International Journal of Multidisciplinary Innovation and Research Methodology (IJMIRM)
ISSN: 2960-2068, Volume 2, Issue 2, April-June, 2023, Available online at: https://ijmirm.com

The Role of Modern Technology in Preventing and Detecting Accounting Fraud

Alabdulhadi Mohammed Abdullah[1], Albalawi Ahmed Mousa[2], Almubireek Mohammed Abdulrahman[3], Alqahtani Naif Mesfer[4], Almohsen Ali Mohammed[5], Almadhi Khalifah Salman[6], Almadhi Abdullaziz Madhi[7], Alfaez Mohammed Nasser[8]

[1,2]Accounting trainer, at TVTC Aljouf Technical College, Saudi Arabia
[3]Accounting trainer, at TVTC Hafer Albattin Technical College, Saudi Arabia
[4]Accounting trainer, at TVTC Alquwiiyah Technical College, Saudi Arabia
[5]Accounting trainer, at TVTC Dammam Technical College, Saudi Arabia
[6,7]Marketing trainer, at TVTC Hafer Albattin Technical College, Saudi Arabia
[8]Management trainer, at TVTC Alrass Technical College, Saudi Arabia

ABSTRACT

Fraud is a deliberately deceiving action designed to offer the perpetrator with an illegal gain or to forbid a right to a victim. Forms of fraud entail credit card fraud, tax fraud, bankruptcy fraud, and securities fraud. Fraud can easily be perpetrated, especially in the digital era. Hacking can be traced, but it is a tiresome process. Thus, organizations will seek to access specialized services that provide improved protection. They include fraud prevention policies as well as internal controls and audits. According to the study, the available Technical Methods and Tools That Prevent and Detect Accounting Fraud are Embedded Audit Modules, The Monitoring and Control Layer, Audit Data Warehouse, and Audit Applications Approach. Future audit techniques are likely to necessitate auditors, standard setters and regulators to initiate crucial adjustments. The modifications include transformation in the frequency and timing of the audit, increased training in analytic approaches or technology, adoption of entire society analysis rather than sampling, re-evaluation of topics like independence and materiality, and authorization of the provisioning of the audit data principle.

Keywords: Fraud, security, scam, access, Occupational Fraud, Abuse, hacking, prevention policies, risks, malware attacks, password cracking, theft, AICPA.

INTRODUCTION

Fraud is a deliberately deceiving action designed to offer the perpetrator with an illegal gain or to forbid a right to a victim. Occasionally, fraud takes place in insurance, real estate, investment, and finance. Also, it can appear in the sale of real assets, like land, personal assets, like collectibles and art, including intangible assets, like bonds and stocks. Forms of fraud entail credit card fraud, tax fraud, bankruptcy fraud, and securities fraud. A fraudulent operation can be perpetrated by an entire business firm, a group of people or an individual.

Fraud is costly in various approaches (Bowers, 2011). It ruins reputations, inflicts mental anguish and decimates retirement accounts. Investors, owners, and businesses lose billions as a result of the theft of cash among other properties, lost economic opportunities as well as devaluation. According to 2008 Report statistics from Association of Certified Fraud Examiners in the Nation, on Occupational Fraud and Abuse, U.S. firms lose about 7% or their proceeds to scam.

The figures for fraud change from one sector to the other, but they all indicate the extent of the issue: Customer fraud accounts for more than 50% of all incidents. The great percentage entails some type of data misinterpretation or massage.

Total fraud losses on UK credit and debit cards reached a peak at £360 million in 2010.

Student finance fraud expenses are approximated to be about £31 million per annum.

Telecom fraud costs about £730 million per year.

General insurance fraud losses are currently at the top at £2.1 billion per annum.

There is a common notion that charity organization loses about £1.3 billion per year to fraudsters. This is about 2.4% of their yearly income.

Motor fraud, including "staged accidents" is approximated to be £350 million per year, thus increasing the price of motor insurance.

Fraud can easily be perpetrated, especially in the digital era. Reports from across the globe reveal increasing incidents of fraud every year. Regardless of the security measures set in place, organizations are still hit by fraud owing to the online setting they are linked to. With adequate hacking skills and knowledge, nearly everyone can embezzle sensitive data or interrupt normal operations in a firm or for an individual (Rahman & Anwar, 2014). Hacking can be traced, but it is a tiresome process. Thus, organizations will seek to access specialized services that provide improved protection. They include fraud prevention policies as well as internal controls and audits.

In extreme incidents, fraud might pose risks to the survival of an enterprise itself by restricting the confidence of clients and partners have in it or by endorsing distrust in the agency.

The Impact on the Business

The key manner in which fraud can affect small enterprise is a financial loss. For instance, employees might be interfering with the general cash flow in a manner that is not easily noticeable by the owner. The businesses are increasingly becoming sophisticated, making it hard to track cash flow and bad faith lures everyone at any given time. A firm dealing with fraud cases is mostly avoided by business partners and investors. It is hard for people to deal with firms that have a bad reputation and thus cannot be entirely trusted.

