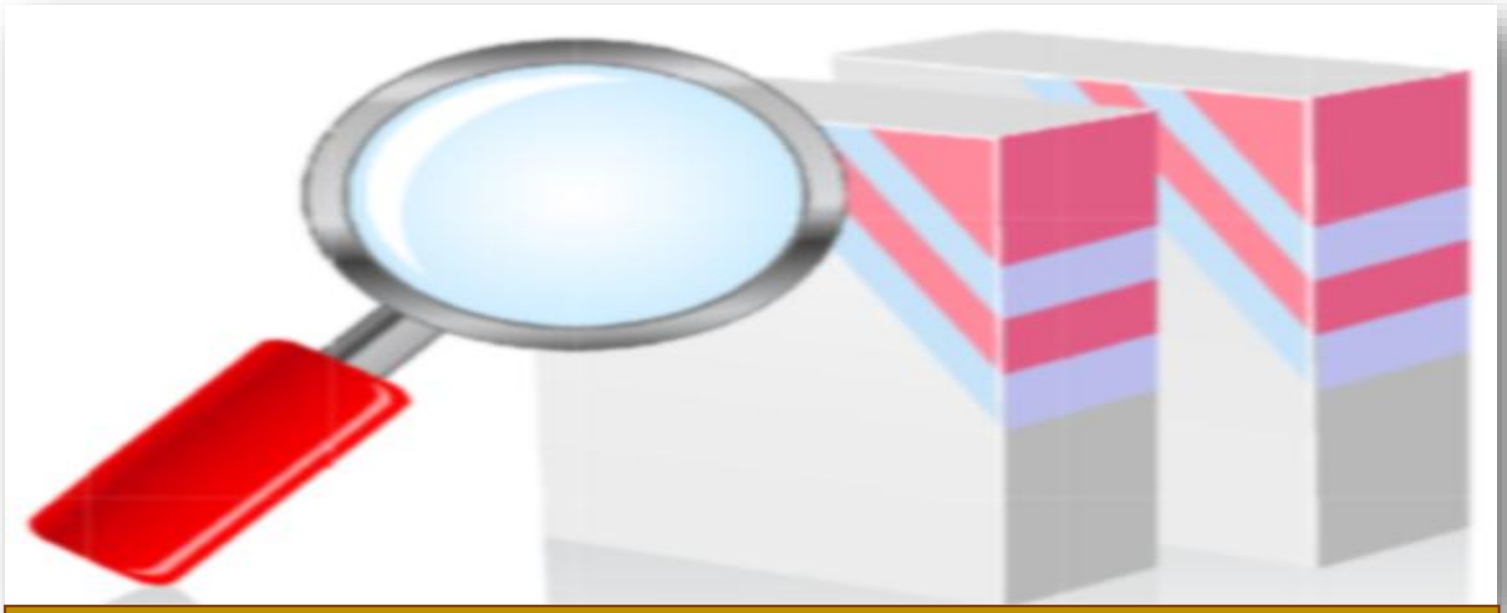


Fraud Risk Assessment

Learning Outcomes

By the end of this unit the learner will be able to:

- ✓ Define Fraud Risk Assessment
- ✓ Describe the factors involved in Risk Assessment
- ✓ Identify Risk Assessment Best Practices

Fraud Risk Assessment

Fraud risk assessment depends on the investigator's knowledge of fraud concepts, such as the fraud triangle, fraud indicators, fraud schemes and accounting information systems, and an understanding of the fraud environment, which includes timeframe, entity, efficacy of internal controls, etc. Effective risk management, as opposed to a point-in-time risk assessment, is a continuous process. This unit deals with risk assessment concepts and tools that help in the process of risk management. While most of these tools and concepts are applicable in internal investigations, they might also be used during external fraud inquiries.

