International Professional Practices Framework

Supplemental Guidance
Practice Guide

Engagement Planning

Assessing Fraud Risks

The Institute of Internal Auditors | Global

Table of Contents

Executive Summary

Fraud can disrupt operations, pose compliance risks, blemish an organization's reputation, and cost an organization and its stakeholders substantial amounts of money. While management, with board oversight, holds the primary responsibility for establishing and monitoring effective controls to deter and detect fraud, the internal audit activity is required to evaluate the risk of fraud, according to the *International Standards for the Professional Practice of Internal Auditing*. Additionally, the chief audit executive (CAE) must report significant risk and control issues, including fraud, to senior management and the board (Standard 2060 – Reporting to Senior Management and the Board).

The *Standards* require the internal audit activity to assess fraud risks at the organizational and engagement level. To ensure adequate review of the risks relevant to each engagement, internal auditors should conduct a fraud risk assessment as part of engagement planning (Standard 2210.A1). Over time, the knowledge the internal audit activity obtains during individual engagements can be compiled into a more robust and comprehensive organizationwide fraud risk assessment.

This practice guide describes the characteristics of fraud and the process of identifying and assessing fraud risks during engagement planning. The exact process of incorporating a fraud risk assessment into engagement planning may vary according to the needs of the individual organization, internal audit activity, and engagement. However, the process generally includes the following steps:

- Gather information to understand the purpose and context of the engagement, as well as the governance, risk management, and controls relevant to the area or process under review.
- Brainstorm fraud scenarios to identify potential fraud risks.
- Assess the identified fraud risks to determine which risks require further evaluation during the engagement.

Introduction

The internal audit activity is responsible for assessing the organization's risk management processes and their effectiveness, including the evaluation of fraud risks and how they are managed by the organization (2120.A2). However, assessing the potential for the occurrence of fraud when planning each engagement is just as important because new fraud risks can arise at any time. Therefore, internal auditors must consider the probability of fraud when they develop the objectives of each engagement (Standard 2210.A2).

Performing a fraud risk assessment at the start of an engagement enables internal auditors to discover fraud risks that may not have been present when the organizationwide risk assessment was last updated. Additionally, fraud risks that may be insignificant at the organizational level may achieve significance in an individual area or process.

While internal auditors must have sufficient knowledge to evaluate the risk of fraud and how it is managed by the organization, they are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud (Standard 1210.A2). When assessing fraud risks, internal auditors are expected to exercise due professional care (Standard 1220.A1) and maintain an impartial, unbiased attitude (Standard 1120 – Individual Objectivity). Internal auditors also exhibit professional skepticism – an inquisitive attitude, free of bias or assumptions about the inherent honesty of management or employees – because it enables an objective, critical assessment of the area of process under review.

This practice guide provides a brief overview of the characteristics of fraud, followed by a description of how to assess fraud risks as part of engagement planning. The guide describes how to gather information, brainstorm fraud scenarios, identify fraud risks and rate their significance to determine which fraud risks should be evaluated further during the engagement.

Understanding Fraud

While many definitions exist, The IIA defines *fraud* as "any illegal act characterized by deceit, concealment, or violation of trust." The definition captures the characteristic that makes it unique among risks: intent. Fraudulent acts involve people that intend to circumvent controls or exploit weaknesses in the organization. The IIA definition also notes that "frauds are perpetrated to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage."

Because laws vary, the legality of a fraudulent act may be questionable. For example, a multinational organization headquartered in a country where an act is illegal may conduct business in other countries where the same act does not violate local laws. No matter the legal distinctions, the purpose of a fraud risk assessment is to identify the potential for trust violations, exploitations of weaknesses, and circumvention of controls.

Three factors are consistently present when people commit fraud: pressure or incentive, perceived opportunity, and rationalization.[1]

Pressure or Incentive – An actual or perceived need that provides a reason or motive, such as:

- The need to achieve organizational performance targets or financial goals.
- Personal struggles or external stressors (e.g., financial problems, health issues, or addictions).
- The desire to gain power, influence, or esteem in the eyes of family, friends, colleagues, or management (e.g., computer hackers who commit fraud, intending to show off their capabilities rather than to cause harm).

