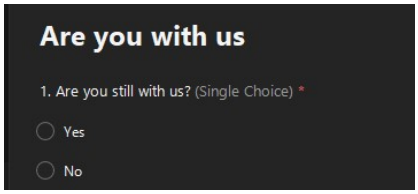
Identifying and Addressing the Risk of Fraud in Nonprofit Organizations

(IAR4)

KAPLAN

Tips for a Successful Experience

- **Technical Difficulty?** Try refreshing your page, reconnecting to the class, or rebooting (chat the moderator if you do this, so they can keep track of your presence). Also, logging in under your company's VPN may cause technical difficulty. Turn off your pop up blocker! Tech Support Team 866.265.1561 Option 1 then Option 2
- **Earning CPE:** Throughout the presentation a presence manager will pop up to check your attendance. Answer the questions with the appropriate response to record your attendance. Credit is earned by acknowledging 75% of these pop-ups per hour.



- **Chats:** You may be asked to reply to the moderator in the chat box to confirm attendance. Please be aware of any chats.
- **Questions:** Use the Chat box to ask any questions you may have about today's webcast. Someone is available to assist with your technology related concerns. The instructor will address your content related questions during the presentation or follow up after.
- **Once you are logged in please do not log out even during breaks.**

Course Topics

- Introduction
- AU-C 240 Revisited
- Characteristics of Fraud Schemes
- Case Studies: Fraud Schemes and Internal Controls

Introduction

Learning Objectives

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

Introduction

- Risk of fraud became a significant issue in the early 2000's
- Trickle down to not-for-profits
- PWC Global Economic Crime and Fraud Survey (2022) identified supply chain issues, uncertain economy, talent shortages as factors that heighten risk.
- 46% of organizations will encounter fraud.
- Remote employees- digital security.
- Lessons learned from last downturn show that the effects of a downturn take 18-24 months to materialize.

Introduction

- Association of Certified Fraud Examiners (ACFE) – fraud loss accounts for 5% of annual revenues
- Asset misappropriation -86%, fraudulent financial reporting- 9%. Remainder classified as other.
- Companies are spending more than ever to combat fraud. In 2020 companies44% of companies in the PWC survey reported that they intend to continue over the next 2 years
- Putting in additional technology controls, expanding whistle blower programs and focusing on governance and leadership.

Recent Changes to Professional Literature

1988- SAS 53, *Auditor's Responsibility to Detect and Report Errors and Irregularities*- removed the requirement to plan the audit to **search** for errors or irregularities. Plan and perform the audit to obtain reasonable assurance of identifying material errors and irregularities

1997- SAS 82- *Consideration of Fraud in a Financial Statement Audit*- changed so that auditor was responsible to plan and perform the audit to obtain reasonable assurance that the financial statements were free from material misstatement due to fraud or error. Identified fraudulent financial reporting and asset misappropriation as fraud types.

2002- SAS 99- expanded procedures to use in financial statement audit.

2011- SAS 122- clarified and codified existing standards including consideration of fraud into AU-C 240.

Recent Changes to Professional Literature

Amendments made to AU-C 240 with issuance of new standards (SAS 134-145)

SAS 134 made modifications to independent auditor's report particularly dealing with auditor's responsibilities

Reasonable assurance is a high level of assurance but is not absolute assurance and therefore is not a guarantee that an audit conducted in accordance with GAAS will always detect a material misstatement when it exists. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control. *Misstatements are considered material if there is a substantial likelihood that individually or in aggregate, they would influence the judgment made by a reasonable user based on the financial statements. In performing an audit in accordance with GAAS, we:*

Exercise ***professional judgment and maintain professional skepticism*** *throughout the audit.*

- ***Identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, and design and perform audit procedures responsive to those risks.*** *Such procedures include examining, on a test basis, evidence regarding the amounts and disclosures in the financial statements.*

Recent Changes to Professional Literature

- SAS 134 – communication of significant risks in planning. This may be done in the engagement letter, governance letter or orally.
- SAS 135, Omnibus Statement on Auditing Standards made modifications to independent auditor's report particularly dealing with auditor's responsibilities.
  - Significant unusual transactions, related parties and consideration of the risk of fraud
- SAS 143, Auditing Accounting Estimates and Related Disclosures highlights the requirement for the auditor to perform a retrospective, or hindsight, review on accounting estimates.
  - Requires that the auditor evaluate whether management's judgments and decisions in making accounting estimates indicate a possible bias
  - Indicators of possible management bias that may also be a fraud risk factor could cause the auditor to reassess whether the auditor's risk assessments, especially fraud risk assessment and related responses remain appropriate.

Types of Frauds

- Association of Certified Fraud Examiners, Joseph T Wells
- Report to the Nations 2022
- Global losses estimated at $4.5 trillion each year
- Not-for-profit organizations in study had a median loss of $60,000 and an average loss of $851,000.
- Classification includes charitable, religious, social service, educational and healthcare related not-for-profits

Cost of Fraud

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

Source: ACFE 2022 Report to the Nations

Types of Fraud

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

Source: ACFE 2022 Report to the Nations

Types of Fraud

- 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.
- These schemes result in the lowest median loss per case.
- Fraudulent financial reporting, although less prevalent, results in the highest median loss per case.
- Accurate financial reporting is very important because donors, grantors, financial institutions, and others rely on financial statements to make decisions.

Source: ACFE 2022 Report to the Nations

Types of Fraud

- Not-for-profit organizations, have fewer anti-fraud controls in place, leaving them more vulnerable to fraud.

The top organizational weaknesses identified for NFPs in the study:

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

Source: ACFE 2022 Report to the Nations

COVID-19 Issues

- COVID-19 pandemic is no longer as relevant of a factor, but it made changes to organization's way of doing business that are not likely to change.
  - Organizations still have a significant number of remote employees.
  - Organizations have embraced more complex technology to do more work remotely.
  - Electronic transmission of documents from the organization to vendors or customers, online payment capabilities and approvals within the electronic systems are just a few of the changes that organizations have made.

COVID-19 Issues

- Many U.S.-based not-for-profits have seen extraordinary increases in funding in 2020 to address the COVID-19 crisis ($11.4 billion).
- Significant amount of the funding came from the federal government in the form of the PPP loans
- Approximately 60% of not-for-profits received them
- Federal awards (including the PPP loan) related to COVID-19 amounted to $4.3 trillion.
- Most of the federal funding was awarded to large for profits and governments, but not-for-profits also benefited by the federal programs.
- In addition, approximately $20 billion in philanthropic funding by institutional grant makers and high net worth donors was given to not-for-profits.

COVID-19 Issues

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

Incentives to Commit Fraud

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

Focus on Transparency & Accountability

- Changes to Not-for-Profit Financial Statements - Accounting Standards Update (ASU) 2016-14
  - Functional Expense Presentation
  - Liquidity Information

Discussion Question 1

Which type of fraud is identified by the Association of Certified Fraud Examiners that is not identified as a fraud category in AU-C 240?

A. Asset misappropriation

B. Corruption

C. Financial statement fraud

D. All of the above

Discussion Question 1—Solution

Which type of fraud is identified by the Association of Certified Fraud Examiners that is not identified as a fraud category in AU-C 240?

A. Asset misappropriation

B. Corruption

C. Financial statement fraud

D. All of the above

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

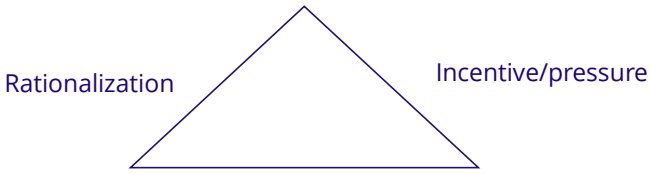
AU-C 240 Revisited

Introduction

AU-C 200 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."

Fraud Triangle

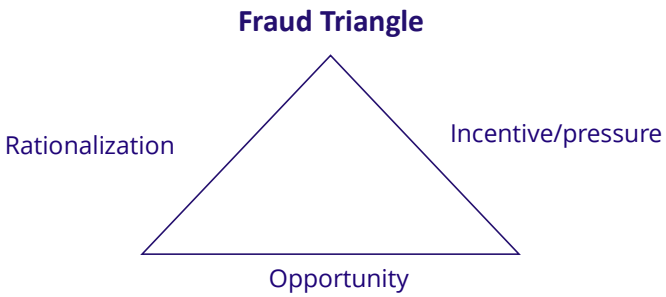


AU-C 240 Revisited

Auditor's Objectives

- Identify and assess the risks of material misstatement of the financial statements due to fraud.
- Obtain sufficient appropriate audit evidence regarding the assessed risks of material misstatement due to fraud, through designing and implementing appropriate responses.
- Respond appropriately to fraud or suspected fraud identified during the audit.
- Auditors should conduct the audit with professional skepticism.

