Fraud Risk Management – Discussion on an Effective Fraud Risk Management Framework, Challenges and Trends

Research Project for Emerging Issues/Advanced Topics Course

Master of Forensic Accounting Program University of Toronto

Prepared by Flora Chau

June 19, 2022

For Prof. Leonard Brooks

Table of Contents

1. Introduction

According to a 2021 report by Crowe U.K. LLP, fraud costs over USD 5.38 trillion globally, which is equivalent to 6.4% of global GDP[1] (Gee & Button, 2021). This is detrimental to businesses and individuals. Fraud is inevitable but an effective fraud risk management framework would help prevent, detect, and respond to fraud incidents.

This paper will discuss the major internal control/ risk management framework developed by the Committee on Sponsoring Organization of the Treadway Commission ("COSO") – (i) the internal control framework covers five areas including control environment, risk assessment, control activities, information and communication and monitoring activities; (ii) the enterprise risk management framework covers five areas including governance and culture, strategy and objective-setting, performance, review and revision and information, communication, and reporting and; (iii) the fraud risk management guide covers fraud risk governance, fraud risk assessment, fraud control activity, fraud investigation and corrective action and fraud risk management monitoring activities. The three framework/ guides share similarities with the focus to enhancing internal control, risk management, governance, and fraud deterrence.

The paper will further discuss a fraud risk management framework from the angles of governance, fraud prevention, fraud detection and fraud response and examines how it reconciles with the major framework. This paper also includes a case study on the establishment of a fraud risk management framework for a Southeast Asian Bank. The Southeast Asian Bank, with little to no fraud risk management measures, suffered from an

[1] Gee, J., & Button, M. (2021, June 23). The financial cost of fraud 2021 - the latest data from around the world. (p.6)

internal fraud of over CAD 42 million in 2017. The paper will cover the key observations and findings as well as the scope of work of the engagement.

Given technological advancement and the impact of the pandemic, the mode of business operations has evolved. At the same time, fraudsters have become more sophisticated. In the last two sections of the paper, challenges and trends in fraud risk management will be discussed.

2. Definitions

2.1 Operational Risk

Operational risk is defined as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events"[2] (Basel Committee on Banking Supervision, 2006). This definition includes legal risks but excludes strategic and reputational risks. The scope of operational risk includes fraud, security, legal and compliance risks.

2.2 Fraud

According to Black's Law Dictionary, fraud is defined as the "knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment" (The Law Dictionary, n.d.). The Institute of Internal Auditors ("IIA") defines fraud as "any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of

[2] Basel Committee on Banking Supervision, International Convergence of Capital Measurement and Capital Standards, June 2006, Paragraph 644.

services; or to secure personal or business advantage" (The Institute of Internal Auditors, n.d.). Fraud generally refers to any intentional act committed to secure an unfair or unlawful gain. Examples of fraud include, but not limited to bribery and corruption, asset misappropriation, and financial statement fraud.

2.2.1 Internal Fraud

Internal fraud is sometimes referred to as occupational fraud (Association of Certified Fraud Examiners, 2022). Internal or employee frauds occur when the fraud is committed against the company or organization with the intent for personal monetary gain (CFI Education Inc., 2022).

2.2.2 External Fraud

"External fraud is the risk of unexpected financial, material or reputational loss as a result of fraudulent action of persons external to the firm" (Open Risk Manual, n.d.)

2.3 Inherent Fraud Risk

Inherent fraud risk refers to the fraud risk that an organization faces in the absence of any actions that the management might take to alter either the likelihood or impact of a risk (i.e. the risk before controls is considered) (Accounting Tools, 2022).

2.4 Internal Control

Internal Control is defined as "a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance" (COSO, 2013).

According to the Institute of Internal Auditors, control is referred to as "any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved" (The Institute of Internal Auditors, n.d.).

2.5 Residual Fraud Risk

Residual fraud risk refers to the "remaining" fraud risk exposure that an organization faces after controls are considered (Shackleford, 2022).

2.6 Fraud Triangle

The Fraud Triangle was developed by Dr. Donald Cressey, a criminologist, in 1953[3] (Sujeewa, Yajid, Khatibi, Azam, & Dharmaratne, 2018). Dr. Cressey described embezzlers as "trusted violators". The Fraud Triangle consists of three components: pressure, opportunity, and rationalization.

2.6.1 Pressure

Pressure is the incentive that could motivate an individual to be involved in fraud. Pressure could result from personal pressure, for example, health problems, financial problems, gambling addiction, etc. It could result from pressure from organizations where employees feel pressured to meet financial targets, to compete with competitors, etc.

2.6.2 Opportunity

Opportunity creates an avenue for fraud. It refers to the circumstances that allow fraud to occur. In the Fraud Triangle, opportunity could be weak internal controls where there is lack of supervision, poor segregation of duties, in which a person sees an opportunity to commit fraud.

[3] Sujeewa, G. M., Yajid, M. S., Khatibi, A., Azam, S. F., & Dharmaratne, I. (2018, August). The New Fraud Triangle Theory - Integrating Ethical Values of Employees. International Journal of Business, Economics and Law, Vol. 16, Issue 5. (p. 52-57)

2.6.3 Rationalization

Rationalization refers to an individual's justification(s) for committing fraud.

2.7 Fraud Risk Management

Risk management is defined as the "process of understanding and managing risks that the entity is inevitably subject to in attempting to achieve its corporate objectives" (CIMA, 2005). Fraud is a type of risks that an organization manages. Fraud risk management is the process of assessing risks within an organization and then developing a systematic method to prevent, detect, and respond to fraud.

3. Discussion on Major Internal Control/ Risk Management Framework

3.1 The Committee on Sponsoring Organizations of the Treadway Commission

The Committee on Sponsoring Organization of the Treadway Commission ("COSO") was formed in 1985. COSO's mission is to "help organizations improve performance by developing thought leadership that enhances internal control, risk management, governance and fraud deterrence" (COSO, 2022). COSO was organized to sponsor the National Commission on Fraudulent Financial Reporting, an independent private sector initiative that studies the causal factors of fraud and fraudulent financial reporting[4]. COSO continues to develop recommendations and best practices for industries and their independent auditors. In addition, many of these recommendations are implemented and

[4] Cendrowski, H., Martin, J., & Petro, L. (2007). The handbook of fraud deterrence. (p.119)

codified by regulators such as the Securities and Exchange Commission ("SEC") and Public Companies Accounting Oversight Board ("PCAOB").

The first chairman of the National Commission was James C. Treadway, Jr., former commissioner of the SEC. Treadway was named to the SEC by President Ronald Reagan in 1982 and served until April 17, 1985. The National Commission was therefore named after him – "Treadway Commission"[5] (Cendrowski, Martin, & Petro, 2007).

The five non-profit professional associations that sponsored the Treadway Commission include:

- The American Accounting Association ("AAA");
- The American Institute of Certified Public Accountants ("AICPA");
- Financial Executives International ("FEI");
- The Institute of Internal Auditors ("IIA"); and
- The National Association of Accountants (now the Institute of Management Accountants ("IMA").

COSO's goal is to provide thought leadership dealing with three interrelated subjects: internal control, enterprise risk management ("ERM"), and fraud deterrence (COSO, 2022). COSO has issued various publications related to the three subjects. Some of the examples are listed below:

Regarding internal control, in 1992, COSO published the Internal Control — Integrated Framework. This framework was revised and reissued in May 2013. Effective December 15, 2014, the 1992 framework is superseded and no longer available (COSO, 2022).

[5] Cendrowski, H., Martin, J., & Petro, L. (2007). The handbook of fraud deterrence. (p.119)

In relation to ERM, in 2004, COSO issued the Enterprise Risk Management — Integrated Framework. This framework was updated with the release in 2017 of "Enterprise Risk Management – Integrating with Strategy and Performance," which highlights the importance of considering risk in both the strategy-setting process and in driving performance (COSO, 2022).

In the area of fraud deterrence, COSO has published two research studies. The first study released in 1999 was titled Fraudulent Financial Reporting: 1987-1997. A continuation study called Fraudulent Financial Reporting: 1998-2007 was released in 2010 (COSO, 2022).

This paper will discuss the 2013 Internal Control – Integrated Framework, the 2017 Enterprise Risk Management – Integrated Framework and the Fraud Risk Management Guide.

3.1.1 Internal Control – Integrated Framework (2013)

COSO first released its Internal Control – Integrated Framework ("the original framework" or "the 1992 Framework")) in 1992. It has gained broad acceptance and is widely used around the world. On May 14 2013, COSO released an updated version of its Internal Control – Integrated Framework ("the Framework" or "the enhanced Framework" or "the 2013 Framework"). The Framework and related illustrative documents are updated from the 1992 Framework with the intension to:

- Clarify the requirements of effective internal control;
- Update the context for applying internal control by reflecting the changes in business and operating environments; and

- Broaden its application by expanding the operations and reporting objectives[6] (COSO, 2013).

The enhanced Framework includes three objectives, which allow organizations to focus on differing aspects of internal control:

- Operations objectives – these pertain to effectiveness and efficiency of the organization's operations, including operational and financial performance goals, and safeguarding assets against loss.
- Reporting objectives – these pertain to internal and external financial and non-financial reporting and may encompass reliability, timeliness, transparency, or other terms as set forth by regulators, recognized standard setters, or the organization's policies.
- Compliance objectives – these pertain to adherence to laws and regulations to which the organization is subject[7] (COSO, 2013).

The COSO Integrated Framework identifies five components of internal control. For an organization to achieve effective internal controls, all five layers must be "present" and "functioning". COSO refers "present" as "the determination that the components and relevant principles exist in the design and implementation of the system of internal control to achieve specified objectives" (COSO, 2013). "Functioning" refers to "the determination that the components and relevant principles continue to exist in the operations and conduct of the system of internal control to achieve specified objectives" (COSO, 2013). Weakness

[6] Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013, May). COSO Internal Control-Integrated Framework Frequently Asked Questions. (p.1)

[7] Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013, May). Internal Control - Integrated Framework Executive Summary. (p.3)

in one or more of the components will degrade the effectiveness of the system. The five components are:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring activities

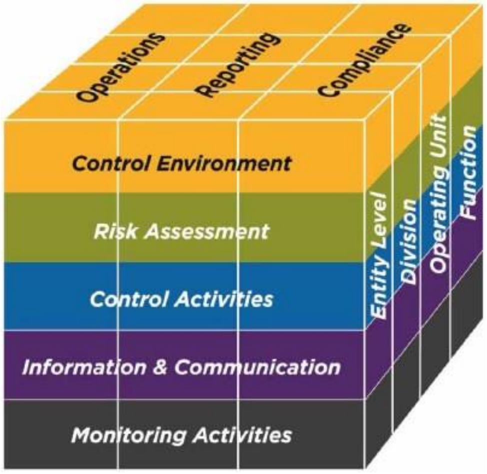

Figure 1 The COSO Cube from the Internal Control - Integrated Framework (2013) (COSO, 2013)

Figure is the illustration by COSO which explains the direct relationship between objectives, which are what an organization strives to achieve; components, which represent what is required to achieve the objectives; and the organizational structure of an organization (e.g. the operating units, functions, etc.).

