© Universiti Tun Hussein Onn Malaysia Publisher's Office

JTMB

http://penerbit.uthm.edu.my/ojs/index.php/jtmb
ISSN 2289-7224 e -ISSN 2600-7967

Journal of Technology Management and Business

Diagnostic Risk Management System (DRMS): An Assessment of Financial Risk

Shuhaida Mohamed Shuhidan[1]*, Farah Aida Ahmad Nadzri[2], Marhamah Rafidi[3] and Jamaliah Said[2]

[1]Centre for Research in Data Science, Computer and Information Sciences Department,
Universiti Teknologi PETRONAS, 32610 Seri Iskandar, Perak, MALAYSIA

[2]Accounting Research Institute (ARI), Level 12, Menara SAAS,
UiTM Shah Alam, 40450 Shah Alam Selangor, MALAYSIA

[3]Taylors University, 47500 Subang Jaya Selangor, MALAYSIA

*Corresponding Author

DOI: https://doi.org/10.30880/jtmb.2023.10.01.007
Received 15 August 2022; Accepted 22 June 2023; Available online 25 June 2023

Abstract: Risk management is critical for any organisation to manage risk appropriately, as an undesirable risk event can have a huge negative impact on finances. Poor risk management leads to uncertain business performance or in the worst-case scenario, the collapse of the business. Sound risk management requires that the elements of risk in the business are considered before a decision is made. It is also important to know how the risk can be mitigated if it occurs, who is responsible for managing the risk, whether the likelihood and severity of the risk should be reduced or the risk should be avoided and transferred to others. This can help organisations to carry out the necessary assessments and analysis to understand the extent of their risk exposure and then plan mitigation measures. This paper highlights the importance of the Diagnostic Risk Management System (DRMS) as a lifesaver for organisations. Scholars, experts and practitioners generally agreed that DRMS reflects a company's image and subsequently reduces opportunities for fraud. DRMS is a user-friendly system that helps companies manage and view overall risk and find appropriate solutions to mitigate individual risks. DRMS focuses on the overall risk, especially on the risk assessment of financial reporting. DRMS is suitable for companies to create a competitive but healthy business environment that is free from destructive elements such as corruption, fraud and white-collar crime. This in turn ensures the creation of wealth for the business environment in Malaysia.

Keywords: Diagnostic risk management system, financial risk

1. Introduction

Generally, organisations, whether for-profit or non-profit, are set up with specific goals in mind. However, many of these organisations face hurdles and problems in achieving their goals because they fail to determine the financial risk and manage the problem (Gaultier-Gaillard et al., 2009; Racca & Cavallo, 2014; Arbe & Feria-Dominguez, 2022). The problem arises from poor internal control and poor identification of financial risks. The spark spreads to threats, governance failures, financial scandals, corruption and ends with the collapse of organisations (Dorminey et al., 2012, ACFE, 2018, ACFE, 2014; KPMG Malaysia, 2014). Therefore, to provide reasonable assurance that objectives can be achieved, the management of organisations must be able to manage their risks - uncertain events that may occur and prevent organisations from achieving their objectives. For this reason, we have developed a system that can help companies deal with uncertainties that arise from poor risk management. This system is called Diagnostic Management System (DRMS). DRMS was developed based on researchers' understanding of risk management approaches in the

**Corresponding author: shuhaida@tmsk.uitm.edu.my* past (Cooper & Chapman, 1987; Hertz & Thomas, 1983; and Charette, 1989). For example, Cooper & Chapman (1987) and Hertz & Thomas (1983) highlighted different phases of risk analysis that include identification, assessment, control and management of different types of risks. In addition, Hayes (1987) developed a risk management strategy that includes identification, analysis and response to risks. Similarly, these three studies established a logical sequence of procedures that included risk identification, risk measurement and risk assessment or reassessment, which linked risk management with strategic planning and management.

However, Charette (1989) used a different approach, viewing risk analysis and risk management as independent concepts and defining risk engineering as a process that encompasses both risk analysis and risk management. Today, the risk management frameworks published by the Organisation for Standardisation (ISO) and the Committee of Sponsoring Organisation of the Treadway Commission (COSO) are recognised as the two most widely used frameworks in the world (Fox, 2018). Referring to ISO 31000, the risk management process includes various activities such as communication and consultation; scope, context, and criteria setting; risk assessment, which includes risk identification, analysis, and evaluation; risk treatment; monitoring and review; and recording and reporting (ISO, 2018). Figure 1 below summarises the risk management process based on ISO 31000.

