Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 3, 125-144
2024
Publisher: Learning Gate
DOI: 10.55214/25768484.v8i3.804

Examining government officials' perceived risk management and internal control in combating fraud in the public sector

Azleen Ilias[1], Nasrudin Baidi[2], Erlane K. Ghani[3*], Kamaruzzaman Mohammad[3], Akrom Omonov[4]
[1]Department of Accounting and Finance, College of Business and Administration, Uniten Business School, Institute of Energy, Policy, and Research, Universiti Tenaga Nasional, 26700, Pahang, Malaysia; azleens@uniten.edu.my (A.I.).
[2]Department of Business and Management, College of Business and Administration, Uniten Business School, Institute of Energy, Policy, and Research, Universiti Tenaga Nasional, 26700, Pahang, Malaysia; nasrudin@uniten.edu.my (N.B.).
[3]Faculty of Accountancy, UniversitiTeknologi MARA Cawangan Selangor, 42300 Bandar Puncak Alam, Selangor, Malaysia; erlanekg@uitm.edu.my (E.K.G); kamaruzzaman@uitm.edu.my (K.M.).
[4]Department of Banking, Tashkent Institute of Finance, Uzbekistan; akromomonov66@gmail.com (A.O.).

Abstract: This study aims to examine the perception of risk management and internal control in the public sector, specifically concerning preventing fraud. Specifically, this study examines the various aspects of fraud prevention among employees in the public sector, including goal formulation, internal environment, and communication of information, risk response, monitoring, risk assessment, and control actions. A total of 537 individuals working in the procurement and finance departments of federal ministries participated in a questionnaire survey conducted using the Committee of Sponsoring Organizations framework and focused on fraud prevention. This study shows that risk assessment, control actions, and information and communication exert a favorable influence on the prevention of fraudulent activities. This study revealed that risk assessment, control actions, and information and communication exert a favorable influence on the prevention of fraudulent activities. This study can contribute to the government's efforts in improving risk management, addressing corruption, and advancing the Sustainable Development Goal (SDG) 12 and 16 initiatives.

Keywords: *Committee of sponsoring organizations, Enterprise risk management, Federal ministries, Fraud, Internal control, Malaysia, Risk management, Sustainable development goal.*

1. Introduction

Fraud risk is one of the hot issues, whether in the public or private sector, that could happen at the management and supporting levels. Fraud could occur due to factors such as a lack of internal control in the organisation, limited employee education and competence, and a lack of tone at the top [1]. According to the Association of Certified Fraud Examiners (ACFE) [1], corruption is the highest standard fraud scheme for the government sector, and this is aligned with the Malaysian Corruption Perceptions Index (CPI) in Table 1, while external audit of financial statements, code of conduct, internal audit department, and hotline are the most common anti-fraud controls. According to the data, Malaysia's CPI ratings have fluctuated over the years but have consistently remained around the late 40s to early 50s. The CPI implies that the country's impression of moderate corruption is stable, with slight changes from year to year. The CPI scores have been relatively stable, with most years falling within a small range. It could imply that the perception of corruption in Malaysia has not changed significantly during this period. CPI ratings have stayed in the upper 40s to low 50s in recent years (2020, 2021, and 2022), indicating a moderate level of perceived corruption. The external variables such as changes in government policy, anti-corruption campaigns, and high-profile corruption cases can all impact a country's image of corruption.

History: Received: 29 December 2023; Revised: 16 February 2024; Accepted: 27 February 2024; Published: 19 March 2024
* Correspondence: erlanekg@uitm.edu.my

Identifying corruption risks relevant to the Malaysian context should be part of risk management practices. Over time, the volatility in CPI scores demonstrates that the corruption landscape is changing, emphasising the significance of continuing risk assessment and monitoring. In an environment where corruption threats abound, the requirement for strong internal controls is obvious. Risk management and internal control should work in tandem to handle corruption issues. They should be incorporated into an organization's governance framework to ensure that anti-corruption initiatives are consistent with overall risk mitigation and control techniques.

Table 1.
Malaysian corruption perceptions index (CPI).

Year	CPI score over 100 points
2012	49
2013	50
2014	52
2015	50
2016	49
2017	47
2018	47
2019	53
2020	51
2021	48
2022	47

Source: Transparency International [2].

Hence, a thorough analysis of the significance of risk management and internal control elements that could impact fraud prevention is warranted to enhance the comprehension of risk management among public sector personnel. However, limited research has investigated employees' opinions of risk management and internal control in fraud prevention within the public sector [3, 4]and the early process of the implementation of risk management and internal control (such as Ilias, et al. [5] and Setapa and Zakwan [6]).

Therefore, this study investigates the public sector's perception of risk management and internal control regarding fraud prevention. The outcomes of this investigation are anticipated to provide valuable insights for the government in formulating a more extensive risk management and internal control structure to mitigate corruption within the public sector. The results of this current study align with the government's Sustainable Development Goal [7], which aims to advance sustainable public procurement practices through national policies and priorities. Additionally, it aligns with the Sustainable Development Goal [7] initiative, which seeks to foster peace, justice, and strong institutions. Sustainable Development Goal [7] aims to mitigate the prevalence of corruption and bribery in all their forms.

The subsequent part, Section 2, provides an overview of the existing literature. Subsequently, Section 3 outlines the research design, while Section 4 provides the results and engages in a comprehensive debate. The study is concluded in the final part, namely, Section 5.

2. Literature Review

2.1. Fraud Prevention

Prevention is important in order to reduce possible fraud, such as corruption. Peltier-Rivest [8] proposed prevention model, such as the implementation of efficacious prevention programmes within organisations and governmental entities, has the potential to eliminate the underlying causes of corruption and mitigate the accompanying negative consequences by formulating and executing preventive frameworks that effectively mitigate factors that drive fraudulent behaviour, diminish

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 3: 125-144, 2024
DOI: 10.55214/25768484.v8i3.804

perceived possibilities for misconduct, and enhance ethical standards. The primary types of occupational fraud fall into three categories, according to a report published by the Association of Certified Fraud Examiners (ACFE) [1]. The first category is asset misappropriation, which refers to instances where an employee unlawfully appropriates or misuses the resources belonging to their employer. The second category is financial statement fraud, when a perpetrator deliberately manipulates an organisation's financial statements, leading to material misstatements or omissions. The third category is corruption, encompassing various offenses such as bribery, conflicts of interest, and extortion. According to theAssociation of Certified Fraud Examiners (ACFE) [1], it has been noted that there are eight prevalent behavioural indicators of fraud. These include living beyond one's means, experiencing financial difficulties, maintaining an unusually close relationship with a vendor or customer, exhibiting excessive control tendencies or reluctance to delegate responsibilities, displaying abnormal levels of irritability, suspicion, or defensiveness, engaging in bullying or intimidation tactics, undergoing recent divorce or family issues, and demonstrating a general inclination towards shrewd or unscrupulous behaviour, commonly referred to as a "wheeler-dealer" attitude. The detection and prevention of fraud concerns in organisations pose significant challenges, necessitating robust measures to mitigate losses. Fraud prevention refers to a set of proactive measures and strategies implemented by organisations to avoid or mitigate the occurrence of fraudulent activities and reduce the risk of fraud [9].