The Framework also sets out 17 principles in relation to the five components. The 17 principles were conceptually introduced in the original Framework but are not explicitly articulated in the enhanced Framework. These 17 principles are listed in Appendix 1 for completeness of the discussion of the Framework.

3.1.1.1 Control environment

The control environment is the basis for carrying internal control across the organization. It is generally referred to as "management's tone at the top". It comprises the integrity and ethical values of the organization and the expected standards of conduct. The control environment also defines the control culture of an organization. This guides appropriate behaviors within the organization in the absence of defined policies and procedures (Cendrowski, Martin, & Petro, 2007).

The Association of Certified Fraud Examiners' ("ACFE") 2022 Report to the Nations suggested that poor tone at the top is one of the primary internal control weaknesses which contributed to 10% of occupational fraud in victim organizations[8]. In fact, based on the perpetrators' position, a poor tone at the top was the most common factor underlying schemes perpetrated by owners or executives (i.e. 23%). Although owners or executives committed only 23% of occupation fraud, as compared to employees (i.e. 37%) and managers (i.e. 39%), they caused the largest losses (i.e. USD 337,000, as compared to USD 125,000 by managers and USD 50,000 by employees.) (Association of Certified Fraud Examiners, 2022).

Since management is primarily responsible for the design, implementation, and maintenance of internal control, an organization is always exposed to the danger of management override of controls. Management override continues to be a primary concern of the accounting profession and regulators. The AICPA refers to this situation as the

[8] Association of Certified Fraud Examiners. (2022). Occupational Fraud 2022: A Report to the Nations. (p.42-44).

Archilles' heel of financial reporting (American Institute of Certified Public Accountants, 2016). Despite having sound controls in the other components, as mentioned earlier, weakness in one or more of the components will degrade the effectiveness of the system. If the management failed to behave according to the written policies and procedures, or if they demonstrate a lack of integrity in their actions, it will allow employees to rationalize their inappropriate behaviors.

3.1.1.2 Risk assessment

Every organization faces a variety of risks from external and internal sources. Risk is defined as "the possibility that an event will occur and adversely affect the achievement of objectives" (COSO, 2013). Every organization has different levels of risk tolerance. A risk assessment is therefore needed to evaluate the situation of the organization to determine how risks will be managed. Risks assessments shall be conducted periodically to ensure the right approach in meeting an organization's objectives.

It was found that formal fraud risk assessments are one of the five anti-fraud controls that have increased the most over the last decade (i.e. from 36% to 46%)[9] (Association of Certified Fraud Examiners, 2022). There has been a rising importance of formal fraud risk assessments in organizations.

3.1.1.3 Control activities

COSO defined control activities as "the actions established through policies and procedures that help ensure the management's directives to mitigate risks to the achievement of objectives are carried out"[10] (COSO, 2013). These control activities are

[9] Association of Certified Fraud Examiners. (2022). Occupational Fraud 2022: A Report to the Nations. (p.19).

[10] Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013, May). Internal Control - Integrated Framework Executive Summary. (p.4)

designed by management, implemented, and consistently enforced to ensure that assets are safeguarded, and financial reporting is accurate. Control activities may be preventive or detective in nature and may encompass a range of manual and automated activities from authorizations and approvals to verifications to reconciliations or even business performance reviews.

The concept of segregation of duties is crucial when selecting and developing control activities. In general, there should be a separation between the duties of: (i) authorization or approval; (ii) custody of assets; (iii) recording transactions and (iv) reconciliation/ control activity.

3.1.1.4 Information and communication

An organization needs to provide, share, and obtain information to and from relevant stakeholders to support the achievement of its objectives. Communication includes internal and external sources where both have two dimensions. Internal communication refers to the communication within the organization where (i) a downward flow of information from management to employees to allow them to produce the best results possible and (ii) an upwards flow from employees to management to provide feedback[11]. External communication enables (i) inbound communication of relevant external information and provides (ii) information to external stakeholders.

3.1.1.5 Monitoring activities

Monitoring activities include ongoing evaluations, separate evaluations, or combination of both to ascertain whether each of the five components of internal control is present and functioning. Management must ensure that the control processes are performed as designed

[11] Cendrowski, H., Martin, J., & Petro, L. (2007). The handbook of fraud deterrence.(p.126)

and approved. The control activities shall also be evaluated against criteria established by regulators, recognized standard-setting bodies. Any deficiencies identified through the monitoring activities shall be communicated to management and the board of directors, and to be remediated appropriately.

3.1.2 Enterprise Risk Management – Integrating with Strategy and Performance (2017)

In 2004, COSO published the Enterprise Risk Management – Integrated Framework to provide guidance to organizations in managing risk. The publication has gained broad acceptance by organizations in their efforts to manage risk. However, over the past decade, the complexity of risk has changed, new risks have emerged, and both boards and executives have enhanced their awareness and oversight of enterprise risk management while asking for improved risk reporting. As a result, in 2017, COSO published an updated document titled Enterprise Risk Management – Integrating with Strategy and Performance ("the Updated Document" or "the 2017 Framework"). The document highlights the importance of considering risk in both the strategy-setting process and in driving performance (COSO, 2022). Internal control is positioned within the Updated Document as a fundamental aspect of enterprise risk management (COSO, 2016)[12]. The COSO Board believes that enterprise risk management is broader in scope than internal control. Therefore, the 2013 Framework constitutes an essential building block for enterprise risk management[13].

[12] Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2016, November). Enterprise Risk Management – Integrating with Strategy and Performance Frequently Asked Questions. (p.4)

[13] Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013, May). COSO Internal Control-Integrated Framework Frequently Asked Questions. (p.8)

Like the 2013 Framework, the 2017 Framework has five interrelated components[14]:

- Governance and culture
- Strategy and objective-setting
- Performance
- Review and revision
- Information, communication, and reporting

3.1.2.1 Governance and culture

Governance refers to the overall management of an organization. It sets the organization's tone. It involves exercising board risk oversight, establishing operating structures and defining roles and responsibilities in an organization. Culture pertains to "ethical values, desired behaviors, and understanding of risk in the entity" (COSO, 2017). It is not uncommon that organizations establish a code of conduct to govern the behaviors of their employees. Also, organizations with good culture tends to attract, develop, and retain capable individuals.

3.1.2.2 Strategy and objective-setting

Strategy and object-setting refers to analyzing business context, establishing risk appetite, evaluating alternative strategies, and formulating business objectives.

3.1.2.3 Performance

Risks that may impact the performance of the organization need to be identified and assessed. Given limited resources, risks shall be prioritized by severity in relation to risk

[14] Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017, June). Enterprise Risk Management Aligning Risk with Strategy and Performance Executive Summary.
(p.6)

appetite. Appropriate risk responses shall be conducted, and the results shall be reported to key risk stakeholders.

3.1.2.4 Review and revision

This aspect is like “monitoring activities” in the 2013 Framework where it is essential to review the organization’s performance. This is to assess how well the enterprise risk management components are functioning and whether revisions are needed.

3.1.2.5 Information, communication, and reporting

As in the 2013 Framework, enterprise risk management requires a continual process of obtaining and sharing information to and from internal and external sources.

The five components in the updated Framework are supported by a set of principles, which are listed in Appendix 2 for reference.

3.1.3 Fraud Risk Management Guide

In 2016, COSO published the Fraud Risk Management guide (“the FRM guide”) which is intended to supplement the 2013 Framework and serve as best practices guidance[15]. The Fraud Risks Management Guide contains five components:

- Fraud risk governance
- Fraud risk assessment
- Fraud control activity
- Fraud investigation and corrective action
- Fraud risk management monitoring activities

The five components will be discussed further in the next Section.

[15] Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2016, September). Fraud Risk Management Guide.(p.v)

4. Overview of Fraud Risk Management Framework[16]

Every organization faces a unique set of fraud risks based on its business nature, the environment in which it operates, the internal control it puts in place, the ethics and values of the organization and its employees, etc., an effective fraud risk management framework should be tailored to the specific needs of the organization.

4.1 Governance

The first component in COSO's FRM guide is "fraud risk governance". A robust governance framework is crucial to effective fraud risk management as it enables an organization to manage its fraud risk exposure holistically. A robust governance framework covers five main disciplines:

- Senior management oversight
- Organizational structure
- Roles and responsibilities
- Policy and procedures
- Management information reporting

4.1.1 Senior Management Oversight

Consistent with the 2013 and 2017 Framework, it is important for the board and senior management of an organization to set an appropriate "tone at the top" and lead by example. They should express their commitment towards achieving and maintaining a strong organizational culture that is founded on integrity and create an environment in which employees feel safe to speak up if they think something is wrong. Organizations should

[16] The author of this paper had taken part in an engagement in establishing a fraud risk management framework for a Southeast Asian bank, which will be discussed further in Section 5. The content of this section is based on the author's experience and knowledge in the subject.

have a dedicated board-level committee to advise and assist the board in discharging its responsibilities in managing fraud. The committee should regularly review and confirm the effectiveness of the overall fraud risk management program of the organization. In particular, the committee should ensure that the organization's values and strategy of managing fraud risks are translated into written policies and procedures of the day-to-day operation of the organizations.

4.1.2 Organizational Structure

A well-designed organizational structure, where key areas of authority and reporting lines are clearly defined, can be an effective fraud prevention measure.

4.1.3 Roles and Responsibilities

To uphold accountability and set out clear definitions of the roles and responsibilities in managing fraud risks, organizations often adopt the Three Lines of Defense Model.