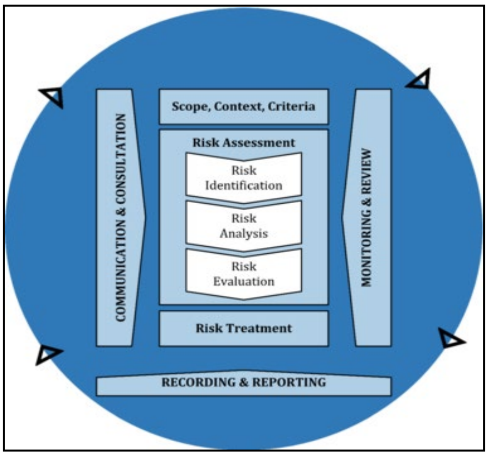


Fig. 1 - Risk management process (ISO 31000)

On the other hand, the COSO 2017 ERM (Enterprise Risk Management) Framework has integrated risk management with organisational strategy and performance. In the new framework COSO ERM, the process of risk management, such as risk appetite setting, risk identification, and risk severity assessment, is embedded in five interrelated ERM components: i) governance and culture; ii) strategy and goal setting; iii) performance; iv) review and revision; and v) information, communication, and reporting (see Figure 2). Although adoption of the COSO 2017 ERM framework is not mandatory and organisations can continue to use the original COSO 2004 ERM framework, some believe that the new COSO ERM framework is better because it emphasises the importance of aligning risk with the organisation's core values and activities (Fox, 2018; Lee, 2021).

Table 1 - Enterprise risk management framework (COSO, 2017)

Governance & Culture	Strategy & Objective-Setting	Business Objective Formulation	Review & Revision	Information, Communication & Reporting
1. Exercises Board Risk Oversight	6. Analyses Business Context	10. Identifies Risk	15. Assesses Substantial Change	18. Leverages Information and Technology
2. Establishes Operating Structures	7. Defines Risk Appetite	11. Assesses Severity of Risk	16. Reviews Risk and Performance	19. Communicates Risk Information
3. Defines Desired Culture	8. Evaluates Alternative Strategies	12. Prioritises Risk	17. Pursues Improvement in Enterprise Risk Management	20. Reports on Risk, Culture, and Performance
4. Demonstrates Commitment to Core Values	9. Formulates Business Objectives	13. Implements Risk Responses		
5. Attracts, Develops, and Retains Capable Individuals		14. Develops Portfolio View		

It is assumed that no framework is superior or better than the other (Leech, 2018; Prewett & Terry, 2018). According to Williams (2019), organisations are not obliged to follow a framework exclusively, but to use the framework as a guide and adapt it based on the needs and culture of the organisation. Therefore, this study aims to promote Diagnostic Risk Management System (DRMS) as a tool for organisations to identify potential risks, plan alternatives and avoid risks that could affect the organisation's performance. DRMS is proposed in this study to bridge the gap and help the enterprise to manage and monitor its risks from time to time.

2. Financial Reporting Fraud Risk

With the advancement of technology, enterprises nowadays operate in a multi-dimensional global business environment. In general, companies need to adapt to the threats of doing business in new markets and managing large amounts of digital data. Many struggle to comply with restrictive regulations to avoid costly litigation. In addition, corporate scandals are on the rise and managing the risk of fraud and misconduct has never been more difficult. Financial fraud scandals are costly, involving economic costs in the form of investigations and penalties, as well as individual costs in the form of prosecution. Worse, studies have shown how corruption and fraud scandals result in significant reputational damage to the company (Gaultier-Gaillard et al.., 2009; Racca & Cavallo, 2014; Arbe & Feria-Dominguez, 2022).

The complexity of fraudulent financial reporting has attracted considerable attention in recent years and will continue to be a problem in the future. Fraudulent financial reporting can arise in numerous ways. For example, once fraudulent accounting practises are implemented, myriad manipulation schemes are used to maintain sustainability. Common methods of artificially inflating manipulated financial statements include overstating revenues by booking future expected sales, understating expenses by capitalising operating costs, inflating assets by manipulating depreciation expense, exploiting off-balance sheet commitments, and falsely disclosing related party transactions and improperly structuring financial transactions. Another alternative to fraudulent financial reporting is so-called " biscuit jar" accounting, a practise whereby a company understates revenue in one accounting period and holds it in reserve for future periods, especially those in which it expects poor performance. In this way, the appearance of volatility is removed from their business (Zimbelman & Albrecht, 2012).

Fraudulent activity is an extortionate threat that can affect the integrity of the business and thus impact on its performance. Fraud can happen internally, such as subordinates altering financial records, or through an external threat, such as credit card fraud by customers. A report published by the Association of Fraud Examiners (ACFE, 2018) found that of the three categories of workplace fraud, financial statement fraud is the least likely to occur, but is the most expensive fraud, with an average loss of $800,000 dollars. This usually happens because of financial pressure, a perceived opportunity and the way the fraudster rationalises their actions, as outlined in the fraud triangle theory.