This will act in favor of business competitors, thus affecting businesses negatively (Whyte, 2016). Also, brand loyalty can slow down or stop leaving the business owner with little to do especially with recurrent or serious fraud. For a start-up business, fraud will increase operating expenses and might increase bureaucracy.

In general, it causes complicated relations, loss of growth momentum and eroded confidence. Therefore, fraud triggers a rethinking of the business plan with the connected expenses in regard to time and money.

The Impact on the Company Team

Fraud impacts spirits inside the firm and can interrupt the ordinary momentum a small enterprise depends on to cultivate stability and access growth. In general, fraud is uncomfortable with any involved parties. When one of the employees is discovered to be the one behind the fraud, others might feel awful for not recognizing the risk emerging from the inside (Kronenberg, 2015). Furthermore, fraud discovered at management level can cause a detrimental impact on the spirits.

The Impact on the Company Audits

The audit becomes more complicated and hard due to fraud. Auditors will cautiously look at the firm's inventory prior to signing the financial statements and is likely to request data that is tricky to find. In rare cases, they will request for, stakeholders where accounting was sourced from and might decide to terminate the contract (Zhu et al., 2017). This implies that once involved in fraudulent activities, people will be cautious before they conduct any business with them.

The Impact On Company's Financial Credit

Most starting enterprises require bank loans in the initial years of their operations. Information regarding fraud spreads fast, thus making banks to consider the peril and asking a higher price for a loan. In various states, banks possess a common black book of firms that generate issues and complications, and it is the same case across the board (banks asking a higher price for loans).

The Key Forms of Accounting Fraud

There are three major forms of fraud namely: data fraud, fraudulent financial reporting, and misappropriation of assets (Kratcoski, 2018). Data fraud can be perpetrated by both the management and the employees. On the other hand, fraudulent financial reporting is conducted by the management while misappropriation of assets is executed by employees. In all these forms of fraud, inaccurate or misleading financial data is disseminated to the stakeholders, the public and the investors.

Data Fraud

It is an illegal storage and transfer of any data that is personal, financial or confidential in nature, including algorithms, software codes, passwords, technologies or proprietary-oriented data (Kowaleski, Cannon, Schnader, & Bedard, 2018). It is considered a serious privacy and security breach, and its impact can be stern for businesses and individuals. The general forms of data fraud include the following:

- Email- there is a common approach to transmitting data via emails.
- USB drive- via the thumb-sucking approach, the data can be transmitted to a USB drive or a thumb drive. It is regarded as the effortless approach of data fraud as the storage space of USB devices are escalating with time as the expenses rise as well.
- Portable hard drive- huge data can be transmitted via a portable hard drive.
- Printing- this is another approach used in data fraud where data is printed and unlawfully storing and disbursing the same.
- Malware attack- virus or malware attacks have the capacity to extract sensitive data.
- Remote sharing- via remote access, information can be transmitted to another gadget from where information can be disbursed.
- Data fraud is increasingly an issue for personal computer users and well established corporate organizations. Some of the most commonly used techniques of data fraud include:
- Password cracking-Hackers can access an individual's personal computer and obtain worthwhile information especially if not password-secured or has a weak password.
- Laptop theft-The world is experiencing increasing incidents of laptop theft from corporate organizations with worthwhile data stored on the computer being sold to rivals. Lack of data security and carelessness can be costly to a firm.
- Eavesdropping-Data transferred from insecure sources can easily be recorded and wiretapped. If no security approach is utilized, there is a loophole to lose the password as well as confidential data to eavesdroppers.
- E-commerce-People should ensure that their information is secure from snooping eyes when they buy or sell things online. Carelessness can result to leakage of confidential account data.

Misappropriation of Assets

This is the most prevalent form of fraud across the board and is also the effortless schemes to comprehend. Misappropriation of assets can entail issues like thievery of funds, theft of inventory, forgery of checks, services theft and payroll scheme (Hay, 2014). According to recent statistics reported, misappropriation of assets accounts for more than 91% of fraud incidents.

Although it is the common form of fraud, statistics reveal that it is the least costly racket based on per-fraud. The standard asset embezzlement expense for a firm is $150000. It is also referred to as embezzlement and occurs because of a lack of internal controls, allowing staff members to steal money from the business without being noticed. It can be perpetrated in various methods:

- Employees claim expenses of commodities that are not related to the business
- The individual in charge of payment completes the payroll. The individual can generate ghost workers to receive salaries of fictitious staff members.
- The person in charge of payment is the individual who approves payment. This can enable payment of personal items by the organization.

Misappropriation of assets is prone to take place in close-knit job settings where the internal controls are imperfect, and employees are entrusted to have general liability as compared in established firms (Krambia-Kapardis, 2016).