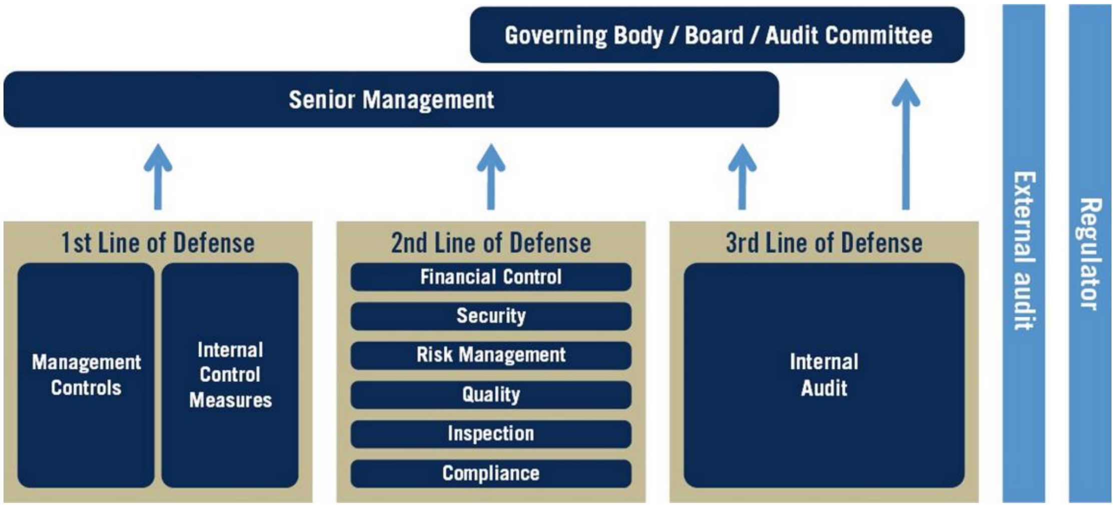

Figure 2 The Three Lines of Defense Model (Davies & Zhivitskaya, 2018)

Figure 2 shows the Three Lines of Defense Model where the first line of defense is risk management within the front office (Davies & Zhivitskaya, 2018). The first line of defense is the risk owner of an organization. The first line of defense is the risk owner. It has the ownership, responsibility, and accountability for assessing, controlling, and mitigating risks together with maintaining effective internal controls (ECIIA/FERMA, 2010). The second line of defense is the risk steward of an organization. It includes support functions, such as risk management, compliance, legal, etc., which provides the tools to manage risks and monitor compliance (Besson, 2018). The third line of defense is internal audit, which observes and evaluates of the effectiveness of risk management as well as other conduct within the business (Davies & Zhivitskaya, 2018). It has the responsibility of conducting independent testing to assess compliance by the first and second lines of defense.

4.1.4 Policies and Procedures

A clearly written anti-fraud policies and procedures is crucial to effective fraud risk management.

Anti-fraud policies and procedures should address the following questions:

- What is considered as fraud to the organization?
- What are some of the actions that constitute fraud?
- What are the consequences of committing fraud?
- What are the roles and responsibilities of the different parties in managing fraud?
- What should be done in case of a fraud suspicion?

4.1.5 Management Information Reporting

Management information reporting is another key element for an organization to effectively manage its fraud risks, as it serves as a basis for the recipients (e.g. the board, senior management, risk management functions) to understand the fraud risks faced by the organization before they can manage it accordingly.

Hence, management information reporting should not only focus on the numbers, such as the number fraud incidents and loss amounts, it should also focus on analyzing the root causes behind the numbers so that the reporting could reflect the substances of the fraud risks faced by the organization. Level of details of the management information should also be commensurate with the positions of the recipients.

In general, an effective fraud risk management framework encompasses controls that have three objectives:

- Fraud prevention – to proactively prevent fraud to minimize the likelihood of occurrence of fraud incidents in the first place.
- Fraud detection – to detect and fraud instances when they do occur.
- Fraud response – to take corrective actions and to investigate fraud-related matters.

4.2 Fraud Prevention

4.2.1 Fraud Risk Assessment ("FRA")

Fraud risk assessment is a comprehensive risk assessment to identify specific fraud schemes and inherent risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate key residual fraud risks. It is the basis of fraud risk management as it informs an organization the type and level of risks it is exposed to. An organization shall conduct an FRA on an annual basis or more frequently as needed. Upon completion of the FRA, there shall be a report of findings, of which may include heat map of fraud risks exposure, design deficiencies identified and recommendations to mitigate the identified fraud risks. Issues identified in the FRA shall be prioritized based on their risk level and potential exposure. The corresponding recommendations shall also be prioritized based on complexity and amount of time required for implementation and be used in developing the organization's fraud control and response plan.

ACFE's Report to the Nations Report found that formal fraud risk assessment is an effective anti-fraud control where there is a 45% reduction in median loss with such control in place as compared to organizations without such control. In addition, fraud only lasted for 10 months for organizations where formal fraud risk assessments were conducted as compared to 18 months for organizations without formal fraud risk assessments[17].

To illustrate an approach of a comprehensive FRA, the following could be considered:

- Identification of responsible process owners – the risk assessment process shall involve relevant employees across different departments and grades, as perception of employees towards fraud may be different when they are in different positions.
- Fraud risk assessment questionnaire – a fraud risk assessment questionnaire shall be designed for each key business area. The FRA questionnaire should cover, at a minimum, general fraud management questions, types of fraud risk, new and/or key changes in procedures and controls.
- Fraud incident analysis – analysis of past fraud cases that had occurred in the organization would allow the organization to identify common fraud schemes/ trends as well as business areas that are more exposed to fraud risks. Adequate considerations shall also be put on recent industry fraud trends and other major fraud cases identified by peer organizations.
- Focus groups/ interviews/ fraud risk assessment workshops – by allowing employees from different departments across different grades to share observations

[17] Association of Certified Fraud Examiners. (2022). Occupational Fraud 2022: A Report to the Nations. (p.36-37).

and challenges arising from daily activities to understand potential areas for fraud and their understanding of controls that are in place to mitigate fraud risks. This would allow the organization to address and review fraud risks from different perspectives.

- Stress testing – development of fraud threat scenarios based on control gaps identified from focus groups/ interviews/ fraud risk assessment workshops. Subsequently, conduct vulnerability analyses on the control breaks by overlaying the fraud scenarios. This would allow the relevant stakeholders and management to identify the impact of the fraud risks have on the organization.

4.2.2 Fraud Awareness Training and Communications

To be effective in fraud prevention, it is crucial to enhance employees' fraud awareness. Employees shall be encouraged and trained to speak up when faced ethical dilemmas and report wrongdoings or irregularities. Fraud awareness training aimed at training employees to recognize red flags that may appear, guiding them where to seek assistance, and advice and demonstrating management's commitment to combating fraud. Communications related to latest fraud matters or trends shall be cascaded to all employees on a periodic basis or as needed to convey new information related to fraud risks and reinforce previously acquired knowledge. According to the ACFE's Report to the Nations, fraud training for employees is one of the top 10 most common fraud controls in the surveyed organizations[18]. It was also found that fraud training for employee is an effective anti-fraud control where there is a 45% reduction in median loss with such control in place as compared to organizations without such control. In addition, fraud only lasted for 12 months for

[18] Association of Certified Fraud Examiners. (2022). Occupational Fraud 2022: A Report to the Nations. (p.34).

organizations where fraud training was conducted as compared to 18 months for organizations without fraud training[19].

Fraud awareness training and communications shall include but not be limited to the following:

- Induction training for newly hired employees upon joining the organization.
- Refresher training for existing employees on an annual basis with certification by the employees to acknowledge their understanding of their responsibilities and commitment in managing and mitigating fraud risks.
- Training on newly identified fraud risks and prevention mechanisms, on an as needed basis.
- Training on the whistleblower programme and reassurance of the anonymity of the whistleblowers.
- Fraud awareness communications via e-mails, townhalls, or other mediums of communication (e.g. posters, leaflets, etc.).

4.3 Fraud Detection

4.3.1 Fraud Analytics

Proactive data monitoring/ analysis is found to be the most effective anti-fraud control in shortening the duration of fraud[20]. Fraud analytics involved the use of tools or techniques to analyze large volume of data to detect suspicious or anomalous transactions. Analytics is generally implemented as either preventive (real-time blocking) or detective (post-event

[19] Association of Certified Fraud Examiners. (2022). Occupational Fraud 2022: A Report to the Nations. (p.36-37).

[20] Association of Certified Fraud Examiners. (2022). Occupational Fraud 2022: A Report to the Nations. (p.37).

identification). When deciding which type should be implemented, it often involves considering fraud risk appetite (size/ risk of transactions), the ability to investigate/ enforce/ recover later, and customer experience.

There are two broad categories of fraud analytics techniques: statistical data analysis techniques and artificial-intelligence-based techniques (Kanade, 2021).

4.3.1.1 Statistical data analysis techniques

Statistical data analysis for fraud detection involves various statistical operations such as fraud data collection, fraud detection, and fraud validation by conducting detailed investigations (Kanade, 2021). The following are the different types of statistical data analysis techniques:

- Statistical parameter calculation

  Statistical parameter calculation refers to the calculation of various statistical parameters within a population. For example, averages, standard deviations, percentages, and probability distributions for fraud-related data collected during the data collection process (Kanade, 2021). The objective of statistical analysis can be thought of as returning suspicious scores, where higher scores are interpreted as more suspicious than lower scores. The higher the score, the more unusual the observation, or the more it resembles a previous fraud value (Bolton & Hand, 2002).

- Regression analysis

  Regression analysis is defined as “a technique for representing the functional relationships between variables so that we may be able to predict the value of one on the basis of another or others” (Mercer, 1990). Regression analysis allows the estimation of relationship between independent and dependent variables. This helps understand and identify relationships between several fraud variables.

- Probability distributions and models

  "A probability distribution is a statistical function that describes all the possible values and likelihoods that a random variable can take within a given range" (Hayes, Probability Distribution, 2022). A bell curve represents normal probability distribution where the mean of the distribution is represented by the top of the bell curve (Giardino, 2014). One can analyze activities or transactions to determine the normal distribution. When an instance is beyond the normal probability distribution, it could be a red flag of fraudulent activities.

- Data matching

  Data matching refers to the comparison between two sets of data. It could be carried out based on algorithms or programmed loops, "where processors perform sequential analyses of each individual piece of a data set, matching it against each individual piece of another data set, or comparing complex variables like strings for particular similarities" (Janalta Interactive, n.d.). For example, data matching could be used to identify potential claims fraud where the same invoice was submitted more than once for reimbursement.

