Business Management and Strategy
ISSN 2157-6068
2019, Vol. 10, No. 2

Effectiveness of Enterprise Risk Management Practices: A Case Study

Hafizah Zainol Abidin

Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia

54100 Kuala Lumpur, Malaysia

Tel: 6-03-21805011 E-mail: hafizah_za@gmail.com

Siti Zaleha Abdul Rasid (Corresponding author)

Azman Hashim International Business School, Universiti Teknologi Malaysia

54100 Kuala Lumpur, Malaysia

Tel: 6-03-21805011 E-mail: szaleha.kl@utm.my

Haliyana Khalid

Azman Hashim International Business School, Universiti Teknologi Malaysia

54100 Kuala Lumpur, Malaysia

Tel: 6-03-21805011 E-mail: haliyana@ibs.utm.my

Rohaida Basiruddin

Azman Hashim International Business School, Universiti Teknologi Malaysia

54100 Kuala Lumpur, Malaysia

Tel: 6-03-21805009 E-mail: rohaida@ibs.utm.my

Shathees Baskaran

Azman Hashim International Business School, Universiti Teknologi Malaysia

54100 Kuala Lumpur, Malaysia

Tel: 6-07-5610112 E-mail: shathees@ibs.utm.my

Macrothink Institute™

Business Management and Strategy
ISSN 2157-6068
2019, Vol. 10, No. 2

Received: September 27, 2019 Accepted: October 18, 2019 Published: November 12, 2019

doi:10.5296/bms.v10i2.15800 URL: https://doi.org/10.5296/bms.v10i2.15800

Abstract

Enterprise risk management (ERM) is used to manage, integrate and aggregate all types of risks encountered by the concerned organisation. Despite having established framework and guidelines, the implementation of ERM at divisional level seemed to be lacking. There are gaps in the actual risk management practices that need to be studied and narrowed to ensure a more effective implementation of risk management. Therefore, the objective of this study is to identify characteristics of effective risk management practices and to gauge the effectiveness level at a telecommunication company. The gaps between the actual practices and the expected practices based on twenty-four (24) identified characteristics are identified and compared upon before recommendations are made to close the gaps and further enhance the risk management practices. For the purpose of this research the self-administered, web-based questionnaires were distributed to a total number of 130 engineers who were actively involved with network infrastructure planning, development and maintenance. The feedbacks received indicated that the respondents agreed with the identified characteristics of effective risk management practices and generally agreed that the effectiveness level of current risk management practices in the company is moderate or average. Furthermore, the gap analysis based on the variances indicates that there are rooms for further improvement. The study is important for more effective risk management practices in telecommunication companies.

Keywords: Enterprise risk management (ERM), COSO Framework, Telecommunication, ISO31000

1. Introduction

The Risk Management Standard, AS/NZS 4360:1995 was first published by the multi-disciplinary task force of Standards Australia/Standard New Zealand. This standard was then used to develop the COSO Integrated Framework and ISO13000 Risk Management Standard. An effective risk management involved the process of mitigating risk through risk management planning, risk identification, qualitative risk analysis, quantitative risk analysis, risk response planning and risk monitoring and controlling. Risk can either be classified by events or the impact they may have on the organisation. Risk management is a continuous process where tracking and evaluating the identified risks are done and new risks are analysed. Risk management also includes execution of risk mitigations plans and evaluate their effectiveness in reducing or overcoming the risks (Buhr, Nel, & dos Santos, 2006).

Enterprise risk management (ERM) is an on-going process that encompasses all the activities within an organisation and requires the cooperation and involvement of all personnel at strategic, division and entity level. It is able to provide assurance to the organisation's

management and Board of Directors (BOD) in achieving one or more strategic objectives. ERM is used to manage, integrates and aggregates all types of risks encountered by the concerned organisation (Schiller & Prpich, 2014). It involves planning, organizing, leading, and controlling the activities in order to minimize the effects of the risk. ERM holds a centralised risk register and database containing all the obtained information in accordance to their risk exposure. An effective ERM approach aligns strategy, processes, people, technology and knowledge. According to Mikes (2005), ERM is a systematic approach for managing risk. By effectively managing risk, companies and organisations alike, could possibly achieve their corporate objectives and eventually create value for their stakeholders.

The Board of Directors (BOD) of the case company has approved Risk Policy and ERM Framework for all its business ventures and Line of Business (LOB) in view of the diversification of operating units and the ever increasing risks the company had been facing. To provide reasonable assurance in all the groups' efforts in achieving both the corporate and business objectives, the risk-based system of internal controls is embedded in all business processes in the company.

The proactive approach in identifying the current or potential risks and to put in place reasonable and adequate mitigation strategies in the case company remain as one of the strategic management priority. The developed ERM framework acts as a platform to establish integrated ERM and simultaneously allow for the systematic and proactive identification of threats to resources and encourage the development of appropriate strategies to minimise risks.