Opportunity – A combination of circumstances or conditions that enable fraud to occur, such as:

- Poor control design, lack of controls, insufficient security or segregation of duties, or other circumstances that can enable a control failure.
- A level of trust, authority, knowledge of, and/or access to control processes that enables personnel to circumvent or override existing controls.
- Inadequate supervision, training, or communication regarding policies of professional conduct and the consequences of violations.

[1] Cressey, D.R. "The Criminal Violation of Financial Trust," *American Sociological Review*, 15, no. 6 (1950): 738-743.

Rationalization – A concocted, convincing, and plausible justification, such as:

- Feelings of entitlement due to organizational commitment (e.g., tenure, excessive unpaid hours worked, or unrewarded performance).
- Belief that actions are acceptable because "others probably do it too."
- Belief that actions are acceptable because they are culturally commonplace or were considered acceptable in previous organizations.
- Belief that policies and procedures do not make sense or are not justified.
- Reasoning that actions are temporary and/or a one-time event (e.g., "borrowing money and will pay it back" or "just this once").
- Belief that the action is victimless or so insignificant that no one would notice and/or care.

Of the three factors, opportunity is the only one that organizations can control directly. Management can design internal controls to try to prevent opportunities for fraud and to detect fraudulent activities if they occur.

Internal auditors should note that those who engage in fraudulent activities may rationalize fraud not only for their own benefit, but also for the benefit of their organization or an external individual or organization. Fraud committed to benefit the organization is usually executed by exploiting an opportunity to gain an unfair or dishonest advantage through deception of an outside party. However, even when employees use such a rationalization, they typically receive an indirect personal benefit, such as the achievement of a performance target, a financial reward, and/or a promotion. Appendix C lists examples of fraudulent acts and how they are rationalized.

Gathering Information

To identify fraud risks in the area or process under review, internal auditors should understand the organization and the larger context in which it operates (i.e., legal, political, social, economic, market, industry, and cultural environments). Additionally, internal auditors must understand the strategic and operational objectives of the organization and how they align with the objectives of the area or process under review (Standard 2200 – Engagement Planning).

To attain this insight, internal auditors should seek information from an array of sources, including:

- Prior assessments and investigations.
- Formal reporting mechanisms and interviews.
- A preliminary review of the control environment.
- External research and specialists.

When gathering information to develop an engagement's fraud risk assessment, the internal audit activity's role is to assess the fraud risks relevant to an engagement, rather than to investigate a potential fraud. Thus, internal auditors should communicate discretely, maintain confidentiality, and avoid expressing any suspicions or accusations of fraud. Careless communication could disrupt a potential investigation and needlessly introduce unwanted reputational and legal risks.

Prior Assessments and Investigations

The organizationwide risk assessment, which documents the significant risks identified at the organizational level and forms the basis for the annual internal audit plan (Standard 2010.A1), is a good starting point for identifying risks that could be relevant to the area or process under review. Assessments centered on fraud risks only, whether organizationwide or limited to the area or process under review, may also be useful sources of information. Internal auditors should review relevant risk assessments and fraud investigations performed by the management of the area under review and other providers of assurance and consulting services, both internal and external. To be efficient, internal auditors typically consider only recent assessments.

Although prior assessments and investigations may provide valuable insight, the significance of fraud risks can be affected by many factors and may change quickly. Thus, conducting a preliminary assessment of risks for each individual engagement is essential to effective engagement planning.

Formal Reporting Mechanisms and Interviews

An organization's personnel can provide useful information about fraud risks. In fact, the Association of Certified Fraud Examiners (ACFE) reports that regardless of the size or type of organization, or whether a formal reporting mechanism exists, personnel are the source of more than 50 percent of fraud tips, the most common way to detect fraud.[2] Notably, the internal audit activity was identified as the second most common method of detecting fraud.