Fraudulent Financial Reporting

It is the least common form of fraud since it accounts for 10% of fraud incident, but is the most costly. The standard financial statement fraud will cost a firm about $2 million. The form of fraud revolves on financial statements manipulations to generate openings for an entity or an individual (Halbouni, 2015). This can entail stock price manipulation, flattering loan conditions, year-end bonuses increase, among other circumlocutory benefits from the financial statement scheme. False accounting can also entail overstating assets or revenue, to create a perception that a business worth is more, thus increasing share prices.

There is a general rule that Public Limited Firms with earnings exceeding £6.5 million to be audited to safeguard its stakeholders. Also, there are International Accounting Standards, austere policies that guide organizations on account reporting.

Other forms of fraud that a business can be exposed to include:

- Professional fraud-This occurs when a trusted advisor makes efforts to divert funds belonging to an organization for their benefit.
- Sleeper fraud-It takes place when an individual creates rapport with another to build a credit trust before they steal their money.
- Customer fraud-It takes place when an individual knowingly gives false information with an aim of defrauding other people.
- Account takeover-It occurs when an individual access other people's account data and starts utilizing it without their awareness.
- Insider fraud-It occurs when an agent, trusted adviser or colleague utilizes private data with an aim of cheating them.
- Payment fraud-It occurs when fraudulent operations are perpetrated by an individual using a lawful client's account.
- Money laundering-This is a method of disguising unlawful funds to make them appear as if they come from a lawful source.

Individuals perpetrating fraud are fully aware of data that the projected victim is not, thereby enabling the fraudster to deceive the victim. Basically, the company or individual perpetrating fraud is capitalizing on information asymmetry, particularly, that the resource expense of verifying and scrutinizing that data can be substantial to generate a hindrance to entirely invest in fraud deterrence. The federal government and the states have policies that criminalize hoax, but fraudulent proceedings might not at all times lead in a criminal trial. When fraud incidents reached the trial stage, the fraudster might be convicted or detained (Evans, 2012). In order to prove that fraud occurred necessitates the fraudster to have executed particular actions. Initially, they have to offer a false declaration as material information. Secondly, the fraudster had to have understood that the declaration was incorrect. Third, the fraudster ought to have an intention of deceiving the victim.

Fourth, the victim has to reveal that it relied on the forged statement. Lastly, the victim had to have experienced detrimental harm because of acting on the deliberately untrue statement. For instance, in 2001, a great corporate fraud was discovered at Enron, an American-based energy firm. The management utilized several approaches to disguise the firm's financial welfare, including the purposeful obfuscation of misrepresentation of incomes and revenue. Following the unmasking of the fraud, shareholders experienced a sharp decline of share prices from $90 to less than $1 within15 months. Enron staff equity was eradicated and they also lost their jobs after the company was declared bankrupt. The Enron fraud was a key contributor behind the policies stipulated in the Sarbanes-Oxley Act approved in 2002(Sewe, 2012).

Traditional Auditing

Though procedures of auditing have been depending on for a long time, the official auditing practice has existed for quite a short era. In the past fraud took long to be uncovered after its occurrence or even undetected. Owing to recent technological developments and other changes, it is vital for auditors to comprehend what the impending audit is all about and how they ought to visualize a rational progression on such a circumstance. To facilitate the understanding, it is vital to consider the evolution of auditing from its legal start in the 20th century.

The industrialization and the resulting emergence of business operations caused the extensive adoption of auditing techniques. The railway, the endeavors to control and report expenses, operation ratios, and production were key contributors of materialization of the accounting profession in the U.S. In particular, organizations understood the

significance for methods of financial accountability and fraud detection, and investors increasingly depended on financial reports as firms started to take part in the stock bazaar. Though these factors initiated an extension of the application of auditing and accounting techniques, it is the 1929 stock market crash that made auditing a compulsory procedure in U.S. The Securities and Exchange Act of 1934 developed the Securities and Exchange Commission, which was mandated to oversee auditor oversight tasks as well as dissemination of accounting principles. Various audit operations existing at this time were not executed autonomously and rather, basically relied upon data from the executive. Moreover, improvements of audit principles basically comprised of reactionary procedures that happened in response to crucial unconstructive business proceedings. In 1939, AICPA brought forward Statement on Auditing Procedure (SAP) that necessitated auditors to confirm receivables and inspect inventories. As a result, auditors became liable for auditing the enterprise unit itself instead of basically depending on the executive verification procedures.

Auditing by observation and inspection became the order of the day. Computerized accounting systems started to appear in the 1950s, but manual auditing routines persisted to be applied entirely. Auditors started to consider automated auditing at the beginning of the 1960s, which was triggered by two particular events.

First, the book 'Electric Data Processing and Auditing' by Felix Kaufman were very crucial. The author contrasts auditing through and around the computer. Traditionally, around the computer auditing comprises of customary physical routines where the reality of programmed tools is overlooked (Abuaddous, Hanefah, & Laili, 2015). Auditing with the computer or through the computer was regarded as more reliable in terms of assurance as compared to around the computer auditing.