4.3.1.2 Artificial-intelligence-based techniques

Artificial intelligence ("AI") is a new technical science that studies and develops theories, methods, technologies, and application systems used to simulate, extend, and expand human intelligence. Moreover, AI is a branch of computer science to understand the essence of intelligence and produce a new intelligent machine that can respond similarly to human intelligence (Li, 2022). AI-based fraud detection techniques include the following methods:

- Data mining

  Bose & Mahapatra define data mining as a process of identifying interesting patterns in databases that can then be used in decision making[21]. Data mining includes classification, clustering, prediction, outlier detection, regression, and visualization (Ngai, Hu, Wong, Chen, & Sun, 2011). In fraud detection, data mining acts to find associates in the data set, which could be used for further analysis.

- Neural networks

  A neural network is a series of algorithms that tries to recognize underlying relationships in a set of data through a process that mimics the way the human brain operates (Chen, 2021). Neural networks under fraud detection perform classification, clustering, generalization, and forecasting of fraud-related data (Kanade, 2021).

  The Health Insurance Commission of Australia uses a number of automated neural network-based classification systems to classify the practice profiles of practitioners who participate in the national medical coverage programme (i.e. Medicare), to help identify those who are practicing inappropriately. This includes those who are providing more services than what is necessary for the medical conditions of the patients (He, Wang, Graco, & Hawkins, 1997).

- Machine learning

[21] Bose, I., & Mahapatra, R. K. (2001). Business data mining — a machine learning perspective. Information & Management, 39(3) (p.211-225)

There are two types of machine learning: supervised and unsupervised. In the paper of He, Wang, Graco, & Hawkins, "supervised learning refers to learning involving feedback which shows the correct response (e.g. the required classification) to an input (e.g. practice profile), whereas unsupervised learning refers to learning without the aid of feedback and the system itself has to recognize patterns (e.g. different types of practice profiles) in the data" [22]. In other words, supervised machine learning is using previous known fraud cases to predict similar unknown cases, and/or as part of alert management. On the other hand, unsupervised machine learning is advanced analytical techniques to detect items which are "abnormal" compared to their peer segment, an anomaly detection.

- Pattern recognition

Theodoridis and Koutroumbas define pattern recognition as "the scientific discipline whose goal is the classification of objects into a number of categories or classes" [23]. In other words, it is the process of identifying the trends in the given pattern. One of the examples of pattern recognition could be the identification of "red flags behaviors" in behavioral analytics. For example, an employee usually logs into the company system Monday to Friday between 8:30 am to 9:00 am. A login record at 11:00 pm on a Saturday could be a suspicious behavior for follow-up. The login record at 11:00 pm on a Saturday is outside the "normal" pattern of the employee and it warrants a follow up.

[22] He, H., Wang, J., Graco, W., & Hawkins, S. (1997, November). Application of Neural Networks to Detection of Medical Fraud. Expert Systems with Applications, 13(4) (p.329).

[23] Theodoridis, S., & Koutroumbas, K. (2006). Pattern Recognition (3rd ed.). San Diego, CA: Academic Press. Chapter 1 – Introduction. (p.1)

Fraud analytics involves the use of algorithms, rules, and scenarios. Continuous data analytics are required to ensure that potential fraud risks are detected in a timely manner. Organizations shall produce data analytics reports, detailing procedures performed, parameter settings, results of data analytics (e.g. trends, patterns, anomalies, etc.) and action plan. For potentially fraudulent activities identified, they should be followed up and investigated appropriately.

4.3.2 Fraud Reporting (Whistleblower Programme)

Whistleblowing is “the disclosure by organization members (former or current) of illegal, immoral, or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action” (Near & Miceli, 1985). According to the 2022 ACFE Report to the Nations, 42% of frauds were detected by tips, which is nearly three times as many cases as the next most common method (i.e. internal audit, 16%)[24]. Maintaining a hotline or reporting mechanism increases the chances of earlier fraud detection and reduces losses. Fraud losses were twice higher at organizations without hotlines than organizations with hotlines (Association of Certified Fraud Examiners, 2022). A fraud risk management framework should include whistleblowing mechanisms for receiving reports both internally and externally.

An organization’s whistleblower programme should adhere to the followings:

- A clear whistleblower policy should be in place

The policy should state that the organization has zero tolerance for fraud. It should include, at a minimum, information on the scope of reporting, how and to whom to make a disclosure, procedures of an investigation and protection for whistleblowers. It

[24] Association of Certified Fraud Examiners. (2022). Occupational Fraud 2022: A Report to the Nations. (p.26)

should emphasize that confidentiality will be maintained unless the whistleblower agrees to be identified, identification is necessary to allow the organization to investigate or respond effectively to the disclosure or required by law.

- The whistleblower policy and programme should be clearly communicated

Organizations should consider how best to publicize and communicate the whistleblower policy to its employees.

- Organizations should set the expectations that suspected fraud should be immediately reported.

This would require a healthy and sustainable ethical culture within the organization. Employees should be encouraged to report wrongdoings in a timely manner.

Among the 42% of frauds detected from tips, 55% were reported by employees (Association of Certified Fraud Examiners, 2022). When looking at internal fraud reporting, whistleblowers mostly made their initial report to their direct supervisors (30%), executives of the organizations (15%), internal audit (12%) and the fraud investigation team (12%) (Association of Certified Fraud Examiners, 2022). Employees' perception towards the whistleblower programme is the key to its effectiveness. The programme will not be as effective as intended if employees do not feel safe in reporting. The word "retaliation" refers to any form of negative consequences of filing a report. From the NAVEX Global's 2021 Regional Whistleblowing Hotline Benchmark Report, there has been a decreasing trend of percentage of retaliation reports in the North American organizations since 2018 but a rising trend in the European organizations[25]. NAVEX Global further conducted a

[25] Penman, C., Painter, I., & Burt, A. (2021). Regional Whistleblowing Hotline Benchmark Report 2021. NAVEX Global, Inc. (p.35)

survey named “The State of Whistleblowing in Europe” in 2021 and it was found that “organizations are failing to put adequate protections in place to protect those who speak up” (Penman, Painter, & Burt, 2021). The survey found that “merely 56% of companies protect the confidentiality of whistleblowers and 31% track retaliations against a whistleblower after a report is produced” (Painter, 2022). Although the deadline for the EU member states to incorporate the EU Whistleblower Protection into their national laws was December 17th, 2021, a vast majority of countries did not meet this date due to local political bureaucracy, down-prioritization in the wake of COVID-19 pandemic, or other obstacles (Henriksson & Stappers, 2022). More work has to be done around protecting the whistleblowers. Ensuring retaliation does not occur may require training, policy or code of conduct updates and internal control. This is a key point of compliance, but more importantly contributes to ethical business and a healthy workplace environment.

4.3.3 Fraud Monitoring and Compliance Testing

Compliance testing can be defined as a periodic, independent, and objective assessment of compliance-related processes and/or controls. The aim of compliance testing is to assess whether the elements, processes and controls of the compliance programme are designed appropriately and are operating as designed. Compliance testing follows an established process and plan as well as, according to best practices, a risk-based approach. In general, compliance testing activities are performed within all three lines of defense where some are conducted by independent functions within the business, some are performed by compliance personnel, and others by the internal audit function (Besson, 2018).

Elements of fraud monitoring and compliance testing include:

4.3.3.1 Establish risk-based monitoring and testing plan

The monitoring and testing plan shall be derived from the relevant regulatory requirements as well as internal policies and procedures. The specific risks, and the elements of the monitoring and testing programme that will be tested, shall be identified based on a risk assessment in conjunction with the results of previous testing, the number of incidents and other metrics used by the organization to evaluate inherent and residual risks (Besson, 2018). The risk assessment performed to identify the areas of testing shall be documented with adequate rationale.

4.3.3.2 Execute plan

Testing shall be performed based on testing methodologies including sample methodologies, documentation standards, as well as standards and procedures for assessing the risk rating and classifying the nature of findings (Besson, 2018). Testing shall be performed by personnel independent from the testing process. The personnel shall also have adequate knowledge of the business process and risks involved.

4.3.3.3 Inform and report

Regular reporting to management is required to report findings and measures to be taken by the relevant process owners based on predefined reporting standards and procedures (Besson, 2018).

4.3.3.4 Track agreed remediation actions

A process should be put in place to ensure that remediation actions are tracked and completed accordingly.

4.3.3.5 Perform testing quality assessment

To ensure effectiveness, testing, reporting and remediation activities should be assessed on a regular basis to ensure that they are appropriate and are performed in accordance with predefined standards (Besson, 2018). Due to the change in business activities or market conditions, there may be improvement measures to the programme. These shall be communicated to the management as a feedback loop for continuous enhancement of the programme.

4.3.4 Auditing

4.3.4.1 Internal audit

The Institute of Internal Auditors defines internal audit as “an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes” (The Institute of Internal Auditors, n.d.).

Under a robust fraud risk management framework, independent audit (including regular and surprise audits) shall be performed by the internal audit team to evaluate first line and second line processes and determine whether controls are operating effectively to mitigate any fraud risks. Also, by performing audits, there could be a possibility to discover suspicious activities or potentially fraudulent activities. According to the 2022 ACFE Report to the Nations, internal audit is the second most common method for detecting occupation fraud[26] (Association of Certified Fraud Examiners, 2022).

[26] Association of Certified Fraud Examiners. (2022). Occupational Fraud 2022: A Report to the Nations. (p.22)

Although organizations vary in purpose, size, complexity, and structure, it is essential that internal auditors conform with the IIAA's International Standards for the Professional Practice of Internal Auditing ("the Standards") when conducting internal audit activities. The Standards are a set of principles-based, mandatory requirements consisting of basic requirements for the professional practice of internal auditing and for evaluating the effectiveness of performance. The Standards are internationally applicable at organizational and individual levels and include interpretations that clarified terms or concepts within the Standards (The Institute of Internal Auditors, n.d.).

4.3.4.2 External audit

External audit is required for public companies. External audit means "an examination of the financial statements, reports, documents, procedures, controls, or notices of any issuer, broker, or dealer by an independent public accounting firm in accordance with the rules of the Board or the Commission, for the purpose of expressing an opinion on the financial statements or providing an audit report" (Public Company Accounting Oversight Board (PCAOB), n.d.). The purpose of an external audit is to provide assurance that the books of an organization is free of material misstatement.