A risk assessment process should also take into consideration the various fraud schemes that may occur during the process of an anti-fraud program. Countermeasures intended to detect and prevent are most effective if they are able to deal with the fraud schemes most likely to occur. For example, in financial statement frauds, the executives of the company are the ones most likely to commit fraud; therefore, a risk assessment process should take them into consideration. Similarly, in asset misappropriation cases, a trusted employee will be the most likely culprit. Corruption cases may involve a trusted employee as well as someone on the outside who is colluding with the internal fraudster. Productive brainstorming among cross-functional teams and statistics from Report to the Nations provided by the Association of Certified Fraud Examiners may help with risk assessment.

Risk Assessment Factors

Probability (the likelihood of an event occurring) and impact (the magnitude of the event) form the foundation of risk assessment. Although these concepts are fairly simple, their application is difficult. Several questions must be answered: Which factors should be considered? How might risk be measured precisely? Which tools will help in risk assessment?

Risk assessment factors can be considered on different levels such as entity, behavioural, products and services, geography, divisions, accounting and business processes, controls, computerized systems, etc. Usually, factors are initially considered at the entity level because fraud, embezzlement or theft can only be successful with the combination of executive and employee personalities, working environment, organizational culture and internal controls. After the process is initiated, different perspectives, such as the ability of management to incorporate risk management practices, should also be examined.

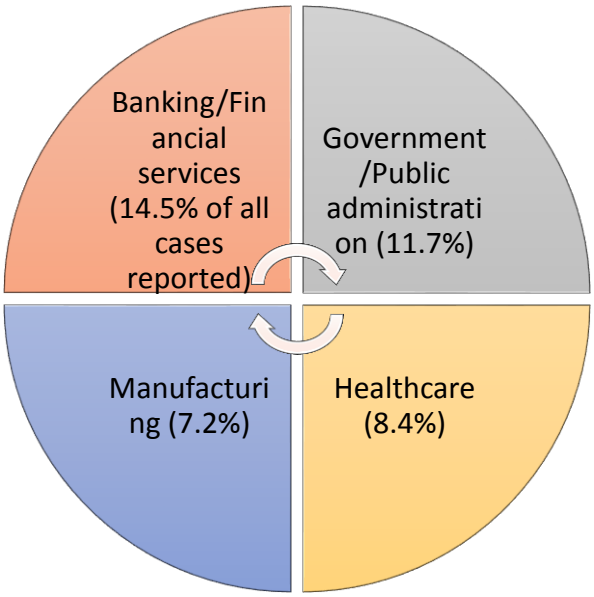
Corporate Environment Factors

According to the Association of Certified Fraud Examiners (ACFE) 2008 Report to the Nation (RTTN), when its members were surveyed regarding resolved frauds, it was revealed that 959 cases had been reported. One of the statistics concerned the industries represented in these cases. Some industries and organizations are more vulnerable to theft, fraud and embezzlement than others. While ACFE statistical results show the industries that need to hire Certified Fraud Examiners (CFE), they may also indicate different industries' susceptibility to fraud. A factor to consider while conducting risk assessment is

whether the entities working in industries that have a higher susceptibility to fraud are at a greater risk of fraud as well.

The 2008RTTN (USA) results are as follows:

Industry by Frequency:



Industry by Median Loss:

Economy is another factor to consider during risk assessment. People steal in good times, and in bad times they steal even more! In a 2008-2009 survey ACFE asked 507 CFEs to report fraud that had occurred since the beginning of the economic crisis. According to this survey, more than half of the CFEs reported that fraud had increased during the economic downturn.

Internal Factors

Internal factors that contribute to the increased probability of fraud and embezzlement are lack of monitoring activities and inadequate controls such as:

- Absence of a culture that encourages honesty.
- Inability to set and communicate performance standards and standards for personal conduct.
- Inadequate legal, ethical, fraud detection and security-related training.
- Absence of company policy regarding sanctions for financial crime and breach of security.
- Failure to provide counsel or take action against unsatisfactory levels of performance or questionable personal behaviour that violates organizational principles.
- Lack of clarity in job roles, accountability, duties and responsibilities.
- Irregular audits, inspections and follow-throughs to monitor compliance with organizational goals, policies, procedures, priorities and government regulations due to which there is a general lack of accountability in key positions.