Fraud Triangle



The **fraud triangle** actually dates back to 1974 when Donald Cressey published a hypothesis about what drives people to violate trust.

Considerations Specific to Not-for-Profits

- Yellow Book audits and Single Audits
- Change the responsibilities related to the auditor's assessment of the risk of fraud and reporting should it be identified.
- A not-for-profit organization may have certain mandates or other requirements that are applicable to those to whom it provides funding.

Conditions Specific to Smaller Organizations

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

AU-C 240 Revisited

- Understand the entity and its environment.
- Make inquiries of management and others about their views on fraud, the risks of fraud, and how they are addressed.
- Make inquiries of management and those charged with governance about related parties and significant unusual transactions.
- Consider unusual relationships identified during planning such as preliminary analytical procedures on revenue (AU-C 240 requires these procedures to be performed sometime during the audit).

AU-C 240 Revisited

- Consider fraud risk factors that correspond to the three legs of the fraud triangle: incentive/pressure, opportunity, and rationalization.
- Consider any other information gathered during the process of new client acceptance or client continuance.
- The information obtained is synthesized in a discussion with the audit team that explores how and where fraud could occur, identifies specific risks of fraud, and emphasizes professional skepticism.
- Presume that revenue recognition is a significant risk of fraud. If the auditor believes that it is not a risk of fraud, this must be justified and documented.

AU-C 240 Revisited

- Perform procedures related to management override of controls since it is deemed a risk of fraud.
- Remain alert during the audit process for circumstances that might indicate the possibility of fraud.
- Report suspicions of fraud as required by professional standards, government regulations or legal requirements.

Incentive/Pressure—Examples

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

Incentive/Pressure—Examples

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

Incentive/Pressure—Examples

The Board of Directors of a YMCA recently replaced its management team. Attendance at the center was at an all-time low and the new team was charged with getting the organization back on its feet. The new team was offered bonuses if they hit certain targets. Although the new management team worked hard to restore member confidence by investing in new equipment, improving the programming, and making improvements to the structure itself, 11 months into the year, they were still $75,000 short of meeting their financial target. The advancement director decided to go back to existing donors and ask them to extend their yearly pledges by one year. The accounting staff were instructed to reverse the remainder of the old pledges and record the new pledges at the new number of years outstanding. The advancement director felt like the whole management team had earned the bonus and should be rewarded.

Opportunity—Examples

An executive director was revered by the board of directors. She had a significant presence in the community and was the founder of the organization. She had influence not only over the board, who never questioned her actions but over the staff who did whatever she requested without question. She refused to follow internal controls over significant procurements and awarded contracts to her relatives and friends. The treasurer retired from the board and a CPA in public practice was asked to join the board in that position. After several months the treasurer brought the improper behavior with contracts and the executive director's refusal to implement recommendations by the independent auditor to the attention of the board chair, the chair told him that she would bring the situation up to the executive director. After 3 months the treasurer concluded that that board was not interested in crossing the executive director and resigned citing the lack of oversight from the board as his reason.

Opportunity—Examples

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

Opportunity—Examples

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

Rationalization—Examples

An altruistic woman who valued childhood education was concerned about the quality of education in the city's economically disadvantaged neighborhoods. She applied and was approved to start a Charter School. She appointed herself as "head of school." Since the school was a startup there were very few employees. The school depended on federal and state funding. The government funding provided the basics to the school. As an educator the head of school wanted to provide more including bus services and free meals to children who could not afford them. She intended to pay for these extra benefits through grants and contributions. Unfortunately, those funds did not materialize. When money became tight, and she could not meet payroll she used payroll withholdings to pay salaries. She also claimed to have spent grant money for equipment but used it for payroll instead. She justified her actions to herself as "for the good of the children and the school." As Head of School no one questioned her instructions.

Circumstances That Might Indicate a Risk of Fraud

- Significant transfers or transactions between funds or programs, or both, without supporting documents
- Significant budget adjustments made without approval
- Large amounts of over-or-under spending
- Grant programs with an emphasis on spending money quickly
- Complaints received from potential suppliers about questionable practices related to awarding of contracts

Circumstances That Might Indicate a Risk of Fraud

- Programs experiencing unusual growth due to conditions beyond the control of management
- Grant and donor funding conditions such as noncompliance with grant requirements, complaints from intended recipients or interest groups
- Lack of monitoring of grantee compliance with applicable law or regulation
- Client says they cannot locate documents or that the only documents they can provide are electronic or photocopied.

Circumstances That Might Indicate a Risk of Fraud

- The auditor observes that certain documents appear to have been altered. Note that the auditor should remain alert for altered documents although the auditor is not responsible for identifying whether all documents obtained from the client are authentic.
- Electronic evidence is missing or unavailable.
- The client denies the auditor access to electronic files, operations staff, or certain facilities.
- The client is slow to provide information requested by the auditor. The auditor should consider whether this is due to disorganization or limited staff.
- Information provided by operations personnel is not able to be reconciled to the general ledger.
- Confirmations returned to the auditor show discrepancies and the client is not able to provide adequate explanations.

Circumstances That Might Indicate a Risk of Fraud

- There are numerous topside adjustments to the financial statements. Note that the auditor is required to understand internal controls over journal entries, particularly those made at the end of the year and those that are not posted to the general ledger.
- Transactions are not supported by evidence and are not approved.
- Accounting estimates appear to be consistently either low or high.
- Client reconciliations contain large unsupported differences.
- Excessive write-offs of receivables or other assets.
- Internal control deficiencies ignored by the client.

Circumstances That Might Indicate a Risk of Fraud

- Employees can access systems and records that are inconsistent with their duties.
- Management tolerates or commits violations of their code of conduct.
- Answers given to the audit team in response to questions are inconsistent or implausible.
- Management gives the auditor unreasonable deadlines or fails to provide answers to complex or unusual and significant issues that arise at the end of the audit when there are tight deadlines.
- The auditor notes several changes to accounting estimates that appear unrelated to other activity in the general ledger or changes in circumstances.
- Client has implausible reasons for fluctuations or other issues noted in the auditor's analytical review procedures.

Revenue Recognition—Presumed to be a Fraud Risk

- AU-C 240 presumes that fraudulent financial reporting due to inappropriate revenue recognition is a risk of fraud.
  - moving revenue from the current period to a later period
  - recording fictitious revenue
  - misclassification of revenue in the wrong net asset class.
- This presumption can be rebutted by the auditor.
- However, the auditor should have a compelling reason and thoroughly document the circumstances.
- Not all sources of revenue may have a risk of fraud.

Revenue Recognition—Presumed to be a Fraud Risk

EXAMPLE

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

- Revenue recognition as a risk of fraud should be treated as a significant risk.
- Auditor should obtain an understanding of the organization's controls, including the control activities, related to the risk.
- The auditor should evaluate whether those controls have been suitably designed and implemented to mitigate the fraud risks.

Inquiries of Management, Governance, and Others

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

Inquiries of Management

- Whether management has knowledge of any fraud or suspected fraud affecting the organization.
- Whether management is aware of allegations of fraud or suspected fraud affecting the organization; for example, received in communications from employees, former employees, analysts, regulators, or others.
- The extent of management's understanding about the risks of fraud in the organization, including any specific fraud risks the organization has identified or account balances or classes of transactions for which a risk of fraud may be likely to exist.
- The existence of programs and controls the organization has established to mitigate specific fraud risks the organization has identified or that otherwise help to prevent, deter, and detect fraud, and how management monitors those programs and controls.

Inquiries of Management

- The nature and extent to which organizations with multiple locations monitor them and whether there are operating locations for which the risk of fraud may be more likely to exist.
- Whether and how management communicates to employees its views on business practices and ethical behavior.
- Whether and how management has reported to the audit committee or others with equivalent authority and responsibility on how the organization's internal control serves to prevent, deter, or detect material misstatements due to fraud.
- Whether the organization has entered into any significant unusual transactions and, if so, the nature, terms, and business purpose (or the lack thereof) of those transactions and whether such transactions involved related parties.

Inquiries of Governance

- Its views on fraud and whether or how it exercises oversight.
- Whether the members have any knowledge of fraud that has occurred.
- Where and how fraud might occur.
- Whether the organization has entered into any significant unusual transactions and, if so, the nature, terms, and business purpose (or the lack thereof) of those transactions and whether such transactions involved related parties.

