Fraud: Preventing, Whistleblower Programs, Detecting, Reporting, Investigating and Managing Cases

© Copyrighted Sustainability Solutions PC, 2020

Fraud Defined

- The Association of Certified Fraud Examiners quotes Black’s Law Dictionary’s definition of fraud: “A knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment.”
- ACFE further explains that “Consequently, fraud includes any intentional or deliberate act to deprive another of property or money by guile, deception, or other unfair means.”
Fraud Defined

Rules 200.435 a (3) and 75.435 a (3) define fraud as:

“(i) Acts of fraud or corruption or attempts to defraud the Federal government or to corrupt its agents,
(ii) Acts that constitute a cause for debarment or suspension (as specified in agency regulations), and
(iii) Acts which violate the False Claims Act (31 U.S.C. 3729–3732) or the Anti-kickback Act (41 U.S.C. 1320a–7b(b)).”

Key Regulatory Requirements on Fraud

- § 200.113 Mandatory Disclosures and MSP M26
  “The non-Federal entity or applicant for a Federal award must disclose, in a timely manner, in writing to the Federal awarding agency or pass-through entity all violations of Federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the Federal award. Failure to make required disclosures can result in any of the remedies described in § 200.338. Remedies for non-compliance, including suspension or debarment.

Mandatory Provisions on Fraud

M12c of the Mandatory Provisions (303 mab)

“c. The recipient must notify the Agreement Officer immediately upon learning that it or any of its principals, at any time prior to or during the duration of this award:

(1) Are presently excluded or disqualified from doing business with any U.S. Government entity;
(2) Have been convicted or found liable within the preceding three years for committing any offense indicating a lack of business integrity or business honesty such as fraud, embezzlement, theft, forgery, bribery or lying;”
Mandatory Provisions on Fraud

M24b of the Mandatory Provisions (303 mab)

“(b) The recipient must not require its employees, subrecipients, or contractors to sign or comply with internal confidentiality agreements or statements that prohibit or otherwise restrict employees, subrecipients, or contractors from lawfully reporting waste, fraud, or abuse related to the performance of a Federal award to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information (for example, the Agency Office of the Inspector General).”

Fraud Prevalence

According to the PWC 2020 Global Economic Crime and Fraud Survey, 47% of the global organizations said they had been victim of fraud and economic crime in the past 24 months. This is the second highest reported level of incidents in the past 20 years. Below are the survey results broken down by territory.

<table>
<thead>
<tr>
<th>Region</th>
<th>2020</th>
<th>2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa</td>
<td>58%</td>
<td>54%</td>
</tr>
<tr>
<td>North America</td>
<td>52%</td>
<td>54%</td>
</tr>
<tr>
<td>Latin America</td>
<td>49%</td>
<td>53%</td>
</tr>
<tr>
<td>Middle East</td>
<td>46%</td>
<td>39%</td>
</tr>
<tr>
<td>Europe</td>
<td>44%</td>
<td>49%</td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td>42%</td>
<td>46%</td>
</tr>
</tbody>
</table>

Fraud Prevalence

According to the PWC 2020 Global Economic Crime and Fraud Survey, the table below shows the results of a survey on whether selected organizations across the globe experienced any fraud and economic crime within the last 2 years.

<table>
<thead>
<tr>
<th>Country</th>
<th>2020</th>
<th>2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>India</td>
<td>87%</td>
<td>87%</td>
</tr>
<tr>
<td>China</td>
<td>80%</td>
<td>82%</td>
</tr>
<tr>
<td>Australia</td>
<td>62%</td>
<td>67%</td>
</tr>
<tr>
<td>Brazil</td>
<td>56%</td>
<td>68%</td>
</tr>
<tr>
<td>France</td>
<td>54%</td>
<td>64%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>52%</td>
<td>62%</td>
</tr>
<tr>
<td>United States</td>
<td>50%</td>
<td>63%</td>
</tr>
<tr>
<td>Italy</td>
<td>47%</td>
<td>51%</td>
</tr>
<tr>
<td>Singapore</td>
<td>45%</td>
<td>51%</td>
</tr>
<tr>
<td>Ireland</td>
<td>51%</td>
<td>59%</td>
</tr>
</tbody>
</table>
According to the Association Certified Fraud Examiners (ACFE) 2020 Global Study on Occupational Fraud and Abuse, Nonprofit organizations can be more susceptible to fraud due to having fewer resources available to help prevent and recover from a fraud loss. This sector is particularly vulnerable because of less oversight and lack of certain internal controls.