Fraud Factors

Risk assessment should also consider fraud schemes that have the probability of occurring while guiding the anti-fraud program. For example, in financial statement fraud, executives have a higher probability of being involved, and in asset misappropriation and corruption a trusted employee is more likely to be involved. Corruption cases may also involve outsiders who collude with fraudsters working for the entity. It is important during risk assessment to take these individuals into account and take countermeasures to detect fraud.

Risk Assessment Best Practices

Without risk assessment, an entity is unable to defend itself from the risk of fraud. Management needs to take a formal, effective, and conscientious approach in order to assess risk and mitigate it. This process requires the following kind of people and strategy:

Leader(s)

The risk assessment process needs a suitable person or team. Persons with sufficient independence and the ability to carry out effective risk management are required for organizational management. These kinds of people can be found among the organization's internal audit personnel. It is vital to have someone with experience of performing effective risk assessment who has the support of the organization's board of directors and its audit committee.

Team

It is important to choose the team carefully. While it should start with internal experts and consultants, it should also involve people from a broad cross-section of the entity. This includes different levels of management. All major business units of the organization, especially accounting and sales (which are more vulnerable to fraud), all business processes, key positions, and perspectives should be represented in the team to provide high-quality risk assessment. Moreover, people who are creative, capable of reasoning logically, have an understanding of the business and the industry, and are able to present arguments in favour of the opposing side should be sought and chosen regardless of their position in the entity.

It is critical to document risk assessment because these documents might be reviewed later when risk has been assessed but not yet realized. Documents can act as learning tools for better and more effective risk assessments because the lessons learnt in previous risk assessments might be used to fine-tune future assessments. Another purpose of documentation is to hold the participants in risk assessments accountable. There are several tools of risk assessment that also serve the purpose of documentation. The checklist below is an example of how to organize risk assessment.

Frequency and Alignment with Finance

Every entity should conduct a formal risk assessment regularly, ideally every 12 to 24 months. An annual risk assessment should be synchronized with financial planning and reporting timeframes. While financial planning involves future plans and considerations overlapping finance and fraud, financial reporting includes findings such as adjustments, disclosures and control deficiencies that will require help from the Risk Management Checklist. Risk assessment is a continuous process requiring central position holders to constantly monitor and adapt to the fraud environment and refresh the process and plan for response regularly.

	Yes	No	N/A	Ref
1. Does the organization have an adequate level of **fraud awareness and are there appropriate policies to minimize fraud risk?** Specifically:				

a. Generic risk factors Has each employee been assigned a maximum ‘‘opportunity level’’ to commit fraud; has management asked itself, ‘‘What is the maximum amount in which this employee might defraud the organization, and does this represent an acceptable risk for each employee”? Has management asked itself the question, ‘‘Have we ensured that no single employee - or group of employees in collusion - can commit a fraud that would place the organization at imminent risk of collapse?’’; i.e. has a “catastrophic” opportunity level				

been assigned to each employee? As per organizational policy, can the management immediately dismiss anyone who has committed fraud? As per organizational policy, are all frauds reported to the authorities, and do they press charges? Have the reasons for all past frauds experienced by the entity been evaluated, and has corrective action been taken? **b. Managing individual risk factors by promoting** **moral behaviour and minimizing the motivation to**				

commit fraud Does the organization's mission statement include good corporate citizenship (maintaining a good standing in the community) as a goal? Is there a written code of ethical and business conduct? Are there ethical and security training programs for new employees and updates for existing ones? Does management set a clear, visible and correct example for other employees by following the mission statement, conforming to the				

code of ethics and business conduct, and following other organizational policies?				
Does corporate culture shun unethical behaviour such as hostile competitiveness with colleagues, rigid and petty policies, over-centralization of authority, etc.?				
Does the organization favour individuals of high moral character over unethical people during the hiring process?				
Are screening procedures such as background checks, psychological tests, drug tests, and lie detector test used for				

sensitive positions? Are employees with alcohol or drug abuse problems provided counselling by the entity? Does the organization maintain healthy employee relationships and fair compensation policies including salaries, fringe benefits, promotions, performance appraisals, and severance packages? Are these policies favourable as compared to competitor organizations' policies and are they successful in deterring fraud and employee disenchantment? Are employee grievances dealt				

with fairly? In order to obtain feedback on its employee relations policies, does the organization conduct exit interviews with employees who are leaving? **c. Management awareness** Does management seem aware of the possibility of fraud and how it might be committed; i.e. does it see signs of potential fraud such as drug abuse by low-paid employees who suddenly seem to have acquired wealth?				
2. Does the organization have an adequate internal control mechanism?				

