

## 3.3 Identify Red Flags

### Session Overview

This session forms part of the process of detecting fraud and corruption wherein we will have an understanding of fraud indicators or popularly known as red flags. The red flags give the auditors a clue of a possibility of fraud. In the previous session we studied the fraud and corruption detection process, risk assessment of fraud in each major area. In this session we would be referring to those identified major areas and study the different types of red flags found in each high risk area. During this session we shall also see what types of frauds are commonly found in each major area.

### Learning Objectives

Given list of red flags, ASOSAI Guidelines, exercise and case study, participants will be able to identify red flags in major areas of fraud and possible types of fraud or corruption in these major areas to the extent that they are in accordance ASOSAI guidelines and other best practices, as evaluated by instructors.

#### 1. Introduction to Fraud Indicators- Red Flags

Fraud indicators are best described as clues or hints that a closer look should be made at an area or activity. Generally there are two approaches that the person who is intent on committing fraud will consider,

- The activities for committing the fraud either be completely covert or hidden from view ,
- Or they may be conducted in open, completely obvious to all, but disguised to appear as if they are part of the normal operations.

The selection of any one of the above approaches by the perpetrator depends on the skill, experience, inclination of the perpetrator and the level of internal controls in the organization. In the first case when a possibility of fraud is detected, it may be much easier to determine what is going on because red flags can be easily found and a fraud can be established. Whereas in case of the second approach, if well done, may be much more difficult to decipher as red flags will not be so obvious or complex. Auditors should undertake further work and seek explanations for any red flags identified and should avoid making quick conclusions that wrongdoing or fraud exists. It is not necessary that the way wrongdoing and fraud has been carried out is complex and cleverly concealed; start with the simplest explanations first. If the evidence still warrants, tests can be developed and carried out for more complicated scenarios.

One more element is worth noting with regard to potential indicators of fraudulent activity. The auditor must know the industry, the system, or the field and must establish what are accepted practices. It is hard to spot an aberration when the auditors don't know the norm. It is difficult, if not almost impossible; to detect a well designed

fraud if the auditor does not know what he/she is looking for. Therefore the auditor should bear in mind that a fraud indicator may or may not be significant, depending on what it is, what other indicators are present and the context of the organization's transactions. The more red flags there are, the greater the risk that wrongdoing and fraud have occurred. Auditors should seek straightforward explanations for red flags. They should not assume that discrepancies indicated by a red flag might not appear significant in themselves, but that an accumulation of small differences is often indicative of a material wrongdoing or fraud.

Although poor management's decisions or negligence may give rise to possible indications of fraud, the difference between fraud and negligence is a fine line called intent. What fraud indicators/red flags can do is to point the way for further detailed inquiry. The intent in a financial fraud is to divert or misdirect assets or information, while preventing the disclosure of fraud. These two requirements often cause a trail of irregularities to be left behind. These irregularities may serve to alert the auditors.

Intelligent information gathering becomes crucial to fraud detection. Auditors must make sure that their focus is not biased by assumptions about people or events or by "inside" information provided by interested parties. They must remain independent and objective, and consider all possible interpretations of events. In many cases, wrongdoing and fraud come to light because of whistleblowers or complainants within the organization who are aware of what is happening. All disclosures or complaints received on inappropriate activities should be taken seriously and reported to the authorities concerned.

## 2. Definition of red flags

The term "**red flag**" refers to anomalies, unusual events, a signal that informs or indicates, announces or communicates that something is different from the norm or the expected activity. These anomalies are symptoms or indicators that have been associated with irregularities and fraud in the past. Auditors should therefore be aware of red flags, know when to use them and understand their strengths and limitations.

A complaint or disclosure received regarding an inappropriate activity is by itself a red flag. The auditors should request a list of the complaints or allegation disclosures received from their auditees to assist them in assessing the risk of irregularities, wrongdoing and fraud. The auditor should also request and review articles on their auditees relating to irregularities, wrongdoing and fraud previously published. The auditor should also review complaints or allegation disclosures received by the SAI on the entity being audited.