As the ERM framework is embedded in the daily activities within the company, a risk culture will ultimately be created within the organisation. All personnel are expected to be aware of the Group's Risk Management and Internal Control Policy and subsequently implement them. An effective risk management practice requires effective risk identification and assessment and drawing up the appropriate mitigation plans. The formulation of business and corporate strategies are then aligned with the identified risks. As a result of company's commitment to implement ERM and the possible accessibility to the valuable information such as ERM policy and guidelines, this company has been chosen in this study.

The risk universe of the telecommunications sector is changing rapidly due to the consistent and persistent evolving challenges and opportunities faced by telecoms operators around the world. Thus a firm's ability to identify and respond to changes are key success factors for future market leaders. The developed and rolled-out ERM framework and guideline is implemented in all divisions across the organisation. All divisions are also expected to realise that sound risk management will strategically affect and influence the "bottom-line" of a business organisation.

General observation indicates that, even though the company has developed ERM framework however some divisions seem to be lacking in terms of planning, implementation, control and monitoring of risk management in its daily operations. In other words, there are gaps in the

risk management practices that need to be further scrutinised and closed to ensure a more effective risk management practices in all divisions. Risk management may have been explicitly implemented in completing day-to-day work but the awareness and understanding level as well as risk culture is still lacking.

Capital projects are the heart of day-to-day work of some divisions. The work carried out involved billions and millions of capital expenses ("CAPEX") allocated. As such, risk planning, implementation, control and monitoring should be the heart of the daily operations within the division. Some personnel within the division are not aware on the existence of the ERM framework and guideline established by the group Corporate Strategy and does not know how to handle risks as they progress with their projects. Failure to comply to sound risk management may result in strategic, operational and financial risks in the organisation. Poor risk management within certain division have resulted in a few problems which may contribute to failure or delay of some capital projects which inherently affects the bottom-line of the company as well customers retention.

To date, most of the literature on ERM assesses the effectiveness of the practices at an organisational level. The impact of an efficiently implemented ERM framework is assessed on enterprise-wide level and its impact on the performance of the company. Most of the studies on ERM also highlighted the usage of COSO framework instead of the ISO31000 which is currently being adopted by the case company. The study on effectiveness of risk management practices among companies is relatively limited. Therefore, this study assesses the effectiveness of ERM practices at divisional level of a telecommunication company.

The characteristics for an effective risk management practices in terms of risk assessment and risk mitigation plans were determined. From there, the gaps between the identified standard and expectations against the perception or actual practices of risk management practices in the company was identified and evaluated. Following which, the recommendation for gaps closure and mitigation plan were established and put forth.

This study is important for future improvement for a more effective implementation of risk management practices. The objectives of this study are as follows:

1. To determine the characteristics for effective enterprise risk management practices.
2. To assess the effectiveness of ERM practices in a division of a telecommunication company.
3. To identify the gap between current practices against the established characteristics for effective risk management.

2. Literature Review

2.1 Enterprise Risk Management

Risk is the result of an organisation's decisions in setting and pursuing objectives against uncertainties which arise from internal and external environment as well as other factors that are beyond the control of the firm (Purdy, 2010). Risk may even result in financial loss or

gain, injury to people and damage to environment. Therefore, an effective risk management practices have to be in place to ensure that risks are managed appropriately. To manage the identified risks efficiently, an organisation usually adopts and implements a framework, which typically includes risk planning, risk assessment (identification and analysing) issues with regards to risk, developing risk mitigation strategies and monitoring, controlling and reviewing the risks (Purdy, 2010). Good risk management practices must be proactive rather than reactive, improves decision making and provides a platform for a logical and systematic approach in exploiting opportunities and minimising losses.

In the past, many organisations assess and mitigate risks in "silos" with the management of insurance, foreign exchange, operations, credit, and commodities each conducted as narrowly focused and fragmented activities (Yazid, Razali, & Hussin, 2012). Traditional risk management is inefficient due to lack of synergy between the various risk management units. If risk management activities are not linked or integrated with strategic planning, strategic risks can be overlooked. This may create dangerous "blind spots" and loopholes in strategy formulation and execution which can be catastrophic. Enterprise risk management (ERM) is an increasingly popular concept that is catching much attention among businesses and industries today and it is viewed as the ultimate approach to an effective risk management practices and processes (Yazid et al., 2012; Arena, Arnaboldi, & Azzone, 2011). The process encompasses all divisions and units at all levels within the organisation. Bowen, Cassel, Dickson, Fleet and Ingram (2006) argued that ERM could increase shareholders' value while Stoh (2005) postulated that ERM would provide a significant source of competitive advantage for those who can demonstrate a strong ERM capability and strength.

