SCITECH
RESEARCH ORGANISATION

Volume 2, Issue 2
April, 2015

Journal of Research in Business, Economics and Management
www.scitecresearch.com

Financial Institutions Statements of Accounting Information Systems – Threats and Controls

[1]Dr M Moses Antony Rajendran, [2]Mrs. M. Hebsibah Paulin
[1]Associate Professor, Department of Accounting and Finance, College of Business and Economics, Wollega University Main Campus,Wollega, Ethiopia.
[2]Assistant Professor, Department of Computer Science, Government Arts and Science College, Chengalpet, Tamil Nadu, India.

Abstract

In this article it mentioned about meaning of money, Introduction of money and money system, frauds and control concepts of information technology. A long ago our human community used the barter system which means they exchange the commodity or services for their requirements of commodities and services. Though there are different sources of money has been generated in the country for the economy and welfare of the people in the country, there is a fraud system and financial statement fraud have been occurring while dealing the money.

Keywords: Accounting Information Systems; Fraudulent Financial Statements; Different types of Frauds in Finance; Finance Threads and Control.

Introduction

First let us understand the meaning of money. It is a metal, currency and soft cards which has the value for the exchanges of commodity, goods and services. A long ago our human community used the barter system which means they exchange the commodity or services for their requirement of commodity and services. For example, if they give rice they get wheat. After several centuries, the barter system has been replaced by the currency or coin system. That means they were using the different sizes, shapes and weight of gold, silver, iron and bronze for a coins and different sizes and shapes of leathers they were using it for the currencies which have had a different values for the exchange of commodity and services in different emperors in the world. After these periods, the different emperors started the paper currencies and metal coins. As we all are know that even now different governments are using the paper currencies and metal coins. Why? even some countries are using the plastic currencies and coins. Over all, the different values of currencies and coins have different values which is very useful for the exchanges of commodity and services. Due to security reasons and comfortability the paper currencies and coins have been being replaced by the soft cards i.e. electronic money using the information technology system. All of sudden changing one system of medium of currencies to another system of updated currencies is not so easy. So during the transitional stages, the system is using the different proportions of coin, paper currencies, soft card or soft money which is based on the country development nature.

As we are all know that financial institutions are major role in using the money for the promotional activities of the economy through the different markets and services. We all are also know that the country of the economy depends upon the domestic goods and services, foreign exchanges, intellectual properties and aided money. All these have a link with the financial institutions. Usually in every country we could find 5 to 10 percentage of high income people (rich), 60-70 percentage are middle income group and remaining may come under poverty or below poverty line

people. Usually investors from rich people. They give the money to the investment banking and investment banking provide the loan amount to the needy people. Though there are different sources of money has been generated in the country for the economy and welfare of the people in the country, there is a financial statement fraud has been occurring in the dealing the money.

However, there are so many fraudulent activities are involving in dealing the money by the professionals and the institutions. Now, the following information mentioned about fraud and its types.

Fraud: It means any and all means a person uses to attain the gain an unfair advantage over another person in terms of money and its related values. There are different types of frauds are occurring while dealing the money. They are,

1. Occupational Fraud

a. **Fraudulent Financial Statements:** Financial statement fraud involves misstating the financial condition of things by intentionally misstating amounts or disclosures in order to deceive users by cooking books and cute accounting. Financial statements can be misstated as a result of intentional efforts to cheat or as a result of undetected asset misappropriations that are so large that cause misstatement.

b. **Asset misappropriation:** It involves theft, embezzlement, or misuse of organization assets which has money or money value for personal gain. Example, theft of cash, fraudulent disbursements and misuses of inventory and other assets which has a money value.

c. **Bribery and Corruption:** Corruption involves the wrongful use of a positon, contrary to the responsibilities of the positon which hold. This may be bribery, illegal gratuities, economic extortion and conflict of interest with cold blood of human beings.

2. Other Thefts: It May be

a. Intellectual property theft

b. Financial institutions fraud

c. Check and credit card fraud

d. Insurance fraud

e. Healthcare fraud

f. Bankruptcy fraud

g. Tax fraud

h. Securities fraud

i. Money laundering

j. Money monkers

k. Consumer fraud

l. Computer and Internet fraud

Since, these days soft money and net banking involved in dealing the money and money value related items. We should know computer and internet fraud. Computer fraud includes, unauthorized theft, use/access/modification/copying and destruction of software or data; theft of money by altering computer records; theft of computer time; theft or destruction of computer hardware; use or the conspiracy to use computer resources to commit a felony; and intent to illegally obtain information or tangible property through the use of computers by software modifications.

