IIA Audit Tool

Fraud Risk Management Strategies

Category: Professional

Purpose: How To

The Institute of Internal Auditors

Introduction

Fraud has always been and will continue to be a key risk that organizations must account for, and a risk that internal audit must keep as a key focus in their annual plans. Although fraud attempts by bad actors have often grown more sophisticated, there remain simple, proven ways internal auditors can be leveraged to not just respond to fraud incidents, but to proactively identify fraud risk at entity and process levels.

This tool, taken from The IIA's Supplimental Guidance Practice Guide "Engagement Planning: Assessing Fraud Risk," is designed to supplement these strategies with a convenient, succinct process template that can be easily referenced in future assessments.

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.

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.

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.

Figure 2: Brainstorming Fraud Scenarios

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

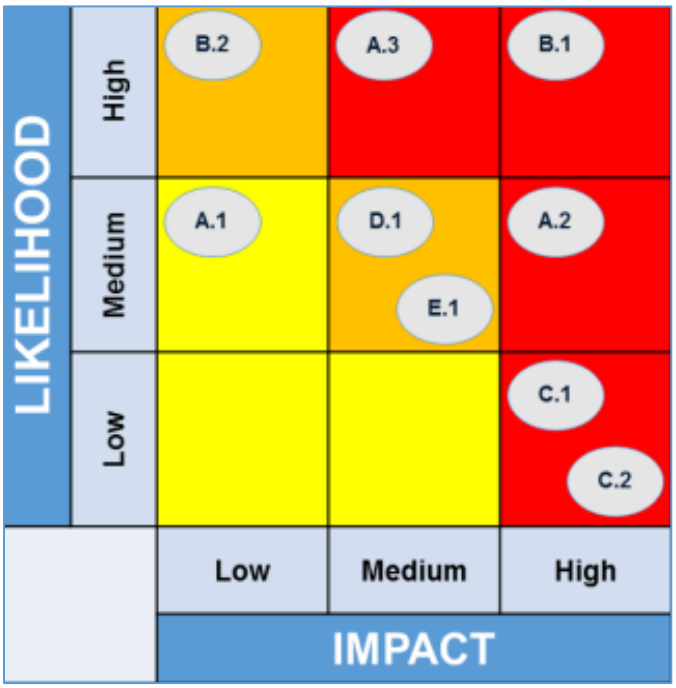
Assessing impact can be complicated because it involves both quantitative and qualitative factors. Internal auditors should account for not only the financial, operational, and regulatory impact of the potential fraud risks, but also the nonfinancial impacts, such as damage to the organization's reputation 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.

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

Figure 3: Heat Map



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.

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.

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

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.

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.

Figure 5: Significant Fraud Risks

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.

The Institute of Internal Auditors

Global Headquarters

The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA Phone:
+1-407-937-1111