Second, the release of International Business Machines in 1963 made computing inexpensive than ever before. This progress gave a sign of a change of how bookkeeping operations ought to be executed in upcoming and assisted stern considerations of a shift from the customary labor-intensive audit. In spite of the great stride towards programmed accounting, several auditors persisted to do auditing around the computer and others who chose to audit through the computer depended on various proprietary curriculums that were inefficient, burdensome, expensive and necessitated frequent reprogramming. In 1967, another firm urbanized between 150 and 250 exceptional auditing schemes, but about 80% of them needed more modification based on transformation in audit prerequisites as well as developments in computer systems. 1967 was also a significant year since Haskins and Sells launched the AUDIOTAPE, a card-oriented auditor-affable computer-aided audit tool (CAAT). This tool enticed auditors to shift to automated auditing. Alongside these key developments, electronic data processing could not be ignored in systems of accounting especially when undertaking audits. However, auditing around the computer necessitated being tested and reviewed on its reliability. Auditing and accounting landscapes also faced major changes due to 2 key occurrences in the 1970s.

First, the scandal at Equity Funding Corporation in 1973 that was substantial in the quest for a transfer from around the computer auditing. Moreover, the event initiated the appraisal of the prevailing audit process in an endeavor to tackle audit procedures and internal controls for information structures. Secondly, the 1977 Foreign Corrupt Practices Act had a great impact on accountants. It required organizations under SEC to keep an inventory thereby ensuring accurate and fair reporting as well as frequent utilization of satisfactory systems of internal monitoring. As a result, U.S. firms were obliged to apply notably more solid accounting structures in conjunction with internal monitoring.

The following 25 years saw more crucial occurrences involving information systems auditing related to refinement and improvement of programmed vendor offerings with an aim of improving efficiency and effectiveness in auditing. Also, the rise and advancement of technologies like the private computer resulted in electronic information dispensation becoming more rampant across firms. Security risk and computer power led to increased need and demand for increased security aimed to assist in making the auditing process automatic. Indeed, power and flexibility of CAATS aided to bring enhanced audit speed and quality when operating with increased data availability linked to automated systems. The necessity for accounting organizations to persist in creating proprietary in-house audit equipment declined with a great margin. Other tools such as Interactive Data Extraction and Analysis and Audit Command Language materialized and provided great benefits over the COBOL- based systems of the preceding period. Since then, the tools are frequently developed and carry on offering worthwhile help to individuals seeking to audit via the computer in the modern world. Though CAATS have been of great use in endorsing people to shift from customary manual auditing, an additional quite recent tool has also had a substantial impact. Sarbanes-Oxley Act (SOX) that was passed in 2002 brought up major transformations on the accounting profession as well as publicly traded firms. The act proposed that assurance regarding financial reporting, as well as internal control operations and practices, were liabilities of auditors and the executive. Moreover, SOX made the accounting profession to dedicate more focus to tackling fraud during auditing. For example, the section on Auditing principles No. 99, Consideration of Fraud in a Financial Statement Audit (AICPA, Professional Standards, AU sec. 316), necessitates auditors

to develop audit processes that offer the logical assurance of discovering scam that could severely impact the financial statements.

As indicated in the above discussion, auditing sustains a very stunning tradition and developments have taken place gradually along the path thereby eventually developed abilities for an advanced audit experience. Nevertheless, hindrances still prevail in the progression towards impending inventory. For instance, the conventional auditing program where businesses are grouped based on risk deliberation continues to be rampant in the auditing discipline currently. Regrettably, the procedure usually falls short to exploit efficacy in the information era. On the other hand, an upcoming audit that depends on the leveraging of processes and technologies had the ability to extend the examination of an organization's working operation and thus offer advanced audit quality. For instance, Kuhn and Sutton (2006) evaluated falsified capital costs at WorldCom and established that, in case of breakdown of manual auditing, an appropriately planned continuous assurance (CA) structure would effectively identify dubious dealings in a well-timed fashion. Organizations like WorldCom and others can mitigate fraud with a well put in place CA structures. Global fraud costs continue to increase, which calls for improvements in a future audit. Though some facets of the conventional audit will continue helping, future audit offers openings to increase the application of computerized equipment and remains crucial for providing advanced assurances comparative to the account management and deployment of stakeholder assets.

An audit task basically ensues with a menace evaluation and creation of an appraisal strategy, defining the objectives and scope of the inventory. Thus, auditors gather and examine audit facts and generate views regarding the internal controls and consistency of the data offered by the executive. At the end of the task, auditors come up with an official report stating their view. Indeed, this technique reveals the 20th-century approach where there is great time delays, high expenses connected to information gathering, processing as well as reporting. Nonetheless, the traditional expenses and delays are not usually the custom in the modern auditing. The current business environment transactions are usually aggregated and entered in such a manner that they can offer an almost immediate response to the pertinent stakeholder. Moreover, practitioners and academicians alike discover this data shift and generated various remedies that more appropriately reveal the modern business setting (Kaur, 2012).