Fraud against an organization can be committed either **internally** by employees, managers, officers, or owners of the company, or **externally** by customers, vendors, and other parties.
Internal Fraud

Internal fraud, also called occupational fraud, can be defined as: “the use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the organization’s resources or assets.”

Simply stated, this type of fraud occurs when an employee, manager, or executive commits fraud against his or her employer.

External Fraud

External fraud against a company covers a broad range of schemes. Dishonest vendors might engage in bid-rigging schemes, bill the company for goods or services not provided, or demand bribes from employees.

Likewise, dishonest customers might submit bad checks or falsified account information for payment, or might attempt to return stolen or knock-off products for a refund. In addition, organizations also face threats of security breaches and thefts of intellectual property perpetrated by unknown third parties.

In many cases, employees have been found to be assisting external parties in perpetrating fraud.

Factors that Influence Fraud

The following factors influence an organization’s risk:

- Nature of the business it is in
- The environment in which it operates
- The effectiveness of its internal controls
- The ethics and values of the company and its employees
The best and most widely accepted model for explaining why people commit fraud is the fraud triangle. This is a model developed by Dr. Donald Cressey, a criminologist.

**Motivation for Fraud**

Pressure

Opportunity

Rationalization

**Fraud Triangle**

The Fraud Triangle

Opportunity

Opportunity is the ability to commit fraud and not be detected.

- It is created by a poor design of control mechanisms and lack of controls.
- Persons in positions of authority can create opportunities to override existing controls because subordinates and weak controls allow them to circumvent the established controls.
**The Fraud Triangle**

**Pressure (also called incentive or motive)**
Pressure represents a need that an individual attempts to satisfy by committing fraud.
- Often, motive comes from a significant financial need or problem.
- Gratification of a desire such as greed or addiction is a common motive.

**Rationalisation**
Rationalisation is the ability for a person to justify a fraud. It is a crucial component in most frauds.
- Rationalisation involves a person reconciling his/her behavior (e.g. stealing) with the commonly accepted notions of decency and trust.

**The Fraud Triangle as a Tool Against Fraud**
- An excellent way to frame the problem of internal fraud is to use the fraud triangle construct.
- It is a powerful method for understanding and measuring the individual drivers of internal fraud — and an ideal springboard for focusing on ways to prevent it, holistically.
A global survey conducted by PWC revealed the following percentages of respondents who ranked the factor as the leading contributing factor to internal fraud (Source: PWC's Global Economic Crime and Fraud Surveys 2018):

**Most Common Contributing Factor to Internal Fraud**

Management must have an ongoing process that provides an organization with the tools to manage fraud risk in a manner consistent with the regulatory requirements as well as entity’s needs.

Fraud Risk Management may be broken into the following five components:
1. Fraud Risk Governance
2. Fraud Risk Assessment
3. Fraud Control Activity
   i) Fraud Prevention
   ii) Fraud Detection
4. Fraud Investigation and Corrective Action
5. Fraud Risk Management Monitoring Activities

Fraud Risk Assessments

- A fraud risk assessment is a dynamic process for identifying and assessing fraud risks that are relevant to an organization.
- The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and impact, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.
- The assessment results are recorded in the organization’s risk register, or some organizations maintain separate fraud risk registers.
A fraud control activity is an action established through policies and procedures that helps ensure that management’s directives to mitigate fraud risks are carried out. A fraud control activity is a specific procedure or process intended either to prevent fraud from occurring or to detect fraud quickly in the event that it occurs.

Fraud control activities are generally classified as either preventive or detective.