The auditor should remember that a red flag does not always indicate irregularities, wrongdoing and fraud, and a red flag list cannot be all inclusive. The presence of one or more indicators should alert the auditor to the possibility of irregularities, wrongdoing and fraud. While red flags might be present, irregularities, wrongdoing and fraud might not be. The auditor should avoid jumping to conclusions that irregularities, wrongdoing and fraud exist. They should also not disregard the symptoms without proper verification and explanation.

## 2. General red flags

According to ASOSAI Guidelines on Fraud and Corruption Clause # 2.28, the High risk areas have been identified for the purpose of making the auditors aware of the areas which are most prone to frauds in the ASOSAI member countries. The detailed red flags pertaining to each major area may be seen at the Appendices A to F, to these notes but here we take a look at the general red flags which apply to all entities and all areas. The following are some general examples and detailed descriptions of red flags of fraud and corruption:

- **Weak ethical practices.** Senior management sets a poor example for employees to emulate. A code of ethics policy may not exist.
- **The employees take no long vacations and are posted on the same position for more than the normal tenure time.**
- **Inadequate review process.** If there is inadequate review processes the likelihood of an increase in irregularities and fraud increases.
- **Approval fails to meet standard or normal approval processes.** Exceptions to approval processes should be reviewed to determine why these were processed differently.
- **Non-compliance with authorities.** Entity does not comply with government acts and statutory regulations.
- **Conflicting evidence.** When supporting documentation is in conflict with management's or employees' response to inquiries, the transaction should be considered suspicious.
- **Internal controls that are not enforced or are overridden by management.** When management frequently overrides key internal controls or does not enforce the controls, this may suggest a pattern that indicates possible wrongdoing and fraud.
- **Information is provided to the auditor unwillingly or following unreasonable delays.** Failure to respond to information requests in a timely manner raises suspicion about the integrity of the transaction; delays could enable the perpetrators to create fictitious documentation to support the requested transactions.
- **Missing documentation.** The absence of invoices, delivery receipts or consultants' products may indicate that a payment was made for goods that had not been received or services that had not been provided. Missing signed approval forms for invoices, contracts, or grants and contribution awards may indicate that appropriate approvals had not been obtained.
- **Only photocopies, faxes or scanned documents are available.** Auditors should review original documentation for proper examination. If only photocopies, faxes or scanned documents are available, this could indicate that originals do not exist or portions of original documents are being hidden from management or auditors or original documents were altered through the photocopying, faxing or scanning process.
- **Alterations and discrepancies in documentation.** Documents should be considered suspicious when an addition, deletion or variation has been made to the original content. Alterations may include erasures, opaque or obliterated

entries, the addition of new last letters or numbers, the distortion of patches over existing content. In the case of typed or printed text, changes may include adding or deleting sections after the original document has been approved and signed. Payment information that is different from the supporting documentation, for example a new amount or a different name of the payee, should raise questions with the auditor.

- **Bogus documents or fictitious invoices.** When a document's origin cannot be identified or it contains suspicious content, it is most likely fraudulent. Signs of fraud may include using more than one typewriting style, font or typeface, and inconsistent spacing of data. Invoices that do not contain a street address, postal code or telephone number are questionable and need to be investigated. An invoice with only a post office box number for an address or without a goods and services tax registration number and tax amounts may indicate fraud.
- **Hand-written documents are provided instead of computerized documents.** In cases where one would normally expect to find a computerized document, a hand-written document may indicate a fictitious document.
- **Incorrect or revised versions of key documents.** Auditors should ensure they have the final version of contracts and agreements to ensure a proper review. They must also watch out for substituted or missing pages in long documents.
- **Fictitious contractor or supplier.** Invoices from a company with a name that is similar to a legitimate vendor name may be fictitious.
- **Transactions that are not processed through the normal accounting process.** Failure to follow normal accounting processes should be looked at to determine why these transactions have been processed differently. Such practices could suggest a pattern of irregularities.
- **Transactions not recorded in a complete or timely manner.** Transactions that are not completed in a timely manner or are improperly recorded as to classification or accounting period may indicate irregularities.
- **Odd, unusual or different transactions.** Transactions that do not make sense or are out of the ordinary need to be examined thoroughly by the auditor. Transactions that are peculiar in the time of day or week, in frequency (too many or too few), in place (too far or too near) or in amount (too high, too low, too consistent or too different) may be suspect.