The Association of Certified Fraud Examiners (ACFE) suggests using anti-fraud measures to reduce fraudulent actions. These procedures encompass the implementation of external audits to assess the accuracy of financial accounts and the establishment of a documented code of conduct. Significantly, these measures were observed to be implemented in 82% of the businesses that experienced fraud. Other commonly used measures include the existence of an internal audit department, which is found in 77% of cases; management certification of financial statements, observed in 74% of instances; and an external (independent) audit of the internal controls over financial reporting, which is implemented in 71% of scenarios.Shonhadji and Maulidi [10] proposed the implementation of fraud awareness and whistleblowing mechanisms as a means to discourage the creation of fake financial statements. Tarjo, et al. [11] discuss the tactics and strategies used to reduce fraudulent activity in an organization or system. Halbouni, et al. [12] highlighted the significance of internal and external audits as well as governance in preventing and detecting fraud. Enterprise Risk Management (ERM) encompasses the evaluation and control of hazards in several aspects of an organisation, such as the control environment, risk assessment, control activities, information and communication, and monitoring. This aligns with the preventative model described in Peltier-Rivest [8]. The aforementioned elements of risk management have been determined to exert a noteworthy influence on the prevention and identification of fraudulent activities. Organisations should take a proactive approach by implementing a complete range of anti-fraud procedures, internal controls, and risk management techniques to strengthen their defenses against fraudulent activity.

2.2. Concept of Risk Management and Internal Control

The COSO [13] refers to the Committee of Sponsoring Organizations' Enterprise Risk Management Framework, published in 2004. The 2004 COSO ERM Framework expanded on the Risk Assessment component of the Internal Control Framework and provided comprehensive guidance on enterprise risk management.Prewett and Terry [14] also suggested that the 2017 COSO ERM Framework be released to address the need for more depth, clarity, and integration with strategy and performance. The 2004 framework is still considered viable for designing, implementing, and assessing the effectiveness of internal control. The COSO [15] ERM Framework introduces five principles and twenty components that organizations can use to implement effective enterprise risk management. The five principles are: establishing a governance structure and fostering a risk-aware culture; aligning risk management with strategic goals and objectives; enhancing performance by identifying and managing risks; continuously reviewing and improving the risk management process; and ensuring effective communication and reporting of risk-related information. The twenty components are organized under

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 3: 125-144, 2024
DOI: 10.55214/25768484.v8i3.804

the five principles and include elements such as risk appetite, risk identification, risk assessment, risk response, and monitoring activities. These components provide a comprehensive framework for organisations to integrate risk management into their strategic decision-making processes. Prewett and Terry [14] highlighted that the COSO [15] ERM Framework aims to help organisations enhance their risk management practices and improve their ability to identify, assess, and respond to risks in a dynamic business environment.

The systematic process of recognising, assessing, and responding to potential events or uncertainties that can negatively or favourably impact an organisation's capacity to achieve its objectives is referred to as risk management. This process includes developing strategies, techniques, and controls to deal with these uncertainties and guarantee meeting the organisation's goals [15]. Internal control is a procedure that an entity's board of directors, management, and other people use to provide reasonable assurance about attaining operational, reporting, and compliance objectives. It is a system of rules, regulations, and procedures that an organisation uses to protect the integrity of financial and accounting data, encourage accountability, and prevent fraud [15].

Some of the past studies did not directly mention the risk management process, such as Maulidi and Ansell [16]; Mendes de Oliveira, et al. [17] and Musah, et al. [18]. Still, the study done by Omar, et al. [19] suggested closed supervision, fraud awareness training, more detailed job descriptions, an upbeat work environment, and tighter security to combat fraud. While Ayagre [20] emphasised that internal auditing in government agencies improves governance by keeping an eye on risk management practices. Effective risk management relies heavily on the technical and professional abilities, motivation, and resources that can be evaluated through internal audit monitoring.

2.3. Risk Management and Internal Control Impact on Fraud Prevention

This study examines seven distinct components that can influence the prevention of fraudulent activities. These components are objective setting, internal environment, risk response, risk assessment, information and communication, control activities, and monitoring. Effective risk management can significantly affect fraud occurrence, indicating that a well-implemented risk management system can help mitigate the likelihood of fraud [9]. Organisations must recognise that establishing objectives constitutes a primary concern for management, as it ensures alignment with the subsequent implementation of strategic planning. However, Rahman and Al-Dhaimesh [21] found that objective setting does affect reducing fraudulent financial reporting. Therefore, the research hypothesis developed is:

H_1: The objective setting does affect fraud prevention.

The enhancement of the internal environment is an additional element within an organisation, necessitating the involvement of management at every level and supporting operations. For example, a procurement policy inside a company is vital to facilitate efficient implementation and address any instances of non-compliance and errors. In the context of fraud prevention, the control environment plays a significant role in local government as a critical determinant for enhancing fraud prevention measures [11, 22]. At the same time, the internal environment does affect reducing fraudulent financial reporting [21]. Therefore, the research hypothesis developed is:

H_2: The control environment does affect fraud prevention.

In addition to any existing policy in the organisation, it is imperative to identify and evaluate risks and potential hazards that can undermine the organisation's objectives. The risks that may arise in the public sector can be categorised as either internal or external, encompassing several dimensions such as financial, operational, strategic, regulatory, or reputational threats. Once risks have been identified, organisations undergo an assessment process to evaluate the possible impact and likelihood of their occurrence. In fraud prevention, risk management activities such as internal risk treatment can help prevent and detect fraudulent activities [22]. In the research done by Tarjo, et al. [11], risk assessment in local government significantly impacts the prevention of fraud. In fraudulent financial reporting, Rahman and Al-Dhaimesh [21] conducted a study that revealed the significance of risk assessment and

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 3: 125-144, 2024
DOI: 10.55214/25768484.v8i3.804

response variables in mitigating false financial reporting within commercial banks. Therefore, the research hypotheses developed are:

H₃: The risk assessment does affect fraud prevention.

H₄: The risk response does affect fraud prevention.

Control operations consist of a range of measures, including approvals, reconciliations, and segregation of roles, which public sector employees should possess knowledge of and actively participate in. While the organisation is currently working on implementing control measures, the management must oversee the entire implementation process and control activities actively. This includes monitoring whistleblowing channels and conducting continuing assessments, audits, and evaluations of controls. Such proactive involvement by management is essential in mitigating the risk of fraudulent actions. In the context of fraud prevention, risk management activities such as internal controls can help prevent and detect fraudulent activities [22].In their study conducted in 2022, Tarjo, et al. [11] observed that implementing robust internal control mechanisms can potentially mitigate the occurrence of fraudulent activities. On the issue of false financial reporting, Rahman and Al-Dhaimesh [21] found the importance of control activities in commercial banks. Therefore, the research hypothesis developed is:

H₅: The control activities do affect fraud prevention.

This assessment aids in prioritising risks for subsequent control and monitoring measures. Once the assessment of risks has been conducted, procurement policies, procedures, and practices are put into effect in order to mitigate potential risks and facilitate the seamless and effective implementation of activities. In the context of fraud prevention, monitoring involves continuously monitoring activities and transactions to detect any suspicious or fraudulent behavior [22]. Monitoring plays a crucial role in enhancing good governance and ensuring the efficiency and effectiveness of public sector organisations. Monitoring helps evaluate internal audit units' capacity to enhance good governance, including fraud prevention Ayagre [20]. Tarjo, et al. [11] have discovered that the enhancement of monitoring activities by local governments can improve fraud prevention. However, Rahman and Al-Dhaimesh [21] found no relationship between monitoring and reducing fraudulent financial reporting in commercial banks operating. Therefore, the research hypothesis developed is:

H₆: The monitoring does affect fraud prevention.