ERM proponents argue that an integrated risk management approach increases firm value by reducing inefficiencies inherent in the traditional approach, avoiding duplication of risk management expenditures, improving capital efficiency, reducing earnings volatility, and reducing the expected costs of external capital and regulatory scrutiny (Hoyt & Liebenberg, 2011). While risk management is coordinated by the senior or executive management, employees at all levels of the organisation are encouraged to view risk management as an integral and continuous part of their jobs.

Of late, ERM has become one of the top priorities for directors and executive management of a company due to their realisation of its importance. It emphasises a top-down, holistic approach to effective risk management for the entire enterprise. It is aimed at increasing the likelihood of an organisation to achieve its core strategic objectives by managing and balancing portfolio risks to be within the stakeholders' risk appetite (Fraser & Simkins, 2010). As such in order for it to be effective, ERM must be part of the strategic planning and execution processes. As ERM is a coordinated and consistent approach to avoid major losses in handling overall risks, a successfully implemented ERM will result in better risk integration and communication between departments within the organisation. It benefits the "company-wide philosophy", resulting in better understanding for everyone to achieve company's objective. ERM helps to increase Board of Directors' risk awareness level and

extend more knowledge in term of decision making processes and achieving better organisational results. ERM also helps in detecting early warning signs in managing both recurrent and new issues concerning the daily operations (Fraser & Simkins, 2010).

Narrowing down the scope to telecommunication industry, managing operational risks holistically will ensure better service delivery and service level management between customer and service provider. The occurrence of extensive losses due to operational failure calls for the need of operational risk management. Of late, operational risk management is integrated and embedded into the much holistic ERM. This may lead to an effective service level management which will act as an advantage over competitors and threats from potential new entrants (Santos, Clarke, & Nel, 2007). Service level management is affected by the service level agreement (SLA) and the prescribed quality of service. The SLA will act as the platform for common understanding about the services to be rendered or subscribed, responsibilities of both parties and contractual component of the subscribed service quality. By understanding and managing operational risk, both service provider and customers will be aware and come to an agreement of the accepted level of service quality (Santos et al., 2007). An effective implementation of ERM helps an organisation to achieve its targeted objectives and goals and subsequently increases its value. McShane, Nair, & Rustambekov (2011) found that there is a positive relationship between risk management and the firm value. A significant amount of commitment by BOD and top management is required for a successful implementation. Risk management has to become an integral part of how things are managed within the organisation rather than having it as an add-on or separate entity. Past studies have proven that the performance of an organisation is positively correlated with the adoption of ERM (Yazid et al., 2012; Quon, Zeghal, & Maingot, 2012). The benefits listed should be able to stimulate firms to adopt ERM into their organisational framework.

2.2 Enterprise Risk Management Framework

ERM provides a framework for management to deal effectively with uncertainty and associated risk and opportunity for firms to enhance its capacity to build its value. Two of the most popular and widely adopted standards are the ones established by the International Organization for Standardization known as ISO 31000:2009 and by the Committee of Sponsoring Organisations of the Treadway Commission, (COSO) known as COSO's Enterprise Risk Management Integrated Framework. Although they are different in name, their goals and themes are similar; to identify, prioritise and quantify risks in order to help organisations effectively manage their exposure. Both frameworks will be analysed in detail in this study.

The ERM Integrated Framework published by COSO (2004) was developed to help organisations in meeting the financial reporting requirements established by the United States Sarbanes-Oxley Act. It provides risk management architecture in terms of eight components. The framework defines essential components, suggesting a common language and providing a clear direction and guidance for ERM. The components within the framework are internal environment, objective setting, event identification, risk assessment, risk response, control

activities, information and communication and monitoring. Each of these components is to be considered under each of the four categories of entity objectives, which are strategic, operations, reporting and compliance. The ERM framework also considers activities at all levels of the organisation, namely enterprise-level, division or subsidiary and business unit processes. Hence, each level of the organisation applies the eight interrelated components of ERM to the four categories of objectives (COSO, 2004).

In November 2009, the International Standards guide, ISO 31000 Risk Management Principles and Guidelines, was developed and published by a work group of international experts from more than 30 countries (Purdy, 2010). The framework is the current best practice for risk management frameworks as it incorporates best practice from COSO, PMI (Project Management Institute), the Australian and New Zealand Standard (AS/NZS 4360:2004) and other leading international risk management standards. However, ISO 31000:2009 was based mostly from the Australian and New Zealand Risk Management Standards, AS/NZS 4360:1995 (Fraser & Simkins, 2010). ISO 31000:2009 contains principles, a framework, and a process to manage risk that can be tailored to meet the objectives of any organisation regardless of its size, activity or sector. It can be applied to a wide range of activities, processes, products or services for any types of risk, whatever its nature or possible consequences. The same working group also provides definitions for risk management after the revision of ISO Guide 73 (2002) in 2009.