Inquiries of Others

- Their views about the risk of fraud and how it might occur.
- Whether they have seen or suspected fraud.
- If internal auditors, whether they have performed any procedures to detect fraud and if there were findings, how management responded.

Significant Unusual Transactions

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

Significant Unusual Transactions—Example

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

Significant Unusual Transactions—Example

The auditor of a not-for-profit health research collaborative was aware that the consolidated entity included 4 organizations that were headquartered overseas. During the year there were wire transfers from the reporting entity to the overseas organizations and vice versa. There were also wires between the overseas organizations. The documentation for the wires stated that the transfers were related to payment of expenses paid by one entity on another's behalf. In addition, the intercompany accounts did not reconcile. The auditor was aware that the research was performed related to health disparities in developing countries. However, there did not appear to be a good business rationale for the transfers. This was deemed to be a significant unusual transaction.

Significant Unusual Transactions

- SAS 135 requires the auditor to make additional inquiries of management about whether the organization has entered into any significant unusual transactions
- If there are- the nature, terms, and business purpose (or the lack thereof) of those transactions and whether such transactions involved related parties.
- Indicators that may suggest that significant unusual transactions may have been entered into to engage in fraudulent financial reporting or to conceal misappropriation of assets include:
    - Form of such transactions appears overly complex (for example, the transaction involves multiple organizations within a consolidated group or multiple unrelated third parties).
    - Management has not discussed the nature of and accounting for such transactions with those charged with governance of the organization, and inadequate documentation exists

Significant Unusual Transactions

Indicators that may suggest that significant unusual transactions have a fraudulent purpose (con't)

- Management is placing more emphasis on the need for a particular accounting treatment than on the economic substance of the transaction.
- Transactions involve nonconsolidated related parties, including special purpose organizations, have not been properly reviewed or approved by those charged with governance.
- Transactions involve related parties or relationships or transactions with related parties previously undisclosed to the auditor.
- Transactions involve other parties that do not have the financial strength to support the transaction without assistance from the organization under audit or any related party.

Significant Unusual Transactions

Indicators that may suggest that significant unusual transactions have a fraudulent purpose (con't)

- Transactions lack commercial or economic substance or are part of a larger series of transactions. For example, a transaction that is entered into shortly prior to period end and is unwound shortly after period end.
- Transactions occur with a party that falls outside the definition of a related party with one party able to negotiate terms that may not be available for other, more clearly independent parties on an arm's-length basis.
- Transactions exist to enable the organization to achieve certain financial targets.

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

Significant Unusual Transactions—Example

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

Significant Unusual Transactions—New Procedures

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

Remote Audits and Electronic Communication

- Remote audits appear to have increased the tendency that has been growing in audits to move away from face-to-face conversations with client personnel and governance
- Information and impressions that can be gained by a face-to-face conversation are lost.
- The AICPA strongly encourages auditors to use face-to-face conversations and if that is not feasible to use technology such as Zoom or Teams to conduct conversations.
- Clients with locations throughout the country.
- Electronic surveys may be helpful

AU-C 240 Revisited

Integrating AU-C 240 and 315 Inquiries

EXAMPLE:

- Market and competition
- Accounting principles and industry
- New projects
- General level of economic activity
- Compliance with Laws & Regs
- Significant Unusual Transactions and whether they involve Related Parties
- Interest rates and availability of financing
- Impact of factors on funding sources
- Impact on demand for services
- Preliminary analytical procedures

AU-C 240 Revisited

Integrating AU-C 240 and 315 Inquiries – Open-ended Questions

- 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?

AU-C 240 Revisited

Integrating AU-C 240 and 315 Inquiries – Open-ended Questions

- 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 …

Making Inquiries of Employees—Example

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

Anti-Fraud Questionnaire

Anti-Fraud Provision	Question
Training	Do employees receive training that helps to educate them about: • What constitutes fraud? • Have costs of fraud such as job loss, publicity issues, etc., been discussed with employees? • Have employees been told where to go for help if they see something? • Is there a zero-tolerance policy for fraud and has it been communicated?
Reporting	Does the organization have an effective way for employees to report fraud? • Are there anonymous reporting mechanisms? • Do employees understand that those issues reported will be investigated?
Perception of Detection	Does the organization seek knowledge of fraudulent activity? • Does management send a message that there will be tests made to look for fraud? • Are there surprise audits? • Is software used to identify issues from data?
Management's Tone from the Top	• Does the organization value honesty and integrity? • Are employees surveyed to determine whether they believe that management acts with integrity? • Have fraud prevention goals been set for management and are they evaluated on them as an element of compensation? • Is there an appropriate oversight process by the board or others charged with governance?

Anti-Fraud Questionnaire

Anti-Fraud Provision	Question
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—Team Meeting

- Auditor assesses risk at the overall account level and by account balance /class of transaction and assertion.
- Auditors will identify where they believe there is significant risk and design audit procedures to be responsive to those risks.
- Note that all “fraud” risks are also “significant” risks; however, not all “significant” risks are “fraud” risks.
- Known external and internal factors affecting the organization that may create incentive or pressure for management or others to commit fraud
- Internal factors that provide the opportunity for fraud to be perpetrated
- Likelihood of a culture or environment at the client that enables management or others to rationalize committing fraud

Synthesizing the Information Obtained—Team Meeting

- Risks of management override include:
  - Recording fictitious journal entries,
  - Intentionally biasing assumptions and judgments in management’s estimates, and
  - Altering records and terms of significant or unusual transactions
- Consideration of circumstances that might be indicative of revenue or expense management or manipulation of other financial measures and the practices that might be followed by management committing fraudulent financial reporting
- How the audit team might respond to the susceptibility of the organization's financial statements to material misstatement due to fraud.

Synthesizing the Information Obtained—Team Meeting

Consider areas where there may have been significant changes in risks, including:

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

Synthesizing the Information Obtained—Team Meeting

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
6. Financial issues due to COVID-19 may have been partially or fully mitigated by federal and state funding.
   - An important issue may be what happens now that there is less funding available if the organization has not recovered to its pre-pandemic levels and is unable to meet its obligations

If other risks surface during the engagement the risk assessment should be revised, and communication take place in the audit team.

Assessing Fraud Risk

- Narrow down to risks that could have the risk of **material** misstatement and a likelihood of occurring.
- Consider internal controls that could mitigate the risk of fraud either at the company or transaction level (or both) should be considered.
- 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.

Assessing Fraud Risk—Example

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

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

*** Bold items are either a required fraud risk of presumed to be a fraud risk

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 should also specifically link audit procedures to the risks identified by altering the nature, timing, and extent of procedures to be performed.

Addressing the Risk of Fraud—Example

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

Management Override—Journal Entries

- Manipulation of the financial reporting process may occur if personnel record unauthorized or inappropriate journal entries. This may occur manually or within the computerized information system.
- Even if specific risks of material misstatement due to fraud are not identified by the auditor, there is always the possibility that management override of controls could occur.
- Auditor is required to design and perform procedures to test the journal entries recorded in the general ledger and other adjustments made in the preparation of the financial statements, including entries posted directly to financial statement drafts.
- Auditor may want to also understand and perform procedures on other journal entries made throughout the reporting period.

Management Override—Journal Entries

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

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

Management Override—Journal Entries

- When testing journal entries, it is important to document the entries tested. Some possible attributes for testing might be:
  - Entry was approved by someone with the appropriate level of authority
  - Entry was for a bona fide business purpose
  - Entry appeared to have no bias
  - Entry had the appropriate level of supporting documentation
  - Entry did not give the appearance of fraud

Accounting Estimates

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

Related Parties

- AU-C 240 requires the auditor to obtain an understanding of the entity's related party relationships and transactions.
- Fraud may be more easily committed through related parties.
- The auditor should make inquiries of management and others within the organization as follows:
  - The identity of the organization's related parties, including changes from the prior period
  - The nature of the relationships between the organization and these related parties
  - The business purpose of a related party transaction versus an unrelated party
  - If the organization entered into, modified, or terminated any transactions with related parties during the period and the type and business purpose of the transactions

Related Parties

Indicators of dominant influence exerted by a related party include the following:

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

Related Parties—Example

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

Related Party Transactions

- SAS 135 requires the auditor to make the following inquiries about:
  - identity of the entity's related parties, including changes from the prior period
  - nature of the relationships (including ownership structure) between the entity and these related parties
  - business purpose of conducting a transaction with a related party versus an unrelated party

Related Party Transactions

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

Related Party Transactions—Example

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

Related Party Transactions

- When the auditor encounters related party transactions, they should evaluate the transaction considering their understanding of the organization and its environment
- Consider other information obtained during the audit, whether the business purpose of significant unusual transactions suggests that they were undertaken for purposes of fraudulent financial reporting or to conceal misappropriation of assets.
- The auditor should consider performing the following:
  - Read the underlying documentation and evaluate whether the terms and other information about the transaction are consistent with explanations from inquiries and other audit evidence about the business purpose of the transaction.
  - Determine whether the transaction has been authorized and approved in accordance with the organization's established policies and procedures
  - Evaluate whether significant unusual transactions with related parties have been properly accounted for and disclosed in the financial statements

Discussion Question 2

The auditor is required to perform procedures related to management override of controls. Which of the following is true?