Many organizations have established formal mechanisms (e.g., whistleblower hotlines, online forms, or email submissions) to facilitate the reporting of suspected fraudulent acts and internal control weaknesses that could expose the organization to fraud risk. Commonly reported concerns include allegations of waste, abuse of authority, misappropriation of assets, collusion, and other unethical or suspicious behavior. If a formal fraud reporting mechanism exists, internal auditors may ask the individual(s) responsible for its management to provide

[2] Association of Certified Fraud Examiners, *2016 Report to the Nations on Occupational Fraud and Abuse* (Austin, TX: Association of Certified Fraud Examiners, 2016), 20-25, http://www.acfe.com/rttn2016.aspx (accessed October 31, 2017).

access to any information pertinent to the area or process under review, such as recorded phone calls or documented statements.

To gain insight into past fraudulent activities that have been alleged, discovered, and/or investigated, internal auditors typically query other organizational personnel responsible for managing fraud risks, allegations, and occurrences. Such personnel may include legal counsel, human resources, ethics officers, risk and compliance officers, security, and fraud risk management.

Additionally, interviewing personnel at all levels in the area or process under review may yield valuable information not otherwise available. The individuals who perform the daily tasks and functions of the area or process often provide the most accurate and up-to-date description of how the process and relevant controls *actually* operate, compared to how they are *intended* to operate. Understanding the actual operations may reveal various ways the controls could be circumvented. To identify interviewees, internal auditors may refer to an organizational chart containing the roles and responsibilities of personnel in the area under review or a process map with a list of key controls (whether provided by management or created by the internal audit activity).

Potential Red Flag Phrases

Certain phrases used by interviewees may indicate potential control deficiencies and/or fraud risks:

- "As a work around …"
- "Just this one time …"
- "I have always done it this way."
- "Once in a while we …"
- "Off the record …"
- "There are no policies or procedures for this process."
- "Someone told me to do it this way; however, I am not sure why."
- "This is *really* how it is done."
- "The way it is *supposed* to work …"

Appendix D lists potential red flag words.

Preliminary Review of the Control Environment

Formal reporting mechanisms and interviews often expose issues related to the organization's control environment that could lead to fraud. Additional red flags may be discovered through a review the elements of the control environment, such as the organization's structure and ethical values, as well as management's philosophy and operating style. An assessment of the control environment should include evaluating the maturity of the control environment and the effectiveness of relevant controls. The assessment may reveal potential behavioral drivers and/or pressures that could lead employees to rationalize committing fraud. For example, personnel may express awareness of performance pressures or concerns of unrealistic goals that individuals could use to justify fraudulent behavior. To gain insight into the potential pressures, internal auditors should identify the performance goals and measurements (i.e., key performance indicators) and related incentives in the area under review.

Because internal auditors have a holistic view of the organization and its control environment, they may become aware of cultural shifts across the organization over time. Cultural shifts could increase the likelihood that fraud may occur and go unnoticed. At the engagement level, internal auditors may be closer than senior management (and others that manage organizationwide fraud risks) to the detailed operations, systems, and personnel of the area or process under review. Thus, it is vital for internal auditors to be alert to the words or actions of personnel that may indicate weaknesses in the control environment. If weaknesses in the control environment are suspected, the engagement supervisor should communicate the information to the CAE, because the issue may exceed the scope of the engagement. The IIA Practice Guide "Auditing the Control Environment" covers this topic in greater detail.

Potential Red Flags

Management Issues:

- Lack of area expertise
- Lack of supervision
- History of legal violations

Personnel Issues:

- Lack of background checks
- Dissatisfied employees
- Unwillingness to share duties

Process Issues:

- Duties not segregated
- Poor physical security
- Poor access controls

External Research and Specialists

Internal auditors are not required to have the expertise of a specialized fraud investigator. However, they must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization (Standard 1210.A2). Internal auditors can gain such knowledge by researching frauds that have occurred in similar organizations or industries and studying fraud trends. In addition, internal auditors can use benchmarks to compare the fraud risk management practices of the organization and the area under review to those of comparable and/or more mature organizations. Knowledge can also be acquired by reading relevant publications, keeping current with changes in regulations, and attending conferences and trainings. Relevant professional organizations often provide such tools and information, as well as professional standards.

The CAE must ensure that the internal audit activity collectively possesses or obtains the competencies necessary to perform its responsibilities (Standard 1210 – Proficiency) and must obtain competent advice and assistance if internal auditors lack the competencies needed to perform all or part of the engagement (Standard 1210.A1). In addition to providing training and mentoring opportunities for internal audit staff, the CAE may solicit specialists with knowledge of the industry or specific functional areas or processes. When brainstorming fraud scenarios or performing an engagement that includes fraud risks, internal auditors may confer with such specialists as needed.