## 4. Commonly found Frauds in Major Areas.

### 4.1 Contracts (Procurement, Service and Construction)

The following are common methods of perpetrating contract fraud,

- **Bribery and kickbacks**—a contractor gives a government employee money, gifts, or other favors in order to obtain business or favorable treatment.
- **Change order abuse**—changes are made to the original contract conditions, resulting in a need for more funds than were provided in the original contract.

Change orders may be issued throughout the life of the contract to compensate a contractor who initially submitted a low bid.

- **Collusive bidding, price fixing, or bid-rigging**—a group of prospective contractors may make an arrangement to eliminate or limit competition
- **Co-mingling of contracts**—a contractor bills for the same work under more than one contract.
- **Conflict of interest**—contracts are awarded to organizations that employ government employees or their families, or to companies in which government employees or their families have an undisclosed financial interest.
- **Defective pricing**—a contractor submits inflated invoices that do not comply with the costs/prices specified in the contract.
- **Duplicate invoices**—a contractor submits separately two copies of the same invoice and is subsequently paid twice.
- **False invoices**—a contractor submits invoices for goods that have not been delivered, or the invoice does not reflect the contract terms.
- **False quality and performance representations**—a contractor makes false representations about the quality of the products to be supplied or qualifications to perform the requested services.
- **Information disclosure**—a government employee releases unauthorized information to a contractor to assist that contractor to win the contract
- **Local purchase order abuse or split purchases**—the total cost of purchasing goods and services exceeds the local authority limit, or a competitive process is required to provide such goods or services. To bypass these rules, the purchases are split into two or more segments.
- **Phantom contractor**— a contractor submits an invoice from a nonexistent company to support fictitious costs contained in a government cost-plus contract.
- **Product substitution**—a contractor fails to deliver the goods or services as specified in the contract. The contractor may substitute an inferior product without informing the government.
- **Progress payment abuse: front-end loading or advance payment**— under government contracts, payments are made as work progresses. The payments are based on the costs incurred, the percentage of work completed, or the completion of particular stages of work. Progress payment fraud normally includes falsified certification of the work completed in order to receive payments prior to the work being done. The contractor may inflate the costs of the initial work so that, when the percentage of completion billing method is applied; the contractor would receive higher cash flows relative to the actual work completed. The cost of subsequent contract work would be understated with the anticipation that change orders would be approved for additional compensation.
- **Purchases for personal use**— a government official purchases items for personal use, or makes excess purchases of which some items are diverted for personal use.
- **Short bidding time limits**—the lead-time for responding to a proposal is unusually short so that only bidders with inside knowledge will be able to

prepare a proposal on time. There is no compelling reason to justify a markedly reduced response time.

- **Tailored specifications**—a government official establishes unnecessary or highly restrictive product specifications that only one contractor can meet.
- **Unnecessary purchases**—goods or services that have been previously purchased are purchased again when there is no additional need.

## 4.2 Revenue collection

The following are the frauds commonly found in the area of revenue collection

- **False disclosure**—an organization makes false disclosures to the government to maximize its profits.. The organization submits false information on the quantity and quality of the resources to minimize the taxes it must pay. The organization submits false information concerning the revenues earned from its commercial application
- **Theft of revenue receivable**—an employee steals a payment of revenue received. Or an employee enters only part of the payment of revenue received in the accounting records and pockets the difference. To avoid being detected, the employee posts B's payment to A's account, C's payment to B's account, etc. This process, called lapping, requires continuous manipulation and monitoring of many accounts and transactions.
- **Revenue receivable write-offs**—an employee writes off as uncollectible, revenue receivable that are not really in arrears or will likely be collected. This is done to conceal the theft of accounts receivable payments or the future theft of payments.
- **Bribery or kickbacks**—an individual gives a government employee money or gifts in order to receive preferential treatment. For example, an individual gives money to a government employee to obtain surplus Government assets at a low price.
- **Conflict of interest**—a government employee has an undisclosed personal interest that may affect, or be perceived to affect, his/her independence and objectivity in carrying out his/her job responsibilities. In the context of revenues, a government official sells goods or services to a company that employs his/her spouse at lower prices or collects less revenue from an industry on favourable terms than those that could have been negotiated with another company.
- **Disposal of assets for personal gain**—a government employee with a personal interest in government assets could identify those assets as surplus goods even though they still have a government purpose. The sole reason the employee identifies those assets as surplus is to purchase them for personal benefit.
- **Information theft**—a government employee releases information to a third party without charge when the information should have been sold.