A. Auditors can rebut the presumption that management override is a risk of fraud

B. The auditor should test 10 percent of the client's journal entries

C. The auditor is required to test the appropriateness of journal entries at the end of the period and in the financial reporting process and consider testing those throughout the period.

D. The auditor is required to test one of each type of journal entry

Discussion Question 2—Solution

The auditor is required to perform procedures related to management override of controls. Which of the following is true?

A. Auditors can rebut the presumption that management override is a risk of fraud

B. The auditor should test 10 percent of the client's journal entries

C. The auditor is required to test the appropriateness of journal entries at the end of the period and in the financial reporting process and consider testing those throughout the period.

D. The auditor is required to test one of each type of journal entry

Responding to Suspected Fraud

- Bring this to the attention of management so it can be investigated- in a timely manner.
- If the auditor has identified or suspects fraud involving management, employees who have significant roles in internal control, or material misstatement in the financial statements the auditor should communicate these matters to those charged with governance on a timely basis.
- If the auditor suspects fraud involving management, the auditor should communicate these suspicions to those charged with governance and discuss with them the nature, timing, and extent of audit procedures necessary to complete the audit.
- Auditor should communicate with those charged with governance any other matters related to fraud that are, in the auditor's professional judgment, relevant to their responsibilities.

Near the End of the Audit

- Auditor should look at the accumulated results of auditing procedures, including the final analytical review, to determine if any evidence came to light that would affect the assessment of the risks of material misstatement due to fraud made earlier in the audit or indicate might a previously unrecognized risk of material misstatement due to fraud.
- If analytical procedures related to revenue have not been performed along with the final analytical review, they should be performed at this time so see if any previous conclusions related to revenue recognition appear appropriate.
- Auditor should also evaluate any misstatements noted during the audit where adjustments were proposed by the auditor for the risk of fraud.
- Auditor should consider how these misstatements might impact the audit, specifically in the areas of materiality, management and employee integrity, and the reliability of management representations. Instances of fraud are unlikely to be an isolated occurrence.

Reevaluate the Risk Assessment

- If suspected fraud is noted the auditor should reevaluate the previous risk assessment considering whether circumstances or conditions indicate possible collusion involving employees, management, or third parties.
- This may impact the reliability of evidence and the auditor may find it is appropriate to perform additional work.
- If the auditor concludes that, or is unable to conclude whether, the financial statements are materially misstated because of fraud, the auditor should evaluate the implications for the audit.
- If the auditor believes they should not continue performing the audit, they should:
    - Determine the professional and legal responsibilities
    - Determine if a requirement exists for the auditor to report to regulatory authorities
    - Consider whether withdrawal is possible under applicable law or regulation

Reevaluate the Risk Assessment

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

Discussion Question 3

Which audit area is required to be tested analytically when evaluating the risk of fraud?

A. Revenues

B. Management override

C. Related party transactions

D. Operating expenses

Discussion Question 3—Solution

Which audit area is required to be tested analytically when evaluating the risk of fraud?

A. Revenue

B. Management override

C. Related party transactions

D. Operating expenses

Communication to Management, Governance, Regulators, and Enforcement Authorities

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

Government Auditing Standards and Single Audit

- Many not-for-profits have financial statement audits under GAS (Yellow Book) or Single Audits
- Additional requirements
- If the auditor has identified or suspects a fraud, it may be necessary to report to a party outside the organization. This overrides confidentiality standards.
- The Yellow Book requires the auditor to issue a report on internal control and compliance with provisions of laws and regulations.
- The internal control report identifies material weaknesses and significant deficiencies as noted above.
- The compliance report identifies instances of noncompliance with provisions of laws and regulations, contracts, and grant agreements.

Government Auditing Standards and Single Audit

- Auditors should include the relevant information about noncompliance and fraud when:
  - noncompliance with provisions of laws, regulations, contracts, or grant agreements that has a material effect on the financial statements
  - fraud that is material, either quantitatively or qualitatively, to the financial statements
- Effect on the financial statements is less than material but warrants the attention of those charged with governance or the auditor has obtained evidence of suspected fraud that is less than material but warrant the attention of those charged with governance.
- This is reported to audited entity officials in writing and may be in a separate communication.

Government Auditing Standards and Single Audit

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

Government Auditing Standards and Single Audit

- Auditors should report identified or suspected noncompliance with provisions of laws, regulations, contracts, and grant agreements and instances of fraud directly to parties outside the audited entity when either of these situations are present:
    - Audited entity management fails to satisfy legal or regulatory requirements to report the information to external parties specified in law or regulation.
    - Auditors should first report management's failure to take timely and appropriate steps to those charged with governance.
        - If the audited entity still does not take timely and appropriate steps as soon as practicable then the auditors should report the audited entity's failure to take timely and appropriate steps directly to the funding agency.

Documentation

- Understanding of organization and environment and the assessment of the risks of material misstatement including fraud
- Significant decisions reached during the discussion among the engagement team regarding the susceptibility of the F/S to fraud
- The assessed risks of material misstatement due to fraud at the financial statement level and at the assertion level
- Audit responses to the assessed risks of material misstatement

Documentation

- Overall responses and the linkage of procedures with assessed risks of material misstatement due to fraud by assertion
- Results of the audit procedures, including those designed to address the risk of management override of controls
- Any communications about fraud made to management, those charged with governance, regulators, and others.
- If the auditor has concluded that the presumption that there is a risk of material misstatement due to fraud related to revenue recognition is overcome in the circumstances of the engagement, the auditor should discuss the reasons for that conclusion.

Use of Practice Aids

- The consideration of fraud is very important.
- Auditor is not performing the audit to search for fraud.
- When fraud occurs and the appropriate procedures, according to professional guidance were not performed, then the auditor comes under more scrutiny.
- Practice aids are important, but the auditor will want to ensure that they perform all the procedures prescribed in AU-C 240.
- Example completed practice aid in manual

Discussion Question 4

What is one way to ensure that the auditor performs all of the appropriate procedures in considering fraud?

A. Using commercial practice aids

B. Perform all the prescribed procedures in AU-C 240, *Consideration of Fraud in a Financial Statement Audit*

C. Prescribed procedures by the Association of Certified Fraud Examiners (ACFE)

D. None of the above

Discussion Question 4—Solution

What is one way to ensure that the auditor performs all of the appropriate procedures in considering fraud?

A. Using commercial practice aids

B. Perform all the prescribed procedures in AU-C 240, *Consideration of Fraud in a Financial Statement Audit*

C. Prescribed procedures by the Association of Certified Fraud Examiners (ACFE)

D. None of the above

Common Characteristics of Fraud Schemes

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.
- Identify components of an organization's system of internal control that support the its ability to prevent and detect fraud.