Brainstorming Fraud Scenarios

Based on the information gathered, internal auditors can begin contemplating potential fraud scenarios and fraud risks relevant to the area or process under review. Brainstorming fraud scenarios is an effective way to determine the characteristics and circumstances unique to the specific area or process under review that may produce opportunities and incentives for fraud.

The need for brainstorming sessions, the complexity of the sessions, and the participants involved vary from engagement to engagement, depending on the needs of the internal audit activity, organization, and engagement, as well as the internal auditors' knowledge of the area or process under review. To achieve a thorough list of fraud scenarios, internal auditors should brainstorm with individuals diverse in their knowledge, perspective, and relationship to the area or process under review.

Potential Brainstorming Participants

- Accounting and Finance
- Internal Audit
- Legal and Compliance
- Operations
- Process Owners
- Senior Management
- Other Assurance Service Providers

When brainstorming fraud risks, participants should consider potential pressures and opportunities to commit fraud in the area or process under review. Participants should also consider fraud scenarios involving internal and external IT threats, such as access to override system configurations, which could allow fraudulent transactions and/or theft of sensitive organizational information.

Brainstorming is intended to encourage open participation and sharing of thoughts and ideas without inhibition. Therefore, when reviewing the fraud scenarios that have been proposed, internal auditors should recognize that some potential fraud risks may be highly unlikely, not well aligned with the engagement objectives, or beyond the scope and resource allocations of the current engagement.

The information gathered during brainstorming sessions could be used to develop a list of fraud scenarios and fraud risks in any auditable area or process. To illustrate, **Figure 1** presents fraud scenarios and corresponding risks that might be identified during a brainstorming session for an accounts payable assurance engagement. Appendix E shows a fraud risk assessment in a cash disbursements process engagement.

Figure 1: Brainstorming Fraud Scenarios

Fraud Scenario	Fraud Risk
A. Fictitious personnel expenses.	A.1 Corporate cards are intentionally issued inappropriately, resulting in fraudulent expenses.
	A.2 Expenses submitted for services or goods are not actually provided to the organization.
	A.3 Multiple expense reimbursements are submitted for same expense.
B. Fraudulent disbursements.	B.1 Fictitious vendors are set up in the system, resulting in fraudulent payments.
	B.2 False refunds and/or voids are processed.
C. Concealed liabilities and expenses.	C.1 Bad debt expense is intentionally omitted.
	C.2 Expenses are capitalized.
D. Related party transactions.	D.1 One party receives some benefit not obtainable in an arm's-length transaction.
E. Embezzlement.	E.1 Personnel pay personal expenses with the organization's funds and falsify financial records to cover it up.

Assessing Fraud Risks

Because the engagement cannot cover every risk, internal auditors assess the significance of the fraud risks that were identified during brainstorming to determine which risks should be evaluated further during the engagement. An effective way to perform and document the fraud risk assessment is to create a fraud risk matrix listing the fraud scenarios and relevant risks and then expand the matrix to include measures of significance.

A fraud risk matrix may be created using a spreadsheet or similar document, with or without an audit software program. The format of the matrix may vary but typically includes a row for each risk and a column for each risk measure, such as impact and likelihood.

Figure 2 depicts how the fraud scenarios documented in Figure 1 could be expanded to include the impact and likelihood risk ratings.

Assessing impact can be complicated because it involves both quantitative and qualitative factors. Internal auditors should account for not only the financial, operational, and regulatory impact of the potential fraud risks, but also the nonfinancial impacts, such as damage to the organization's reputation or relationships with customers or vendors. For example, a fraud risk with an immaterial, direct financial impact to the organization could still greatly affect its reputation and therefore may be categorized as high impact.