Current Business Environment

Automated Auditing

Firms traditionally familiarized to physical audit processes may profit from following the upcoming audit in an augmentation mode. Such a method typically leads to conducting a pilot research to determine the probable advantages of data audit. Since struggle to transformation is normal across the globe, careful and gradual progress is likely to be a more well-mannered method. Consequently, this can ultimately lead to greater succeeding support for the growth of computerized audit procedures and schemes and could greatly advance the likelihood of accomplishment in ultimately reaching the upcoming audit. Less costly remedies for attaining an initial programmed audit incident entail preliminary CAATS that assist data sorting, mining and evaluation processes. These plans necessitate petite training, no restricted file size, offer comprehensive audit logs for utilization as work manuscript certification, and permit for the development of auditor-precise reports that might be functional to the modern and upcoming information sets. This equipment ought to be primarily utilized to substitute manual audit operations since these are the aspects where the most significant advantages might be accumulated. For instance, the programs can be programmed to tackle tasks like choosing statistical samples, footing ledgers, detection of dubious transactions and generation of confirmations. Also, such equipment is able to analyze 100% of the inventory integrated in a file; a recognized development over the sampling procedures traditionally identified in the customary labor-intensive audit. Via these curriculums, auditors gain the capacity to get an improved knowledge of commerce as well as advanced ranks of professional skepticism and expertise.

Owing to profits, equipment in this group does not function on a truthfully unremitting basis. Principally, they are consignment system curriculums activated gradually as per the audit strategy. Though they definitely provide the purpose to advance audit feature, it might ultimately be desirable to regard other approaches that nearly side with the impending audit. Also, the previous software considerations, instruction aspects ought to be addressed in the course of the computerizing the audit occupation. However, although tools such as CAATS have the capacity to advance the effectiveness and efficiency of auditing roles, they might be underutilized. Consequently, appropriately developed and implemented training schemes might aid more adoption and utilization of CAATS by auditors and accountants. Appropriate training will be a crucial aspect of any audit mechanization program in order to maximize the probability that the auditors will take advantage of the benefits that programmed equipment can offer. A tactically created and executed strategy that encompasses cautious deliberation about aspects of struggle, training, project scope, and trade and cost tradeoffs brings more constructive results. CAATS have the likelihood to act as a conduit pursuit between the labor-intensive audit and the

eventual impending audit. When executed and used appropriately, great benefits will be realized such that organizations ought to welcome the idea of investing more in the aspect of automation or technology (Bănărescu, 2015).

The Future Audit

As mentioned earlier, fundamental CAATS have the capacity to improve audit efficiency and effectiveness. Nonetheless, they do not operate all round the clock scope and thus fail to generate a truthfully unremitting auditing setting where irregularities and exceptions might be discovered as they happen. Also, they fail to operate under synchronized or near synchronized information sets, and, therefore, are unable to tackle uncertain occurrences like probable irregularities or fraud in an optimized approach. Owing to recent developments in business technologies, the ongoing stress on the traditional or manual audit is basically an archaic scheme. Rather, real-time remedies should be developed. Organizations that have effectively experimented with the CAATS highlighted above ought to provide eventual deliberation to more sophisticated plans that include functionalities similar to the upcoming audit and offer a superior guarantee. Luckily, lately proposed remedies better gratify this vision. Generally, the schemes in this group encompass the ability to constantly capture outliers and exceptions in information sets from different systems, offer data and alerting methods to pertinent people in a continuous manner, and basically confront aspects like misuse of funds, errors and fraud in the shortest time possible. The proactive method increases effectiveness and efficiency in identifying opportunities and issues for business advancement. However, before shifting to this more sophisticated domain, extra deliberations regarding business activities are called for.

In line with this stance, there should be a maximum alignment of audit and enterprise data processes. For instance, labor-intensive auditing procedures align with manual data. Organizational information that is not stringently physical might be subject to mechanized processes to some extent. To discover the probable utility of an appropriate auditing structure, a business ought to initially reflect on the level that its information is automated. Consequently, the more organizational data is manual, the less it might basically gain from audit automation. The identified manual business data can sensibly be transformed to a more programmed position before the incorporation of equipment for mechanizing the audit procedure.

Moreover, during the transition to upcoming audit, the level that processes and data are mechanized should be deliberated. A firm that is overloaded by labor-intensive audit procedures will require tackling this aspect at some juncture if the aim is to attain maximum gains from the upcoming audit. Basically, if a firm programs its processes, controls, and data such that they are in line with the roles of the technology being incorporated, the organization is likely to be in a state to maximize the audit feature.