Pressure on NFPs to Strengthen Controls

Good Governance Principles

- Independent Sector—33 principles for transparency and accountability—4 categories
    - Legal Compliance and Public Disclosure
    - Effective Governance
    - Strong Financial Oversight
    - Responsible Fundraising

Pressure on NFPs to Strengthen Controls

Characteristics of Fraud Schemes

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

Source: ACFE 2022 Report to the Nations

Fraudulent Financial Reporting Schemes

- Fraudulent financial reporting scheme resulted in a median loss of $593,000, which is significantly higher than the other categories.
- The most prevalent ways that fraudulent financial reporting occurs is:
    - Timing differences
    - Fictitious revenue
    - Concealed liabilities/expenses
    - Improper valuation
    - Improper disclosure

Asset Misappropriation Schemes

- Median Asset Appropriation Scheme—$100,000

Scheme	Description	Median Loss
Billing	A disbursement scheme in which a person causes an organization to issue a payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases.	$100,000
Noncash misappropriation	An employee steals or misuses noncash assets of the organization.	$78,000
Expense reimbursement	A disbursement scheme in which an employee makes a claim for reimbursement for fictitious expenses or inflated expenses.	$40,000
Skimming	A scheme in which cash is stolen before it is recorded in the books and records of the organization.	$50,000
Cash on hand misappropriation	A scheme in which an employee steals cash kept on hand at the organization.	$15,000
Check or payment tampering	A disbursement scheme in which an employee steals the organization's funds by intercepting, forging, or altering a check or electronic payment drawn on one of the organization's bank accounts.	$100,000

Source: ACFE 2022 Report to the Nations

Asset Misappropriation Schemes

Scheme	Description	Median Loss
Payroll scheme	A disbursement scheme in which an employee causes his employing organization to issue a payment for an improper amount or for a fictitious employee.	$45,000
Cash larceny	A scheme in which cash receipts are stolen after they have been recorded in the books and records (cash is recorded but the checks are stolen before they go to the bank).	$50,000
Register disbursements	A disbursement scheme in which an employee makes incorrect entries on a cash register to hide the removal of cash.	$10,000

Source: ACFE 2022 Report to the Nations

Corruption and Collusion

Corruption may take the form of:

- conflicts of interest
- purchasing schemes
- sales schemes, bribery
- kickbacks
- bid rigging
- illegal gratuities

Approximately 35% of perpetrators committed more than one type of fraud

Combination of Schemes

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

Source: ACFE 2022 Report to the Nations

Duration of Fraud Schemes

Scheme	Duration of Scheme Before Identification (months)
Payroll	18
Check tampering	18
Financial statement fraud	18
Expense reimbursement	18
Billing	18
Cash Larceny	14
Corruption	12
Cash on hand	12
Noncash	12
Register disbursements	12

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

Source: ACFE 2022 Report to the Nations

Collusion

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

Source: ACFE 2022 Report to the Nations

Concealment of Fraud

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

Source: ACFE 2022 Report to the Nations

Behavioral Red Flags

Red Flag	Percentage
Living beyond means	39%
Financial difficulties	25%
Unusually close association with vendor or customer	20%
No behavioral red flags	15%
Control issues, unwilling to share duties	13%
Irritability, suspiciousness, or defensiveness	12%
Bullying or intimidation	12%

Source: ACFE 2022 Report to the Nations

Behavioral Red Flags

Red Flag	Percentage
Divorce/ family problems	11%
"Wheeler-dealer" attitude	10%
Excessive pressure from within the organization	8%
Addiction problems	7%
Complaints about inadequate pay	7%
Refusal to take vacations	7%
Social isolation	6%

Source: ACFE 2022 Report to the Nations

Behavioral Red Flags

Red Flag	Percentage
Past legal problems	5%
Complaints about lack of authority	5%
Other employment related problems	4%
Excessive family/peer pressure for success	4%
Excessive tardiness or absenteeism	3%
Instability in life circumstances	4%
Excessive internet browsing	2%

Source: ACFE 2022 Report to the Nations

HR Red Flags

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

Source: ACFE 2022 Report to the Nations

The Report to the Nations indicated that 50% of perpetrators exhibited at least one HR-related red flag prior to or during the time of their frauds.

Pressure on NFPs to Strengthen Controls

COSO Framework

- Control environment
- Risk assessment

} Primarily indirect

- Control activities
- Information and communication

} Primarily direct (application information controls may be primarily direct

- Monitoring

} Primarily indirect

SAS 145 identifies controls as either primarily indirect or primarily direct.

Corporate Failures

- International Federation of Accountants and the Chartered Institute of Management Accountants performed an analysis of large corporate failures.
- Study found that the failure of the primarily indirect controls was the main cause of the large frauds
  - lack of ethics
  - weak board
  - lack of a compliance/risk management function
  - role of the CEO

Weaknesses in Internal Control

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

Source: ACFE 2022 Report to the Nations

Discussion Question 5

A disbursement scheme where a person causes an organization to issue a payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases is called_____.

A. Payroll scheme

B. Kiting

C. Lapping

D. Billing scheme

Discussion Question 5—Solution

A disbursement scheme where a person causes an organization to issue a payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases is called_____.

A. Payroll scheme

B. Kiting

C. Lapping

D. Billing scheme

Fraud Case—Executive Director Embezzles Funds

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

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

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

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

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

Collusion Results in $250 Million in Federal Award Fraud

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

Federal authorities charged 47 people with conspiracy in one of the largest fraud scheme to take advantage of the COVID-19 pandemic by stealing $250 million from a federal program that provides meals to low-income children. **Feeding Our Future** (FOF) created other organizations that claimed to be offering food to tens of thousands of children across Minnesota, submitting requests for reimbursement for those meals through the child nutrition programs. Few meals were really served. The perpetrators used the money to buy luxury cars, property, and jewelry. The organization's founder and executive director was indicted although she claimed to have no knowledge of the fraud. Investigators stated that she and others in her organization submitted fraudulent claims for reimbursement and received kickbacks.

Government was billed for more than 125 million fake meals, with some defendants making up names for children by using an online random name generator. One reimbursement claimed a site served exactly 2,500 meals each day M-F. During that time no children were ever reported as sick or were otherwise missing from the program. Government has so far recovered $50 million in money and property and expects to recover more. As a sponsoring agency FOF retains 10 percent to 15 percent of the reimbursement funds as an administrative fee in exchange for submitting claims, sponsoring sites, and disbursing the funds.

During the pandemic, the USDA allowed for-profit restaurants to participate and allowed food to be distributed outside educational programs. Perpetrators exploited these rule changes for personal gain. FOF sponsored the opening of nearly 200 federal child nutrition program sites. Court documents described a small storefront restaurant that typically served only a few dozen people a day. Two defendants offered the owner $40,000 a month to use his restaurant, then billed the government for 1.6 million meals through 11 months of 2021, listing the names of around 2,000 children — nearly half of the local school district's total enrollment. Only 33 names matched actual students. FOF received nearly $18 million in program funds as administrative fees in 2021 alone, and the ED and others received additional kickbacks, disguised as "consulting fees" paid to shell companies.

Primarily Indirect Controls—Control Environment

- **Control Environment-** Organization level commitment to integrity and ethical values, independence, and oversight of internal control by the board of directors, and organization level commitment to attract and retain competent staff.
- Reporting Mechanisms- 2022 *Report to the Nations* identifies formal reporting mechanisms as a technique that can have a substantial impact on reporting.

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

Source: ACFE 2022 Report to the Nations

Primarily Indirect Controls—Reporting Mechanism

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

Source: ACFE 2022 Report to the Nations

Primarily Indirect Controls—Reporting Mechanism

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

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

Source: ACFE 2022 Report to the Nations

Reporting Suspicions of Fraud

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

Source: ACFE 2022 Report to the Nations

Primarily Indirect Controls

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

Source: ACFE 2022 Report to the Nations

Fraud Is Not Always Reported

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%

Source: ACFE 2022 Report to the Nations

Anti-Fraud Controls

Anti-fraud control	Percentage implemented	COSO Category
External audit (note that the external audit is not a control even though it is listed in the ACFE survey.	82%	NA
Code of Conduct	82%	Control Environment
Internal audit department (if the internal auditors focus on the area of financial reporting)	77%	Monitoring
Management Certification of Financial Statements	74%	Monitoring
External audit of internal controls over financial reporting (if performed as a control and not a required integrated audit)	71%	Monitoring
Hotline	70%	Control Environment

Source: ACFE 2022 Report to the Nations

Anti-Fraud Controls

Anti-fraud control	Percentage implemented	COSO Category
Management review (could be monitoring if management is reviewing internal control effectiveness. Or could be a control activity.	69%	Monitoring or Control Activity
Independent audit committee	67%	Control environment
Fraud training for employees	61%	Control environment
Anti-fraud policy	60%	Control environment
Fraud training for management and executives	59%	Control environment
Employee support programs	56%	Control environment

Source: ACFE 2022 Report to the Nations

Anti-Fraud Controls

Anti-fraud control	Percentage implemented	COSO Category
Dedicated fraud department, function, or team	48%	Control environment/ monitoring
Formal fraud risk assessment	46%	Risk assessment
Proactive data monitoring/analysis	45%	Control activity
Surprise audits	42%	Monitoring
Job rotation/mandatory vacation	25%	Control environment
Rewards for whistle blowers	15%	Control environment

Source: ACFE 2022 Report to the Nations

Increase in Implementation of Anti-Fraud Controls

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

Source: ACFE 2022 Report to the Nations

Risk Assessment

- Covers 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- **The organization considers the potential for fraud in assessing risks to the achievement of objectives.**
- Management and the board should consider the potential for fraud in financial reporting, non-financial reporting, misappropriation, and illegal acts.
- Lack of segregation of duties, management bias, estimates, common frauds in their industry, geographic regions, incentives, IT, complex or unusual transactions, and management override.
- Fraud risk assessment should identify where the organization is vulnerable to fraud.