Figure 2: Fraud Risk Matrix for Accounts Payable

Fraud Scenario	Fraud Risk	Impact (L,M,H)	Likelihood (L,M,H)
A. Fictitious personnel expenses.	A.1 Corporate cards are intentionally issued inappropriately, resulting in fraudulent expenses.	L	M
	A.2 Expenses submitted for services or goods are not actually provided to the organization.	H	M
	A.3 Multiple expense reimbursements are submitted for same expense.	M	H
B. Fraudulent disbursements.	B.1 Fictitious vendors are set up in system, resulting in fraudulent payments.	H	H
	B.2 False refunds and/or voids are processed.	L	H
C. Concealed liabilities and expenses.	C.1 Bad debt expense is intentionally omitted.	H	L
	C.2 Expenses are capitalized.	H	L
D. Related party transactions.	D.1 One party receives some benefit not obtainable in an arm's-length transaction.	M	M
E. Embezzlement.	E.1 Personnel pay personal expenses with organization's funds and falsify financial records to cover it up.	M	M

Factors to consider when assessing likelihood include past fraud allegations or occurrences, prevalence of similar frauds in the industry, and the complexity and number of people involved in the process.

The risk ratings from the fraud risk matrix can then be represented on a basic graph, such as a heat map. By plotting each risk's impact along one axis and its likelihood along the other axis, internal auditors clearly depict the risk's overall significance, or priority. Typically, the combined significance of impact and likelihood is indicated using a color system: red denotes the highest priorities, orange denotes risks that are significant enough to warrant consideration, and yellow denotes risks that are not significant.

Figure 3 shows a heat map created from the information in the fraud risk matrix presented in Figure 2. The heat map should be included in the engagement workpapers because it supports internal auditors' decisions about risk significance.

One limitation of heat maps is that impact and likelihood appear to be equally important. While such equivalence might be true at times, impact usually takes priority over likelihood. For example, in most cases, a risk rated high impact and low likelihood (H, L) should be prioritized over a risk considered low impact, even if the likelihood of its occurrence is high (L, H).

An additional limitation of heat maps is that only two measures can be considered at a time (in this case, impact and likelihood). It may be desirable or necessary to also consider such measures as velocity, vulnerability, volatility, interdependency, and/or correlation when determining the significance of risk.

Based on the completed heat map, internal auditors can easily visualize the significant fraud risks that should be included in the engagement for further testing. **Figure 4** shows the fraud risk matrix adjusted to reflect only the prioritized fraud risks in the accounts payable engagement example.

Internal auditors can provide management with the identified fraud risks to be considered for inclusion in the organizationwide risk assessment. The fraud risks that are not selected for further evaluation during this engagement may be transferred to internal audit's fraud risk inventory, or watch list, to be considered for future engagements.

Figure 3: Heat Map

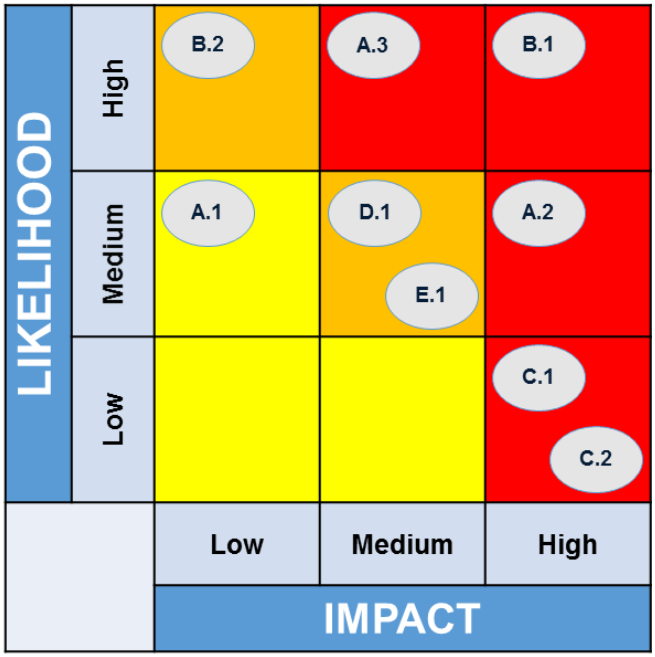

Figure 4: Significant Fraud Risks

Fraud Risk	Impact (L,M,H)	Likelihood (L,M,H)
B.1 Fictitious vendors are set up in system, resulting in fraudulent payments.	H	H
A.2 Expenses submitted for services or goods are not actually provided to the organization.	H	M
A.3 Multiple expense reimbursements are submitted for same expense.	M	H
C.1 Bad debt expense is intentionally omitted.	H	L
C.2 Expenses are capitalized.	H	L
D.1 One party receives some benefit not obtainable in an arm's-length transaction.	M	M
E.1 Personnel pay personal expenses with organization's funds and falsify financial records to cover it up.	M	M