4.4 Fraud Response

4.4.1 Fraud Investigations[27]

Fraud investigations are broadly categorized into two categories: reactive and proactive. Reactive fraud investigations are performed in response to an alert of potential internal or external fraud. Conversely, proactive investigations occur as the result of investigator-

[27] The author of this paper had taken part in various forensic investigations since 2016. The content of this section is based on the author's experience and knowledge in the subject.

initiated action. Sometimes, investigators may be following the leads identified in a reactive investigation which allowed for deeper probe and the discovery of other fraudulent activities (Silverstone, Sheetz, & Pedneault, 2012). Nonetheless, both reactive and proactive investigations aim to determining whether allegations are substantiated, identifying the personnel involved, quantifying monetary losses, identifying whether similar fraud patterns or activities exist and making recommendations to prevent future occurrences of fraud with similar nature.

Organizations should include considerations for fraud investigations in their fraud risk management framework.

A fraud investigation is a fact-finding exercise which should address, at a minimum, the following questions:

- What?
    - What is the incident?
    - What are the allegations?
    - What is the impact?
- Who?
    - Who is the suspect/ target?
    - Who else was involved/ had knowledge of the incident?
- Where?
    - Where was the potential fraud happened?
    - Where does the report come from?
- How?
    - How was the potential fraud uncovered?

    - How is the potential fraud committed?
- When?
    - When was the potential fraud uncovered?
    - When did the potential fraud occur?
    - How long was the impacted period?
- Why?
    - Why was the perpetrator able to do what they did?

There could be different approaches in conducting a fraud investigation, but they all largely follow the same approach. An investigation lifecycle involves three stages: planning, execution, reporting and remediation.

4.4.1.1 Planning

A fraud investigation is often time sensitive and dependent on a detailed analysis of a large volume of information. It is important to develop an investigative plan for an investigation.

4.4.1.1.1 A good investigative plan

A good investigative plan has three major goals: to maintain focus, control growth, and promote adaptability (Silverstone, Sheetz, & Pedneault, 2012).

- Focus

  A strong investigative plan should focus investigators' efforts in-line with the goals of the investigation. This will minimize duplication of investigative efforts and oversight of areas which may be important to the investigation. In addition, this will also avoid the inefficient use of resources in an investigation.
- Control

Fraud investigations could grow extensively and without careful management, it could be catastrophic. It is important to define the scope of the investigation and maintain control over the investigative plan.

- Adaptability

  During an investigation, there could be situations that would require modifications to the investigative plan. Investigators may need to operate ad hoc or take the time to reevaluate and replan (Silverstone, Sheetz, & Pedneault, 2012). It is therefore necessary to allow buffer for built-in adaptability for an investigative plan.

4.4.1.1.2 3 C's of investigative management

Silverstone, Sheetz and Pedneault stated that there are 3 C's of investigative management: competence, corroboration, and common sense[28] (Silverstone, Sheetz, & Pedneault, 2012).

- Competence

  This refers to individuals that have the required skillsets as well as tools and solutions that are necessary to conduct a thorough analysis of the potential issues. Furthermore, considerations shall be given on additional resources to assist with a more effective investigation.

- Corroboration

  The concept of professional skepticism is crucial in a fraud investigation where no information should be taken at face value. The information that an investigator collected may include deficiencies, gaps, and weaknesses. An investigator should use multiple sources to check, review and verify the facts before making any conclusions.

[28] Silverstone, H., Sheetz, M., & Pedneault, S. (2012). Forensic accounting and fraud investigation for non-experts (3rd ed.) (p.152)

- Common sense

  Silverstone, Sheetz and Pedneault referred this as the "most important element [that] is the all-too-often forgotten piece that must be practiced throughout the investigative process" [29] (Silverstone, Sheetz, & Pedneault, 2012). It is essential to evaluate whether the elements (e.g. allegations, processes, witness accounts, etc.) in an investigation make sense.

4.4.1.1.3 Planning considerations

When planning an investigation, the following areas should be considered:

- Conflict of interest and independence

  "A conflict of interest occurs when an entity or individual becomes unreliable because of a clash between personal (or self-serving) interests and professional duties or responsibilities" (Segal, 2022). Considerations shall be given to ensure there is no conflict of interest which would impair the independence of the investigators of the investigated matters. For example, if an investigator is the person who reported the incident, he or she shall not be involved in the investigation. This is because there could be potential bias towards the case and there may be a tendency for the investigator to substantiate the case even if evidence failed to prove so.

- Legal considerations

  When the investigation is expected to bring civil liability for the organization, it may be more appropriate to structure the investigation as privilege. Legal professional privilege protects the communications between a professional legal

[29] Silverstone, H., Sheetz, M., & Pedneault, S. (2012). Forensic accounting and fraud investigation for non-experts (3rd ed.) (p.153)

advisor and his or her clients from being disclosed without the permission of the client.

- Competency and expertise of investigators

  An investigation could be more effective when investigators are teamed up with relevant expertise in the concerned subject matter (e.g. counsel, compliance, internal audit, external specialist, etc.).

- Establishment of scope and procedures

  Resonating with Silverstone, Sheetz and Pedneault's idea on "control", during the planning stage, it is necessary to define the scope of the investigation and determine the investigation procedures to avoid unnecessary delays in the investigation.

- Reporting obligations and potential consequences

  There could be potential reporting obligations to markets and regulators, as well as the potential legal or regulatory consequences (e.g. fines, prosecution, regulators rights, etc.) as a result of the investigation. When planning an investigation, it is necessary to identify such obligations and/or potential consequences to ensure compliance (e.g. reporting timeline, payment of fines, etc.).

4.4.1.2 Execution

Upon establishing an investigative plan, the investigation team could execute the investigation. An investigation requires the corroboration of information from multiple sources. As a result, it is necessary to identify the relevant information for an investigation.

4.4.1.2.1 Data universe

Information can be found in many different areas. The sources of information are broadly categorized in four areas as the followings:

- Electronic data (“e-discovery”)
    - E-mails
    - Financial data
    - Phone data
- Public domain
    - Public databases
    - Social media
    - Internet
- Hard copy documents
    - Contracts
    - Policies and procedures
    - Financial records
    - Supporting documents for transaction
- Meetings and interviews
    - Records – notes, transcript, meeting minutes, etc.
    - Whistleblowers
    - Witnesses
    - Suspects
    - Relevant stakeholders (e.g. suppliers, distributors, etc.)

4.4.1.2.2 Key considerations when collecting the information

With the sources of information, a decision needs to be made around data sources to collect, for which custodians, and for which period. Key questions when considering the scope are:

- What type of evidence will be most useful for the investigation?

- How long will evidence exist for – and can it be deleted?
- Company versus personal devices – what does the organization have access to?
- What is the cost of collection or processing?
- Is it worth "tipping off" the suspect to collect evidence? Is covert possible?

The following sections will discuss each source of information in greater detail.

4.4.1.2.3 Dealing with electronic data

Today, organizations use a wide range of devices and applications to store data. In order for electronic data to be entered as valid evidence in a court or in disciplinary proceedings, it is vital that an image of the relevant storage device (hard disk, server, cloud, smartphone, drone, smartwatch etc.) is taken at the earliest possible point in the investigation or even earlier to preserve the information in contemplation of a possible investigation (PwC Singapore, 2022). Forensic imaging is one element of computer forensics which involves taking a direct copy from the source so it cannot be later altered (TechTarget Contributor, 2022). Organizations should consider the feasibility and appropriateness of computer forensics in an investigation.

4.4.1.2.4 Gathering evidence from public domain

Another method to gather evidence is by conducting background search using public domains. A background search is a process to validate information about companies or individuals and to verify who they claim to be (TalentLyft, 2022). Investigators could gather evidence from the following sources:

- Corporate registry
- Regulation databases
- Litigation database

- Government tender records
- Global sanction records
- Media and Internet

4.4.1.2.5 Dealing with hard copy documents

Document review is a form of qualitative analysis that uses a systematic procedure to analyze documentary evidence. By reviewing hard copy documents, the investigations team could gain a better understanding of the concerned matter. It may also be possible to identify abnormalities or patterns that could be relevant findings for the investigation.

4.4.1.2.6 Interview

When deciding whether to conduct an interview during an investigation, the interviewer must consider the implications of each interview. The interview subject, who may be the victim, witness, or suspect, will learn much about the investigation based on the questions asked by the interviewer (Cendrowski, Martin, & Petro, 2007). Therefore, it is necessary to plan for the interview and consider the timing and/or sequence of the interviews.

4.4.1.3 Reporting and remediation

Upon conducting an investigation, one or more of the following actions may be taken:

- Reporting

  Reporting is a key component of an investigation. It communicates the investigation findings, ensures appropriate records and audit trails are maintained to connect investigation activities back to the approved plans, and document critical decisions made during the investigation.
- Internal control review

By applying the concept of the Three Lines of Defense Model, fraud risk management of an organization requires the collaborations between business. The investigation team could share findings of the investigation, with regards to confidentially, to the internal audit team to conduct an internal control review. This is to identify any internal control design weaknesses and operating weaknesses which might have been the cause of the fraud incident. The gaps shall be addressed to prevent future occurrences of similar fraud incidents.

- Remediation

  It is necessary to implement the recommended control procedures and remedial actions to strengthen risk management. The implementation of the controls shall be tracked and monitored.

- Public announcements

  Organizations may also share the investigation and internal control review results and the remediation work performed by making public announcements.

5. Case Study – Establishing a Fraud Risk Management Framework for a Southeast Asian Bank[30]

In 2017, a senior executive of an international bank ("the Bank") with headquarter in Southeast Asia was arrested and charged for alleged qualified theft, falsification, and violation of the local banking law. The trusted employee of the Bank for over 30 years

[30] In 2018, the author of this paper had taken part in an engagement for an independent review on governance and internal control framework for an international bank headquartered in Southeast Asia. In 2019, as the second phase of the engagement, the author had taken part in establishing a fraud risk management framework for the bank. Due to confidentiality, the name of the bank is not disclosed. The content of this section is based on the author's experience and knowledge of the engagement.

defrauded the bank by disbursing loans into fictitious accounts created in the name of one of the Bank's biggest corporate clients as well as various pseudo accounts. The fraud was discovered after a client denied drawing the loans. At least 12 executives and officers at the Bank were suspended over the CAD 42 million internal fraud cases, which included a 90-day suspension on the Bank's president as part of the sanctions imposed by the local regulator who "failed to perform adequate oversight" that led to the embezzlement by the bank officer. The news resulted in a dip of more than 5% in the Bank's shares. Subsequently, the local central bank required the Bank to allocate CAD 108 million to "to enhance protocols to improve corporate governance, credit administration, internal controls and audit, risk management, and customer onboarding and monitor within a year to prevent a repeat of the case".