One of the unfortunate warning signs of the occurence of financial fraud is rationalisation, which is not generally observed. Since it is difficult to measure the occurrence of fraudulent financial reporting, the International Standard of Auditing 240 has suggested several elements that may be considered a risk for the occurrence of fraud in the annual report. The first factor rationalising the illegal acts is the share price effect where there is inflation of the share price when the company is involved in fraudulent financial reporting (Karpoff & Lou, 2010). The second rationalisation factor associated with the occurrence of accounting fraud is aggressive earnings management (Dechow et al., 1996; Hasnan et al, 2012). Although previous studies state that aggressive earnings management is committed when management is under financial pressure, meeting analysts' forecast created the strongest pressure leading to earnings manipulation. Moreover, companies involved in fraudulent financial reporting manipulate earnings long before they are discovered, as shown by the study of Enron's earnings performance (Beneish, 1999).

The falsification of an organisation's financial statements through the fabrication of false revenue, the understatement of liabilities and the mispricing of assets is known as fraudulent financial reporting (ACFE, 2014; KPMG Malaysia, 2014). Top management manipulates information and commits fraud because they want to show off their performance to shareholders and also satisfy their own needs. Previous literature has extensively addressed and discussed fraudulent financial reporting. Numerous studies have been conducted on the detection and occurrence of accounting fraud. Beneish (1999) developed a model to identify fraudulent financial reporting. Spathis (2002) used a logistic regression model to identify factors associated with fraudulent financial reporting. Similarly, Beneish used financial ratios as a method to identify fraudulent financial reporting by comparing samples of fraudulent and non-fraudulent companies.

Spathis et al. (2002) supported the empirical evidence of Altman (1968), and Deshmukh et al. (1997) by using the financial ratios method to detect fraudulent financial reports. Altman (1968) created five financial ratios including their weights for each ratio based on the standard ratio category of liquidity, profitability, debt, solvency and activity ratios to predict bankruptcy of manufacturing companies. Deshmukh et al. (1997) use a fuzzy quantity model to assess the risk of fraud by management. The risk is essentially based on the auditor's belief in management's internal control. The result shows that fuzzy sets (for example, fuzzy numbers and fuzzy inferences) can be used to measure the auditor's beliefs about the presence of each red flag. When two or more of the auditor's beliefs are used to measure the red flags, these beliefs can be combined into a fuzzy set or fuzzy number.

Deshmukh & Talluru (1998) had used the same fuzzy sets method in their study. However, they focused on the risk of management fraud, which is similar to the study of Eining et al. (1997). The reason they adopted risk management as a variable was that they found that management detection of fraud and management assessment of the risk of fraud are antithetical to the audit profession. On the other hand, Beasley et al, (1999) developed a study based on SAS No. 82 to estimate the likelihood of fraudulent financial reporting for an audit client based on a number of risk factors, including lax internal controls, rapid corporate growth, ownership, and management's attitude toward financial reporting. They used a sample of 77 fraudulent companies and 305 non-fraudulent companies to detect fraudulent financial reporting.

Perols (2011) uses predictor like audit turnover, Big Four auditors, unexpected employee productivity and several financial ratios such as accounts receivable in detecting fraudulent financial statement between fraud companies and non-fraud companies. Chen et al. (2009) studied on the prediction of fraud processes by implementing a neural network system to assist auditors in audit strategy. This study also uses SAS No. 82 as indicators, including management characteristics and capabilities, operational characteristics and financial stability, and asset vulnerability to misappropriation. Thus, there is no specific method to determine which risk should be used for financial fraud detection. Based on previous studies, common ratios are used as a proxy for financial statement analysis and are widely used in forensic accounting research. In addition, the guidance contained in ISA 240 can also be used to manage audit risk.

Table 2 and Table 3 describe existing risk assessment tools on the market. The proposed DRMS differs from these as it assesses overall risk and also focuses on assessing the risk of fraud in financial reporting. In addition, it can be assessed online and mobile.

3. Risk Management

ISO Guide 73 defines risk management as "coordinated activities to manage and control an organisation with respect to risk", while the Institute of Risk Management (IRM) relates risk management to "understanding, analysing and managing risk to ensure that organisations achieve their objectives". Earlier, in the 1950s, the concept of risk management was closely associated with the function of insurance (Dionne, 2013; Kousky & Kunreuther, 2018). In the 1970s, the concept evolved as organisations began to realise that there are many organisational risks that are not insurable, such as reputational, political, market and pandemic risks. Therefore, the link between risk management and insurance is much less strong nowadays. Today, insurance is only seen as one of the risk control techniques used by the organisation to minimise the impact of events by transferring the risk to the insurance company (Hopkin, 2018).

Recent events such as corporate scandals, financial crises, and health pandemics have increased the interest of various parties, including researchers, practitioners, policy makers, and the public, in the issue of risk management, especially in corporations. Various studies on ERM have been conducted around the world, focusing on ERM implementation (for example, Ahmed & Manab, 2016; Fraser & Simkins, 2016; Strelcova et al., 2018), the relationship between ERM and performance (Florio & Leoni, 2017; Karanja, 2017; Lechner & Gatzert, 2018 Zou et al., 2019), determinants of ERM adoption (e.g., Gordon, Loeb & Tseng, 2009; Lechner & Gatzert, 2018), and ERM effectiveness (e.g., Florio & Leoni, 2017; Hiebl, Duller & Neubauer, 2019.). Recently, due to the Covid-19 pandemic, more and more research is being conducted on crisis risk management, for instance, the studies by Alijoyo & Norimarna (2021), Deshpande & Desai (2021); Grondys et al. (2021) and Jeynak & Bak (2021).