- Preventive and detective controls may be completely manual, involve some degree of computer automation, or be completely automated.
Fraud Prevention

- Fraud is costly, both in terms of reputational risk and financial losses, as well as time-consuming to identify and investigate, disruptive and unpleasant.
- In the case of deliberate acts of fraud, the aim of preventative controls is to reduce opportunity and remove temptation from potential offenders.

Prevention techniques include the introduction of policies, procedures and controls, and activities such as training and fraud awareness to minimise the possibility of fraud.

*It is worth bearing in mind though, that fraud prevention techniques, while worth investing in, cannot provide 100% protection. It is difficult, if not impossible, to remove all opportunities for perpetrating fraud.*

Management role in Fraud Prevention

Management must establish a “tone from the top” which may be demonstrated by:

- Policy and procedure manuals: define ethical behavior, acceptable and unacceptable behavior and the consequences thereof.
- Maintaining a system of internal controls: define standard operating practices, which should include segregation of duties and appropriate review.
- Effective hiring practices: clearly outline expectations of the role, perform verification of qualifications and background checks.
Management role in Fraud Prevention

Management must establish a “tone from the top” which may be demonstrated by:

- Addressing concerns or allegations promptly: follow up complaints of wrong doing, or poor employee performance promptly.
- Identification of key fraud risks: identify the areas where fraud could occur, establish appropriate authorization limits and reporting.
- Conflict of interest policy: define when a conflict is perceived to exist, and how the conflict will be resolved.

Anti-Fraud in Small Businesses

A strong system of internal controls is considered by the Association of Certified Fraud Examiners (ACFE) to be ‘the most valuable fraud prevention device by a wide margin’.

Small businesses face different types of fraud risks than larger organizations, and they also experience unique challenges in combating occupational fraud. ACFE 2020 Report to the Nations, the following was observed:

Anti-Fraud Controls in Small Businesses

- Small businesses implement anti-fraud controls at a much lower rate than their larger counterparts.
- The chart shows the data on how antifraud controls vary by size of victim organization.

Source: ACFE 2020 Report to the Nations
According to the ACFE 2020 Report to the Nations, Nonprofit organizations have fewer anti-fraud controls in place, leaving them more vulnerable to fraud. Below are the top 3 control weaknesses reported, and a comparison of how effective controls are between NPO and Other organizations.

**Anti-fraud Controls in the NPO Sector**

**Fraud Detection**
- As fraud prevention techniques may not stop all potential perpetrators, organizations should ensure that systems are in place that will highlight occurrences of fraud in a timely manner. This is achieved through fraud detection.

**Fraud Detection**
- A fraud detection strategy should involve use of analytical and other procedures to highlight anomalies, and the introduction of reporting mechanisms that provide for communication of suspected fraudulent acts.
- Key elements of a comprehensive fraud detection system would include exception reporting, data mining, trend analysis and ongoing risk assessment.
- Fraud detection may highlight ongoing frauds that are taking place or offences that have already happened.
Detection of Controls in the NPO Sector

According to the survey results shared in the ACFE 2020 Report to the Nations, the following fraud detection methods were identified in the NPO sector:

Management Role in Fraud Detection

- The day to day management supervision is the best and most effective way to detect any possible Fraud. In terms of Internal Controls, Management supervision is the “First Line of Defence”.
- Management is responsible for establishing and maintaining an effective control system at a reasonable cost. This includes designing some controls to indicate when other controls are not working effectively.

Preventive and Detective Controls - Exercise

Please indicate whether the controls listed below are preventive or detective controls:

1. Screening of potential employees during recruitment.
   
   **Please raise your hand if you believe the answer is preventive.** Keep your hand down if you think it is detective.

2. Bank reconciliations
3. Use of Closed Circuit Television Recordings (CCTV's).

Hand up preventive. Keep down detective.