Risk Assessment—Example

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

Information and Communication

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

Monitoring

- Monitoring is where management and the board evaluate the quality of the organization's internal control including anti-fraud controls. Examples:
  - Board receives and reviews periodic reports describing the nature, status, and disposition of alleged or suspected fraud and misconduct
  - An internal audit plan 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
  - 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

Primarily Direct Controls—Control Activities

- Management evaluates a mix of control activity types to prevent, detect and correct the risk of error and fraud.
  - Authorizations and approvals
  - Verifications
  - Physical controls
  - Controls over standing data (e.g., master files)
  - Reconciliations
  - Supervisory controls
  - Mix of preventive and detective controls

Primarily Direct Controls—Control Activities

- Management addresses segregation of duties
- Management designs procedures that specify when a control and any corrective actions should be performed to help ensure that controls are executed in a timely manner.
- Management ensures that corrective action is taken in response to issues identified.
- Matters identified for follow-up should be investigated and corrective action taken if needed.
- In performing a control, management evaluates the competency of personnel performing the control.
- Management periodically reassesses policies and procedures and related controls for continued relevance and effectiveness.

Discussion Question 6

The most prevalent reason that organizations do not report fraud is:

A. Fear of bad publicity

B. Too costly

C. Internal discipline is sufficient

D. Private settlement with perpetrator

Discussion Question 6—Solution

The most prevalent reason that organizations do not report fraud is:

A. Fear of bad publicity

B. Too costly

C. Internal discipline is sufficient

D. Private settlement with perpetrator

Cyber Threats

- According to Venable, a national law firm, cybercrimes affect approximately 1 million victims daily and cost over $450 billion a year globally
- Ransomware is the fastest growing type of cybercrime
- Cyber incidents are becoming more sophisticated and targeted as criminals seek higher rewards with extortion demand
- Three main causes of data breach:
  - Malicious attack (52%)
  - System glitch (25%)
  - Human error (23%)

Cyber Risks

- *Managing Cyber Risks in a Digital Age*, COSO in collaboration with Deloitte
- The guidance provides insight into how not-for-profit organizations can leverage the five components and 20 principles of the ERM Framework to identify and manage cyber risks.
- Not-for-profit organizations should consider its need for insurance.
- Incident response plan to help contain any breach that occurs.
- Evaluate the entity's firewalls and spam filtering system.
- Operating system updates
- Intrusion prevention and detection software could be used in addition to next-generation anti-virus/anti-malware software.
- 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 risks of cyberfraud.

Cyber Threats

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.

Increased Threats Caused by COVID-19

- COVID-19 pandemic has had an incredible impact on the way many not-for-profit entities operate
- Seventy-six percent of organizations that participated in a Ponemon Institute study indicated that remote work made responding to a potential data breach a much more difficult ordeal
- Remote work during the COVID-19 pandemic:
  - Increases the time to identify and contain a potential data breach
  - Increases the total average cost of a data breach by nearly $137,000

Cyber Frauds

- AICPA Identified Top Cybercrimes
- Corporate account takeover
- Identity theft
- Theft of sensitive data
- Theft of intellectual property

Discussion Question—7

How is fraud most likely to be detected in an organization?

A. External audits

B. Internal control structure

C. Tips from employees and others

D. Internal audits

Discussion Question 7—Solution

How is fraud most likely to be detected in an organization?

A. External audits

B. Internal control structure

C. Tips from employees and others

D. Internal audits

Fraud Schemes and Controls

Anti-Fraud Controls Reduce Time to Detect

Anti-Fraud Control	Percentage of cases	Percentage reduction in loss if control is in place	Difference in time to detect when control is implemented
External audit of financial statements*	82%	33%	18 mos. to 12 mos.
Code of conduct	82%	40%	18 mos. to 12 mos.
Management certification of financial statements	74%	29%	18 mos. to 12 mos.
Management review	69%	33%	18 mos. to 12 mos.

Source: ACFE 2022 Report to the Nations

Anti-Fraud Controls Reduce Time to Detect

Anti-Fraud Control	Percentage of cases	Percentage reduction in loss if control is in place	Difference in time to detect when control is implemented
External audit of internal control over financial reporting	71%	33%	18 mos. to 12 mos.
Internal audit department	77%	33%	18 mos. to 12 mos.
Employee support programs	56%	25%	No change
Independent audit committee	25%	54%	18 mos. to 12 mos.
Hotline	70%	50%	18 mos. to 12 mos.

Source: ACFE 2022 Report to the Nations

Anti-Fraud Controls Reduce Time to Detect

Anti-Fraud Control	Percentage of cases	Percentage reduction in loss if control is in place	Difference in time to detect when control is implemented
Anti-fraud policy	60%	45%	18 mos. to 12 mos.
Fraud training for employees	61%	45%	18 mos. to 12 mos.
Fraud training for managers/executives	59%	39%	18 mos. to 12 mos.
Proactive data monitoring/analysis	45%	47%	18 mos. to 8 mos.

Source: ACFE 2022 Report to the Nations

Anti-Fraud Controls Reduce Time to Detect

Anti-Fraud Control	Percentage of cases	Percentage reduction in loss if control is in place	Difference in time to detect when control is implemented
Surprise audit	42%	50%	18 mos. to 9 mos.
Dedicated fraud department or team	48%	33%	18 mos. to 10 mos.
Formal fraud risk assessment	46%	45%	18 mos. to 10 mos.
Job rotation/mandatory vacation	25%	54%	16 mos. to 8 mos.
Rewards for whistleblowers	15%	5%	13 mos. to 8 mos.

Source: ACFE 2022 Report to the Nations

Frauds Committed in Smaller vs. Larger Organizations

- Smaller organizations experience fraud in different ways than larger ones.
- Smaller organizations are defined as those with less than 100 employees.
- Larger ones have 100 or more employees.
- Fraudulent financial reporting occurred in 5 percent of smaller organizations and 10% of larger ones.
- Corruption occurred in 24% of smaller organizations and 54% of larger ones.

Frauds Committed in Smaller vs. Larger Organizations

Scheme	Description	Median Loss (all organizations)	% Smaller organizations	% Larger organizations
Billing	A disbursement scheme in which a person causes an organization to issue a payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases.	$100,000	13%	19%
Expense reimbursement	A disbursement scheme in which an employee makes a claim for reimbursement for fictitious expenses or inflated expenses.	$40,000	7%	11%
Skimming	A scheme in which cash is stolen before it is recorded in the books and records of the organization.	$50,000	9%	8%

Source: ACFE 2022 Report to the Nations

Frauds Committed in Smaller vs. Larger Organizations

Scheme	Description	Median Loss (all organizations)	% Smaller organizations	% Larger organizations
Check or payment tampering	A disbursement scheme in which an employee steals the organization's funds by intercepting, forging, or altering a check or electronic payment drawn on one of the organization's bank accounts.	$100,000	10%	8%
Payroll scheme	A disbursement scheme in which an employee causes his employing organization to issue a payment for an improper amount or for a fictitious employee.	$45,000	8%	8%
Cash larceny	A scheme in which cash receipts are stolen after they have been recorded in the books and records (cash is recorded but the checks are stolen before they go to the bank).	$50,000	7%	7%

Source: ACFE 2022 Report to the Nations

Frauds Committed in Smaller vs. Larger Organizations

Scheme	Description	Median Loss (all organizations)	% Smaller organizations	% Larger organizations
Register disbursements	A disbursement scheme in which an employee makes incorrect entries on a cash register to hide the removal of cash.	$10,000	1%	3%
Cash on hand misappropriation	A scheme in which an employee steals cash kept on hand at the organization.	$15,000	7%	9%
Noncash	Scheme where noncash assets such as equipment and supplies are stolen	$78,000	9%	19%

Source: ACFE 2022 Report to the Nations

Case Study 1—Billing Schemes: Juvenile Justice Organization Defrauded of $1.8 Million

A small juvenile justice organization was short staffed. One woman, who held the position of Secretary to the Board, had the ability to initiate transactions, process transactions, approve transactions, and write checks. She reconciled the bank statements and performed analytics for the board package. Unbeknownst to the CFO and board she created a fictitious company. Her scheme lasted over 7 years.