## 4.3 Asset management (Cash & Inventory)

The types of assets frauds include:

- **Employees take assets for personal use**—an employee misappropriates an organization’s assets for his/her personal use without attempting to conceal the theft in the organizations books. Or, an employee sells assets for cash without recording the disposal.
- **Assets are sold at less than fair market value**—assets are sold or disposed of at less than fair market value to someone related to an employee. Or, asset disposal may be recorded at a value less than what was received, and the employee misappropriates the difference.
- **Asset requisitions and other documents are used to move assets to another location to facilitate theft**—an employee overstates the amount of supplies and materials needed for a project and takes the excess. Or, false shipping documents are used to ship assets to the employee or to an accomplice.
- **Purchasing and receiving functions are manipulated**—an employee receiving goods on behalf of the organization falsifies incoming shipments and takes part of the shipment.
- **Shipment of excessive quantities to a third party, who then declares bankruptcy.** This is common fraud found in the area of asset management
- **Large unexplained inventory shortage**, particularly of inventory that has resale value. This is a symptom of employee theft of assets .
- **Non Existent inventory pledged as collateral**

#### 4.4 Program management

- **Conflict of interest**—having undeclared private interests that could affect, or be perceived to affect, the independence and objectivity of an individual in carrying out official duties. For example, a government official recommends that a program be funded by the government where his relatives be in the management
- **Embezzlement**—taking money that has been lawfully received and using it, without the knowledge and consent of the provider of the funds, for other purposes.
- **False representation**—knowingly making false or misleading statements to gain an improper advantage. In the context of program management, this could involve making false statements to mislead the government in order to obtain funding.
- **Fraudulent concealment**—knowingly hiding information that is necessary and important to the funding decision and program monitoring.
- **Improper or unusual approval authorities**—those approving funding applications do not have the require delegated authority. Or senior officials, who would not normally be involved in the approval process, take a special interest in the approval of the funding application of a program and its subsequent management.
- **Questionable or fraudulent performance reporting**—a funding recipient does not submit all the performance information required by the agreement Or the quality and completeness of the performance is so poor that there are suspicions about how funds were used. Minimum or no performance

information may indicate that government funds were diverted to other unauthorized projects or used for personal benefit.

#### 4.5 General expenditure (Payroll, expense and credit cards)

The commonly found frauds in Payroll accounts are,

- **Overtime abuse**—employees are responsible for approving their own overtime without supervisory oversight. Sometimes supervisors and employees collude in overtime abuse by splitting the overtime payments.
- **Overpayment**—an employee is paid at a higher rate of pay than he/she is entitled to and does not disclose the errors.
- **Annual leave cash out**—an employee cashes out his/her annual leave, even though he/she took leave throughout the year but did not submit leave notices.
- **Severance pay**—an employee receives severance pay even though he/she is still working for a department, or is ineligible.
- **Ghost employees**—a fictitious employee is put on a department's payroll, and payments for that employee are deposited into the perpetrator's bank account or the account of one of his/her family members. With electronic payroll deposits, it is more difficult to uncover ghost employees.
- **Terminated employees are not deleted from the payroll system**—Payments continue to be made to terminated or retired employees, those who have resigned, or those who are on medical leave. Payroll payments are deposited into the perpetrator's bank account or the account of one of his/her family members.
- **Employment insurance fraud**—false records of employment are issued to an employee so that he/she can meet the eligibility requirements of the employment insurance program.
- **Staffing and classification abuse**—managers who are behaving inappropriately may gain the cooperation of their staff by reclassifying positions to higher salary levels or changing casual or term positions indeterminate positions.
- **Personal expenses are submitted as business expenditures.** An employee submits personal expenses such as computer accessories, automobile fuel purchases, or personal meals as business expenses.
- **Expenses are submitted twice.** An employee is reimbursed more than once for the same expenses or items that have been purchased and paid for by the entity, and also claimed in an expense report or claim. For example, the government may prepay an expense such as an airline ticket. The ticket is changed and a new ticket is issued for a nominal charge; the employee submits the total charges of the revised airline ticket for reimbursement.
- **A claim for expenses that someone else paid for is submitted for reimbursement.** For example, three government employees share a taxi and all three submit the taxi fare on their expense reports. Or, a meal already paid for under a hospitality expense or conference is subsequently claimed by an employee as part of his/her daily meal allowance.