Both COSO Integrated Framework and the ISO31000 have a lot of similarities as well as a few differences. COSO (2004) and ISO 31000:2009 share these characteristics: (1) adoption of an enterprise approach; (2) structured process steps; (3) understanding of and accountability for defining risk appetite; (4) formal documentation of risks in risk assessment activities; (5) establishment and communication of risk management process goals and activities and (6) monitored treatment plans. Despite sharing a few characteristics, COSO (2004) and ISO 31000:2009 do differ in certain aspects, which are:

1. COSO focused on ERM specifically whereas ISO31000 laid out a general approach to risk management based on a management processes
2. COSO is summarised and presented in a cube-like, complex and multi-layered figure whereas ISO31000 presented a framework and process.
3. The definition of risk in COSO is highly skewed to negative but the risk in ISO31000 can either be negative or positive.
4. COSO's process is sequential whereas ISO31000's process is iterative.
5. COSO framework components do not address root cause analysis and the origin of the framework is in financial risk whereas ISO31000 addresses the root cause of identified risks.
6. COSO was developed by auditors, accountants and financial experts whereas ISO was established by risk management practitioners and international standards experts.

2.3 Enterprise Risk Management Practices in the Case Company

Risk Management Unit (RMU) has been set up as part of Corporate Finance when the case company was corporatised and privatised. RMU main focus was primarily on insurance management and insurable risks with intention to prevent and control the accidental losses. Upon the introduction of the Code of Corporate Governance, RMU expanded its strategic scope of service to encompass ERM. At the early stage of ERM implementation, the case company was reactive in terms of its response to risks or crisis in the sense that there was no early preparation to mitigate risk or to response to crisis.

The company was gradually moving towards tactical and its ERM journey started two years later. The first risk policy and framework was developed back then and the BOD has approved the company Risk Policy and ERM Framework for all its business ventures and LOB. To provide reasonable assurance in all the groups' efforts in achieving both the corporate and business objectives, the risk-based system of internal controls is embedded in all business processes. The formation of Board Risk Committee (BRC) has further strengthened board commitment towards risk management and contributes towards a robust ERM environment. BRC members possess sound judgment objectivity, vast management experience, professionalism, integrity and comprehensive knowledge of the telecommunication industry.

Since its inception, the company's ERM framework has undergone a few modifications. The first framework was the Australia and New Zealand Risk Management Standards 4360:1999. Later, the company revised its ERM framework and guideline and adopted the COSO Framework. Currently, the company adopts the MS ISO 31000 framework with the aim of achieving a common understanding and standardisation of ERM processes and procedures across the group. The move to adopt ISO 31000:2009 came into picture as the company realised that the risk analysis and treatment should be based on the impact rather than an individual event. The new ERM framework seems to be beneficial for the standardization process between ERM and Group Internal Audit (GIA).

The ERM process in the company is spearheaded by the BRC and assisted by the RMU, Group Business Assurance Division. The proactive approach in identifying the existing or potential risk and to put in place reasonable and adequate controls remains as one of the strategic management priorities. The successful implementation of ERM at the strategic level is followed by institutionalisation at the operational level. The company's management is committed to manage risk at every stage of product and project development. Embedding risk management methodology into core business and operational processes across the group will assist in the pro-active recognition of risks and their treatment plan at every level of the organisation.

A risk maturity study conducted in 2012 has proven that the company's ERM Framework is relatively matured with the overall risk maturity of 3.00 (Masuan, 2013). Despite an encouraging result, the implementation wise at divisional level was pretty much very minimal.

At enterprise or organisation wide level, the risk management practices might have matured and managed to comply with the Communication and Multimedia Commission. This however, was not successfully cascaded down the line to every personnel or division. Risk ownership should have been spread throughout the company and dealing with risk is not limited to the ERM unit or a certain employees or managers. Therefore, it is important to gauge the effectiveness level at divisional level and analyse the gaps before recommending improvement plans on the areas that require further attention.

2.4 Effective Risk Management Practices

Lam (2000) postulated that ERM practices should consist of seven components which include corporate governance, line management, portfolio management, risk transfer, risk analytics, data and technology resources and stakeholder management. On the other hand, Shenkir and Walker (2006) proposed that an effective ERM implementation requires a company or organisation context that includes strong commitment from the top management, Risk Management philosophy and risk appetite, integrity and ethical values, and also the scope and infrastructure for ERM.