As a result, the Bank engaged a third party to perform an independent review on the Bank's corporate governance and internal controls framework ("the Review").

5.1.1 Independent Review on the Bank's Corporate Governance and Internal Controls Framework

5.1.1.1 Scope of work

The key objective of the Review was to identify any deficiency in the Bank's corporate governance and internal controls framework and report to the Bank's management the findings and recommendations based on international practices. The scope of the review covered the evaluation of the Bank's governance framework, the design and operating effectiveness of its internal controls, development and overlay of fraud threat scenarios to identify control weaknesses, its cyber security capabilities as well as the IT governance and controls framework.

5.1.1.2 Key observations and findings

The Review covered a wide scope, based on the focus of the paper, details related to fraud risk management will be discussed.

5.1.1.2.1 Governance

During the review, it was identified that the Board of Directors and several Board-level committees are responsible for managing bank-wide fraud risk from different perspectives. For example, the Risk Committee is responsible for overseeing the relevant risk management policies and processes, whereas the Audit Committee oversees, and reviews fraud investigations and fraud risk assessment conducted by the Internal Audit Group. The Corporate Governance and Compensation Committee is responsible for approving the Code of Conduct as well as receiving monthly summary of fraud cases reported to the regular. It also oversees the business unit which is responsible for detecting and monitoring fraud risks for e-channels. There is a lack of oversight of bank-wide fraud risk holistically. It was noted that issues or red flags being identified in separate forums were not shared amongst relevant parties in a timely manner.

5.1.1.2.2 Fraud risk assessment

The Bank conducted its first fraud risk assessment in 2016 where the analysis was mainly based on historical fraud incidents. The FRA only covered business areas where fraud incidents occurred but did not assess the fraud risk exposure of other business areas. In addition, the assessment focused on customer-related fraud and did not consider other types of fraud such as third-party payment fraud and expense fraud. With the limited scope, the assessment did not appear to be comprehensive enough to help the Bank identify control gaps which has yet been exploited by fraudsters. This hindered the Bank from developing and performing process/ policy enhancements against potential fraud schemes.

5.1.1.2.3 Fraud analytics

The Bank has a team dedicated to performing fraud analytics and transaction monitoring. However, it only covered credit card transactions. It was noted that the Bank relied heavily on manual checking. For example, during the end of a business day, a branch officer would generate various reports for validation and reconciliation. This included reports on account opening, account closing, high-value withdrawals and more. Using the account opening report as an example, the officer would cross-check the logbook for new cards issued with the account opening report to ensure that there is no discrepancy. The officer would then sign the report as proof of validation. However, it was noted that the officers would simply sign the reports without checking the details. More analysis could be performed to identify anomalies if fraud analytics were available. For example, analysis could be performed on the number of bank accounts opened by the same employee over a period to identify abnormal activities. It could also be possible for the Bank to identify a customer who opened an account at various branches. Fraud analytics would allow the Bank to detect and identify areas for further investigation.

5.1.1.2.4 Fraud awareness training and communications

The Bank provided fraud-related training to staff during their induction and when they were being promoted to officers. However, it was noted that no other refresher training was provided to staff on a regular basis to keep them informed of any latest regulatory changes and/or market trends. Staff was also not required to perform annual certification to confirm their understanding of their responsibilities in managing and mitigating fraud risk. The

Bank started to conduct fraud roadshows during the time of the review. However, the roadshows only targeted to branch banking staff and did not apply to other business areas of the Bank. From time to time, the Bank would send communications related to fraud risks and/or fraud case studies to employees' company e-mail. However, it was noted that such communication did not reach all staff within the Bank as some of them did not have access to an e-mail account.

5.1.1.2.5 Fraud reporting (whistleblower programme)

The Bank has a whistleblower programme for individuals to report concerns. However, it was noted that no clear guidance was in place to report a case. In addition, cases were handled by different teams. There was no central depository of the cases, which made it difficult to generate meaningful management information. Some bank employees also mentioned that there were instances where employees had experienced retaliation (e.g. being identified and nicknamed as "the troublemaker", received a "non-satisfactory" performance rating despite exceeding sales target, etc.)

5.1.2 Enhancement on Existing processes and Establishment of a Fraud Risk Management Framework

With the above deficiencies identified, the Bank further requested for the enhancement on existing processes and establishment of a fraud risk management framework.

5.1.2.1.1 Governance

From the first phase of the engagement, it was identified that there is a lack of oversight in bank-wide fraud risks. A proposed target operating model was developed where a specific committee is created to oversee fraud risks. The committee includes several divisions for handling fraud prevention, detection, investigations, and monitoring and testing. One of the issues noted was that there were no formal policies and procedures for governing fraud risk management. As such, formalized policies, and procedures in relation to the fraud risk management were created.

5.1.2.1.2 Fraud risk assessment

The first fraud risk assessment conducted by the Bank was mainly based on the analysis on past incidents. The FRA methodology was uplifted to include the assessment of inherent risks, existing internal controls, and residual risks. In addition, FRA workshops were conducted with relevant stakeholders to obtain their input for a more comprehensive analysis.

5.1.2.1.3 Fraud analytics

Although fraud analytics was not included in the second phase, an introductory workshop on fraud analytics was conducted for the Bank's existing fraud analytics team as knowledge sharing.

5.1.2.1.4 Fraud awareness training and communications

The training materials were redesigned to include concepts of fraud prevention, detection, and response. Cases studies were also changed from hypothetical cases to actual cases faced by the Bank and/or other Banks. This would raise the Bank's employees' awareness on recent fraud cases.

5.1.2.1.5 Fraud reporting (whistleblower programme)

As part of the uplifted policies and procedures, clear guidelines on fraud reporting were included.

6. Challenges in Fraud Risk Management

Although there is a structured framework, organizations still face different types of challenges in fraud risk management. Listed below are some of the challenges that may be faced by organizations.

6.1.1 Fraud analytics-related challenges

Fraud analytics is an effective way to identifying fraud as much as when data is available and that they are of good quality. Inability to access data required for analytics or poor data quality will limit the effectiveness of the analysis. Organizations should ensure data analytics is a consideration when designing processes, systems, or controls. Even when data is available and is of good quality, the value of the analytics will be limited when data analysts lack understanding in the business processes or environments. Organizations should ensure data analysts are involved in the end-to-end audit or investigation and consider upskilling current business/ functional SMEs to data analysts, rather than the other way around. Also, it is not uncommon that fraud monitoring tools generate too many false positives. Organizations should ensure that appropriate piloting and testing is performed before rolling out enterprise wide. It is crucial to have appropriate feedback and tuning mechanism to improve the fraud analytics tools. In addition, organizations may not have enough demand for dedicated data analysts in each business area. As such, they may consider pooling resources.

6.1.2 Difficulties in Cost-Benefit Analysis

It was estimated that organizations lose 5% of revenue to fraud every year which was estimated to more than USD 4.7 trillion lost to fraud globally (Association of Certified

Fraud Examiners, 2022). A head of fraud investigation for a major bank expressed that “A £1m increase in expenditure on fraud prevention has led to a
£25m increase in profits” (CIMA, 2008). Resources are limited and every organization is different. There is no one equation to analysis the cost-benefit in fraud risk management. There are generic framework and guidelines on best practice regarding fraud risk management. However, it is difficult to measure what “good” or “enough” is. An organization which follows the COSO framework could still suffer from substantial fraud losses. This would depend on the risk appetite of an organization to decide how much to put into fraud risk management.

6.1.3 Lack of a Holistic View on Risks

As in the case of the case study, organizations may lack a holistic view on risks. Actions taken may well often be reactive where the intention is to respond to a fraud that occurred. However, management may not understand the fraud implications for a failure. A fraud that occurred in a division may be caused by the internal control weakness of another division. There is a need to perform root cause analysis and allow a feedback loop for a comprehensive information flow.

7. Looking Ahead – Trends in Fraud and Fraud Risk Management

Fraud is inevitable but organizations can learn about the trends in fraud and fraud in fraud risk management to better prepare themselves.

7.1.1 Increasing Fraud Loss in Wire Fraud through Business E-mail Compromise ("BEC")/ E-mail Account Compromise ("EAC")

An electronic fund transfer, also known as wire transfer, is "a transaction by which funds move from one institution to another or one account to another at the direction of an institution's customer and through the transmission of electronic instruction
messages that cause the institutions to make the required bookkeeping entries
and make the funds available" (U.S. Department of the Treasury, n.d.). There are various wire transfer operations, for example, Fedwire, Clearing House Interbank Payments System (CHIPS) and Society for Worldwide Interbank Financial Telecommunication (SWIFT) (Internet Crime Complaint Center, Federal Bureau of Investigation, 2022). A wire fraud is a type of fraud that involves the use of some form of telecommunications or the internet. These include all forms of electronic media including telephone, e-mail, social media, or text messaging (Hayes, Wire Fraud, 2021).

In the past, fraudsters hacked or spoofed business and personal e-mail accounts and requested wire payments to fraudulent bank accounts (Internet Crime Complaint Center, Federal Bureau of Investigation, 2022). The COVID-19 pandemic and the restrictions on in-person meetings led to increases in online collaboration or virtual communication practices for organizations (Internet Crime Complaint Center, Federal Bureau of Investigation, 2022). Fraudsters have become more sophisticated where they are now using virtual meeting platforms to hack e-mails and spoof executive's credentials to initiate fraudulent wire transfers (Internet Crime Complaint Center, Federal Bureau of Investigation, 2022). According to the Internet Crime Complain Center's ("IC3") 2021 Internet Crime Report, there has been a rising trend in losses through BEC/EAC in the past three years. There was a 5.07% surge from 2019 to 2020 and a 28.36% surge from 2020 to 2021. This represents a total of 34.87% increase from 2019 to 2021, with USD 2.4 billion loss in 2021[31] (Internet Crime Complaint Center, Federal Bureau of Investigation, 2022). This could be an indication for organizations to enhance their IT security as well as educating their employees to raise their awareness.