Specifically: **a. Fraud integral to internal controls** Does the organization's internal control mechanism express an unambiguous need to prevent fraud? **b. Control over physical and logical access** Does the organization take precautionary fraud prevention measures such as locking doors, desks and cabinets when left unattended, especially in sensitive departments that hold valuable assets and files and documents related to personnel, payroll, cheques, customer and vendor lists,				

corporate strategies, marketing plans, and research? As per organizational policy, are passwords and IDs required to access general computers? Does the computer system require additional access information for sensitive files and applications? For instance, does each user ID have limited access and are there additional requirements such as biometrics, smart cards and temporary PINs for remote access? Does the organization ensure that access is restricted to those who need it to perform their jobs and prohibit the loaning of keys to or the sharing				

of passwordswith unauthorized employees who do not have access? Are there additional computer security and electronic surveillance systems for sensitive areas? Does the organization appear to have sufficient internal controls to an unbiased observer? **c. Job descriptions** Are job descriptions written and specific in the organization? Do employees and managers adhere to their job descriptions? Is there an organizational chart that reflects				

and is consistent with employee job descriptions?				
Is there segregation of incompatible duties such as handling cash and other valuable assets, and related records?				
Is there proper segregation of the purchasing function, i.e. ensuring that the same person does not requisition goods and services, approves their payment, and accesses accounts payable?				
Is there duplication of especially sensitive duties? For example, ensuring that cheques worth over a specific amount are				

double-signed. Are annual vacations specified in job descriptions? Has the process of formulating and specifying job descriptions been integrated with the consideration to prevent fraud? **d. Regular accounting reconciliations and analyses** Are bank reconciliations carried out for all accounts? Are accounts receivable being reconciled month to month, and general ledger to sub-ledger? Are accounts payable being reconciled month				

to month, and general ledger to sub-ledger? Is there variance analysis of general ledger accounts such as budget to actual and current year to previous year? Is there vertical analysis of profit and loss accounts i.e. profit/loss as a percentage of sales, and against historical or budgeted amounts? Has there been a detailed analysis of sales and major expenses by product line and geographic territory? **e. Supervision** Are supervisors and managers aware of fraud indicators and are they alert when an unusual event occurs or when a				

supplier or customer complains about their accounts? Do supervisors and managers diligently carry out employee performance reviews by conducting account reconciliations and even (where appropriate and required) asking the employee to re-perform the task? For smaller businesses where segregation of tasks and duties is not possible, do managers closely supervise the work being performed by employees to compensate for the lack of division of labour? Are instances of management override, i.e. when supervisors or managers take charge of, alter, or interfere in				

subordinates' work, prohibited and are others aware of it as a fraud indicator? **f. Audit** Does the organization have an internal audit function? Does the internal audit function regularly monitor and perform checks to ensure the effective performance and maintenance of fraud prevention mechanisms? Are external audits performed regularly, i.e. quarterly in large organizations? Do external auditors receive the full cooperation of the management through the audit committee during audits and especially during fraud investigations?				

3. Has the organization addressed the following **fraud prevention issues?** Promoting an ethical environment Risk financing				

Risk Management Checklists and Documentation

The checklist shown above is intended to assist accountants in assessingand managing fraud risk in their own organizations and in those of their clients. All questions answered with “No” require investigation and follow-up, with their results documented. Additional documentation is for the “Ref” column to cross-reference the checklist and the source.

Fraud Schemes Checklist

Use of the appropriate taxonomy of fraud schemes is another approach to risk assessment. The ACFE fraud tree is a useful tool for determining the initial list of fraud schemes, and it may work particularly well.