A study conducted by Institute of Management Accountants (2007) suggested the common elements of effective ERM which are top management commitment, established risk policies and framework, established processes and techniques for risk identification, assessment, reporting and monitoring, availability of sufficient tools and resources and commitment from all employees. In a Webinar conducted by Deloitte Canada (2012), it was deduced that successful and effective ERM implementation depends on several key success factors. The ERM framework adopted must be tailored to the specific organisation and has established a process of developing a risk management plan. Furthermore a strong leadership and support from the management and the ability of integrating ERM with business processes are required. A successfully implemented ERM is also influenced by the organisational risk culture. Finally, ERM implementation plan must also be in place and be reviewed after a specified duration.

From literature review, the characteristics of ERM based on ISO and COSO frameworks were defined and used in the questionnaire to gauge the effectiveness of ERM practices in the case company. The deduced characteristics do not deviate much from COSO ERM Framework and ISO 31000:2009 Standard. The elements in both frameworks include roles and accountability, leadership, commitment, adequate tools and information system, communication and reporting. Thus, these elements are deemed to be the attributes of an effective risk management. The following are the characteristics that will aid in contributing to the effective risk management:

1. Established and structured risk management framework and guideline.
2. Commitment and support from the management
3. Has an established team who is responsible for managing risk
4. Clear roles and accountability for managing the risks

5. Involves all personnel from all levels within the organization
6. Sufficient capable resources to promote and back risk management
7. Availability related information
8. Regular and periodic review of the risk management system
9. Clearly defined accountability for risk treatment
10. Continuous improvement plans i.e. Plan, Do, Check, Act
11. Established risk management reporting process

These characteristics act as the foundation in the development of questionnaire survey for the purpose of data collection.

2.5 Determining ERM Effectiveness Level

There are various ways that can be used in determining the effectiveness of ERM implementation in an organisation or a division. The assessment of the practice must however be based on all aspects of the framework or guideline. A group of experts from The Institute of Internal Auditors (2009) laid out a few bases in determining the effectiveness level of ERM. Firstly, the existence of ERM Framework which can be referred to and adopted by everyone to ensure a consistent approach.

The management must be able to commit and support the risk management activities. This can be demonstrated by the existence of the reporting, communication and compliance to applicable regulations based on the established ERM Guideline or Framework. The extent ERM is embedded within formalised governance and management processes must be assessed. Risk management should not be done externally. Risk culture and awareness among the member of the organisation must be promoted and inculcated. Apart from that, risks should be identified by taking into account both internal and external factors. Risk mitigation activities should consist of repeated evaluation of various available options. All personnel should also be empowered to make suggestions regarding the risks they are facing. Finally, the extent of everyone's involvement in the ERM activities should be gauged. Effective ERM practices involve collaborative and supportive efforts of management, staff, and customers in their planning, execution, and monitoring of their roles and responsibilities for the short-term and long-term welfare of the business. The developed ERM framework must also be reviewed on a timely manner to ensure continuous improvement. This is also suggested by the ISO31000 Standard.

3. Methodology

The data for this study were collected through an online survey in one division of the case company. Questionnaires were distributed to engineers in this division who handled the high cost capital expenses projects. Their projects are to ensure uninterrupted and high quality voice, data and video network to the subscribers. An extensive literature review was carried out to establish the characteristics of effective risk management practices. Among the main references were the standard practice such as ISO 31000, COSO Integrated ERM framework and other literature materials. Then the company's ERM practices were determined by

reviewing the company's ERM Guideline and Framework as well as interview with the respective risk coordinators. The information from the literature were tabulated, compared and selected as the characteristics of effective risk management practices. From there, the characteristics were listed and formed into questionnaire to be distributed to the selected respondents. Before that, these identified characteristics were verified by three experts to ensure the validity. Two of these experts were managers of the Risk and Corporate Compliance Management unit and another one was from the Planning and Project Management unit.

The survey consists of three parts which are Part A, Part B and Part C. Part A is the respondent background. Part B contains 24 questions which represent the characteristics of effective risk management practices that cover all the eight components of COSO ERM Framework. Each of the components is assessed with three questions. The components are internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication and monitoring. Part B is to get the respondent agreement on those statements or characteristics of effective ERM practices using the Likert scale (Zikmund, Babin, Carr, & Griffin, 2013). The level of agreement was determined using a 5-point scale ranging from "least agree" (1) to "highly agree" (5). Part C contains the same 24 set of questions which specifically asked the respondent agreement towards the company current risk management practices. Similar to Part B, Likert scale was once again applied to the questions. The level of agreement is determined using a 5-point scale ranging from "least agree" (1) to "highly agree" (5). The survey was administered via two stages, i.e. pilot test and final survey. Modifications on the questions and eliminations of ambiguous questions were done before the actual survey being distributed to the identified group of respondents. A total number of 130 questionnaires were distributed to the identified members of the selected divisions and 73 valid and reliable responses were received. This constituted 56% of response rate. All the data collected were processed and analysed quantitatively using statistical Package Social Science (SPSS) version 19.