7.1.2 Rising trend in identity theft/ account takeover

Identity theft is when someone steals and uses personal identifying information (e.g. name, identification number, date of birth, etc.) without permission to commit fraud or other crimes and/or, in the case of an account takeover, a fraudster obtains account information to perpetrate fraud on existing accounts (Internet Crime Complaint Center, Federal Bureau of Investigation, 2022). Identity theft is one of the top five crimes reported in 2021[32]. Fraudsters targeted the real estate and rental sector where they would assume the identity of the title, real estate agent or closing attorney and forge the individual's email and other details about the transaction. The fraudsters would then send an e-mail to the unknowing buyer, with an e-mail address that is similar to the individual's and provide new wire instructions to the criminal's bank account (Chatman, 2022).

Another prevailing area of account takeover is through SIM swap fraud. Fraudsters would gather personal details about the victim and contact the victim's mobile telephone provider to transfer the phone number to the fraudster's SIM. This allows the fraudster to begin receiving communications associated with the victim's phone number, including access to social media profiles, bank accounts and more (Cellular Telecommunications Industry

[31] Internet Crime Complaint Center, Federal Bureau of Investigation. (2022, March 22). Internet Crime Report 2021. (p.25)

[32] Internet Crime Complaint Center, Federal Bureau of Investigation. (2022, March 22). Internet Crime Report 2021. (p.22)

Association, 2022). Research by Javelin indicated that mobile account takeover through SIM swap fraud doubled from 360,000 cases to more than 680,000 cases in a year (SAS, 2022). In addition, fraudsters are using sophisticated bots to automate account takeover attempts which further adds challenges for companies to distinguish legitimate customers from fraudsters (LexisNexis, 2022).

With the growing concerns with OTP-based authentication, organizations shall explore other risk-based authentication mechanisms leveraging biometrics, location, historical payments, digital tokens, and in-app notifications (Bose S. , 2022).

7.1.3 Need for real-time assessment/ demand for information transparency

The Central Bank of India expects the Immediate Payment Service ("IMPS") and National Electronic Funds Transfer ("NEFT") to grow at an annual average of 20% (Bose S. , 2022). In the Payments Vision 2025 document by the Department of Payment and Settlement Systems of the Reserve Bank of India, it was stated that "it is essential to move towards real / near real-time reporting of payment frauds and put in place an integrated platform for all stakeholders (payment system operators and participants – banks and non-banks, law enforcement agencies, etc.) to share information and initiate necessary corrective action to prevent frauds"[33] (Reserve Bank of India, 2022).

As a matter of fact, real-time assessments and information sharing between different institutions have become more common to combating fraud. In February 2018, the Internet Crime Complaint Center's Recovery Asset Team ("RAT") was established to streamline communication with financial institutions and assist Federal Bureau of Investigation ("FBI") field offices with the freezing of funds for victims who made transfers to domestic

[33] Reserve Bank of India. (2022, June 17). Vision Documents. (p.14)

accounts under fraudulent pretenses[34]. The RAT functions as a liaison between law enforcement and financial institutions supporting statistical and investigative analysis (Internet Crime Complaint Center, Federal Bureau of Investigation, 2022). When a victim sends a complaint to IC3, it will be automatically triaged through the FBI Internet Crime Database. After performing the analysis and when a complaint is deemed valid, transaction details are forwarded to the relevant point of contact at the recipient bank to notify of fraudulent activity and request freezing of the account. Once response is received from the recipient bank, RAT contacts the appropriate FBI field office(s) for actions (Internet Crime Complaint Center, Federal Bureau of Investigation, 2022). RAT has been proven to be a valuable resource for field offices and victims with a 74% success rate to date. Out of the USD 443.48 million losses, USD 328.32 million had been successfully frozen[35] (Internet Crime Complaint Center, Federal Bureau of Investigation, 2022).

Due to the recent corporate scandals, such as the collapse of one of Asia's largest oil traders Hin Leong Trading Pte Ltd. in 2020, in the trade finance and bunkering industry, Singapore has tightened the oversight in this sector (Daga & Lerh, 2022).

After a year’s effort, the Singapore Trade Data Exchange (“SGTraDex”) was launched on June 1 2022 by Singapore’s Infocomm Media Development Authority (“IMDA”) (Atkins, 2022). SGTraDex is a data-sharing platform with more than 70 banks, ports, shipping companies and commodity exporters. It provides a centralized gateway that allows companies to share trade data securely through Application Programming Interface (“API”) integration (Wragg, 2021). An SGTraDex spokesperson stated that “SGTraDex will

[34] Internet Crime Complaint Center, Federal Bureau of Investigation. (2022, March 22). Internet Crime Report 2021. (p.10)

[35] Internet Crime Complaint Center, Federal Bureau of Investigation. (2022, March 22). Internet Crime Report 2021. (p.11)

connect with existing industry data solution providers and data consolidators supporting the oil trading value chain, container location and status event data, and digitized bunkering transaction data to provide business stakeholders actionable insights from the physical flow of goods and financiers with improved visibility to mitigate potential fraudulent transactions" (Wragg, 2021). One of the main use cases of the platform is to prevent fraud by detecting attempts by companies to fraudulently obtain financing twice from the same cargo or using fake documents (Atkins, 2022).

Although there are benefits from information sharing among organizations, there could be concerns regarding data privacy, information security, cross-border information sharing that need to be considered.

8. Conclusion

Preventing fraud is a complex challenge. There is no one-size-fit-all approach for organizations in managing fraud risks. It depends on the risk appetite of the organizations to decide on the degree of anti-fraud measures. These include governance, training, internal controls and, increasingly, the use of sophisticated technology. Nonetheless, it is proven that fraud costs are lower for organizations with anti-fraud controls than organizations with little to no controls. Organizations shall continue its efforts in protecting themselves against the harms of fraud.

Appendix 1 17 Internal Control Principles of COSO's 2013 Framework[36]

Control Environment

1. The organization demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Risk Assessment

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.
9. The organization identifies and assesses changes that could significantly affect the system of internal control.

[36] Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013, May). Internal Control - Integrated Framework Executive Summary. (p.6-7)

Control Activities

10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
11. The organization selects and develops general control activities over technology to support the achievement of objectives.
12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Information and Communication

13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.
14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
15. The organization communicates with external parties regarding matters affecting the functioning of internal control.

Monitoring Activities

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Appendix 2 20 Enterprise Risk Management Principles of COSO's 2017 Framework[37]

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change

[37] Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017, June). Enterprise Risk Management Integrating with Strategy and Performance Executive Summary. (p.7)

16. Reviews Risk and Performance

17. Pursues Improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology

19. Communicates Risk Information

20. Reports on Risk, Culture, and Performance

Works Cited

Basel Committee on Banking Supervision. (2006, June 30). *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework.* Retrieved June 2022, from Bank for International Settlements: https://www.bis.org/publ/bcbs128.pdf

Accounting Tools. (2022, May 24). *Inherent risk definition*. Retrieved June 2022, from Accounting tools: https://www.accountingtools.com/articles/what-is-inherent-risk.html

American Institute of Certified Public Accountants. (2016). *Management Override of Internal Control: The Archilles' Heel of Fraud Prevention.* Retrieved June 2022, from https://us.aicpa.org/content/dam/aicpa/forthepublic/auditcommitteeeffectiveness/downloadabledocuments/achilles_heel.pdf

Association of Certified Fraud Examiners. (2022). *Occupational Fraud 2022: A Report to the Nations.* Retrieved June 2022, from https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf

Atkins, J. (2022, June 2). *Singapore's trade data platform goes live*. Retrieved June 2022, from Global Trade Review: https://www.gtreview.com/news/asia/singapores-trade-data-platform-goes-live/#:~:text=SGTraDex%20is%20essentially%20a%20data,various%20parties%20involved%20in%20trade.

Besson, V. (2018, April). *How can your organisation perform effective and efficient compliance testing?* Retrieved June 2022, from PricewaterhouseCoopers AG:

https://www.pwc.ch/en/publications/2018/pwc_ch_white%20paper_can%20your%20organisation%20perform%20effective%20compliance%20testing.pdf

Bolton, R. J., & Hand, D. J. (2002, August 1). Statistical Fraud Detection: A Review. *Statistical Science, 17*(3), 235-249. Retrieved June 2022, from: https://projecteuclid-org.myaccess.library.utoronto.ca/journals/statistical-science/volume-17/issue-3/Statistical-Fraud-Detection-A-Review/10.1214/ss/1042727940.full

Bose, I., & Mahapatra, R. K. (2001). Business data mining — a machine learning perspective. *Information & Management, 39*(3), 211-225. Retrieved June 2022, from https://doi-org.myaccess.library.utoronto.ca/10.1016/S0378-7206(01)00091-X

Bose, S. (2022, June 18). *Vision Document: RBI sees digital payment transactions trebling by 2025*. Retrieved June 2022, from Financial Express: https://www.financialexpress.com/industry/banking-finance/vision-document-rbi-sees-digital-payment-transactions-trebling-by-2025/2564665/

Cellular Telecommunications Industry Association. (2022). *Protecting Your Wireless Account Against SIM Swap Fraud*. Retrieved June 2022, from Consumer Resources: https://www.ctia.org/protecting-against-sim-swap-fraud

Cendrowski, H., Martin, J., & Petro, L. (2007). *The handbook of fraud deterrence.* Hoboken, N.J.: Wiley.

CFI Education Inc. (2022, January 30). *Fraud Triangle*. Retrieved June 2022, from CFI:

https://corporatefinanceinstitute.com/resources/knowledge/accounting/fraud-triangle/

Chatman, S. (2022, March 22). *Real estate wire fraud scams cost victims tens of thousands in house down payment money*. Retrieved June 2022, from ABC7 Eyewitness news: https://abc7chicago.com/house-down-payment-wire-transfer-instructions-fraud-mortgage/11670854/

Chen, J. (2021, December 8). *Neural Network*. Retrieved June 2022, from Investopedia: https://www.investopedia.com/terms/n/neuralnetwork.asp

CIMA. (2005). *CIMA Official Terminology.* Oxford.