In conjunction with surveillance, effective communication plays a crucial role in disseminating pertinent information pertaining to the critical aspects that need to be documented for the risk management process within the company. In order to mitigate fraudulent activities, it is imperative to incorporate a comprehensive approach that encompasses both risk management and internal control measures. When considered collectively, these measures represent a comprehensive strategy for addressing and minimising the risks associated with fraudulent activities. By integrating anti-fraud measures into the broader framework of risk management and internal control systems, enterprises can ensure that these procedures are no longer perceived as distinct from the overall operations of the organisation.Tarjo, et al. [11] highlighted the significance of information and communication as integral elements of effective internal control within the realm of fraud prevention. This is contradicted by Rahman and Al-Dhaimesh [21], who found no relationship between information and communication in reducing fraudulent financial reporting. Therefore, the research hypothesis developed is:

H₇: The information and communication do affect fraud prevention.

3. Research Methodology

3.1. Population and Sample

This study's sample consisted of executives and non-executives from the public sector, specifically the procurement unit. This sample was selected based on their prior expertise in managing procurement and finance. As a result, it has been decided that it would be best for them to participate in this study as respondents. 30,000 people work in the procurement and finance section in Putrajaya, and they come from 11 different ministries. The minimal number of participants in a sample should be 380, as Krejcie and Morgan [23] recommended, but the study received replies from approximately 537 people. Using a

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 3: 125-144, 2024
DOI: 10.55214/25768484.v8i3.804

minimum sample size, as proposed by Saunders, et al. [24] and Cohen [25], helps to guarantee that the research sample is sufficiently large to represent the overall population being studied. The minimum sample size is determined by a number of different elements, such as the research design, the required level of precision and confidence, the kind of data being collected, and the statistical analyses that will be carried out. As a result, this particular sample size among personnel who handle procurement units can be regarded as adequate and appropriate for this investigation.

3.2. Data Collection and Instrument

Emails and invitation letters were issued to the relevant officials in each ministry for permission at the start of the data-gathering procedure. Following approval, a cover letter and Google Form link were distributed randomly to each ministry's employees (executives and non-executives) in the procurement and finance (payment process) divisions. The questionnaires were filled out between October and December of 2022. The original data collection period was one month, but it was extended for specific ministries once follow-ups were completed. 537 respondents from 11 ministries in Putrajaya contributed to the study at the end of the data-gathering period.

The questionnaire was employed as the research instrument in this study. The questionnaire was designed using thorough empirical analyses of risk management and internal control publications [26]. The questionnaire includes topics based on the COSO [13] that were scored on a 1-5-point Likert scale (strongly disagree to strongly agree) and related to goal formulation, the internal environment, information sharing, risk response, monitoring, risk assessment, and control actions. For fraud prevention, Yap, et al. [27] and Association of Certified Fraud Examiners (ACFE) [1] used a 1-6-point Likert scale (strongly disagree to strongly agree). Practitioners evaluated the instrument before it was distributed to the ministries to ensure that each item was relevant to the Malaysian public sector.

There were three sections to the questionnaire. The first portion focused on the respondents' profiles, such as gender, age, work experience, position, and function in the public sector, and awareness of risk management and internal control in the public sector. The second segment focused on the public sector's risk management and internal control aspects, as defined by COSO [13] and Aziz, et al. [26]. This part aims to investigate the effects of risk management on fraud. The third section investigates respondents' perceptions of fraud prevention. The results of the reliability analysis of the seven risk management variables and fraud prevention using the Cronbach alpha coefficient are shown in Table 2. The primary function of the Cronbach alpha coefficient is to assess the internal consistency and reliability of a measure or scale. It demonstrates that the variables have strong internal consistency, with Cronbach alpha coefficients ranging from 0.719 to 0.938. According to Hair, et al. [28], 0.719 is a good score. As a result, all of the elements in this study may be rated as excellent or high, but they are not redundant.

Table 2.
Reliability analysis for ERM.

Constructs	Cronbach's alpha	No. of items
Objective setting	0.906	3
Internal environment	0.907	3
Information communication	0.719	2
Risk response	0.917	5
Monitoring	0.943	2
Risk assessment	0.938	7
Control activities	0.900	8
Fraud prevention	0.916	11

Source: COSO [13].

4. Results and Discussion

4.1. Respondents' Profile

Age, gender, qualification, professional qualification, level of education, state, job position, current position, position grade, current place of work, job scope, experience working in the public sector, experience working in the current position, and awareness of the establishment of enterprise risk management and internal control in their organisations are among the factors presented in respondents' profiles, as highlighted in Table 3. Most respondents are between the ages of 31 and 40, accounting for 51.6% of the sample. 37.1% of the sample is between the ages of 41 and 50. The youngest age group, "above 50 years old," accounted for 7.1% of the sample. Individuals under the age of 30 account for 4.3% of the sample. The sample's gender distribution is very unbalanced. Most respondents are female, accounting for 74.3% of the sample, with male respondents accounting for 25.7%. Most respondents (78% of the total) in the sample have an accounting qualification. 22% of respondents have non-accounting qualifications.

Table 3.
Respondents' profile.

Items	Frequency	Percentage (%)
Age		
Below 30 years old	23	4.3
31 to 40 years old	277	51.6
41 to 50 years old	199	37.1
Above 50 years old	38	7.1
Gender		
Male	138	25.7
Female	399	74.3
Qualification		
Accounting	419	78
Non-accounting	118	22
Professional qualification		
Yes	97	18.1
No	431	80.3
Others	9	1.7
Level of education		
Advanced diploma in accountancy	135	25.1
Advanced diploma in other disciplines	59	11
Degree in accounting	170	31.7
Degree in other disciplines	55	10.2
Masters	63	11.7
PhD	3	0.6
Others	52	9.7
Job position		
Supporting staff	327	60.9
Management and professional	202	37.6
Top management	8	1.5
Experience working in the public sector		
1 – 5 years	37	6.9
6 – 10 years	81	15.1
11 – 15 years	206	38.4
16 – 20 years	150	27.9
More than 20 years	63	11.7

In terms of professional qualifications, around 18.1% of respondents hold one. The majority (80.3%) do not have a professional qualification, while minor percentages (1.7%) are classified as "others." The level of education of respondents then varies greatly. The largest group has a "Degree in Accounting," accounting for 31.7% of the sample; the second-largest category, comprising 25.1%, "Masters" and

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 3: 125-144, 2024
DOI: 10.55214/25768484.v8i3.804

"Advanced Diploma in Other Disciplines," have similar percentages, accounting for 11.7% and 11% of the sample, respectively; only a small number of respondents have a "PhD," accounting for 0.6%; and a significant percentage (9.7%) falls into the category of "Others." Most respondents (60.9% of the sample) work in "supporting staff" positions. 37.6% of respondents have "management and professional" positions, whereas very small fractions (1.5%) hold "top management" positions. The sample comprises individuals with varied levels of public sector experience. "11-15 years" is the most common range, accounting for 38.4% of the sample, followed by "16-20 years" and "6-10 years," which account for 27.9% and 15.1%, respectively. Only a tiny percentage of respondents had "more than 20 years" (11.7%) or "1-5 years" (6.9%) of public sector experience. The majority of respondents work in "supporting staff" and "management and professional" roles, revealing the sample's leading employment categories. The distribution of public sector experience levels indicates that a significant number of respondents have more than a decade of experience, which may be helpful for judging expertise and knowledge in public sector concerns. This demographic data lays the groundwork for subsequent research into perceptions of COSO components and fraud prevention.