The Secretary paid legitimate vendors from her fictitious company and then billed the Juvenile Justice organization. Her bills to the Juvenile Justice organization were inflated so she was making a 25% markup on legitimate expenses. To help ensure there were no questions about the expenses she kept the account balances constant. The CFO and the board did not see any significant fluctuations month to month and the auditors never questioned balances that did not have more than a 10% variance.

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

The auditors were notified of the issue when the legislative auditor wrote to them asking to review the workpapers. The fraud was identified by an attorney that was sitting in on a board meeting. During the presentation of financial results for the month he observed that the balance of certain accounts appeared high. He suggested that the organization go out to bid. The CFO handled the search for a new vendor and in the process discovered the fictitious company. The Secretary was prosecuted but was unable to repay the $1.8 million.

Case Study 1—Billing Schemes: Juvenile Justice Organization Defrauded of $1.8 Million

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

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

Case Study 2—Check or Payment Tampering, Embezzlement, Skimming, Billing Schemes, and Cash Larceny

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

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

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

Case Study 2—Check or Payment Tampering, Embezzlement, Skimming, Billing Schemes, and Cash Larceny (con't)

Analysis: Distefano committed the following fraud schemes:

- **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**—Distefano wrote checks to a vendor where services were not rendered (air conditioning company) and wrote checks for personal bills out of the unauthorized bank account.
- **Expense Reimbursement**—Distefano wrote checks to herself reimbursing for supplies that she never purchased on behalf of the entity.
- **Board Discovery**-- Although it took a while, a board member finally looked at the poor financial position of the entity. When he discovered the money was missing, he called in the authorities and terminated Distefano. Many not-for-profits try to handle the issues privately and don't prosecute.

Case Study 2—Check or Payment Tampering, Embezzlement, Skimming, Billing Schemes, and Cash Larceny (con't)

- Some of the fraud symptoms that might have alerted the Board of Directors to fraudulent activity were:
  - Cash sales (boarding revenue) differing from normal or expected patterns
  - Cash deposits differing form normal or expected patterns
  - Lack of segregation of duties
  - Unusual reconciling items on bank reconciliations
  - Differences between daily list of receipts and deposits on bank statements
  - Increased use of petty cash fund
  - Lack of vacation on part of bookkeeper
  - Increase in expenses
  - Unusual vendors noted

Case Study 2—Check or Payment Tampering, Embezzlement, Skimming, Billing Schemes, and Cash Larceny (con't)

- The Board should have reviewed financial statements regularly and asked questions.
- Where there is a lack of segregation of duties, and in this case, where there is a lack of financial executives, it is very important that someone assume the review role, even if it is a board member.
- Background checks and perhaps even credit checks should have been performed.
- Code of conduct/conflict of interest statements for the board and employees— this may or may not have set the tone since there was one employee who had access to virtually all assets and a lack of monitoring. Monitoring in the form of reviewing bank reconciliations, subsidiary ledgers, budget to actual, etc.
- Setting an expectation for boarding revenue and comparing it to actual, monitoring the compliance with the grant document, including ensuring the funds were received and deposited.

Case Study 3—Procurement Fraud, Kickbacks

- Ralph Clark was hired by the Woodruff Arts Center in Atlanta as an HVAC mechanic. The next year he was made acting director of facilities. Five years later Clark pleaded guilty to embezzling more than $1.1 million from the Woodruff Arts Center.
- As director of facilities, Clark was authorized to approve vendor contracts up to $50,000. He embezzled the money by submitting invoices from his wife's business, Lowe's Services, for goods and services that were never provided or were performed by Clark himself. He would then pick up the checks for the payments and deposit them into accounts that he controlled. Clark also demanded that another maintenance vendor inflate invoices to the Center by 30% and remit the extra 30% to him.
- In February 2014, Clark was sentenced to two years and six months in prison plus three years supervised release and ordered to repay $1 million embezzled from the Center.

Case Study 3—Procurement Fraud, Kickbacks (con't)

Analysis: Fraud involving vendor contracts, sometimes with kickbacks generally happens when internal controls over procurement are lax and large procurements are made.

It appears that the organization did not require competitive bidding and monitor to ensure contracts were awarded fairly or have a new vendor approval process. Where with the small juvenile justice organization one might not expect to see this sort of control, in a large organization such as Woodruff Arts Center this control would be expected. This is also a case of collusion. If the vendor was coerced into the kickback scheme as a condition of selection, some type of hotline would have provided them the opportunity to report.

With some kickback schemes there is complete agreement between the procurement official and the vendor making it harder to detect. The organization should perform background check for new employees with significant spending authorization authority, verify new vendors to confirm they exist and can provide the goods/services contracted for and establish an anonymous communication channel for complaints.

Case Study 4—Expense Reimbursement: Inappropriate Credit Card Use, Corruption, and Forgery

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

Much of the money he embezzled was donations 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.

Case Study 4—Expense Reimbursement: Inappropriate Credit Card Use, Corruption, and Forgery (con't)

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

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

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

Case Study 4—Expense Reimbursement: Inappropriate Credit Card Use, Corruption, and Forgery (con't)

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

Case Study 5—Expense Reimbursement: Use of Debit Cards

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

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

Four years later, she pled guilty in federal court to fraud and tax charges. Separately, Florida state prosecutors charged her with defrauding the not-for-profit, Step Up Students, of nearly $7,000.

The charges claimed that while earning more than $140,000 a year, she sent her son to private schools on scholarships meant for low-income children by falsifying tax returns, a birth certificate, and other documents to make it appear her lower-income sister was the boy's guardian, thus fraudulently obtaining nearly $7,000 in scholarships for Step Up Students.

Case Study 5—Expense Reimbursement: Use of Debit Cards (con't)

Analysis: Lack of controls over debit cards, lack of board oversight. Lack of management oversight, lack of policies including conflict of interest, lack of oversight of scholarship programs and verification of documents.

Case Study 6—Expense Reimbursement: Credit Card Fraud, Theft of Checks

- Avelyn Reynolds was the trusted executive assistant to the Chief Operating Officer (COO) at Support Childhood Education (SCE), a prestigious non-profit organization. During her second year at SCE, she got divorced and became embroiled in a lawsuit. Her financial and emotional stress soared, and she began to feel underpaid and to think of ways to get what she deserved from the organization.
- As the COO's assistant, she had an organization credit card, maintained the petty cash, and had the ability to initiate payments by the bank and payment requests to accounts payable, create purchase orders, approve her own timecard, and authorize payments to families awarded assistance from SCE.
- She started small but steadily increased the size of her thefts. She began using the organization credit card for personal purchases, forging the COO's signature. The organization paid her phone bills far above her authorized amount, assuming the charges were the COO's. Her children had different last names, so it was easy for her to authorize thousands of dollars in payments to them as if they had been legitimately awarded educational assistance.

Case Study 6—Expense Reimbursement: Credit Card Fraud, Theft of Checks (con't)

- 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.
- 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 cosmetic surgery. 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.

Case Study 6—Expense Reimbursement: Credit Card Fraud (con't)

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

- Lack of tone from the top (background checks, management, and board fraud risk assessment)
- Lack of segregation of duties
- Lack of manager review of account changes for suspicious transactions
- Failure to check award recipients against the HR 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

Discussion Question 8

The fraud scheme that results in the largest loss to organizations is _____.

A. Cash larceny

B. Check/payment tampering

C. Register disbursements

D. Billing scheme

Discussion Question 8—Solution

The fraud scheme that results in the largest loss to organizations is _____.

A. Cash larceny

B. Check/payment tampering

C. Register disbursements

D. Billing scheme

Case Study 7—Cash Larceny

- A 27-year-old woman was hired as an administrative employee for the College of Nursing of a University. She was responsible for the upkeep of the facilities, College of Nursing staff payroll, budgetary issues, and general administrative duties for the dean and program director of the College of Nursing.
- Three years later, she began intercepting checks intended for College of Nursing and depositing them directly into her personal bank account. She stole nearly $61,000 using this scheme. Four years after that, her bank informed her they would no longer accept deposits into her account of checks on which she was not the payee.
- She came up with a new plan. She had access to the Student Nurses Association bank account at the associated hospital's Employees Credit Union, which was a private savings account owned and funded by the students of the College of Nursing. After her bank shut off her ability to deposit her stolen checks into her bank account, she began to deposit them into the Student Nurses Association bank account. She would then withdraw the funds from that account on the same day.