An organization that shifts towards more mechanization comparative to controls, procedures, monitoring tools, and the data starts to obviously configure itself for the upcoming of the future audit. Owing to the current introduction of the concurrent economy, the positioning is crucial. The establishment of the computerized economy has aided a demand from resolution makers, like creditors and investors, for more opportune notice on an assortment of data subjects extending past the customary financial statements. Thus, if the verdict makers need an ongoing information stream in order to develop decisions, they will also request autonomous guarantees regarding the reliability of that data. As a result, the requisite for all round the clock auditing procedure becomes noticeable if organizations aim to contend for limited assets and eventually succeed in the modern and developing real-time worldwide economy. Therefore, it can be argued that the conventional retrospective and manual audit is becoming an unsustainable position. Additionally, there is a general argument that the application of rudimentary CAATS like those highlighted previously will ultimately be inquired in regard to audit function. Luckily, the notion of the impending audit is not a current event and there are diverse suggestions of methodologies to attain this position.

Available Technical Methods and Tools That Prevent and Detect Accounting Fraud

Embedded Audit Modules

The embedded audit module (EAM) method entails the installation of code segments or files within the host system. For instance, the integrated test facility (ITF) approach, a sequence of auditor-generated “dummy” master records are integrated in the live customer arrangement and test activities are recorded according to the accountant’s wish. The inventories are then processed in such a way that only affects the auditor-generated master file.

One more instance in EAM area entails an obstruction of program code that is inserted and created within the customer’s system code configuration. In this circumstance, the EAM consequently controls operations taking place on the host as stipulated in the code block structure.
If a dubious entry is discovered, pertinent occurrence data are recorded in a log that is frequently reviewed by the auditor.

Though these techniques are brought forward for a couple of years, various issues have emerged in a lack of endorsement by the auditing population. EAM technique might trim down customer's system performance, generate excessive information sets regarding the event log, and be a focus to code alteration by shrewd programmers. Owing to the highlighted problems with the embedded technique, it presently prevails as fundamentally an academic subject (Mironiuc, Robu, & Robu, 2012).

The Monitoring and Control Layer

The MCL technique is regarded as a CAAT that might assist in offering ongoing control and monitoring of bookkeeping information systems. MCL approach serves as an alternative of EAM technique. Diverse researchers have proposed that compared to EAM, MCL has fewer issues concerning software repairs, reliance on organization personnel, legal liability, and client independence.

On the functionality, MCL is basically an independent, middleware remedy that obtains information from systems and performs suitable evaluation as required. The fundamental role of the MCL technique is to constantly evaluate and contrast information extracted against particular benchmarks or additional criterion. When irregularities are discovered, alerts are created and transmitted to the auditors for scrutiny and research. As a result, the MCL technique is preferable compared to EAM technique on various aspects, including joint exceptionality of the client system (s) and auditing module.

Nonetheless, though this approach is considered superior to MCL, it is still seen as a suboptimal remedy. For instance, many organizations maintain an assortment of disparate arrangements and it offers great challenges and issues in developing the necessary links between the MCL and diverse customer systems themselves. Additionally, owing to the intrinsic position as a control and monitoring remedy, some individuals might claim that the preservation of auditor autonomy in the MCL setting is intrinsically challenging. Thus, just like EAM, this approach has not yet gained substantial acceptance in auditing arena (Halbouni, 2015).

Audit Data Warehouse

This approach has been provided as a feasible impending audit remedy. Specifically, this technique seems to lessen the issues and concerns linked to MCL and EAM approaches. According to the definition, a data warehouse is "a huge information pool-a single, firm-wide data repository- with equipment to analyze and extract the information.

Fundamentally, a data warehouse is connected to diverse and incongruent enterprise systems in such a manner that it voluntarily integrates and accepts the relevant data being created all through the organization. Also, the data warehouse might be integrated with data marts that are a group of petite, focused warehouses where everyone tackles a specific functional aspect like marketing or accounting. Moreover, the data mart (s) or audit warehouse can inhabit on the initial audit server.

On the functional viewpoint, enterprise data is obtained, standardized, installed and converted in a continuous approach within the data warehouse framework. Additionally, every data mart collects, loads and transforms suitable information from the warehouse depending on the configurations and specifications. Additionally, every data mart consists of diverse unvarying audit tests that function at set time bars, gather audit facts, and develop exemption reports for assessor investigation and scrutiny. An example representation is AuSoftware that uses the audit warehouse model. The software gathers appropriate information on an ongoing scope in flat file constructions from diverse groups of organizational systems. To reduce processing the yoke, AuSoftware imports information in read-only set-up into a data warehouse or "audit data mart" that offers for ongoing inspection processes. Additionally, as dubious objects are discovered, the software has the capacity to control, transmit and audit alerts through web-based formats or more direct routes like mobile phones.