4. Password and access rights

5. Asset verifications

Hand up – preventive; Keep down detective

6. Hotlines and whistleblower

7. Auditing

UP preventive: Down detective

8. Segregation of duties
Preventive and Detective Controls –
Exercise continued...
Please indicate whether the controls listed below are preventive or detective controls

9. Code of Conduct

   UP preventive: Down detective

10. Budget preparation
Leading Fraud Detection Methods

Chart breaks down the sources of tips that led to fraud detection. Half of all tips came from employees, while a substantial number of tips came from outside parties, including customers, vendors, and competitors. These findings demonstrate that anti-fraud education and the communication of designated reporting mechanisms should target not only internal staff, but external parties as well. (Source: ACFE 2018 Report to the Nation)
Internal Controls - Definition

The COSO framework defines internal control as a process, effected by an entity’s board of directors, management and other personnel, designed to provide “reasonable assurance” regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations.

Internal Controls - Definition

2 CFR 200.61 and 45 CFR 75.2 define internal controls as:
“Internal controls means a process, implemented by a non-Federal entity, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
(1) Effectiveness and efficiency of operations;
(2) Reliability of reporting for internal and external use; and
(3) Compliance with applicable laws and regulations.”
§ 200.303 and § 75.303 Internal Controls.
§ 200.303 a and § 75.303 a state:

“The non-Federal entity must:

(a) Establish and maintain effective internal control over the Federal award that provides reasonable assurance that the non-Federal entity is managing the Federal award in compliance with Federal statutes, regulations, and the terms and conditions of the Federal award. These internal controls should be in compliance with guidance in “Standards for Internal Control in the Federal Government” issued by the Comptroller General of the United States and the “Internal Control Integrated Framework”, issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).”

(b) Comply with Federal statutes, regulations, and the terms and conditions of the Federal awards.

(c) Evaluate and monitor the non-Federal entity’s compliance with statutes, regulations and the terms and conditions of Federal awards.

(d) Take prompt action when instances of noncompliance are identified including noncompliance identified in audit findings.

(e) Take reasonable measures to safeguard protected personally identifiable information and other information the Federal awarding agency or pass-through entity designates as sensitive or the non-Federal entity considers sensitive consistent with applicable Federal, state, local, and tribal laws regarding privacy and obligations of confidentiality.

For HHS/CDC/NIH, 45 CFR 75.303 is effectively the same as 2 CFR 200.303

Overview of Internal Control Systems

Achieving objectives through internal control

Objective Identified → Controls designed → Controls in place → Objective achieved

Possibly!
Limitations of Internal Control

- **Judgment**
  The effectiveness of controls will be limited by decisions made with human judgment under pressures to conduct business based on the information at hand.

- **Breakdowns**
  - Even well-designed internal controls can break down.
  - Employees sometimes misunderstand instructions or simply make mistakes.
  - Errors may also result from new technology and the complexity of computerized information systems.

  *Judgment and Breakdown limitations are usually easy to detect, as there usually is no effort to conceal the act. No fraud is intended to be committed.*

- **Collusion**
  - Control systems can be circumvented by employee collusion. Individuals acting collectively can alter financial data or other management information in a manner that cannot be identified by control systems.
  - The control effect of segregation of duties may be easily negated by collusion.
  - Frauds through collusion are difficult to detect because it is easier to circumvent controls and conceal the fraud for long.

  *From the ACFE global survey conducted on the number of perpetrators in the schemes related to occupational fraud, the results on the next slide were obtained (Source: ACFE 2020 Report to the Nations)*
Notes:
Fraud losses rose significantly when more than one fraudster was involved in a scheme.

One likely explanation is that many anti-fraud controls work on the principles of separation of duties and independent checks. When multiple perpetrators conspire in a fraud scheme, they can circumvent the system of independent verification that might otherwise detect fraud.

Limitations of Internal Control

- **Management override**
  - High level personnel may be able to override prescribed policies and procedures for illegitimate purposes with the intent of personal gain or an improperly enhanced presentation of a company’s financial condition or compliance status.
  - This type of fraud may be difficult to detect due to management’s familiarity with the day to day operations, their high levels of authority and, in some cases, their input in designing and implementing controls.

  From the related to occupational fraud, the results on the next slide were obtained (Source: ACFE 2020 Report to the Nations)
  ACFE global survey conducted on the perpetrators’ levels of authority

Management Override

Notes:
While owners/executives only committed 20% of the frauds in our study, the schemes committed by these individuals resulted in a median loss of USD600,000.