3.1 Risk Management Process

Several studies have proposed a framework for the risk management process. For example, Bandyopadhyay et al. (1999) proposed an integrated risk management process with information technology (IT) to reduce the possibility of losses due to IT threats through risk identification, risk analysis, risk mitigation measures, and risk monitoring. In 2011, Tummala & Schoenherr (2011) proposed more effective management of supply chain risks using Supply Chain Risk Management Process (SCRMP) in three phases, namely risk identification, risk measurement and risk assessment, risk assessment, risk mitigation and contingency plans, and risk control and monitoring. More recently, Ullah et al. (2021) proposed a risk management framework based on technology, organisation, and environment (TOE) to enable better governance of sustainable smart cities.

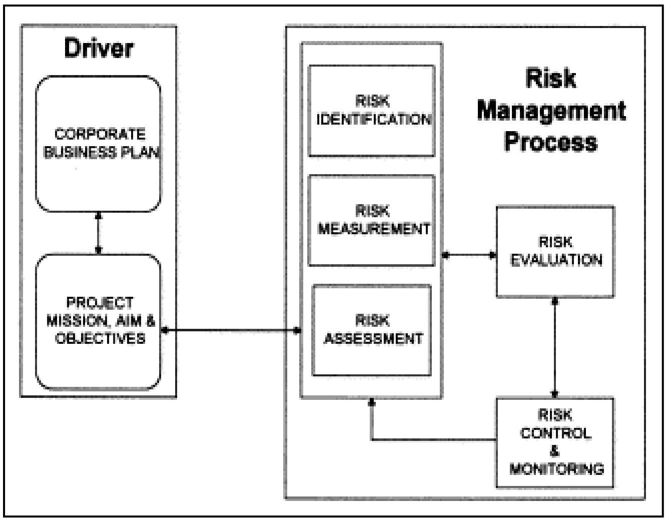


Fig. 2 - Risk management process (Tummala & Burchett, 1999)

Tummala & Burchett (1999) developed a framework known as the risk management process (RMP) to help organisations in determining the probabilities and consequences of all potential risk factors associated with a project. With the help of the RMP, organisations can identify the resources they need and then select appropriate measures to control and manage the identified risk factors. Ultimately, the organisation can achieve the desired outcomes of the project. As shown in Figure 3, the RMP begins by identifying the organisation's business plan and the mission, goal and objectives of the specific project. Based on the desired project objectives, uncertain events (risks) were identified, measured and assessed. In this phase, different techniques were used to calculate the level of risks based on probability and impact. In the risk assessment phase, the RMP identifies several alternatives for necessary corrective actions in case the project results do not turn out as planned.

The existence of a risk management team within an organisation is now standard and common practise as uncertainties increase, which needs them to fulfil larger stakeholder expectations as well as an unlimited number of risks and issues. Therefore, it is essential for an organisation to address risk management in order to achieve effective and efficient strategy and decision-making, and to improve the effectiveness and efficiency of the organisation's operations (Hopkin, 2018).

4. Diagnostic Risk Management System (DRMS)

The Software Development Life Cycle (SDLC) can help develop the dashboard effectively. The phases of SDLC include planning, analysis, design, development, test and evaluation, and maintenance. The SDLC is customised according to the key phases that need to be implemented in the completion of this project. The test, evaluation and maintenance phase will not be carried out for the proposed prototype. However, the proposed prototype is expected to be bug free. Table 3 shows the modified version of SDLC used.

Table 2 - Software Development Life Cycle (SDLC) for DR-MS

Phase	Activities	Deliverables
Planning	• Review refereed journals and papers with references	Details of the background studies
Analysis	• Analyse features with of related existing products.	Features for proposed dashboard.
Design	• Design the user interface creating a storyboard. • Construct Work System Diagram, Use case diagram, Context diagram, Data flow diagram (DFD), Entity Relationship Diagram (ERD)	Storyboard Work System Diagram, Use case diagram, context diagram, DFD, ERD
Development	• Develop the dashboard using R language, using R Studio as the tool.	Prototyping of *DR-MS*

4.1 Planning

In order to establish a baseline understanding of related topics, journals, articles, and books are carefully read during the first phase of the SDLC. Most of the necessary research resources have been acquired, and some of them were put together to provide background information on important topics. As an outcome of this phase, details of the background studies will be delivered.

4.2 Analysis

Next, in the second phase, the existing risk management system features' are studied and analysed in Table 1.