Computer Fraud and Abuse Techniques:

Perpetrators have devised many methods to commit computer fraud and abuses. They are data diddling, data leakage, denial of service attacks, eavesdropping, email threats, email forgery, piggybacking, round-down technique, software piracy, spamming, keystroke loggers, Trojan horse and viruses.

Over View of Control Concepts

Internal control is the process implemented by the board of directors, management, and those under their direction to provide reasonable assurance that the following control objectives are achieved:

- Assets (including data) are safeguarded.
- Records are maintained in sufficient detail to accurately and fairly reflect company assets.
- Accurate and reliable information is provided.
- There is reasonable assurance that financial reports are prepared in accordance with GAAP.
- Operational efficiency is promoted and improved.
- Adherence to prescribed managerial policies is encouraged.
- The organization complies with applicable laws and regulations.

COSO's Internal Control Framework

The Committee of Sponsoring Organizations (COSO) is a private sector group consisting of: The American Accounting Association, the AICPA, The Institute of Internal Auditors, The Institute of Management Accountants, and The Financial Executives Institute.

COSO's internal control model has five crucial components:

Control Environment:

The core of any business is, its people. Their integrity, ethical values, and competence make up the foundation on which everything else rests. A control Environment consists of the following factors:

a. Commitment to integrity and ethical Values: It is important for management to create an organizational culture and strategy that stresses integrity and ethical values. For example top management should make it clear that honest reports are more important than favorable ones. Management should develop clearly stated policies that explicitly describe honest and dishonest behaviors.

b. Management's Philosophy and operating style: the more responsible that management's philosophy and operating different styles are, the more likely it is that employees will behave responsibly in working to achieve the organization's objective. If management shows little concern for internal controls, then employees are less diligent and effective in achieving specific control objectives.

c. Organizational structure: A company's organizational structure defines its lines of authority and responsibility and provides the overall framework for planning, directing and controlling its operations. Important aspects of organizational structure include the centralization or decentralization of authority, the assignment of responsibility for specific tasks, the way responsibility allocation affects the management's information requirements, and the organization of the accounting and information system functions.

d. The Audit committee of the BOD: The audit committee is composed of entirely of outside directors. The audit committee is responsible for examining, investigagting and overseeing the institution's internal control structure, its financial reporting process and its compliance with related laws, regulations and standards. The committee works closely with the organization's internal and external auditors.

e. Methods of assigning authority and responsibility: Management should assign responsibility for specific business objectives to specific departments and individuals and then hold them accountable for achieving those objectives. Authority and responsibility may be assigned through formal job description, employees training and operating plans, schedules and budgets.

f. Human resource policies and Practices: Policies and practices about hiring, training evaluating, compensating and promoting employees affect an organization's ability to minimize threats, risks

and exposures. Employees should be hired and promoted based on how well they meet written job requirements. Resumes, reference letters and background checks are important means of evaluating the qualification of job applicants.

g. External Influences: include regulatory requirements and financial accounting reporting requirements.

Control Activities:

Policies and procedures must be established and executed to ensure that actions identified by management as necessary to address risks are, in fact, carried out. Generally, control procedures fall into one of the following five categories:

a. Proper authorization of transactions and activities: There should be an appropriate authorization before processing. Authorizations are often documented by signing initializing or entering an authorization code on a transaction document or record. Computers are now capable of recording a digital signature, a means of signing a document with a piece of data that cannot be forged. Management may grant specific authorization or general authorization.

b. Segregation of Duties: Good internal control demands that no single employee be given too much responsibility. Effective segregation of duties is achieved when the functions authorization, recording and custody are segregated.

c. Design and use of adequate documents and records: the proper design and use of documents and records helps ensure the accurate and complete recording of all relevant transaction data. Pre-numbering, providing space for authorization are things to consider in designing.

d. Adequate safeguards of assets and records: Steps must be taken to safeguard both information and physical assets. such procedures include-effectively supervising and segregating duties, maintaining accurate records of assets, including information, restricting physical access to assets, protecting records and documents (fire proof storage areas, locked filing cabinets, offsite back up location), controlling the environment (special computer equipments should be kept in a room with adequate cooling and fire proofing), and restricting access to computer rooms, computer files and information.

e. Independent checks on performance: should be conducted by someone other than the person who is responsible for the original operation. it may include reconciliation of two independently maintained sets of records, comparison of actual quantities with recorded amounts, double entry accounting, batch totals(financial total, hash total, record count, Line count, cross footing balance test),independent review.