CIMA. (2008). *Fruad risk management A guide to good practice*. Retrieved June 2022, from CIMA Global: https://www.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf

COSO. (2013, May). *COSO Internal Control-Integrated Framework Frequently Asked Questions.* Retrieved June 2022, from Guidance on Internal Control: https://www.coso.org/Shared%20Documents/COSO-FAQs-May-2013-branded.pdf

COSO. (2013, May). *Internal Control - Integrated Framework Executive Summary.* Retrieved June 2022, from Guidance on Internal Control: https://www.coso.org/Shared%20Documents/Framework-Executive-Summary.pdf

COSO. (2016, November). *Guidance on Enterprise Risk Management Frequently Asked Questions.* Retrieved June 2022, from Guidance on Enterprise Risk

Management: https://www.coso.org/Shared%20Documents/COSO-ERM-FAQ.pdf

COSO. (2016, September). *Fraud Risk Management Guide.* Retrieved June 2022, from https://www.coso.org/Shared%20Documents/COSO-Fraud-Risk-Management-Guide-Executive-Summary.pdf

COSO. (2017, June). *Enterprise Risk Management Aligning Risk with Strategy and Performance Executive Summary.* Retrieved June 2022, from https://www.coso.org/Shared%20Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

COSO. (2022, April 22). *Enterprise Risk Management—Integrating with Strategy and Performance (2017)*. Retrieved June 2022, from https://www.coso.org/SitePages/Enterprise-Risk-Management-Integrating-with-Strategy-and-Performance-2017.aspx?web=1

COSO. (2022, April 26). *About Us*. Retrieved June 2022, from Committee of Sponsoring Organizations of the Treadway Commission: https://www.coso.org/SitePages/About-Us.aspx

Daga, A., & Lerh, J. (2022, June 2). *Singapore's new trade data sharing platform aims to stem fraud*. Retrieved June 2022, from Reuters: https://www.reuters.com/markets/commodities/singapores-new-trade-data-sharing-platform-seeks-stem-fraud-2022-06-01/

Davies, & Zhivitskaya, M. (2018). Three Lines of Defence: A Robust Organising Framework, or Just Lines in the Sand? *Global Policy, 9*(S1), 34–42. https://doi.org/10.1111/1758-5899.12568

ECIIA/FERMA. (2010, September 21). *Guidance on the 8th EU Company Law Directive, Article 41.* Retrieved June 2022, from Guidance for boards and audit committees: https://www.iia.nl/SiteFiles/ECIIA%20FERMA.pdf

Gee, J., & Button, M. (2021, June 23). *The financial cost of fraud 2021 - the latest data from around the world.* Retrieved June 2022, from Insights: https://www.crowe.com/uk/insights/financial-cost-fraud-data-2021

Giardino, J. (2014, March/April). *Caught by the numbers*. Retrieved June 2022, from Fraud Magzine: https://www.fraud-magazine.com/article.aspx?id=4294981970

Hayes, A. (2021, March 8). *Wire Fraud*. Retrieved June 2022, from Investopedia: https://www.investopedia.com/terms/w/wirefraud.asp

Hayes, A. (2022, March 19). *Probability Distribution*. Retrieved June 2022, from Investopedia: https://www.investopedia.com/terms/p/probabilitydistribution.asp#:~:text=A%20probability%20distribution%20is%20a,take%20within%20a%20given%20range.

Hongxing, H., Jincheng, W., Graco, W., & Hawkins, S. (1997). Application of Neural Networks to Detection of Medical Fraud. *Expert Systems with Applications, 13*(4), 329–336. https://doi.org/10.1016/S0957-4174(97)00045-6

Henriksson, K., & Stappers, J. (2022, April 7). *The EU Whistleblowing Directive*. Retrieved June 2022, from Risk & Compliance Matters: https://www.navexglobal.com/blog/article/the-eu-whistleblowing-directive/

Internet Crime Complaint Center, Federal Bureau of Investigation. (2022, March 22). *Internet Crime Report 2021*. Retrieved June 2022, from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Janalta Interactive. (n.d.). *Data Matching*. Retrieved June 2022, from Techopedia: https://www.techopedia.com/definition/28041/data-matching

Kanade, V. (2021, June 16). *What Is Fraud Detection? Definition, Types, Applications, and Best Practices*. Retrieved June 2022, from TOOLBOX: https://www.toolbox.com/it-security/vulnerability-management/articles/what-is-fraud-detection/

KPMG Advisory (China) Limited. (2014, May 19). *Fraud risk management: Developing a strategy for prevention, detection, response.* Retrieved June 2022, from Fraud risk management: Developing a strategy for prevention, detection, response: https://home.kpmg/cn/en/home/insights/2014/05/fraud-risk-management-strategy-prevention-detection-response-o-201405.html

LexisNexis. (2022). *Critical Insights on Key Fraud Cost Drivers*. Retrieved June 2022, from Discover the True Cost of Fraud: https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study#realestate

Li, J. (2022, May 9). E-Commerce Fraud Detection Model by Computer Artificial Intelligence Data Mining. *Computational Intelligence and Neuroscience, 2022*(Article ID 8783783), 9 pages. Retrieved June 2022, from https://doi.org/10.1155/2022/8783783

Lopez, M. (2017, December 1). *Metrobank president, officials to be suspended for fraud case*. Retrieved June 2022, from BusinesWorld:

https://www.bworldonline.com/editors-picks/2017/12/01/85142/metrobank-president-officials-suspended-fraud-case/

Mercer, L. C. (1990). Fraud Detection via Regression Analysis. *Computers & Security, 9*(4), 331-338. Retrieved June 2022, from https://doi.org/10.1016/0167-4048(90)90103-Z

Near, & Miceli, M. P. (1985). Organizational Dissidence: The Case of Whistle-Blowing. *Journal of Business Ethics, 4*(1), 1–16. https://doi.org/10.1007/BF00382668

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems, 50*(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006

Open Risk Manual. (n.d.). *External Fraud*. Retrieved June 2022, from https://www.openriskmanual.org/wiki/External_Fraud

Painter, I. (2022, February 21). *Whistleblowing in Europe: Key Insights for 2022 Webinar*. Retrieved June 2022, from Regulatory Compliance: https://www.navexglobal.com/blog/article/whistleblowing-in-europe-key-insights-for-2022-webinar/

Penman, C., Painter, I., & Burt, A. (2021). *Regional Whistleblowing Hotline Benchmark Report 2021.* NAVEX Global, Inc. Retrieved June 2022, from https://www.navex.com/en-gb/resources/benchmark-report/2021-regional-whistleblowing-hotline-benchmark-report/

Public Company Accounting Oversight Board (PCAOB). (n.d.). *Registration, Annual and Special Reporting*. Retrieved June 2022, from Definitions of Terms Employed in Registration and Reporting Forms: https://rasr.pcaobus.org/GlossaryTerms/GlossaryTerms.aspx

PwC Singapore. (2022). *Forensic Technology Solutions*. Retrieved from https://www.pwc.com/sg/en/services/consulting/forensics/forensic-technology-solutions.html

Radičević, Trivanović, M. S., & Stanojević, L. (2017). Three lines of defence model and the role of internal audit activities as the response to the global economic crisis. *IOP Conference Series: Materials Science and Engineering, 200*(1), 12061–. https://doi.org/10.1088/1757-899X/200/1/012061

Reserve Bank of India. (2022, June 17). *Vision Documents.* Retrieved June 2022, from Reserve Bank of India India's Central Bank: https://rbidocs.rbi.org.in/rdocs//PublicationReport/Pdfs/PAYMENTSVISION2025844D11300C884DC4ACB8E56B7348F4D4.PDF

SAS. (2022). *Managing fraud risk: 10 trends you need to watch*. Retrieved June 2022, from SAS Insights: https://www.sas.com/en_si/insights/articles/risk-fraud/managing-fraud-risk--10-trends-you-need-to-watch.html

Segal, T. (2022, March 24). *Conflict of Interest*. Retrieved June 2022, from Investopedia: https://www.investopedia.com/terms/c/conflict-of-interest.asp

Shackleford, D. (2022). *Residual risk*. Retrieved June 2022, from TechTarget: https://www.techtarget.com/searchsecurity/definition/residual-risk

Silverstone, H., Sheetz, M., & Pedneault, S. (2012). *Forensic accounting and fraud investigation for non-experts (3rd ed.).* Hoboken, N.J.: Wiley.

Sujeewa, G. M., Yajid, M. S., Khatibi, A., Azam, S. F., & Dharmaratne, I. (2018, August). The New Fraud Triangle Theory - Integrating Ethical Values of Employees. *International Journal of Business, Economics and Law, Vol. 16, Issue 5*, 52-57. Retrieved June 2022, from http://ijbel.com/wp-content/uploads/2018/08/ijbel5_216.pdf

TalentLyft. (2022). *What is Background Check?* Retrieved June 2022, from TalentLyft: https://www.talentlyft.com/en/resources/what-is-background-check

TechTarget Contributor. (2022). *Forensic image*. Retrieved June 2022, from https://www.techtarget.com/whatis/definition/forensic-image#:~:text=Forensic%20imaging%20is%20one%20element,backup%20software%20create%20forensic%20images.

The Institute of Internal Auditors. (n.d.). *Definition of Internal Auditing*. Retrieved June 2022, from https://www.theiia.org/en/standards/what-are-the-standards/mandatory-guidance/definition-of-internal-audit/

The Institute of Internal Auditors. (n.d.). *Introduction*. Retrieved June 2022, from https://www.theiia.org/en/standards/what-are-the-standards/mandatory-guidance/standards/introduction/

The Institute of Internal Auditors. (n.d.). *Standards Glossary*. Retrieved June 2022, from https://www.theiia.org/en/standards/what-are-the-standards/mandatory-guidance/standards/standards-glossary/

The Law Dictionary. (n.d.). *Fraud Definition & Legal Meaning*. Retrieved June 2022, from https://thelawdictionary.org/fraud/

Theodoridis, S., & Koutroumbas, K. (2006). *Pattern Recognition (3rd ed.).* San Diego, CA: Academic Press. https://doi.org/10.1016/B978-012369531-4/50000-7

U.S. Department of the Treasury. (n.d.). *Appendix D - Fundamentals of the Funds Transfer Process*. Retrieved June 2022, from https://www.fincen.gov/sites/default/files/shared/Appendix_D.pdf

Venzon, C. (2017, July 21). *Philippine lender hit by $34.5m fraud*. Retrieved from NikkeiAsia: https://asia.nikkei.com/Economy/Philippine-lender-hit-by-34.5m-fraud

Wragg, E. (2021, July 14). *IMDA signs deal with banks, shippers, ports to digitalise supply chain ecosystem*. Retrieved June 2022, from Global Trade Review: https://www.gtreview.com/news/fintech/imda-signs-deal-with-banks-shippers-ports-to-digitalise-supply-chain-ecosystem/