4.2. The COSO Components

4.2.1. Objective Setting

Goal setting is the first component of COSO, as highlighted in Table 4. To begin, the organisation should connect its organisational risks with the aims and objectives of the ministry, department, and unit. This statement shows that most respondents think the organisation's risks should match its aims and objectives. The mean value of 4.61 suggests that respondents agreed on a reasonably high level with minimal variation (low standard deviation of 0.575). Second, for all main risk categories, firms should define unambiguous, corporate-wide risk tolerance levels or boundaries. Similarly, with a mean value of 4.6 and a comparatively low standard deviation of 0.603, this statement suggests a high level of agreement among respondents. According to the results, respondents believe it is vital for the company to create defined risk tolerance levels for significant risk categories. Third, the organisation's risk-taking expectations should be explicitly stated to senior management. This statement has a high mean score of 4.61, indicating that respondents strongly believe that clear communication of risk-taking expectations to top management is essential. However, it has a somewhat higher standard deviation of 0.61 than the previous two assertions, indicating that replies are more variable. This could signal that, while most respondents agree, there are some differences in the clarity of communication on risk-taking expectations.

Table 4.
Descriptive analysis of COSO components.

Items for COSO components	Minimum	Maximum	Mean	Std. deviation
Objective setting				
Organisations should align their organisational risks with ministry, department, and unit goals and objectives.	2	5	4.61	0.575
Organisations should establish explicit, corporate-wide risk tolerance levels or limits for all significant risk categories.	2	5	4.6	0.603
Organisations should clearly communicate their expectations for risk-taking to senior management.	1	5	4.61	0.61
Internal environment				
Organisations should communicate a risk management mission statement, value proposition, and benefits statement to senior management.	1	5	4.64	0.575
Organisations should incorporate responsibility for risk management into the position description of all senior management.	1	5	4.64	0.579

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 3: 125-144, 2024
DOI: 10.55214/25768484.v8i3.804

Items for COSO components	Minimum	Maximum	Mean	Std. deviation
Senior management and all related committees should be actively involved in risk management.	1	5	4.64	0.593
Information communication				
Organisations should have a corporate-wide common language for communicating risk-type exposures, control activities, and monitoring efforts.	1	5	4.6	0.587
Organisation has regular briefs for management on risk management issues.	1	5	4.35	0.758
Risk response				
Organisation should conduct formal risk assessments across the organisation regularly.	1	5	4.61	0.591
Each unit and department should analyze the root cause, impact, and interrelationships of its risks.	1	5	4.62	0.6
Organisations should quantify their key risks to the best extent possible.	1	5	4.63	0.587
Organisations should ensure that all processes integrate the effects of the major risk types (strategic, operational, financial, hazard, and legal).	1	5	4.64	0.57
Each unit and department should develop and determine risk mitigation.	1	5	4.61	0.619
Monitoring				
Organisations should establish written risk policy and procedure manuals that are consistent across significant risks.	1	5	4.65	0.574
Each unit and department should monitor and report on the current status of managing key risks.	1	5	4.62	0.609
Risk assessment				
Risks were analysed by consider likelihood and risk impact as a basis to decide on how to manage the risk.	1	5	4.63	0.579
Risk assessment of the financial aspect should be done.	1	5	4.68	0.565
Risk assessment of the regulation compliance aspect should be done.	1	5	4.66	0.575
Risk assessment of the technology aspect should be done.	1	5	4.64	0.565
Risk assessment of the economical aspect should be done.	1	5	4.6	0.596
Risk assessment of payment should be done.	1	5	4.66	0.567
Risk assessment of procurement should be done.	1	5	4.66	0.572
Control activities				
Policies and procedures were established and implemented to make sure an efficient risk response has been done.	1	5	4.59	0.595
Control of payment and procurement aspects should be done.	1	5	4.67	0.57
Control of emergency planning should be done.	1	5	4.65	0.547
Control routine check on control effectiveness should be done.	1	5	4.64	0.562
Control on task segregation should be done.	1	5	4.66	0.571
Control of authority to approve should be done.	1	5	4.69	0.538
Control of document and records should be done.	1	5	4.67	0.553
Control of the implementation process of ERM should be done.	1	5	4.64	0.583

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 3: 125-144, 2024
DOI: 10.55214/25768484.v8i3.804

4.2.2. Internal Environment

The second COSO component is the internal environment, as highlighted in Table 4. Senior management should be given a risk management mission statement, a value proposition, and benefits statement. This statement implies that respondents agree on the significance of communicating a risk management mission statement, value proposition, and benefits statement to senior management. This practice has good support, with a mean score of 4.64 and a standard deviation of 0.575. The replies range from 1 to 5, but they are closely clustered around the mean, indicating that everyone agrees on the necessity of clear communication. The organisation should incorporate risk management duties into all senior management position descriptions. Similarly, this statement earns a high mean score of 4.64, indicating that most respondents agree. Risk management responsibilities should be included in all senior management job descriptions. The standard deviation of 0.579 suggests a low level of diversity in responses, showing a high level of agreement on this practice. Furthermore, all relevant committees and senior management should actively participate in the risk management process. With a mean score of 4.64, respondents strongly agree that top management and related committees should actively participate in the risk management process. However, it has a somewhat higher standard deviation of 0.593 than the previous two assertions, indicating that replies are more variable. While there is still consensus, there may be disagreements about the extent of involvement or how it should be carried out. In conclusion, the persons questioned strongly endorse essential risk management practices connected to the internal environment. They believe in clear communication of the risk management mission and value, integration of risk management responsibilities into senior management roles, and active engagement in the risk management process by senior management and relevant committees. While these practices are widely accepted, it is worth noting that there may be some disagreements, particularly on the level of senior management involvement. These data reflect a supportive attitude toward rigorous risk management practices within the organisation's internal environment.

4.2.3. Risk Assessment

Risk assessment is the sixth component, as highlighted in Table 4. The risks in the first item were analysed by considering the likelihood and risk impact as a basis for deciding how to manage the risk. This statement indicates that respondents agree on the need to analyze risks based on likelihood and impact when deciding how to manage them. With a comparatively low standard deviation of 0.579, the mean score of 4.63 suggests substantial support for this practice. The responses range from 1 to 5, but they are closely clustered around the mean, demonstrating agreement on the importance of this risk assessment approach. Second, a financial risk assessment should be performed. This statement likewise earns a high mean score of 4.68, showing considerable agreement among respondents that financial risk assessment should be performed. The standard deviation of 0.565 indicates relatively low response variability, indicating agreement on the necessity of financial risk assessment. Third, a risk evaluation of the regulatory compliance element should be performed. Similarly, this statement has a high mean score of 4.66, indicating that respondents strongly agree that risk assessment of regulatory compliance components should be done. The standard deviation of 0.575 suggests some variation in responses, but it also exhibits agreement on the importance of compliance-related risk assessment. Fourth, a risk evaluation of the technology aspect should be performed. This statement likewise earns a high mean score of 4.64, showing that respondents think that a risk assessment of the technological part is necessary. The standard deviation of 0.565 indicates relatively low response variability, indicating agreement on the importance of technology-related risk assessment. Fifth, an economic risk assessment should be performed. This statement earns a mean score of 4.6, indicating that respondents think economic risk assessment is vital. However, it has a somewhat more significant standard deviation of 0.596, showing that attitudes towards the significance of economic risk assessment vary slightly more. Sixth, a payment risk assessment should be performed. This statement had a mean score of 4.66, suggesting that respondents agreed that risk assessment of payment components should be done. The standard deviation of 0.567 indicates relatively low response variability, indicating agreement on the

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 3: 125-144, 2024
DOI: 10.55214/25768484.v8i3.804

relevance of payment-related risk assessment. A seven-item risk assessment of procurement should be performed. Similarly, this statement earns a high mean score of 4.66, indicating that respondents strongly agree that risk assessments of procurement components should be done. The standard deviation of 0.572 suggests some variation in replies but still reflects agreement on the need for procurement-related risk assessment. In conclusion, it is clear that most of those polled support various risk assessment practices within the organisation's risk management framework. These practices include risk analysis based on likelihood and impact and risk assessments in finance, compliance, technology, economics, payment, and procurement. While attitudes on the economic side of risk assessment may differ, the overall results indicate a favorable orientation towards comprehensive risk assessment within the organisation's risk management practices.