The tools have the capacity to discover irregularities and issues on an all round the clock scope and alert auditors in an instantaneous approach to ensure measures take place an at appropriate time. This is a key advancement over the customary audit that basically detects issues too late for appropriate remedies to be put in place (Bănărescu, 2015).

Audit Applications Approach

It is a recent improvement that encompasses the utilization of particular applications in executing the impending inspection. The AICPA Assurance Services Executive Committee had encouraged the notion that homogeneous set of information from manifold cycles is utilized by a sequence of "audit apps" that might be procured and constructed in line with audit strategies and statements to appropriately execute the upcoming audit.

For instance, for the audit operation "appraise aging of accounts receivable," an audit application can be used to query A/R transaction aspects, contrast ratios in every aging groupings with set industry principles. Moreover, extra apps might be

developed and otherwise acquired as needed for finalizing remaining audit operations in fulfillment of the organizational audit assertions and plan (Hay, 2014).

Extra Future Audit Deliberations

The previous debate reveals that complex audit approaches are being aggressively studied and created to endorse the upcoming of audit. Nevertheless, various firms will have a lot to overcome before shifting to that sphere. For instance, the CICA/AICPA (1999) developed the subsequent list of six circumstances vital for growth to the upcoming auditing. They include:

1. Topic matter with appropriate characteristics. Exceedingly programmed procedures are required to offer consistent data shortly following the incident of linked transactions and events. Business has advanced considerably in the provision of nearly real-time data for crucial procedure. However, their use for audit is still blemished.
2. Consistency of systems offering the theme matter. Likelihood the scheme will function successfully over duration of time; dependability maximized when business monitoring is efficient and systems offer accurate and complete data in a well-timed manner. Though Sys Trust has operated for 10 years, it is simply currently that there is more focus on reassurance on system consistency. However, the focus is also faulty.
3. Audit proof offered by highly programmed procedures. Auditors ought to swiftly comprehend sources of all identified errors and anomalies, establish where they came from, and discuss counteractive action with the executive. Researchers have not been able to offer and use timely audit proof.
4. Trustworthy approaches of obtaining outcomes of audit procedures on a well-timed basis. The results of computerized audit processes ought to be successfully reported to auditors; this hints efficient and reliable electronic communication techniques with suitable protection aspects in place.
5. Opportune availability of and monitoring of audit reports. Organizational data and connected audit reports should be obtainable in a continuous way and simply accessed by rightful people. The substantive embracing of audit warehouses, computerized work papers, and business internal information distribution have radically abridged report allocation issues.
6. High level of auditor expertise in IT and the audited topic. The auditor should possess appropriate skill set to tackle the issue. Currently, there is increased understanding of the necessity to advance auditor analytic and IT acquaintances.

Thus an assortment of characteristics and variables ought to be satisfactorily addressed to completely attain the gains of the upcoming audit. Though the system construction and software elements are exceedingly crucial deliberations, corresponding aspects like auditor training, the socio-technical setting of the organization and nature at the executive level are crucial as well. As a result, wide-ranging strategic planning connecting manual with human aspects is also a vital element in aiding to guarantee an effective transition to the upcoming audit (Halbouni, 2015).

CONCLUSION

Auditing sphere has experienced great developments in the precedent decade, though it has not apparently caught up with the current economy. A number of auditing techniques and approaches that were worthwhile ago now seem to be back-dated. Also, the evolution of auditing is at a crucial place where auditors might either result in adopting or promoting the upcoming auditor carries on to stick to the more traditional program in a given way. Future audit techniques are likely to necessitate auditors, standard setters and regulators to initiate crucial adjustments. Examples of such modifications include: (1) transformation in the frequency and timing of the audit, (2) increased training in analytic approaches or technology, (3) adoption of entire society analysis rather than sampling, (4) re-evaluation of topics like independence and materiality, and (5) authorization of the provisioning of the audit data principle. Auditing personnel is necessitated to have crucial analytical and technical skill set that are presently not elements of the most customary accounting curriculum that takes 4 years.

SOX initiated the initial key transformation in the authorization of the public corporation audit. The new instruction concentrates on the auditor evaluation of the internal monitoring, a very crucial stride in the reassurance of the impending systems that will be computerized, modular, and usually sourced from other firms.

Additionally, the accounting discipline currently has a chance of further enriching the audit to a superior extent of computerization. It is significant that accountants eventually pilot the approach of implementation and adoption of the upcoming audit making them persist as experts of choice comparative to future accounting activities.