Table 3 - Risk management system features

	Features		Portal/Platform	
Product	**Risk Assessment**	**Analytics**	**Mobile Assess**	
Camms.Risk	Inspect Risk	Monitor Predictive Analytics	Monitor Mobile Access	iCloud based Mobile: IOS & Android
TeamMate Audit Solutions	Examine Risk	Assists Predictive Analytics	Examine Mobile Access	iCloud & windows based Mobile: NA
ManageEngine ADAudit Plus	Inspect Risk	Assists Predictive Analytics	Secure Mobile Access	Windows based Mobile: NA
audits.io	Inspect Risk	Monitor Predictive Analytics	Monitor Mobile Access	iCloud based Mobile: NA
Diligent Board	Inspect Risk	Assists Predictive Analytics	Assists Mobile Access	iCloud & windows based IOS & Android
Audit Comply	Examine Risk	Monitor Predictive Analytics	Monitor Mobile Access	iCloud based IOS & Android
Project Risk Manager	Inspect Risk	Assists Predictive Analytics	Assists Mobile Access	iCloud & windows based Mobile: NA
Track My Risks	Analyse Risk	Analyse Predictive Analytics	Monitor Mobile Access	iCloud based Mobile: NA
DR-MS	Analyse Risk	Analyse Predictive Analytics	Secure Mobile Access	Windows based Mobile: NA

4.3 Design

The technical aspects of the tool are covered in this section. The use case and its description are used to explain the system. The interaction between users and the tool is shown in the use case diagram. The tool's use case diagram is shown in Fig. 3.

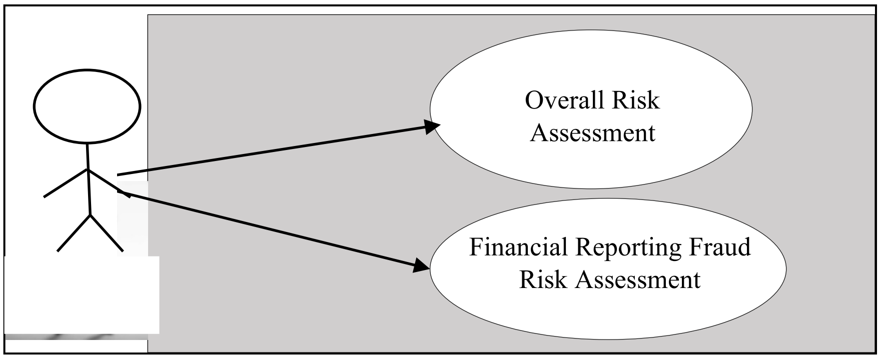


Fig 3 - Use case diagram

The use case diagram consists of two use cases which are overall risk assessment use case and financial reporting fraud risk assessment use case. Each of the use cases will be explained in the use case description as shown in the Table 4 and Table 5.

Table 4 - Use case description for overall risk analysis

Use Case Name	**Overall Risk Assessment**
Triggering Event	User clicks the *Overall Risk Analysis* tab
Actors	User
Pre-Conditions	-
Post-Conditions	Report, filter and visualise overall risk assessment of a particular project
Flow	User selects to menu to view result Use Case ends

Tables 4 display the use case description including the role that has been assigned to the user. The user can generate a report, filter results, and view the overall risk assessment of a certain project by selecting the Overall Risk Analysis tab (see Table 4).

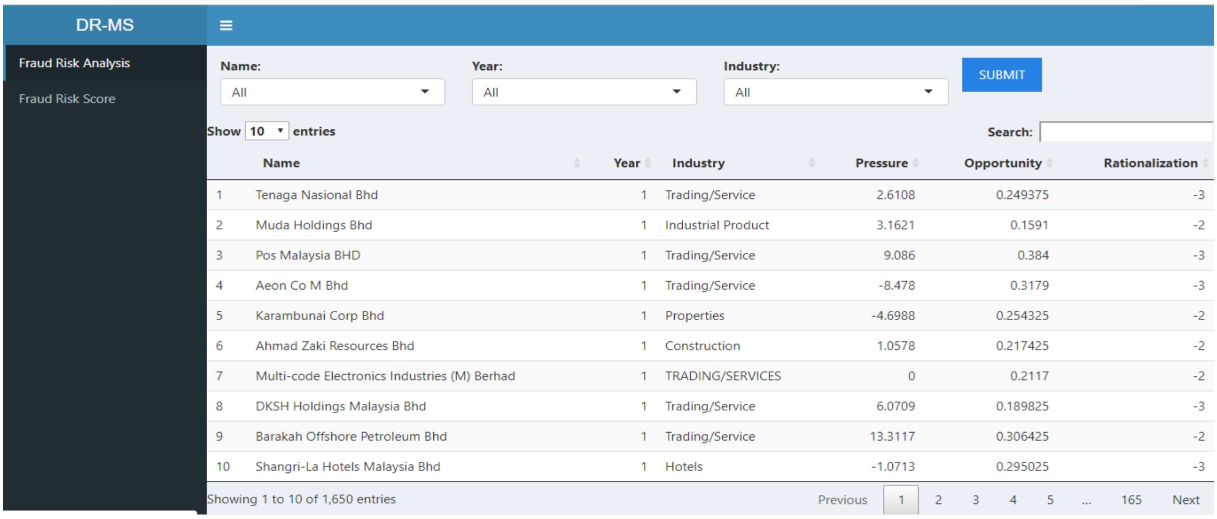
Table 5 - Use case description for financial reporting fraud risk score