Risk Assessment:

The organization must be aware of and deal with the risks it faces. It must set objectives for its diverse activities and establish mechanisms to identify, analyze, and manage the related risks. the major steps in risk assessment are:

a. Identify Threats: companies can face strategic, operating, financial and information threats.

b. Estimate risk: estimate the probability of occurrence.

c. Estimate exposure: Potential loss from each threat.

d. Identify controls: that will protect the company from each threat.

e. Estimate costs and benefits: too many controls ma make the system inefficient and slow the system. The objective in designing an internal control system is to provide reasonable assurance that control problems do not take place. The benefit of an internal control procedure must be greater than its cost. However it is difficult to measure benefit. One way to calculate benefit involves expected loss: Expected loss = Risk X Exposure. The benefit of a control procedure is the difference between the expected loss with the control procedures and the expected loss without it.

f. Determine cost benefit effectiveness.

Information and Communication:

Information and communications systems surround the control activities. They enable the organization's people to capture and exchange information needed to conduct, manage, and control its operations. According to AICPA,an AIS has five primary objectives:

a. Identify and record all valid data

b. Properly classify transactions

c. Record transactions at their proper monetary value

d. Record transactions in the proper accounting period

e. Properly present transactions and related disclosures in the financial statements.

Monitoring:

The entire process must be monitored and modified as necessary. key methods of monitoring performance include,

a. Effective supervision: involves training and assisting employees, monitoring their performance, correcting errors and safeguarding assets by overseeing employees who have access to them.

b. Responsibility accounting: include budgets, quotas, schedules, standard costs and quality standards, performance reports that compare actual with planned performance and highlight significant variances and procedures to investigate variances and take timely action to correct the conditions leading to such variances.

c. Internal auditing: Involves reviewing the reliability and integrity of financial and operating information and providing an appraisal of internal control effectiveness. It also involves assessing employee compliance with management policies and procedures and applicable laws and regulations and evaluating the efficiency and effectiveness of management. Unlike external auditors, internal auditors place greater emphasis on a company's management controls. Objectivity and effectiveness require that internal audit function be organizationally independent of accounting and operating functions.

Internal controls are often classified as:

a. **General Controls:** Those designed to make sure an organization's control environment is stable and well managed. They apply to all sizes and types of systems. Examples: Security management controls.

b. **Application Controls:** Prevent, detect, and correct transaction errors and fraud. Are concerned with accuracy, completeness, validity, and authorization of the data captured, entered into the system, processed, stored, transmitted to other systems, and reported.

Internal Controls Perform Three Important Functions:

- Preventive controls: Deter problems before they arise
- Detective controls: Discover problems quickly when they do arise.
- Corrective controls: Remedy problems that have occurred by:
  - Identifying the cause;
  - Correcting the resulting errors; and
  - Modifying the system to prevent future problems of this sort.

Preventive Controls

Major types of preventive controls used for defense in depth include:

1. **Authentication Controls:** Focuses on verifying the identity of the person or device attempting to gain access. Users can be authenticated by verifying - Something they know, such as passwords or PINs,

Something they have, such as smart cards or ID badges, Some physical characteristic (biometric identifier), such as fingerprints or voice.

Although none of the three basic authentication methods is foolproof by itself, the use of two or three in conjunction, known as multi-factor authentication, is quite effective.

2. **Authorization Controls:** Restricts access of authenticated users to specific portions of the system and specifies what actions they are permitted to perform. Are implemented by creating an access control matrix.

   Specifies what part of the IS a user can access and what actions they are permitted to perform. When an employee tries to access a particular resource, the system performs a compatibility test that matches the user's authentication credentials against the matrix to determine if the action should be allowed.

   The access control matrix should be regularly updated, so that an employee who changes job duties cannot accumulate a set of rights that are incompatible with proper segregation of duties.

3. **Training:** People play a critical role in information security. The effectiveness of specific control procedures depends on how well employees understand and follow the organization's security policies. Employees should be taught why security measures are important to the organization's long-run survival.

   Employees should be trained to follow safe computing practices, such as:

   - Never open unsolicited email attachments.
   - Use only approved software.
   - Never share or reveal passwords.
   - Physically protect laptops, especially when traveling.

   Train employees about social engineering attacks, which use deception to obtain unauthorized access. It is also important to invest in continuing professional education for information security specialists. New technology developments create new security threats and make old solutions obsolete.

4. **Physical Access Controls:** Within a few minutes, a skilled attacker with unsupervised direct physical access to the system can successfully obtain access to sensitive data.

   - Special boot disks exist that, when inserted, provide the person with unfettered privileges and rights on the computer.
   - Keystroke loggers can be installed on the PC through hardware or software, which will capture every one of the authorized user's keystrokes, including his ID and password.
   - A diskette with a publicly available utility can be inserted in a PC which will instantly capture any ID number or password that has been entered on that PC, since the time it was last booted.

   a. Physical access control begins with entry points to the building itself. There should be security guards or receptionist who identifies employees and escorts visitors to their destinations.

   b. Once inside the building, physical access to rooms housing computer equipment must be restricted.