4.2.4. Risk Response

Risk response is the fourth component, as highlighted in Table 4. Regularly, organisations should undertake formal risk assessments across the organisation. This statement indicates that respondents have a high level of agreement on the need to perform frequent formal risk assessments across the organisation. With a comparatively low standard deviation of 0.591, the mean score of 4.61 suggests high support for this practice. The replies range from 1 to 5, but they are tightly clustered around the mean, demonstrating agreement on the importance of regular risk assessments. The second item shown is that each unit and department should investigate the underlying cause, effect, and interdependence of its risks. Similarly, this statement has a high mean score of 4.62, indicating that respondents agree that each unit and department should analyse their risks' root causes, impacts, and interrelationships. The standard deviation of 0.6 indicates relatively low variability in responses, indicating that this practice is well accepted. Third, the organisation should quantify its significant risks as much as is feasible. This statement likewise has a high mean score of 4.63, indicating that respondents agree on the significance of quantifying essential risks to the greatest extent possible. The standard deviation of 0.587 indicates reasonably low response variability, demonstrating agreement on the necessity for quantitative risk assessment. The fourth point is that the organisation should guarantee that all procedures consider the effects of major risk types (strategic, operational, financial, hazard, and legal). This statement has a mean score of 4.64, suggesting that respondents strongly agree that the organisation should incorporate the effects of crucial risk types into its procedures. The low standard deviation of 0.57 indicates a high level of agreement on this practice. Fifth, each unit and department should establish and determine risk mitigation strategies. This statement likewise earns a mean score of 4.61, suggesting that respondents strongly agree that each unit and department should be responsible for designing and determining risk reduction methods. However, it has a somewhat higher standard deviation of 0.619 compared to other statements, indicating disagreement over the specifics of risk mitigation obligations at the unit and department levels. In conclusion, it is clear from the statistics that the surveyed individuals typically support various risk response practices inside the organisation. These practices include regular risk assessments, evaluating the fundamental causes of risks, quantifying significant risks, incorporating main risk types into processes, and involving units and departments in risk mitigation efforts. While there is agreement on the need for these practices, there is some disagreement, particularly on the specifics of risk mitigation obligations at lower organisational levels. These results indicate a favorable attitude towards robust risk response mechanisms within the organisation's risk management system.

4.2.5. Control Activities

Control activities comprise the seventh item, as highlighted in Table 4. The first item demonstrates how policies and procedures were developed and executed to ensure an efficient risk response. This statement indicates that respondents have a relatively high degree of agreement on developing and implementing rules and procedures to guarantee an efficient risk response. With a standard deviation of 0.595, the mean score of 4.59 suggests substantial support for this practice. The feedback ranges from 1 to 5 but is tightly clustered around the mean, demonstrating agreement on the importance of well-

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 3: 125-144, 2024
DOI: 10.55214/25768484.v8i3.804

defined control measures. The second item reflects the need for payment and procurement control. This statement likewise earns a high mean score of 4.67, indicating widespread agreement among respondents that payment and procurement control procedures should be implemented. The standard deviation of 0.57 suggests that replies have relatively low variability, indicating agreement on the relevance of controls in these areas. The third point is to exercise control over emergency planning. Similarly, this statement has a high mean score of 4.65, indicating that respondents strongly agree that control systems for emergency preparation should be in place. The standard deviation of 0.547 indicates reasonably low response variability, indicating agreement on the need for controls in emergency preparation. The fourth item is control over routine checks on control effectiveness. This statement receives a mean score of 4.64, suggesting that respondents agree that controls should include periodic effectiveness reviews. The standard deviation of 0.562 indicates reasonably low response variability, indicating agreement on monitoring control efficacy. The fifth item, task segregation control, should be completed. This statement likewise earns a high mean score of 4.66, indicating that respondents agree that task segregation should be included in control measures. The standard deviation of 0.571 indicates relatively low variability in replies, indicating agreement on the need for task separation for control reasons. The sixth step is to exercise authority over approval. This statement has a mean score of 4.69, indicating that respondents believe control measures should include controls on the power to approve. The low standard deviation of 0.538 suggests that replies are relatively consistent, demonstrating agreement on the significance of managing approval authority. The seventh item is to do document and record control. Similarly, this statement has a high mean score of 4.67, indicating that respondents strongly agree that control methods should include controls on papers and records. The standard deviation of 0.553 indicates that responses have relatively low variability, indicating agreement on the significance of regulating paperwork and recordkeeping. The eighth step is to exercise control over the ERM implementation process. This statement has a mean score of 4.64, suggesting that respondents believe control measures should be used during the Enterprise Risk Management (ERM) implementation phase. The standard deviation of 0.583 indicates some variation in responses, but it still agrees on regulating the ERM implementation process. In conclusion, it is clear from the statistics that the questioned individuals strongly support various control actions within the organisation's risk management framework. These practices include establishing and executing policies and procedures and imposing controls in areas such as payment and procurement, emergency preparation, regular checks, task segregation, approval authority, documentation, records, and ERM implementation. While opinions may differ, particularly on the specifics of control methods, the overall results indicate a favourable orientation towards comprehensive control measures as part of the organisation's risk management practices.

4.2.6. Monitoring

The fifth component is monitoring, as highlighted in Table 4. Organisations should develop written risk policies and procedure guides consistent across main risks. This statement indicates that respondents agree on developing written risk policy and procedure guides that are uniform across significant risks. The mean score of 4.65 suggests substantial support for this practice, with a reasonably low standard deviation of 0.574. The replies range from 1 to 5, but they are closely clustered around the mean, demonstrating agreement on the necessity for standardised risk management paperwork. Then, each unit and department should monitor and report on the present state of critical risk management. Similarly, this statement earns a high mean score of 4.62, showing considerable agreement among respondents that each unit and department should monitor and report on the present status of managing critical risks. The standard deviation of 0.609 indicates some heterogeneity in responses, but it still reveals a consensus on the significance of unit-level risk monitoring and reporting. In conclusion, the surveyed individuals strongly support monitoring practices within the organisation's risk management framework. These practices include creating standardised risk policy and procedure guides and encouraging unit-level monitoring and reporting of significant risks. While perspectives may vary,

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 3: 125-144, 2024
DOI: 10.55214/25768484.v8i3.804

particularly on implementation issues, the results indicate a favorable orientation towards robust risk monitoring inside the organisation. Standardised documentation and regular monitoring at the unit and department levels are seen as critical components of good risk management.

4.2.7. Information Communication

COSO's third component is information communication, as highlighted in Table 4. Organisations should use a uniform language to communicate risk-type exposures, control operations, and monitoring initiatives. This statement implies that respondents agree to use consistent terminology throughout the company to share risk-related information. The mean score of 4.6, with a relatively low standard deviation of 0.587, indicates substantial support for this practice. The replies range from 1 to 5 but are strongly clustered around the mean, demonstrating agreement on the importance of a standardised communication method for risk-related issues despite the firm providing management with regular risk management briefings. This statement likewise has a relatively high mean score of 4.35, showing that respondents agree on the relevance of providing management with frequent risk management briefings. However, it has a higher standard deviation of 0.758 than the previous statement, indicating that replies are more variable. While most respondents believe that regular briefings are essential, they may disagree on the frequency, content, or usefulness of these briefings. To summarise, most of those questioned support using a single language to communicate risk-related information and provide regular risk management briefings to management. These practices are critical for the organisation's efficient risk management. However, it is crucial to highlight that there may be some disagreements, particularly over the specifics of how these practices should be implemented. The higher standard deviation for the second statement shows that perspectives on frequent briefing specifics may be more diverse. Overall, the results indicate a positive attitude towards increasing information communication in the context of risk management.