This correlation likely reflects the fact that high-level fraudsters tend to have greater access to an organization’s assets than low-level personnel. They may also have greater technical ability to commit and conceal fraud, and they might be able to use their authority to override or conceal their crimes in ways that low-level employees cannot.
Fraud Investigation and Corrective Action

- Control activities cannot provide absolute assurance against fraud. As a result, the organization's governing board ensures that the organization develops and implements a system for prompt, competent, and confidential review, investigation, and resolution of instances of non-compliance and allegations involving fraud and misconduct.

- An organization can improve its chances of loss recovery, while minimizing exposure to litigation and damage to reputation, by establishing and carefully preplanning investigation and corrective action processes.

Fraud Investigation and Corrective Action Cont...

- The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.

Why perform investigations

- Where there is suspected fraud, an internal investigation must be undertaken to:
  - determine the facts;
  - consider what, if any, action should be taken against those involved;
  - quantify the losses (for insurance, tax and other purposes);
  - consider what may be done to recover any loss incurred; and
  - identify any system weakness and look at how internal controls could be improved to prevent a recurrence.
After investigation

- After proper investigation, the Company will take legal and/or disciplinary action in all cases where it is considered appropriate.
- There has to be consistent handling of cases without regard to position or length of service of the perpetrator.

Benefits of Sharing Information and Communication

- Convey a clear message about the corporate culture
- Set expectations about ethical employee behavior
- Remind employees about their roles and responsibilities for maintaining an ethical work environment
- Maintain awareness of reporting mechanisms available to employees
- Reinforce the ramifications of improper or unacceptable behavior in order to deter others from similar actions

WHISTLEBLOWER PROTECTION

The Grantee must:

- Inform its employees working under this award in the predominant native language of the workforce that they are afforded the employee whistleblower rights and protections provided under 41 U.S.C. § 4712; and
- Include such requirement in any subaward or subcontract made under this award.
WHISTLEBLOWER PROTECTION Cont...

41 U.S.C. § 4712 states that
- An employee of a Grantee may not be discharged, demoted, or otherwise discriminated against as a reprisal for "whistleblowing.”
- In addition, whistleblower protections cannot be waived by any agreement, policy, form, or condition of employment.
Whistleblowing is defined as making a disclosure "that the employee reasonably believes" is evidence of any of the following:

WHISTLEBLOWER PROTECTION Cont...

- Gross mismanagement of a Federal contract or grant;
- A gross waste of Federal funds;
- An abuse of authority relating to a Federal contract or grant;
- A substantial and specific danger to public health or safety; or
- A violation of law, rule, or regulation related to a Federal contract or grant (including the competition for, or negotiation of, a contract or grant).

WHISTLEBLOWER PROTECTION Cont...

To qualify under the statute, the employee’s disclosure must be made to:
- A Member of the U.S. Congress, or a representative of a U.S. Congressional Committee;
- A cognizant U.S. Inspector General;
- The U.S. Government Accountability Office;
- A Federal employee responsible for contract or grant oversight or management at the relevant agency;
- A U.S. court or grand jury; or,
- A management official or other employee of the Grantee who has the responsibility to investigate, discover, or address misconduct.
From a survey done by ACFE, with results in the ACFE 2020 Report to the Nations, the following mechanisms were identified to have been reported by organizations.

The findings indicate that whistleblower’s preferred methods of reporting fraud may be shifting, particularly toward online and in electronic written form.

---

In approximately 33% of cases where a tip was made, the whistleblowers did not use a formal reporting mechanism. Instead, they reported their suspicions directly to supervisors, investigators, or other interested persons.

Thank you very much for your active participation and time!
Instructor:

Doug Franke
doug.franke@sustainabilitysolutions.co.za
+27824442894

Scholarship link:
https://www.surveymonkey.com/r/ASAPHealthManagerSurvey

Please direct any questions to
ASAPtraining@foundation.co.za.

----------

FINAL WEBINAR
QUESTIONS

----------