      ⇒Rooms should be securely locked.

      ⇒All entries and exits should be monitored by closed-circuit TV, if possible.

      ⇒Multiple failed access attempts should trigger an alarm.

      ⇒Rooms with servers with highly sensitive data should supplement regular locks with Card readers, Numeric keypads or Biometric devices.

   c. Access to wiring used in LANs must be restricted to prevent wiretapping. Cables and wiring should not be exposed; wall jacks not in use should be disconnected from the network.

5. **Remote Access Controls:** Installing devices like firewalls. Firewalls are designed to act as filters and only permit packets that meet specific conditions to pass.
6. **Host and Application Hardening procedures:** Every host should be running anti-virus software that is regularly updated. User accounts must be carefully managed, especially when they have unlimited (administrative) rights on the computer. Users who need administrative powers on a particular computer should be assigned two accounts:

   ⇒One with administrative rights

   ⇒One with limited privileges

   Users should log in under the limited account to perform routine duties. They should be logged into their limited account when browsing the web or reading email. If they visit a compromised website or open an infected email, the attacker will only acquire limited rights. Default accounts such as "Guest" should be disabled.
7. **Encryption:** is the process of transforming normal text, called plaintext, into unreadable gibberish, called cipher text. Decryption reverses this process. To encrypt or decrypt, both a key and an algorithm are needed.
   - Computers represent plaintext and cipher text as a series of binary digits (0s and 1s).
     - The key is also a string of binary digits of a fixed length.
   - The algorithm is a formula for combining the key and the text.
   - Most documents are longer than the key, so the computer first divides the plaintext or cipher text into blocks—each block being of equal length as the key.
   - The computer then applies the algorithm to each block of text.
   - Encryption protects the confidentiality and privacy of the transmission and provides for authentication and non-repudiation of transactions.
8. **Preventive Maintenance:** Regularly testing the system components and replacing those in poor conditions. Installing UPS, regulators etc.
9. **Disaster Recovery Plan:** enables restoration of data processing capabilities in event of major disaster. E.g. Insurance, backup data and program files.

Detective Controls

- Preventive controls are never 100% effective in blocking all attacks.
- So organizations implement detective controls to enhance security by:
  - Monitoring the effectiveness of preventive controls; and
  - Detecting incidents in which preventive controls have been circumvented
- Actual system use must be examined to assess compliance through:
  - Log analysis: Most systems come with extensive capabilities for logging who accesses the system and what specific actions each user performed. Logs form an audit trail of system access. They are of value only if routinely examined.

    Log analysis is the process of examining logs to monitor security.
  - Intrusion detection systems
  - Managerial reports: Management reports are another important detective control. Key performance indicators include Downtime caused by security incidents, Number of systems with IDS installed, Time to react to security incidents once detected.
  - Periodically testing the effectiveness of existing security procedures

Corrective Controls

Detection of attempted and successful intrusions is important but is worthless if not followed by corrective action.

Three key components that satisfy corrective controls are:

1. **Establishment of a computer emergency response team:** should be able to recognize a problem, contain the problem, and recover from damage and follow-up on how the incident occurred the existing security policy to minimize similar incidents.
2. **Designation of a specific individual with organization - wide responsibility for security:** like chief security officer who should be independent of other IS functions and should impartially assess and evaluate the IT environment, conduct vulnerability and risk assessments, and audit the organization's security measures.
3. **An organized patch management system:** Another important corrective control involves fixing known vulnerabilities and installing latest updates to:
    - Anti-virus software
    - Firewalls
    - Operating systems
    - Application programs

    A patch is code released by software developers to fix vulnerabilities that have been discovered.

Conclusion

In this millennium world there is a net banking and soft money moment of the financial instruments that is called soft cards to do the financial functions and activities. From the being of the barter system to this time the different frauds are occurring. In this computer world there are different frauds are occurring in the information technology areas especially in the banking technology. Although there are so many advantages are there it's a mandatory to avoid the different types of frauds in banking technology and a person who deals about the monetary functions in terms of soft card or soft money.

References

[1] Romney and Steinbart, (2003/6) Accounting Information Systems, 9/10th ed., Prentice Hall, USA,
[2] James A. Hall, 2002. Accounting Information Systems, 4th ed., Thomson, South-Western, NJ.
[3] Fabozzi, Frank J, Franco Modigliani, Frank J. Jones."Financial Institutions and Markets", 3rd Edition, USA.
[4] Rose, Peter S., "Money and capital markets: The financial system in an increasingly global economy". 5th Ed.