors to fraudulent activity?**

   - 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

4. **What controls should Turning Pointe put in place to prevent this from happening to them again?**

   - Board should review financial statements regularly and ask 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 take on 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 to actual, monitoring the compliance with the grant document, including ensuring the funds were received and deposited.

Other controls that could help prevent cash schemes in small- to midsize entities are listed in the following tables. Many, although not all the controls, would be applicable in the Turning Pointe situation.

Internal Controls That Could Help Prevent Cash Schemes (Small- to Midsize Entities)					
Control	Stealing Deposits	Stealing Cash on Hand	Skimming Part of Contribution or Sale	Kiting	Lapping
Use pre-numbered deposit slips	✓		✓		
Make all deposits intact daily	✓		✓		

Internal Controls That Could Help Prevent Cash Schemes (Small- to Midsize Entities)					
Keep un-deposited amounts in a safe	✓		✓		
Consider a lockbox for large volumes of cash receipts	✓	✓	✓		
Use multi-part 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	✓	✓			✓
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	✓		✓		✓

Internal Controls That Could Help Prevent Cash Schemes (Small- to Midsize Entities)					
Separation of Duties	Stealing Deposits	Stealing Cash on Hand	Skimming Part of Contribution or Sale	Kiting	Lapping
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	✓		✓		

Internal Controls That Could Help Prevent Cash Schemes (Small- to Midsize Entities)					
Separation of Duties	Stealing Deposits	Stealing Cash on Hand	Skimming Part of Contribution or Sale	Kiting	Lapping
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 Entities)						
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 the majority of bids	✓					
Notify vendors of conflict of interest policy	✓					
Scan general ledger for unusual levels of purchases		✓	✓	✓		
Use data extraction software to search for vendors with same addresses as employees, vendors with PO Boxes, duplicate payments		✓	✓	✓		
Use programmed controls to prevent unauthorized access to check writing and AP systems		✓	✓		✓	

Internal Controls That Could Help Prevent Fraudulent Disbursements (Small- to Midsize Entities)						
Control	Kickbacks	Fictitious or Inflated Invoices	Excess Purchasing Schemes	Duplicate Payment Schemes	Stealing Checks	Stealing Cash by Using Wire Transfers
Use pre-numbered 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/pre-numbered checks		✓				
Investigate void or reissued checks		✓				
Recompute vendor invoices for accuracy		✓				
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		✓		✓		

Internal Controls That Could Help Prevent Fraudulent Disbursements (Small- to Midsize Entities)						
Control	Kickbacks	Fictitious or Inflated Invoices	Excess Purchasing Schemes	Duplicate Payment Schemes	Stealing Checks	Stealing Cash by Using Wire Transfers
Look at returned checks or electronic bank copies to see if there is anything unusual about payee, endorsement, or authorized signature	✓					
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	✓	✓	✓	✓	✓	✓
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				✓		

Internal Controls That Could Help Prevent Fraudulent Disbursements (Small- to Midsize Entities)						
Control	Kickbacks	Fictitious or Inflated Invoices	Excess Purchasing Schemes	Duplicate Payment Schemes	Stealing Checks	Stealing Cash by Using Wire Transfers
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	✓					

Answers to Case Study 2 Questions

1. **What are the internal control deficiencies noted in this case?**

   Lack of segregation of duties is what 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 entity's responsibility to maintain the appropriate level of internal control.

2. **What might have been done to prevent this fraud from occurring?**

   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, entities should cross-train all employees in duties.

   Additional separation of duties is needed. Firms that do not separate the components in the cash, investments, and reconciliation process will face an inordinate level of risk.

   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.

Answers to Case Study 3 Questions

1. **What are the internal control deficiencies noted in this case?**

   - 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

2. **What might have been done to prevent this fraud from occurring?**

   - Segregation of duties (separate the receiving, issuing and collection of payments functions)
   - Background checks
   - Edit reports. Quarterly report of changes in an account so the relevant manager could review it for potentially fraudulent or incorrect changes
   - Check award recipients against the human resources database
   - Require supervisor approval for timesheets
   - Review phone charges carefully to determine if they are legitimate charges for the entity
   - Board monitoring
   - Stronger tone from the top and fraud awareness

Answer to Case Study 4 Question

What are some internal controls that might prevent or detect payroll fraud?

- Segregate duties—payroll preparation, disbursement, and distribution. Although the not-for-profit had good segregation of duties, this control alone is not enough.
- 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 publications available on this fraud where the debits were posted since it was not to payroll expense)

- Change passwords every 90 days

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

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

Internal Controls That Could Help Prevent Payroll Schemes (Small- to Midsize Entities)						
Control	Fictitious Employees	Inflated Payroll	Terminated Employees on Payroll	Expense Report Fraud	Stealing Checks	Payroll Tax Schemes
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	✓	✓	✓		✓	✓

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

Internal Controls That Could Help Prevent Payroll Schemes (Small- to Midsize Entities)						
Control	Fictitious Employees	Inflated Payroll	Terminated Employees on Payroll	Expense Report Fraud	Stealing Checks	Payroll Tax Schemes
accordance with expectations						

Answer to Case Study 5 Question

What could have been done to prevent or detect this fraud?

Frauds where there is collusion involved are very difficult to prevent. The 2020 *Report to the Nations* showed that 51% of the frauds in the study involved collusion. When there is collusion, the loss is greater. The study found that when there is one perpetrator (no collusion) the median loss is $90,000. This loss increases to a median loss of $105,000 when there are two perpetrators and $350,000 when there are three or more perpetrators. In this case, it is possible that a strong code of ethics and conflict of interest policy, which was signed by all employees, a strong whistle blower policy, and anonymous reporting vehicle might have caused the scheme to come to light much earlier. Electronic surveillance equipment may also have been a deterrent.

Other controls that may help to prevent or detect fraud when there is inventory present are:

- 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;
- using sequentially pre-numbered 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;
- clearing policies on the use of company assets. Management must lead the way and set the example;
- counting inventory regularly when inventory is in any way significant to the entity or either given to constituents or clients or sold; and
- reconciling inventory counts to general ledger.

Answers to Case Study 6 Questions

1. **What are the internal control deficiencies noted in this case?**

   - No verification of new vendors
   - No background check
   - Lack of whistle-blower hotline

2. **What might have been done to prevent this fraud from occurring?**

   - Perform background check for new employees with significant spending authorization authority
   - Verify new vendors to confirm they exist and are capable of providing the goods/services contracted for
   - Establish an anonymous communication channel for complaints, such as through a law firm

Answer to Case Study 7 Question

What types of controls should not-for-profits have to prevent these types of losses in the future?

- Investment committees with well thought out and prudent investment policies
- Strict due diligence guidelines for all alternative investments
- Require documentation to support the fair value of alternative investments, this may require obtaining audit reports on funds and other investments. It also may, in some instances required a valuation specialist that is independent from the investment manager.
- A collaborative board that resists group think and makes decisions based on fact rather than on the perception of a fund manager's capabilities

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®