- **A false claim for automobile kilometre charges is submitted.** An employee submits a claim for automobile kilometres that is higher than the actual kilometres driven.
- **An invoice is submitted for an item that was returned for a refund.** For example, an employee submits a copy of the purchase invoice for a computer accessory, when a refund for the item was subsequently received.

For credit cards the following are the commonly found frauds,

- **Personal purchases**—a government employee cardholder purchases goods or services for personal use on their government credit card, without authority to do so, and allows the department or agency to pay for these goods or services without reimbursing the employer. This fraud can go undetected if the goods and services appear to be normal government purchases such as computers, automobile fuel, and travel and hospitality expenses.
- **Unauthorized billings**—an individual who, intentionally and without the cardholder's knowledge, permits the billing of personal or nongovernment items on a government credit card and does not reimburse the government for these purchases. This fraud is often undetected if the government cardholder does not verify all charges on the credit card statement before authorizing the payment of the outstanding balance.
- **Unauthorized charges by retailers, wholesalers, and contractors**—in this kind of fraud, businesses will process charges against government credit cards for goods and services that were never authorized or never provided. This kind of fraud also includes inflating charges on government credit cards that do not reflect the agreed upon amount for the goods and services provided. This fraud goes undetected if the government cardholder does not verify all charges on the government credit card statement against invoices or purchase orders and permits the outstanding credit card balance to be paid.

#### 4.6 I.T environment

The frauds committed in IT environment are,

- **Altering or falsifying computer input** transactions to conceal problems
- such as misappropriation of funds or assets;
- **Implementing computer program changes for personal gain** e.g. an employee manipulating systems to have payments made to himself/ herself
- **Stealing computer data** and selling it to third parties;
- **Direct computer file changes** by an employee for his/her benefit;
- **Transferring funds electronically** and subsequently destroying the audit trail; and inappropriately accessing computer information that can be used to commit an illegal activity (e.g. a person hacks into a government computer server and views confidential information that will be publicly announced shortly which will impact on share values of certain publicly traded companies and uses this confidential information to make gains on the stock market.

Commonly found internet fraud include,

- **Theft of funds through false Government Online applications;**
- **Identity theft** or using such stolen identity through the Internet;
- **Illegal use of government credit card numbers** for purchases on the Internet;
- **Selling on the Internet**, products or services that do not exist;
- **Stealing data via the Internet** for personal benefit or selling it to third parties;
- **Sabotaging computer systems**, including planting viruses and worms by hacking into computer systems via the Internet, which affects network downtime and destroys valuable computer information;
- **Sending endless SPAM** to government Web sites

## Summary

Identifying red flags is very crucial for the process of fraud detection and in the session we discussed in detail the red flags pertaining to different high risk areas, contracts (procurement, service and construction), revenue collection, program management, asset management, general expenditure and IT environment. The commonly found frauds in each high risk area were also categorized to enable auditors to be aware of the possible frauds.

## References

1. Management Antifraud Programs and Controls, USAID Fraud Indicators.
2. Wrongdoings and Fraud Audit Guidance, Office of the Auditor General of Canada, 2005. Reproduced with the permission of the Minister of Public Works and Government Services, Canada, 2005.
3. O' Gara, John, Corporate Fraud, Case studies in Detection and Prevention, 2004, first edition, John Wiley & Sons.
4. Fraud Examiners Manual, Volume I, 2005 US Edition, Association of Certified Fraud Examiners.