Use Case Name	**Financial Reporting Fraud Risk Score**
Triggering Event	User clicks the *Financial Reporting Fraud Risk Score* tab
Actors	User
Pre-Conditions	-
Post-Conditions	Report, filter and visualise financial reporting risk score
Flow	User selects to menu to view result

The user can then generate a report, filter results, and view the financial reporting risk score of a specific project by selecting the Financial Reporting Fraud Risk Score tab, which is based on Table 5.

4.4 Development

Shiny is a package of R Studio. The purpose of Shiny in R is to facilitate the development of interactive web applications using R. This research requires the Shiny package in R to run the application. Shiny Dashboard is very useful in the design phase of this research because it requires less time and reduces the complexity in designing and creating the interface. There are many useful methods and functions the shiny dashboard that is programmed to make the interface as easy to use with minor problems. Fig. 4 and 5 show a screenshot of an interface of current application that is running in Shiny.



Name: All

Year: All

Industry: All

Show 10 entries

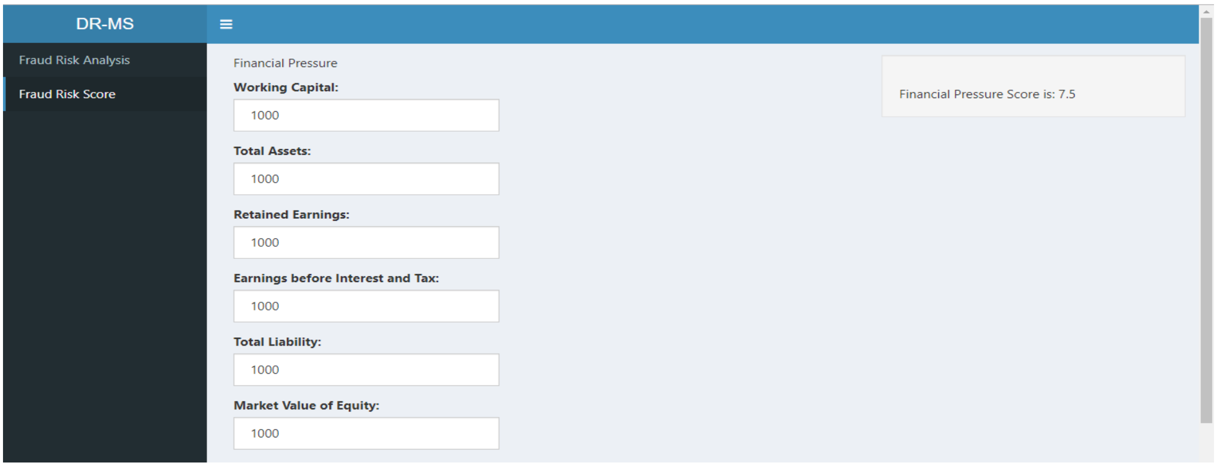
Search:

	Name	Year	Industry	Pressure	Opportunity	Rationalization
1	Tenaga Nasional Bhd	1	Trading/Service	2.6108	0.249375	-3
2	Muda Holdings Bhd	1	Industrial Product	3.1621	0.1591	-2
3	Pos Malaysia BHD	1	Trading/Service	9.086	0.384	-3
4	Aeon Co M Bhd	1	Trading/Service	-8.478	0.3179	-3
5	Karambunai Corp Bhd	1	Properties	-4.6988	0.254325	-2
6	Ahmad Zaki Resources Bhd	1	Construction	1.0578	0.217425	-2
7	Multi-code Electronics Industries (M) Berhad	1	TRADING/SERVICES	0	0.2117	-2
8	DKSH Holdings Malaysia Bhd	1	Trading/Service	6.0709	0.189825	-3
9	Barakah Offshore Petroleum Bhd	1	Trading/Service	13.3117	0.306425	-2
10	Shangri-La Hotels Malaysia Bhd	1	Hotels	-1.0713	0.295025	-3

Showing 1 to 10 of 1,650 entries

Previous 1 2 3 4 5 ... 165 Next

Fig. 4 - Screenshot (1) of DR-MS



Financial Pressure

Working Capital: 1000

Total Assets: 1000

Retained Earnings: 1000

Earnings before Interest and Tax: 1000

Total Liability: 1000

Market Value of Equity: 1000

Financial Pressure Score is: 7.5

Fig. 5 - Screenshot (2) of DR-MS

5. Conclusion

DR-MS is developed to assist in assessing risk based on projects, unit, or even institutional. DR-MS also focus on assess risk on financial reporting fraud risk. DR-MS a user friendly system that can helps company to manage and look at the overall exposure towards risk and help them to identify suitable solutions to mitigate each risk is essential. The system can be accessed online, and also using mobile phone. DR-MS is a self-assessment system suitable for organisation to create a competitive but healthy business environment that is free from destructive elements such as corruption, fraud and economic crime. Monitoring can be done remotely and timely. It is hope that this study will benefit the stakeholders, and in turn will guarantee a wealth creation for business environment in Malaysia. Subsequently, DRMS shall become another prominent industry in future.