If information discovered during the fraud risk assessment indicates a potentially fraudulent act, internal auditors should follow the established protocols for internally reporting and investigating fraud allegations. Typically, internal auditors report the concern and preliminary evidence to the CAE, who then decides whether the issue needs to be escalated to senior management and/or the board.

Identifying Controls

After internal auditors have considered fraud scenarios and identified and prioritized fraud risks, they should determine which controls, if any, are in place to mitigate those risks.

Figure 5 depicts the expansion of the matrix from Figure 4 to include existing controls.

Figure 5: Fraud Risk and Control Matrix for Accounts Payable

Fraud Risk	Impact (L,M,H)	Likelihood (L,M,H)	Control
B.1 Fictitious vendors are set up in system, resulting in fraudulent payments.	H	H	Segregation of duties in vendor management.
A.2 Expenses submitted for services or goods are not actually provided to the organization.	H	M	Confirmation of receipt of goods and services.
A.3 Multiple expense reimbursements are submitted for same expense.	M	H	Automated controls to detect duplicate expense submissions.
C.1 Bad debt expense is intentionally omitted.	H	L	Regular monitoring and approval of bad debt expense calculations.
C.2 Expenses are capitalized.	H	L	Management review and approval of all capitalization entries.
D.1 One party receives some benefit not obtainable in an arm's-length transaction.	M	M	Due diligence for related-party transactions.
E.1 Personnel pay personal expenses with organization's funds and falsify financial records to cover it up.	M	M	Segregation of duties in accounts payable and management approval required for personnel expenses.

Like the heat map, the fraud risk and control matrix should be included in the engagement workpapers. The information from the matrix is then incorporated into the preliminary risk assessment used to establish the engagement objectives and scope. The IIA Practice Guide "Engagement Planning: Establishing Objectives and Scope" provides detailed information about building upon the risk assessment to develop the engagement objectives and scope. In addition, the fraud risk heat map and risk and control matrix will lend support to the engagement results and conclusions, in conformance with Standard 2330 – Documenting Information.

Appendix A. IIA Standards and Guidance

Relevant IIA Standards

The following selections from The IIA's *International Standards for the Professional Practice of Internal Auditing* are relevant to Engagement Planning: Assessing Fraud Risks. Please refer to the *Standards* for the complete pronouncement. To assist with the implementation of the *Standards*, The IIA recommends that internal auditors refer to each standard's respective Implementation Guide.

1210 – Proficiency

1210.A1

1210.A2

1220 – Due Professional Care

1220.A1

2120 – Risk Management

2120.A2

2200 – Engagement Planning

2210 – Engagement Objectives

2210.A1

2210.A2

Related IIA Guidance

Practice Guide, "Auditing the Control Environment."

Practice Guide, "Engagement Planning: Establishing Objectives and Scope."

Practice Guide, "Internal Auditing and Fraud."

Appendix B. Glossary

Terms identified with an asterisk (*) are taken from The IIA's *International Professional Practices Framework* "Glossary," 2017 edition.

Control* – Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.

Control Environment* – The attitude and actions of the board and management regarding the importance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements:

- Integrity and ethical values.
- Management's philosophy and operating style.
- Organizational structure.
- Assignment of authority and responsibility.
- Human resource policies and practices.
- Competence of personnel.

Fraud* – Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss or services; or to secure personal or business advantage.

Risk* – The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

Appendix C. Examples of Fraudulent Acts

The following examples of fraudulent acts do not comprise an exhaustive or prioritized list. Instead, they are provided to stimulate awareness of potential fraud risks categorized by type of rationalization.