4. Data Analysis and Findings

4.1 Characteristics for Effective ERM Practices

Part B of the questionnaire is aimed at assessing the respondents' agreement on the characteristics of effective risk management practices. This part of the questionnaire survey formed the expectation of the respondents towards an effective risk management practices. In order to determine the respondents acceptance and agreement level on the validity of questions in Part B, the frequency of answers given by the respondents with the rating of 3 and above are analysed. The results are tabulated in Table 1.

Table 1. Frequency and percentage of respondents' acceptance for Part B of questionnaires

Item	Characteristics / Statement in Questionnaire	Frequency (Rating ≥ 3)	Percentage (%)
B1	There must be a structured, systematic and timely risk management approach.	73	100.0
B2	Risk management approach is dynamic, responsive and tailored to suit each division's nature of work.	73	100.0
B3	There is a single guideline and framework to be adopted by all personnel across the organisation to ensure consistency of risk management implementation.	73	100.0
B4	The risk management is clearly translated and reflected in all divisions' objectives, mission and goal settings.	71	97.26
B5	Risk tolerance in the division and organisation is aligned with the organisation's objectives	72	98.63
B6	Risk management at divisional and corporate level is aligned with the organisational strategies and goals.	72	98.63
B7	The risk identification, analysis and evaluation involve detecting changes in the external and internal context.	72	98.63
B8	Comprehensive risk identification, assessment and tolerance setting are done at divisional, operational and corporate levels.	73	100.0
B9	Identified risks are linked to the potential impacts it may have on the organisation and mapped to the risk universe and risk register.	73	100.00
B10	Identified risks are assessed in details on the likelihood and impact to the division and organisation.	72	98.63
B11	The identified risks are evaluated and prioritised in all decision making processes especially when it involves CAPEX.	73	100.0
B12	Assessment of identified risks is aligned to organisation's objectives and goals.	73	100.0
B13	Evaluation of possible responses to risk is done at divisional and organisational level.	73	100.0
B14	Responding to risks is monitored via the risk register which	72	98.63

Item	Characteristics / Statement in Questionnaire	Frequency (Rating ≥ 3)	Percentage (%)
	include avoiding, accepting, reducing or sharing the risks across divisions.		
B15	Work activities and project deployment are coordinated to direct and control the division with regards to both internal and external risk and their impact.	71	97.26
B16	Policies, procedures and guidelines in treating identified risks are clearly defined and outlined.	72	98.63
B17	There is full visible commitment and support from top management for the execution and implementation of the risk management plan.	72	98.63
B18	The risk management performance is measured against the division and organisation's performance indicators (e.g. time to deliver, financial performance and operational cost).	73	100.0
B19	There is an established information sharing process on risk management performance to affected stakeholder (e.g. email, newsletter or web-based reporting).	72	98.63
B20	The risk register and risk reports are periodically issued out on a timely manner and mitigation measures are closely monitored and followed up.	73	100.0
B21	Simple and common business risk languages or templates are used in reporting the status (e.g. Coloured diagram, visual aids (dashboard)).	72	98.63
B22	The risk management progress is measured periodically against any deviation from the risk management plan.	70	95.89
B23	The appointed risk coordinator leads the monitoring and review process which involve analysing and learning lessons from the risk management process.	72	98.63
B24	Effectiveness of the current risk management policies, guidelines and practices are always monitored for further improvement plans.	72	98.63

It is clearly visible that the percentages of the frequency for rating 3 and above are more than 90%. From the values, we can conclude that the respondents have agreed that all twenty four (24) questions in Part B, form the characteristics of effective risk management practices.

4.2 Effectiveness of ERM Practices

The respondents' perception on the level of effectiveness of the company's risk management practices were determined by analysing the total scores rated by each respondent in Part C of the questionnaires. Since there were 24 questions with the highest possible score of 5 for each, the maximum overall scores that can be obtained by each respondent were 120. For further analysis, the total score of each respondents' perception in Part C were ranked in accordance to high (score of 96 – 120), medium (score of 49 – 95) and low (score of less than or equal to 48). This was based on the assumption that an individual score of either 4 or 5 for each statement was regarded as high, 3 as average and 2 or 1 as low. The analysis indicates that 68.5% (50 respondents) perceived risk management in the company as average or medium, 27.4% (20 respondents) perceived it as high and 4.1% (3 respondents) perceived it as low. Since 50 out of 73 respondents concur with the findings, the overall conclusion is that the respondents generally perceive the current risk management practices as moderate or average. Table 2 summarised the findings on the perceived effectiveness level of risk management practices in the case company.