REFERENCES

[1]. Abuaddous, M., Hanefah, M. M., & Laili, N. H. (2015). Audit Structure, Time Pressure and Judgment Accuracy: A Comparison between Strategic System Audit and Traditional Audit. *International Journal of Economics and Finance*, *7*(8). doi:10.5539/ijef.v7n8p53
[2]. Arena, M., & Sarens, G. (2015). Editorial: Internal Auditing: Creating Stepping Stones for the Future. *International Journal of Auditing*, *19*(3), 131-133. doi:10.1111/ijau.12053
[3]. Auditing a Client's Internal Controls. (2011). *Auditing for Dummies®*, 111-131. doi:10.1002/9781118269268.ch7
[4]. Background of Federal Auditing: Evolution, Standard Setters, Responsibilities, Audit Types. (2015). *Federal Government Auditing*, 1-15. doi:10.1002/9781118722152.ch1
[5]. Bănărescu, A. (2015). Detecting and Preventing Fraud with Data Analytics. *Procedia Economics and Finance*, *32*, 1827-1836. doi:10.1016/s2212-5671(15)01485-9
[6]. Bowers, T. (2011). Introduction: "Force or Fraud"? *Force or Fraud*, 1-25. doi:10.1093/acprof:oso/9780199592135.003.0001
[7]. Complex Information Systems, Auditing Standards and IT Auditors. (2015). *Information Technology Auditing*, 63-74. doi:10.1007/3-540-27486-3_4
[8]. Evans, S. (2012). Visible ink: the mark of the future accountant? *Accounting, Auditing & Accountability Journal*, *25*(7). doi:10.1108/aaaj.2012.05925gaa.001
[9]. Fraud Prevention and Detection. (2015). *Computer-Aided Fraud Prevention and Detection*, 17-39. doi:10.1002/9781119203971.ch2
[10]. Fraud Profiling Your Organization. (2015). *Profiling the Fraudster*, 197-204. doi:10.1002/9781118929773.ch20
[11]. Halbouni, S. S. (2015). The Role of Auditors in Preventing, Detecting, and Reporting Fraud: The Case of the United Arab Emirates (UAE). *International Journal of Auditing*, *19*(2), 117-130. doi:10.1111/ijau.12040
[12]. Hay, D. (2014). Auditing, International Auditing and the International Journal of Auditing: Editorial. *International Journal of Auditing*, *18*(1), 1-1. doi:10.1111/ijau.12020
[13]. International Internal Auditing and Accounting Standards. (2015). *Brink's Modern Internal Auditing*, 723-729. doi:10.1002/9781118371558.ch33
[14]. Introduction to Fraud Data Analytics. (2016). *Fraud Data Analytics Methodology*, 1-16. doi:10.1002/9781119270331.ch1
[15]. Kaur, H. (2012). Corporate Fraud: Auditors' and Managerial Liability. *Emerging Fraud*, 115-132. doi:10.1007/978-3-642-20826-3_8
[16]. Kowaleski, Z. T., Cannon, N. H., Schnader, A. L., & Bedard, J. C. (2018). The Continuing Evolution of Auditor Reporting in the Broker-Dealer Industry: Issues and Opportunities. *Current Issues in Auditing*. doi:10.2308/ciia-52176
[17]. Krambia-Kapardis, M. (2016). A Holistic Model of Corruption and Corporate Fraud Prevention. *Corporate Fraud and Corruption*, 135-168. doi:10.1057/9781137406439_6
[18]. Kratcoski, P. C. (2018). Introduction: Overview of Major Types of Fraud and Corruption. *Fraud and Corruption*, 3-19. doi:10.1007/978-3-319-92333-8_1
[19]. Kronenberg, S. (2015). The Impact of Communications Infrastructure on Fraud Detection and Deterrence. *The Handbook of Fraud Deterrence*, 177-187. doi:10.1002/9781119202165.ch12
[20]. Mironiuc, M., Robu, I., & Robu, M. (2012). The Fraud Auditing: Empirical Study Concerning the Identification of the Financial Dimensions of Fraud. *Journal of Accounting and Auditing: Research & Practice*, 1-13. doi:10.5171/2012.391631
[21]. Rahman, R. A., & Anwar, I. S. (2014). Types of Fraud among Islamic Banks in Malaysia. *International Journal of Trade, Economics and Finance*, *5*(2), 176-179. doi:10.7763/ijtef.2014.v5.365
[22]. Sewe, F. O. (2012). The Sarbanes Oxley Act and Its Impacts on Corporate Finance and Corporate Governance Behavior. *SSRN Electronic Journal*. doi:10.2139/ssrn.2111505
[23]. The Future of Internal Auditing is Yours. (2015). *Cutting Edge Internal Auditing*, 405-421. doi:10.1002/9781119208440.ch16
[24]. Why No Organization Is Immune to Fraud. (2015). *Anti-Fraud Risk and Control Workbook*, 1-10. doi:10.1002/9781119205654.ch1
[25]. Whyte, D. (2016). Neoliberalism and the Moral Economy of Fraud. doi:10.4324/9781315680545
[26]. Zhu, X., Tao, H., Wu, Z., Cao, J., Kalish, K., & Kayne, J. (2017). Ad Fraud Detection Tools and Systems. *Fraud Prevention in Online Digital Advertising*, 45-49. doi:10.1007/978-3-319-56793-8_6.