Examples of fraud committed for the direct benefit of an individual include:

- Intentional revenue diversion to an employee, stakeholder, or external party that would normally generate profits for the organization.
- Embezzlement (e.g., misappropriation of money or property, and falsification of financial records to cover up the act).
- Espionage, including research and development.
- Intentional concealment or misrepresentation of events, transactions, or data.
- Claims submitted for services or goods not actually provided to the organization.
- Intentional failure to act when action is required by the organization or by law.
- Unauthorized or illegal use of confidential or proprietary information.
- Unauthorized or illegal manipulation of IT networks or operating systems.
- Theft.
- Acceptance of bribes or kickbacks.

Examples of fraud that benefit the organization directly include:

- Misrepresentation of financial or nonfinancial data, including the valuation of transactions, assets, liabilities, income, or statistical data (particularly in mergers and acquisitions).
- Transfer pricing (i.e., the valuation of goods exchanged between related organizations) that enables management to improve results to the detriment of competing organizations.
- Related-party activities whereby one party receives some benefit not obtainable in an arm's-length transaction.
- Failure to record or disclose significant information accurately or completely, which may present an enhanced, but false, representation of the organization to outside parties.
- Sale or assignment of fictitious or misrepresented assets.
- Intentional failure to act when action is required by the organization or by law.
- Material misstatement of financials or other compliance activities to improve stock price, gain a competitive edge, or reduce taxes owed or fines due.
- Business activities that violate government statutes, regulations, or contracts.
- Illegal political contributions, bribes, and kickbacks provided to customers or suppliers, or payoffs to government officials or their intermediaries.

Appendix D. Potential Red Flag Words to Consider

The following table provides examples of interviewee word choices that may raise an internal auditor's skepticism in certain circumstances or context, thereby warranting additional probing.

Potential Red Flag Words to Consider		
Aggressive	Force	Reallocate
Anticipate	Fragmented	Reserves
Assume	Freelance	Revise
Challenging	Interpretation	Risky
Complex	Issue	Situational
Concern	Mask/Masking	Smoothing
Creative	Maverick	Sometimes
Cushion	Modify	Subjective
Depends	New Way	Tailored
Different Approach	Not Sure	Temporary
Difficult	Off-the-record	Transition
Disconnect	Override	Uncertain
Evolving	Possibly	Unconventional

Appendix E. Case Study: Cash Disbursements Assurance Engagement

The following case study illustrates how fraud risks could be identified and documented when planning an assurance engagement of the cash disbursements process. The case study does not cover all fraud risks in an actual cash disbursements process and is not intended to be used as a risk assessment template or program. As the characteristics of every organization differ, so do its fraud risks.

Gathering Information

While planning the cash disbursements assurance engagement, internal auditors gathered the following information:

- There is no record of prior internal or external assessments or investigations.
- Employees that have the ability to update vendor information in the vendor master file also have the ability to process payments in the system.
- Several employees have superuser access to accounts payable functions: managing the vendor master file, creating invoices, overriding approval of invoices, and updating payment information.
- Approval workflow is inconsistently applied and frequently overridden in the system.
- Disbursement reviews and approvals are inconsistently performed.
- Revenue has significantly decreased from the prior year, while operating expenses have unexpectedly increased over the same period.
- Bonuses are only awarded if financial targets are met.
- Interviews with human resources personnel revealed that the supervisor of accounts payable was accused of improper fraternization with employees that report to him.
- The supervisor is quite friendly and trusting with the accounts payable personnel.

Brainstorming Fraud Scenarios

Internal auditors documented the following information during fraud scenario brainstorming sessions.

Fraud Factors	Fraud Scenarios
Pressure	Substantial bonuses are awarded if financial targets are met.
	Some employees are concerned about limited upward mobility and/or fear losing their job.
	Bonuses may not be paid this year.
	One employee has recently been bragging to coworkers about her lavish lifestyle.
Opportunity	Duties are not properly segregated.
	Relationships between employees and management may be inappropriate. One employee has a particularly close relationship with her manager.
	Several employees share administrator login access, and the payment processing data and banking information can be altered by employees with administrator access.
	The vendor master file can be updated by all employees, and the system does not track the change history.
Rationalization	Employees may perceive favoritism and feel overlooked and resentful.
	Employees may perceive management to be fostering a negative "tone at the top."
	Improper behavior seems to be commonplace.