Table 2. Respondents' perception on effectiveness of current risk management practices in the case company

Effectiveness Level	**Frequency**	**Percentage (%)**
High	20	27.4
Medium	50	68.5
Low	3	4.1
Total	**73**	**100**

4.3 Current Practices versus the Established Characteristics for Effective ERM

The data were analysed in terms of the gap between the company's practices and expectations. The differences between the mean of perception (Part C) and the expectation (Part B) represent the gaps that need to be addressed. The gaps for all eight categories as well as for each individual statement were calculated and tabulated. The mean values were then compared to each other. The variances between Part B and Part C represent the gaps between the current risk management practices in the company and the respondents' expectations. Positive variance denotes that the current risk management practices in the company exceed or meet the expectations of risk management practices as specified in Part B of the questionnaire. On the other hand, negative variances reflect that the current risk management

practices in the company do not meet the expectations of the characteristics listed in Part B. Table 3 and Table 4 show the gaps for each category and each statement respectively.

Table 3. Gap analysis based on components - Variance of Part C and B

Variables / Component	Part B Mean (i)	Part C Mean (ii)	Variance of Means (ii – i)
1. Internal Context	4.356	3.703	-0.653
2. Objective Setting	4.000	3.575	-0.425
3. Event Identification	4.009	3.562	-0.447
4. Risk Assessment	4.078	3.553	-0.525
5. Risk Response	3.954	3.534	-0.420
6. Control Activities	4.018	3.566	-0.452
7. Information and Communication	4.018	3.607	-0.411
8. Monitoring	3.936	3.584	-0.352

All eight components have negative variances denoting that current risk management practices in the company do not meet the expected characteristics of effective risk management practices. To provide more clarity, a more detailed analysis on the variance between Part C and Part B for each statement is tabulated in Table 4.

Table 4. Gap analysis based on statements – Variance of Part C and B

Characteristic	Part B Mean	Part C Mean	Variance of Means (Gaps)
1	4.4521	3.7671	-0.6849
2	4.3973	3.7123	-0.6849
3	4.2192	3.6301	-0.5890
4	3.9863	3.5068	-0.4795

Characteristic	Part B Mean	Part C Mean	Variance of Means (Gaps)
5	3.9863	3.5342	-0.4521
6	4.0274	3.6849	-0.3425
7	4.0137	3.6438	-0.3699
8	4.0411	3.5616	-0.4795
9	3.9726	3.4795	-0.4932
10	3.9178	3.4247	-0.4932
11	4.1918	3.6301	-0.5616
12	4.1233	3.6027	-0.5205
13	3.9589	3.4521	-0.5068
14	3.8767	3.5616	-0.3151
15	4.0274	3.5890	-0.4384
16	4.0548	3.5479	-0.5068
17	3.9452	3.4932	-0.4521
18	4.0548	3.6575	-0.3973
19	3.9589	3.6712	-0.2877
20	3.9863	3.4932	-0.4932
21	4.1096	3.6575	-0.4521
22	4.0548	3.5890	-0.4658
23	3.8493	3.5479	-0.3014
24	3.9041	3.6164	-0.2877

Based on the overall results shown in Table 3 and Table 4, the variances between perception and expectation have negative values for all the items. All the variances are less than 1.0 and as such the author will focus on five characteristics that have the largest variances as they are considered more significant than the others and require immediate attention by the ERM unit or the company itself. The items are characteristics number 1, 2, 3, 11 and 12 with the variances of -0.6849, -0.6849, -0.5890, -0.5616 and -0.5205 respectively. Characteristics 1, 2 and 3 belong to Internal Context component whereas items 11 and 12 belong to Risk Assessment component. The negative variances reflect that there are rooms for improvement on the current risk management practices in the company.

Six items had variances larger than negative 0.5 which were considered significant and required immediate action by the responsible units. Detailed analysis was carried out for five characteristics with the biggest gap. The five characteristics are shown in Table 5.

Table 4. Characteristics with the biggest gaps of mean variance

No.	Characteristic	Mean Variance
1	There must be a structured, systematic and timely risk management approach.	-0.6849
2	Risk management approach must be dynamic, responsive and tailored to suit each division's nature of work.	-0.6849
3	There must be a single guideline and framework to be adopted by all personnel across the organisation to ensure consistency of risk management implementation.	-0.5890
11	The identified risks are evaluated and prioritised in all decision making processes especially when it involves CAPEX.	-0.5616
12	Assessment of identified risks must be aligned to organisation's objectives and goals.	-0.5205

Based on the results, most of the respondents were not aware on the existence of the framework and guideline published and approved by the BOD and BRC. Most of the respondents also perceived that the risk management practices in the company were not dynamic. The respondents also believed that the assessment of the risks affecting the company were not prioritised accordingly and not aligned to the organisation's objectives and goals. The respondents were also not aware that risk management is already part of their capital expenditure projects that forms majority of the work being done in the division.