Author Contributions

Shuhaida Mohamed Shuhidan: Writing - original draft, methodology, system development. **Farah Aida Ahmad Nadzri**: Writing - literature review, financial reporting fraud risk, risk management process. **Marhamah Rafidi :** Writing - reviewing and referencing . **Jamaliah Said** : Supervision, Writing - final editing.

Acknowledgments

The authors would like to thank the Universiti Teknologi MARA, Malaysia and Accounting Research Institute (HICoE) and Ministry of Higher Education Malaysia for providing the necessary financial assistance for this study.

References

ACFE, A. o. C. F. E. (2018). Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse.

ACFE, A. o. C. F. E. (2014). Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study.

Ahmed, I., & Manab, N. A. (2016). Moderating effects of board equity ownership on the relationship between enterprise risk management, regulatory compliance and firm performance: Evidence from Nigeria. International Journal of Economics, Management and Accounting, 24(2), 163-187.

Alijoyo, F. A., & Norimarna, S. (2021). Risk management maturity assessment based on iso 31000-a pathway toward the organization's resilience and sustainability post covid-19: the case study of SOE company in Indonesia. In 3rd International Conference on Business, Management and Finance. Oxford, United Kingdom, 3, 125-142).

Altman, E. I. (1968). Financial Ratios, discriminant analysis and the prediction of corporate bankruptcy. The Journal of Finance, 23(4), 589-609.

Arbe, R., & Feria-Domínguez, J. M. (2022). Reputational risk on corporate corruption scandals: evidence from Latin America. Academia Revista Latinoamericana de Administración, 35(3), 329-344.

Bandyopadhyay, K., Mykytyn, P. P., & Mykytyn, K. (1999). A framework for integrated risk management in information technology. Management Decision, 37(5), 437-445.

Beasley, M. S., Carcello, J. V., Hermanson, D. R., & Committee of Sponsoring Organisations of the Treadway Commission. (1999). Fraudulent financial reporting: 1987-1997: an analysis of US public companies, The Auditor's Report, 22(3), 15-17.

Beneish, M. D. (1999). The detection of earnings manipulation. Financial Analysts Journal, 55(5), 24-36.

Charette, R. N. (1989). Software engineering risk analysis and management: McGraw-Hill New York.

Chen, Huang, S.-Y., & Kuo, C.-L. (2009). Using the artificial neural network to predict fraud litigation: some empirical evidence from emerging markets. Expert Systems with Applications, 36(2), 1478-1484.

Cooper, D. F., & Chapman, C. B. (1987). Risk analysis for large projects: models, methods, and cases. John Wiley & Sons Inc.

Dechow, P. M., Sloan, R. G., & Sweeney, A. P. (1996). Causes and consequences of earnings manipulation: an analysis of firms subject to enforcement actions by the sec*. Contemporary Accounting Research, 13(1), 1-36.

Deshmukh, A., Romine, J., & Siegel, P. H. (1997). Measurement and combination of red flags to assess the risk of management fraud: a fuzzy set approach. Managerial Finance, 23(6), 35-48.

Deshmukh, A., & Talluru, L. (1998). A rule-based fuzzy reasoning system for assessing the risk of management fraud. International Journal Of Intelligent Systems In Accounting, Finance & Management, 7(4), 223-241.

Deshpande, V. M., & Desai, A. (2021, April). Smart secure: a novel risk based maturity model for enterprise risk management during global pandemic. In 2021 6th International Conference for Convergence in Technology (I2CT) (pp. 1-7). IEEE.

Dionne, G. (2013). Risk management: History, definition, and critique. Risk management and insurance review, 16(2), 147-166.

Eining, M. M., Jones, D. R., & Loebbecke, J. K. (1997). Reliance on decision aids: an examination of auditors 'assessment of management fraud. Auditing: A Journal of Practice & Theory, 16(2), 16-19.

Dorminey, J. W; Fleming, Scott A.; Kranacher, Riley M.J, Richard A, Jr. The CPA Journal; New York, **82**(6), 61-65.

Florio, C., & Leoni, G. (2017). Enterprise risk management and firm performance: The Italian case. The British Accounting Review, 49(1), 56-74.

Fox, C. (2018). Understanding the New ISO and COSO updates. Risk Management, 65(6), 4-7.