Assessing Fraud Risks and Identifying Controls

Internal auditors created the following fraud risk and control matrix to include in the engagement plan.

Fraud Scenario	Fraud Risk	Impact (L,M,H)	Likelihood (L,M,H)	Control
A. Unapproved vendors.	A.1 Fictitious vendors are set up in the system, which may result in fraudulent payments.	H	H	• Segregation of duties. • Periodic vendor master file review.
	A.2 Vendor addresses are replaced with employee addresses; or payment information is changed to employee bank accounts.	M	M	• Management approval is required for updates to vendor addresses and electronic funds transfer data.
B. Improper payments.	B.1 Fictitious refunds are processed for payment.	M	M	• Management approval is required for disbursements.
	B.2 Fictitious or duplicate invoice approvals are overridden in the system.	H	H	• Management approval is required before payment can be processed.
C. Collusion.	C.1 Supervisor colludes with employee to override existing controls.	H	M	• None

Incorporating Results Into Engagement Plan

After creating the fraud risk and control matrix, the internal auditors incorporated the fraud risk assessment and the preliminary findings into the cash disbursements assurance engagement plan, along with the following notes:

- Review the vendor master file with names and addresses to check for vendors that appear to be duplicates.
- Review similar vendor names with different addresses and/or payment information.
- Check vendor addresses and banking information for matches to employee data.
- Look for vendor addresses that appear to be residential or P.O. boxes.
- Review the history of invoices and corresponding payment amounts to look for duplicate invoice numbers or repeating payment amounts.
- Walk through the payment process and look for segregation-of-duties issues with respect to approvals.

Acknowledgements

Guidance Development Team

Glenn Ho, CIA, CRMA, South Africa (Chairman)
Doug Hileman, CRMA, CPEA, United States (Project Lead)
Caroline Glynn, CIA, United States
John Mickevice, CIA, CRMA, United States
Daniel Samson, CIA, United States

Global Guidance Contributors

Awad Elkarim Mohamed Ahmed, CIA, CCSA, CFSA, CGAP, CRMA, United Arab Emirates
Elastos Chimwanda, CIA, Zimbabwe
Dana Lawrence, CIA, CFSA, CRMA, United States
Barry Smit, CIA, South Africa
Dr. Gokhan Sungun, CIA, CCSA, CRMA, United States
Oliver Sznitkies, France

IIA Global Standards and Guidance

Christine Hovious, CIA, CRMA, Director (Project Lead)
Lisa Hirtzinger, CIA, QIAL, CCSA, CRMA, Vice President
Debi Roth, CIA, Managing Director
Lauressa Nelson, Technical Writer
Christina Brune, Technical Writer

The IIA would like to thank the following oversight bodies for their support: Guidance Development Committee, Professional Guidance Advisory Council, International Internal Audit Standards Board, Professional Responsibility and Ethics Committee, and International Professional Practices Framework Oversight Council.

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 195,000 members from more than 170 countries and territories. The association's global headquarters are in Lake Mary, FL. For more information, visit www.globaliia.org or www.theiia.org.

About Supplemental Guidance

Supplemental Guidance is part of The IIA's International Professional Practices Framework (IPPF) and provides additional recommended (nonmandatory) guidance for conducting internal audit activities. While supporting the *International Standards for the Professional Practice of Internal Auditing*, Supplemental Guidance is not intended to directly link to achievement of conformance with the *Standards*. It is intended instead to address topical areas, as well as sector-specific issues, and it includes detailed processes and procedures. This guidance is endorsed by The IIA through formal review and approval processes.

Practice Guides

Practice Guides are a type of Supplemental Guidance that provide detailed guidance for conducting internal audit activities. They include detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, as well as examples of deliverables. As part of the IPPF Guidance, conformance with Practice Guides is recommended (nonmandatory). Practice Guides are endorsed by The IIA through formal review and approval processes.

A Global Technologies Audit Guide (GTAG) is a type of Practice Guide that is written in straightforward business language to address a timely issue related to information technology management, control, or security.

For other authoritative guidance materials provided by The IIA, please visit our website at www.globaliia.org/standards-guidance or www.theiia.org/guidance.

Disclaimer

Copyright

October 2017