Case Study 7—Cash Larceny

- Using this new scheme, in just two years she was able to steal additional amounts totaling more than $657,000, for a total theft of $717,999.
- As is the most likely case in frauds of this nature, the perpetrator paid no income tax on her ill-gotten gains. Later that year she pleaded guilty to theft of program funds and tax evasion. She was sentenced to 30 months in federal prison without the possibility of parole and was ordered to pay $717,999 in restitution to Mercy Hospital, as well as $115,117 plus interest to the IRS.
- **Analysis**: Lack of segregation of duties is the primary enabler of this fraud. The perpetrator was inventive and determined but more supervision over the cash handling function could have detected this fraud.

Example Matrix of Controls to Prevent Cash Schemes

Internal Controls That Could Help Prevent Cash Schemes (Small- to Midsize Organizations)					
Control	Stealing Deposits	Stealing Cash on Hand	Skimming Part of Contribution or Sale	Kiting	Lapping
Use pre-numbered deposit slips	✓		✓		
Make all deposits intact daily	✓		✓		
Keep un-deposited amounts in a safe	✓		✓		
Consider a lockbox for large volumes of cash receipts	✓	✓	✓		

Example Matrix of Controls to Prevent Fraudulent Disbursements

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

Case Study 8—Payroll Fraud

- A payroll clerk whose responsibilities were posting time and attendance information to the computer system and preparing the payroll disbursement summaries. He was able to steal $112,000 during a two-year period through payroll fraud.
- There was segregation of duties.. A payroll supervisor approved all disbursements and verified the payroll was deposited directly into the employees' bank accounts.
- 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 figured out that the payroll deductions were set for employee numbers within a certain range so when he created the fictitious employees, he made sure that the employee number was outside that range so no deductions would be made for them. He arranged for their wages to be deposited into his bank account. He knew from prior experience that the bank did not match employee names to the depositor's account.
- Since payroll was approved by the supervisor, he prepared a fictitious payroll summary. No one checked his work because his performance had been superior in the past. The fictitious report was prepared with a different type face than the real reports, but that was not noticed by the supervisor.

Case Study 8—Payroll Fraud (con't)

- Turner's concern was creating file copies of the paychecks for the fictitious employees. The check copies printed in the accounting department were yellow. No one noticed until an auditor selected one of the fictitious transactions in his sample. He noted the white copy when the rest were yellow. The employee was not in the payroll register when the auditor went to trace it through the system. This caused the auditor to dig a little further and he found out that there were others. The auditor noted that all the suspicious payroll amounts were being deposited into the same bank account.
- The auditor thought there might be collusion going on, so the auditor performed the following steps:
- Obtained original copies of payroll registers, payroll check summaries, direct-deposit records, personnel files, time sheets and bank documents
- Interviewed the accounting department employees and the supervisor

Case Study 8—Payroll Fraud (con't)

- The auditors noted that there were several red flags as they were performing the extra procedures:
- The passwords were not changed frequently
- The fictitious employees had the social security number of a deceased person.
- The employee ID numbers were higher than those of legitimate employees
- 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
- Multiple direct deposits were made to the same bank account but under different names
- When caught, Turner stated that he needed the money to pay for his expensive HIV drugs.

Case Study 8—Payroll Fraud (con't)

- **Analysis**: Although the not-for-profit had good segregation of duties, this control alone is not enough.
- Adding the following internal controls might have prevented or detected the fraud.
- Inspect paychecks and see if there are any without deductions
- Tie out the payroll summary to expense
- From time to time, do a hand delivery and require positive identification
- Analyze payroll expense (it was not clear from the information available on this fraud where the debits were posted since it was not to payroll expense)
- Change passwords every 90 days

Example Matrix of Controls to Prevent/Detect Payroll Fraud

Internal Controls That Could Help Prevent Payroll Schemes (Small- to Midsize Organizations)						
Control	Fictitious Employees	Inflated Payroll	Terminated Employees on Payroll	Expense Report Fraud	Stealing Checks	Payroll Tax Schemes
Use a payroll service and have senior management review payroll documentation analytically	✓	✓	✓		✓	
Payroll service handles payroll tax payments to IRS						✓
Supervisory approval for additions and terminations	✓		✓			

Case Study 9—Theft of Nonfinancial Assets

- Andrew Liersch was the president of Goodwill Industries. His fraudulent activities cost Goodwill (13 stores) approximately $26 million spanning approximately 18 years. He involved the core store managers in the fraud and paid them $1,000 a week for selling the most valuable items in back-door sales. They also had duplicate registers and that cash was siphoned off in the scheme. There were other employees involved who received payoffs in varying amounts. When sold, investigators believe that Liersch's proceeds were deposited into several bank accounts, some in Switzerland, Scotland, and Austria. This fraud took investigators six years to unravel.
- The fraud came to light when one of the conspirators was going through a contentious divorce. Her husband called to report the fraud. The original mastermind of the scheme was Carol Marrs, Goodwill's director of stores. She originally was skimming valuable items and selling them at garage sales. When Liersch came on board, he took the fraud to a whole new level. Marrs committed suicide after investigators searched her home. They found approximately $1 million in accounts allegedly set up with her share of the profits from the fraud scheme.

Case Study 9—Theft of Nonfinancial Assets (con't)

- Goodwill officials believed that the fraud was undetected for so long because Liersch kept producing superior results for the organization. Donations continued to rise each year. Liersch relied on his control and knowledge of the organization's workings to hide fraud. He also lied to the Board of Directors.
- Liersch eventually pleaded guilty to a charge of tax evasion to avoid being charged with stealing from Goodwill Industries. The plea agreement dismissed the embezzlement charges and did not require prison time. Liersch was ordered to pay $540,000 in restitution.
- **Analysis**: Executive management was corrupt so there was no tone from the top to set an expectation that fraud would not be tolerated.
- The board was not sufficiently involved and since the perpetrator made significant contributions to the organization in other ways, red flags may have been overlooked. If available, a hotline of some kind might have been used by employees, donors, or others to report suspicious activity.

Case Study 9—Theft of Nonfinancial Assets (con't)

- Controls over receipt of goods in donation were deficient. Controls that may help to prevent or detect fraud when there is inventory present are:
  - reconciling donation acknowledgments provided for goods to the level of goods received or sold
  - segregation of larger, more expensive donated items to ensure their placement for sale
  - using physical access controls for all assets and inventory and restricting access to inventory
  - monitoring employees who have access for unusual patterns of entry and departure
  - using electronic surveillance equipment such as video cameras

Case Study 10—Fraudulent Financial Reporting

- Francine Gordon was a model employee at Small Town Federal Credit Union (STFCU). She had been controller for 15 years and managed the IT system, running it herself when the data-processing clerk was sick or on vacation.
- Her great value to STFCU overcame her dictatorial manner and moody temper. A small institution, STFCU had little segregation of duties. Gordon created financial statements, prepared budgets, and forecasts, reconciled STFCU's bank statement, supervised the IT department, and managed the investment portfolio. Gordon was single with no children, had few friends, had a family who lived far away, and was not close with colleagues. She regularly awarded 90% of STFCU's investment business to one of three approved brokers; one whose skillset ran more toward client flattery than investment expertise.
- STFCU decided to hire a CPA for internal audit and financial accounting. Six months after he started, regulators were performing their annual on-site review and found a $130,000 reconciling item by Gordon in the bank reconciliation. Gordon gave the CPA a confusing explanation which he passed on to the regulators, and the regulators accepted it. Two months later, the CPA found the same $130,000 item had not been cleared and was still in the reconciliation.

Case Study 10—Fraudulent Financial Reporting

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

Case Study 10—Fraudulent Financial Reporting

- **Analysis**: Lack of segregation of duties gave Gordon the opportunity to commit this fraud. Gordon's motivation was to save face by not admitting she had chosen an imprudent investment. She also set a poor tone by being dictatorial and causing people to be afraid to question her. The internal auditor should have been able to report directly to the audit committee if the item was not cleared and he expected wrongdoing. Even if the regulator passed on questioning the item further, it is the organization's responsibility to maintain the appropriate level of internal control.
- Gordon rarely took vacation, and when she did it was usually for less than a week. All employees should be required to take an annual vacation of at least a week. In addition, organizations should cross-train all employees in duties.
- All reconciling items should have an explanation and be verified by someone independent of the entry's creator. A recurring reconciling item for the same amount should be investigated particularly closely. The reporting relationship between the internal auditor and the board/audit/finance committee chair should be established. Otherwise, a strong executive such as Gordon will be able to override controls.

Reminders

- **Post event evaluation:** Please complete the course evaluation that will be viewable once the session ends. We welcome your feedback!


KAPLAN