Table 5.
Descriptive analysis for fraud prevention.

Items for fraud prevention	Minimum	Maximum	Mean	Std. deviation
Strongly implementing rules, regulations, and fines is crucial for upholding our organisation's compliance and ethical standards.	2	6	5.408	0.652
I concur with the notion that fostering a culture characterised by elevated levels of integrity and honesty in operational procedures is essential for the prosperity and standing of our organisation.	1	6	5.477	0.655
Establishing an effective reporting channel is of utmost importance in ensuring transparency and accountability in the activities of our organisation, as it provides a means to resolve complaints and breaches.	2	6	5.415	0.653
Implementing a comprehensive audit procedure is crucial for assessing and guaranteeing compliance with established standards, thereby safeguarding our organisation's financial and operational integrity.	2	6	5.443	0.633
I believe establishing a lucid and all-encompassing code of conduct is necessary to foster ethical conduct within our organisation.	2	6	5.406	0.685

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 3: 125-144, 2024
DOI: 10.55214/25768484.v8i3.804

Items for fraud prevention	Minimum	Maximum	Mean	Std. deviation
I concur with the notion that protecting individuals who disclose instances of wrongdoing is vital in cultivating an atmosphere of confidence and responsibility inside our company.	1	6	5.421	0.749
Implementing stringent oversight over processes and personnel is crucial for upholding quality standards and enhancing operational efficiency within our organisation.	1	6	5.413	0.718
I believe that implementing a comprehensive training system that effectively imparts essential skills and knowledge to employees is of utmost importance in fostering their performance and facilitating their professional development inside our organisation.	1	6	5.374	0.677
Providing an income level that aligns with the duties and responsibilities of employees is crucial for ensuring their satisfaction and retention within our organisation.	1	6	5.289	0.768
I concur with the notion that an equitable and thorough employee selection procedure is of utmost importance in recruiting individuals whose skills and attributes align with our organisational values and objectives.	1	6	5.331	0.744
The transparent public disclosure of financial and operational details is essential for fostering trust and confidence among stakeholders and the broader community.	1	6	5.326	0.753

4.3. Fraud Prevention

There are 11 items displayed for fraud prevention, as highlighted in Table 5. The first thing displayed is that I feel that strict adherence to rules, regulations, and fines are critical for maintaining compliance and ethical standards inside our organisation. Respondents highly agree (with a mean of 5.408) that strict enforcement of rules, regulations, and sanctions is critical for sustaining organisational compliance and ethical standards. The presence of a standard deviation of 0.652 indicates the existence of response variability within the data. However, it is important to note that the consensus remains predominantly positive. Second, I agree that developing a culture characterised by high integrity and honesty in operational procedures is critical to our organisation's growth and position. Respondents highly agree (with a mean of 5.477) that maintaining integrity and honesty in operating procedures is critical to the organisation's success and reputation. The presence of a standard deviation of 0.655 suggests the existence of diversity in the responses. Nevertheless, the consensus remains predominantly positive. Third, installing an effective reporting channel is critical to guaranteeing openness and accountability in our organisation's actions since it provides a method to resolve complaints and breaches. Respondents highly agree (with a mean score of 5.415) that an effective reporting channel guarantees transparency and accountability. The standard deviation of 0.653 indicates some response variability, but the overall consensus is fairly positive. Fourth, establishing a complete audit method is critical for reviewing and ensuring compliance with specified standards, thereby protecting our organisation's financial and operational integrity. Respondents strongly agree (with a mean of 5.443) that a comprehensive audit procedure guarantees compliance and maintains the organisation's financial

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 3: 125-144, 2024
DOI: 10.55214/25768484.v8i3.804

and operational integrity. The standard deviation of 0.633 demonstrates considerable response variability but still represents a positive consensus. Fifth, establishing a clear and comprehensive code of conduct is vital to developing ethical behaviour within our organisation. Respondents strongly agree (with a mean of 5.406) that a clear and comprehensive code of conduct is required to foster ethical behaviour inside the organisation. The standard deviation of 0.685 indicates some response variability, but the overall consensus is positive. Sixth, I agree that offering safety to individuals who reveal misconduct is critical to building a culture of trust and accountability inside our organisation. Respondents strongly agree (with a mean of 5.421) that protecting whistleblowers is critical for building an organisational culture of trust and accountability. The standard deviation of 0.749 indicates some response variability, but the overall consensus is positive. Seventh, stringent control of processes and individuals is critical for maintaining quality standards and improving operational efficiency inside our organisation. Respondents highly agree (with a mean score of 5.413) that strict control of procedures and employees is essential for sustaining quality standards and operating efficiency. The standard deviation of 0.718 indicates some response variability, but the overall consensus is positive. Eighth, implementing a thorough training system that successfully transmits necessary skills and knowledge to staff is critical to encouraging their performance and facilitating their professional development inside our organisation.

According to respondents, implementing a thorough training system is critical for staff performance and professional growth (with a mean of 5.374). The standard deviation of 0.677 indicates some response variability, although the overall consensus is positive. Ninth, providing an income level corresponding to employees' roles and responsibilities is critical for maintaining their contentment and retention within our organisation. With a mean of 5.289, respondents think providing suitable salary levels is vital for employee satisfaction and retention. The increased standard deviation of 0.768 indicates greater response variability, but the consensus remains positive. Tenth, I agree that an equal and thorough personnel selection system is critical in recruiting employees whose talents and traits align with our organisational values and objectives. Respondents (with a mean of 5.331) strongly believe that an equal and thorough staff selection system is critical for recruiting personnel corresponding with organisational values and objectives. The standard deviation of 0.744 indicates some response variability, but the overwhelming consensus is positive. Eleventh, transparent public disclosure of financial and operational facts is necessary for cultivating trust and confidence among stakeholders and the larger community. Respondents highly agree (with a mean of 5.326) that full public disclosure of financial and operational facts is critical for creating trust and confidence among stakeholders and the general public. The standard deviation of 0.753 indicates some response variability, but the overwhelming consensus is positive.

In conclusion, respondents generally have excellent attitudes towards fraud prevention procedures within the organisation. They strongly support compliance, integrity, transparency, accountability, and ethical practices. While there is significant variation in responses, especially regarding standard deviations, the broad agreement favors these fraud prevention methods. These results show a strong commitment to the organisation's integrity and ethical behaviour culture. This current result could be aligned with the Association of Certified Fraud Examiners (ACFE) [1], which emphasized that the two predominant controls observed in this study were external audits of financial statements and the implementation of a formal code of conduct. Other frequently used controls included the creation of an internal audit department, management certification of financial statements, independent external audits of internal controls over financial reporting, the provision of a hotline for reporting concerns, regular management reviews, the presence of an audit committee, the provision of fraud training, the implementation of an anti-fraud policy, and the provision of fraud training sp.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 3: 125-144, 2024
DOI: 10.55214/25768484.v8i3.804

Table 6 (a).
Model summary.

Model	R	R square	Adjusted R square	Std. error of the estimate
1	0.589[a]	0.347	0.339	0.513

Note: a: Dependent variable: Fraud prevention.