Fraser, J. R., & Simkins, B. J. (2016). The challenges of and solutions for implementing enterprise risk management. Business horizons, 59(6), 689-698.

Gaultier-Gaillard, S., Louisot, J. P., & Rayner, J. (2009). Managing reputational risk-A cindynic approach. In Reputation capital, 115-141. Springer, Berlin, Heidelberg.

Gordon, L. A., Loeb, M. P., & Tseng, C. Y. (2009). Enterprise Risk management and firm performance: a contingency perspective. Journal of accounting and public policy, 28(4), 301-327.

Grondys, K., Ślusarczyk, O., Hussain, H. I., & Androniceanu, A. (2021). Risk assessment of the sme sector operations during the covid-19 pandemic. International journal of environmental research and public health, 18(8), 4183

Hasnan, S., Rahman, R. A., & Mahenthiran, S. (2012). Management motive, weak governance, earnings management, and fraudulent financial reporting: Malaysian evidence. Journal of International Accounting Research, 12(1), 1-27.

Hayes, R. W. (1987). Risk management in engineering construction: implications for project managers. Amer Society of Civil Engineers.

Hertz, D. B., & Thomas, H. (1983). Risk analysis: Important new tool for business planning. Journal of Business Strategy, 3(3), 20-29.

Hiebl, M.R.W., Duller, C. and Neubauer, H. (2019). Enterprise risk management in family firms: evidence from Austria and Germany. Journal of Risk Finance, 20(1), 39-58.

Hopkin, P. (2018). Fundamentals of risk management: understanding, evaluating and implementing effective risk management: Kogan Page Publishers.

Jedynak, P., & Bąk, S. (2021). Risk management in crisis: winners and losers during the covid-19 pandemic (p. 252). Taylor & Francis.

Karanja, E. (2017). Does the hiring of chief risk officers align with the coso/iso enterprise risk management frameworks? International Journal of Accounting & Information Management, 25(3).

Karpoff, J. M., & Lou, X. (2010). Short sellers and financial misconduct. The Journal of Finance, 65(5), 1879-1913.

Kousky, C., & Kunreuther, H. (2018). Risk management roles of the public and private sector. Risk Management and Insurance Review, 21(1), 181-204.

KPMG Malaysia. (2014). Fraud, bribery and corruption survey 2013.

Lechner, P., & Gatzert, N. (2018). Determinants and value of enterprise risk management: empirical evidence from Germany. The European Journal of Finance, 24(10), 867-887.

Lee, H. (2021). COSO ERM Framework, 35-50. Springer.

Leech, T. (2018). Reinventing ERM to support better decision making. EDPACS, 58(5), 1-4.

Perols, J. (2011). Financial statement fraud detection: an analysis of statistical and machine learning algorithms. auditing: A Journal of Practice & Theory, 30(2), 19-50.

Prewett, K., & Terry, A. (2018). COSO's Updated Enterprise risk management framework—a quest for depth and clarity. Journal of Corporate Accounting & Finance, 29(3), 16-23.

Racca, G. M., & Perin, R. C. (2014). Corruption as a violation of fundamental rights: reputation risk as a deterrent against the lack of loyalty. in integrity and efficiency in sustainable public contracts: balancing corruption, 23-48. Bruylant.

Spathis, Doumpos, M., & Zopounidis, C. (2002). Detecting falsified financial statements: a comparative study using multicriteria analysis and multivariate statistical techniques. European Accounting Review, 11(3), 509-535.

Spathis, C. T. (2002). Detecting false financial statements using published data: some evidence from Greece. Managerial Auditing Journal, 17(4), 179-191.

Strelcova, S., Janasova, D., & Simak, L. (2018). Risk Management at slovak enterprises: an empirical study. Economic Annals-XXI, 174(11-12), 58-62. doi: https://doi.org/10.21003/ea.V174-09

Tummala, V. R., & Burchett, J. F. (1999). Applying a risk management process (rmp) to manage cost risk for an ehv transmission line project. International Journal of Project Management, 17(4), 223-235.

Tummala, V. M., & Schoenherr, T. (2011). Assessing and managing risks using the supply chain risk management process (scrmp). Supply Chain Management: An International Journal, 16(6), 474-483.

Ullah, F., Qayyum, S., Thaheem, M. J., Al-Turjman, F., & Sepasgozar, S. M. (2021). Risk management in sustainable smart cities governance: a TOE framework. Technological Forecasting and Social Change, 167 (C)

Williams, C. (2019, April 8). ISO 31000 Vs. COSO - Comparing and contrasting the world’s leading risk management standards. https://www.erminsightsbycarol.com/iso-31000-vs-coso/

Zimbelman, M. F., & Albrecht, C. C. (2012). Forensic accounting. Canada: South-Western Cengage Learning.

Zou, X., Isa, C. R., & Rahman, M. (2019). Valuation of enterprise risk management in the manufacturing industry. Total Quality Management & Business Excellence, 30(11-12), 1389-1410.