The columns in this risk assessment form include:

- The fraud scheme
- Inherent risk assessment for that fraud scheme in a particular entity or business process.
- The efficacy of internal controls in minimizing and mitigating that risk.
- The ‘‘residual risk’’ (risk remaining after being mitigated by internal controls) associated with the fraud scheme in this particular entity or business process.
- Business processes that are more vulnerable to this fraud scheme, if the fraud occurs.
- Indicators and red flags that help in detecting this fraud scheme.

Different Entities to Assess

In large organizations, a single risk assessment is not enough, and it is important to conduct separate risk assessments. Different assessments and different teams are needed for each business unit, each important business process being conducted in those business units, corporate units comprising executives, and any other element or entity identified by leaders or the team. The larger the organization, the more layers that are required, such as business units rolled up to subsidiaries, leading up to corporate, where higher risks lead up to the specific unit associated with a specific risk. In large organizations, in order to assess risk at a high level accounting or business processes are more effective but are also more challenging. They not only assess risk accurately but are also easily aligned with fraud schemes. Examples include cash management, payroll, research and development, and manufacturing a product "X".

Fraud Schemes Risk Checklist

Fraud Schemes	Inherent Risk	Controls Assessment	Residual Risk	Business Processes	Red Flags
General anti-fraud					
Fraudulent statements					
Financial:					
Overstate revenues					
Timing differences					
Fictitious revenues					
Improper disclosures					
Improper asset Valuation					
Asset/revenue Understated					

Measures and Relationships

Risk is difficult to measure quantitatively. There has to be base against which to measure the impact of potential losses caused by potential fraud. The team determines, according to shared and planned criteria, a relevant and reliable indication of risk that needs to be measured. The importance and difficulty associated with the task of measuring risk reinforces the need for a diverse, organization-encompassing team capable of making informed and logical decisions during risk assessment.

Inherent Risk

Inherent risk associated with a fraud scheme is determined by the team for the entity or a particular business process. It can be expressed in percentage form or simply as high, medium or low risk. A number of factors need to be considered while measuring this risk including industry, strategy, organizational structure and market volatility.

Controls Assessment

During this process, auditors and other team members determine the controls that have been put in place to prevent fraud and mitigate the effects of a particular fraud scheme. Controls assessment is similar to the process of determining inherent risk as it can be expressed both as a percentage and a level (high, medium, low). It is important to consider that people occupying key positions in the organization, with access to internal controls, are able not only to identify weaknesses in controls but also to exploit those weaknesses and commit fraud.

Residual Risk

Residual risk can be simply calculated by subtracting the level of internal controls being used to mitigate risk from the inherent risk. There are two possible responses to residual risk: no response, as it is accepted; or action to take further preventive measures (such as purchasing insurance) in order to mitigate residual risk. In either case, the response should be documented and tracked in order to determine the organization's ability to measure and manage risk.

Business Processes

This column is used to notify the business processes such as cash, payroll, etc. that are involved in the fraud scheme. The business process owner should be appointed as a responsible party for the area; this person should also be responsible for responding to unacceptable residual risk. Measuring the aggregated number and ratings of all fraud schemes by business processes will also highlight fraud risk.

Auditors generally start with risk assessment, which (as we have seen in this section) might also be used as a tool to identify and minimize risk of fraud. Although it is not a step taken during a typical fraud audit process, it is a tool for identifying risk and segregating the most important ones. Risk assessment is a highly recommended exercise, especially for publicly traded businesses. It is also advisable for auditors

to consider these concepts in view of management's ability to manage risk for fraud prevention, detection and investigation.

Further Reading:

- ✓ ***Manning, G. A. (2005) Financial Investigation and Forensic Accounting, 2nd ed.***
- ✓ ***Golden, T.W., Skalak, S., Clayton, M. (2006) A Guide to Forensic Accounting Investigation***
- ✓ ***Singleton, T., et al. (2006) Fraud Auditing and Forensic Accounting***
- ✓ ***Silverstone, H., Sheetz, M. (2006) Forensic Accounting and Fraud Investigation for Non-Experts, 2nd ed.***