Table 6 (b).
ANOVA.

Model		Sum of squares	df	Mean square	F	Sig.
1	Regression	74.047	7	10.578	40.242	0.000[b]
	Residual	139.056	529	0.263		
	Total	213.103	536			

Note: b: Predictors: (Constant), Objective setting, Internal environment, Information and communication, Risk response, Monitoring, Risk assessment, Control activities.

Table 6 (c).
Coefficients between COSO components and fraud prevention.

Model		Unstandardized coefficients	Std. error	Standardized coefficients	t	Sig.
		B		Beta		
1	(Constant)	2.145	0.200		10.700	0.000
	Objective setting	-0.016	0.095	-0.015	-0.168	0.867
	Internal environment	-0.141	0.116	-0.126	-1.213	0.226
	Information and communication	0.242	0.065	0.230	3.709	0.000
	Risk response	0.038	0.123	0.034	0.312	0.755
	Monitoring	0.078	0.098	0.071	0.798	0.426
	Risk assessment	0.275	0.124	0.239	2.214	0.027
	Control activities	0.231	0.118	0.194	1.964	0.049

4.4. COSO Components and Fraud Prevention

Based on Table 6a, the correlation coefficient (R) is 0.589, indicating that the COSO components and fraud prevention have a moderately favourable association. This implies a significant, but not overly strong, relationship between these factors. The R2 value is 0.347, indicating that the independent variables in the model can explain about 34.7% of the variance in fraud prevention. While this accounts for a significant percentage of the variance, it also implies that other factors not included in the model may impact fraud prevention. The adjusted R square, which considers the number of predictors for COSO components, is 0.339. Even after considering the model's complexity with many predictors for COSO components, it still explains around 33.9% of the variance in fraud prevention. The standard error of the estimate (0.51270) shows the average error, or the amount to which anticipated values differ from actual values, and the model fits the data better. According to the ANOVA in Table 6b, the regression model is highly statistically significant (p-value of 000). This implies that at least one independent factor from COSO components substantially impacts fraud prevention. The coefficients shed light on each independent variable's (COSO components) specific contribution to fraud prevention.

The results of the impact of COSO components on fraud prevention are in Table 6c. First, the objective setting has a -0.016 coefficient and a non-significant p-value (0.867). This implies no statistically significant link between objective setting and fraud prevention. Therefore, H1 is rejected. Second, the internal environment has a coefficient of -0.141 and a p-value of 0.226. This model has no statistically significant association between the internal environment and fraud prevention. Therefore, H2 is rejected. Third, risk assessment has a positive coefficient of 0.275 and a p-value of 0.027. This

means that organisations that undertake more thorough risk assessments have more effective fraud prevention procedures. Therefore, H3 is accepted. Fourth, risk response has a coefficient of 0.038 and a non-significant p-value of 0.755, indicating that it does not affect fraud prevention in this scenario. Therefore, H4 is rejected. Fifth, monitoring has a coefficient of 0.078 and a non-significant p-value (0.426) in this model, suggesting that it is not a statistically significant predictor of fraud prevention. Therefore, H5 is rejected. Sixth, control activities have a coefficient of 0.231 and a marginally significant p-value (0.049). While the p-value is near the standard significance level of 0.05, it shows that control activities may favor fraud prevention. However, further research is required to confirm this. Therefore, H6 is accepted. Seventh, information and communication have a positive coefficient of 0.242 and a p-value of 0.000. This suggests that information and communication practices are having a favorable impact on fraud prevention efforts. Fraud prevention is more effective in organisations with better information and communication procedures. Therefore, H7 is accepted.

According to the results, risk assessment, information and communication, and control activities are important drivers of fraud prevention efforts. Organisations may consider investing in clear and effective communication channels connected to fraud prevention and conducting extensive risk assessments to improve their anti-fraud procedures. At the same time, several components (objective setting, internal environment, risk response, and monitoring) were not statistically significant in this study. The current results contradict [11] that proven control environments, risk assessment, control activities, information and communication, and monitoring have a significant impact on fraud prevention and detection. While Bento, et al. [22] proved that control environments and activities were shown to be effective in fraud prevention. Rahman and Al-Dhaimesh [21] show that internal control, event identification, risk assessment and response, and control activity variables affect fraudulent financial reporting.

5. Conclusions, Limitations and Future Research

This study sought to investigate the perceptions of risk management and internal control within the public sector regarding fraud prevention. Through a detailed exploration of a questionnaire survey, the current study found that risk assessment, information and communication, and control activities impact fraud prevention in government agencies. The insights garnered provide a robust foundation for understanding risk management and internal control and underscore the COSO components' significance in government agencies' fraud prevention.

In conclusion, risk assessment, control activities, information, and communication positively impact fraud prevention, as stated in Table 7. More study and a better understanding of the organisation's unique demands may yield more conclusive results for the public sector. Finally, the analysis provides valuable insights into the elements that influence fraud prevention. Organisations should prioritise information, communication, and risk assessment while considering other considerations in their specific circumstances. More research and continuing evaluation are required to develop and sustain effective fraud prevention techniques.

Table 7.
Result summary.

Hypothesis	Hypothesis statement	Result
H1	The objective setting does affect fraud prevention	Reject
H2	The control environment does affect fraud prevention.	Reject
H3	The risk assessment does affect fraud prevention	Accept
H4	The risk response does affect fraud prevention	Reject
H5	The control activities does affect fraud prevention	Accept
H6	The monitoring does affect fraud prevention	Reject
H7	The information and communication does affect fraud prevention	Accept

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 3: 125-144, 2024
DOI: 10.55214/25768484.v8i3.804

Nevertheless, while the study sheds light on risk management and internal control, it also describes that implementing risk management remains complex in government agencies. However, there are certain limitations to this study. Firstly, all of the conclusions in this study are drawn from primary sources among public sectors' employees from federal ministries that participate in the study. Future studies could include participants from specific government agencies that could thoroughly investigate the implementation of risk management and control. Secondly, this study's research instrument relied only on COSO [13] to examine risk management and internal control among public sector employees. Therefore, future studies could also apply ISO 31000 [29] and COSO [15] to enhance the results and understanding of risk management and internal control in the public sector.

5.1. Implication of Research

As information and communication practices substantially benefit fraud prevention, organisations should prioritise clear and effective communication channels linked to fraud detection, reporting, and prevention. Whistleblower hotlines, awareness training, and transparent reporting procedures may be included. Organisations should invest in comprehensive risk assessment processes, given the importance of risk assessment in fraud prevention. This includes detecting potential fraud risks, analysing their likelihood and impact, and devising mitigation methods. Regular and comprehensive risk assessments can be the foundation of effective fraud prevention. Control activities have a marginally significant impact, but organisations should not dismiss their significance. More research is needed to confirm their importance. Practical consequences include analysing and perhaps improving fraud prevention control activities such as internal controls, segregation of roles, and fraud detection technologies. Organisations should be aware that the impact of these elements varies depending on their specific settings and risks. As a result, it is critical to customise fraud prevention measures to specific organisational demands, starting with the findings and conducting internal assessments to identify strengths and shortcomings. Fraud prevention is an ongoing process in which organisations must constantly analyse and change their fraud prevention tactics in response to emerging risks and changing surroundings. Regular monitoring and reassessment of risk indicators can assist organisations in remaining proactive in the fight against fraud.

Funding:
This study received no specific financial support.

Institutional Review Board Statement:
The Ethical Committee of the Universiti Teknologi MARA, Malaysia has granted approval for this study on 2 January 2023 (Ref. No. J5100500002/2022008).

Transparency:
The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Competing Interests:
The authors declare that they have no competing interests.

Authors' Contributions:
All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.

References

[1] Association of Certified Fraud Examiners (ACFE), "Report to the nations 2022 global study on occupational fraud and Abuse-Asia pasific edition. Association of certified fraud examiners," Retrieved: https://legacy.acfe.com/report-to-the-nations/2022/?_ga=2.159646651.768369630.1695131363-526341472.1695033481. [Accessed 5 August 2023], 2022.

[2] Transparency International, "Corruption perceptions index," Retrieved: https://www.transparency.org/en/cpi/2022/index/mys. [Accessed 5 August 2023], 2023.

[3] O. M. Khersiat, "The efficiency of applying the internal control components based on COSO framework to transparently carry out tasks and services, ensure integrity and enhance quality and efficiency: Case study-the greater Amman municipality," *International Journal of Financial Research*, vol. 11, no. 2, pp. 371-381, 2020. https://doi.org/10.5430/ijfr.v11n2p371

[4] Y. Kong, P. Y. Lartey, F. B. M. Bah, and N. B. Biswas, "The value of public sector risk management: An empirical assessment of Ghana," *Administrative Sciences*, vol. 8, no. 3, pp. 1-18, 2018. https://doi.org/10.3390/admsci8030040

[5] A. Ilias, N. Baidi, E. K. Ghani, and A. Omonov, "A qualitative investigation on risk management implementation in the Malaysian public sector," *Economic Affairs*, vol. 68, no. 2, pp. 1247-1261, 2023.

[6] M. Setapa and N. M. Zakwan, "The implementation of enterprise risk management: A study of Malaysian private higher educational institution," *Journal of Mathematics and Computing Science*, vol. 5, no. 1, pp. 39-52, 2019.

[7] Sustainable Development Goal, "United nations," Retrieved: https://www.unep.org/explore-topics/resource-efficiency/what-we-do/sustainable-public-procurement/sdg-127-target-and. [Accessed 25 April 2023], 2023.

[8] D. Peltier-Rivest, "A model for preventing corruption," *Journal of Financial Crime*, vol. 25, no. 2, pp. 545-561, 2018.

[9] Z. Mohd-Sanusi, M. N. F. Rameli, N. Omar, and M. Ozawa, "Governance mechanisms in the Malaysian banking sector: Mitigation of fraud occurrence," *Asian Journal of Criminology*, vol. 10, pp. 231-249, 2015. https://doi.org/10.1007/s11417-015-9211-4

[10] N. Shonhadji and A. Maulidi, "The roles of whistleblowing system and fraud awareness as financial statement fraud deterrent," *International Journal of Ethics and Systems*, vol. 37, no. 3, pp. 370-389, 2021. https://doi.org/10.1108/ijoes-09-2020-0140

[11] T. Tarjo, H. V. Vidyantha, A. Anggono, R. Yuliana, and S. Musyarofah, "The effect of enterprise risk management on prevention and detection fraud in Indonesia's local government," *Cogent Economics & Finance*, vol. 10, no. 1, p. 2101222, 2022. https://doi.org/10.1080/23322039.2022.2101222

[12] S. S. Halbouni, N. Obeid, and A. Garbou, "Corporate governance and information technology in fraud prevention and detection: Evidence from the UAE," *Managerial Auditing Journal*, vol. 31, no. 6/7, pp. 589-628, 2016. https://doi.org/10.1108/maj-02-2015-1163

[13] COSO, "Enterprise risk management – integrated framework. The committee of sponsoring organizations of the tread-way commission," Retrieved: https://www.coso.org/enterprise-risk-management. [Accessed 5 August 2023], 2004.

[14] K. Prewett and A. Terry, "COSO's updated enterprise risk management framework—A quest for depth and clarity," *Journal of Corporate Accounting & Finance*, vol. 29, no. 3, pp. 16-23, 2018. https://doi.org/10.1002/jcaf.22346

[15] COSO, "Enterprise risk management: Integrating with strategy and performance. COSO," Retrieved: https://www.coso.org/enterprise-risk-management. [Accessed 5 August 2023], 2017.

[16] A. Maulidi and J. Ansell, "Corruption as distinct crime: The need to reconceptualise internal control on controlling bureaucratic occupational fraud," *Journal of Financial Crime*, vol. 29, no. 2, pp. 680-700, 2022. https://doi.org/10.1108/jfc-04-2021-0100

[17] D. K. Mendes de Oliveira, J. O. Imoniana, V. Slomski, L. Reginato, and V. G. Slomski, "How do internal control environments connect to sustainable development to curb fraud in Brazil?," *Sustainability*, vol. 14, no. 9, p. 5593, 2022. https://doi.org/10.3390/su14095593

[18] A. Musah, A. Padi, B. Okyere, D. Adenutsi, and C. Ayariga, "Does corporate governance moderate the relationship between internal control system effectiveness and SMEs financial performance in Ghana?," *Cogent Business & Management*, vol. 9, no. 1, p. 2152159, 2022. https://doi.org/10.1080/23311975.2022.2152159

[19] M. Omar, A. Nawawi, and A. S. A. Puteh Salin, "The causes, impact and prevention of employee fraud: A case study of an automotive company," *Journal of Financial Crime*, vol. 23, no. 4, pp. 1012-1027, 2016. https://doi.org/10.1108/JFC-04-2015-0020

[20] P. Ayagre, "Internal audit capacity to enhance good governance of public sector organisations: Developing countries perspective," *Journal of Governance and Development*, vol. 11, no. 1, pp. 39-60, 2015.

[21] A. A. A. A. Rahman and O. H. A. Al-Dhaimesh, "The effect of applying COSO-ERM model on reducing fraudulent financial reporting of commercial banks in Jordan," *Banks & Bank Systems*, vol. 13, no. 2, pp. 107-115, 2018. https://doi.org/10.21511/bbs.13(2).2018.09

[22] R. F. Bento, L. Mertins, and L. F. White, *Risk management and internal control: A study of management accounting practice. In Advances in management accounting*. Emerald Publishing Limited. https://doi.org/10.1108/s1474-787120180000030002, 2018.

[23] R. V. Krejcie and D. W. Morgan, "Determining sample size for research activities," *Educational and Psychological Measurement*, vol. 30, no. 3, pp. 607-610, 1970. https://doi.org/10.1177/001316447003000308

[24] M. Saunders, P. Lewis, and A. Thornhill, *Research methods for business students*. Harlow: Pearson Education Ltd, 2012.

[25] J. Cohen, *Statistical power analysis for the behavioral sciences*, 2nd ed. Hillsdale, NJ: Lawrence Erlbaum Associates, 1988.

[26] K. Aziz *et al.*, "Enterprise risk management (ERM) practices among Malaysian SMEs: The three steps process to identify adopters and non-adopters of ERM for SMEs," *International Journal of Academic Research in Business and Social Sciences*, vol. 8, no. 11, pp. 1232-1245, 2018. https://doi.org/10.6007/ijarbss/v8-i11/5165

[27] J. B. H. Yap, K. Y. Lee, T. Rose, and M. Skitmore, "Corruption in the Malaysian construction industry: Investigating effects, causes, and preventive measures," *International Journal of Construction Management*, vol. 22, no. 8, pp. 1525-1536, 2022. https://doi.org/10.1080/15623599.2020.1728609

[28] J. F. Hair, B. J. Babin, R. E. Anderson, and W. C. Black, *Multivariate data analysis*, 8th ed. England: Pearson Prentice, 2019.

[29] ISO 31000, "Risk management — guidelines," Retrieved: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en. 2018.