5. Discussion and Implication of the Study

This study is carried out with the objectives of identifying the characteristics of effective risk management practices, determining the effectiveness level at a division and obtaining the perception of its implementation in the case company. The review on the effectiveness level is essential to ensure that the implementation has reached its target and to determine any gaps that need to be addressed.

The study has identified twenty-four (24) characteristics for an effective risk management practice in response to the first research objective (see table 1). The results indicate that all 73 respondents agreed that the listed 24 items are the characteristics of an effective risk management practice. In response to objective number (2), the study has successfully determined the level of effectiveness of current risk management practices in the case company. It can be concluded that the respondents generally agreed that the current effectiveness level of risk management practices in the case company is medium.

The results reflect that the current ERM implementation in the company possesses the desired

key successful factors and determinants as discussed in the literature review section. The effectiveness level was measured based on the components and determinants put forth to drive for an efficient ERM implementation. The ERM framework developed and adopted by the company is deemed to be sufficient in managing risks. The findings of the study also indicate that the current ERM practices in the company involved almost all personnel at all levels within the organisation but some personnel are not aware on the processes involved. The company's top management has been committed and supportive in ensuring a successful implementation and this is apparent from the endorsed and published ERM Guideline and Framework for the past 12 years since its first inception. It is also apparent that ERM is embedded and integrated in the daily activities within the division and organisation.

In response to the third objective the results showed that the gaps for all eight categories were in negative values indicating that the current risk management practices in the case company were still behind the expectations. Therefore, it can be concluded that the major areas that required immediate action for further improvement in the risk management practices in the case company are:

1. To ensure structured and systematic approach of risk management at all divisions.
2. To introduce dynamic risk management approach at all divisions to suit the various work nature.
3. To ensure that all personnel are aware of the framework and guidelines that have been established by company's ERM unit for a consistent risk management implementation.
4. Prioritisation in evaluating the identified risks.
5. Alignment of risk assessment with the company's objectives and goals.

Failure to implement both short-term and long-term action plans could jeopardise the overall risk management practices in the company and hence may affect the financial and non-financial performance of the company. Sound and effective decision making processes would also be affected by the gaps in the risk management practices.

6. Conclusion and Recommendations

Despite possessing and demonstrating all the critical success factors and drivers, the ERM implementation in the company still needs to be improved as the overall practice is perceived as average. This is apparent from the gaps identified from the analysis of the responses. This contradicts the results of the study conducted by Masuan (2013) that postulates the company's ERM as matured. This shows that at the organisational level, the ERM practice is already in place. However, at divisional level, there are gaps that need to be closed. An effective practice at divisional level will greatly affect the implementation effectiveness at organisational level. Based on the earlier findings and the above conclusions, in order to further improve and narrow the gaps mentioned above, several recommendations are

suggested. First, it is important to implement all the established 24 characteristics of effective risk management practices in the company. Second, the awareness on the existence of the ERM framework endorsed by the BOD and BRC is still very low among a division personnel. Therefore, it is recommended that the company ERM Unit to conduct and organise roadshows, seminars and introduce compulsory e-learning training courses to improve on the awareness level. Third, risk management practices are already being implemented indirectly in all projects managed by a certain division. However, proper documentations are not prepared and monitored thus some personnel are not certain on the correct approach of mitigating risks. Hence it is suggested that the company ERM Unit needs to ensure that the risk register and the related documentation or reports are easily accessible by all personnel via the company's ERM Web Portal. It is also suggested that the company ERM Unit to issue newsletter and email snippets to all employees on a timely manner to highlight any risks or opportunities undertaken by the company that is aligned with the objectives and goals. Finally, the assessment of the identified risks has to be improved further and all divisions should engage personnel from various job positions and update them on the outcome as well as the progress of the mitigation processes.

Although several encouraging results have been found based on this research, it is important to recognize that the current findings also have some limitation that would further possibilities for future research. As such the sample in this study only covers engineers in a particular division. Thus, the findings will only reflect certain portion of staff excluding non-executive staff. Therefore it is recommended for future research to embrace bigger population and sample size. In addition, future research can expand the study by evaluating the impact of ERM effectiveness on organizational performance.

References

Arena, M., Arnaboldi, M., & Azzone, G. (2011). Is enterprise risk management real?. *Journal of Risk Research*, *14*(7), 779-797. https://doi.org/10.1080/13669877.2011.571775

Bowen, J. K., Cassel, R., Dickson, K., Fleet, M., & Ingram, D. (2006). Enterprise Risk Management Specialty Guide (ERMSG). *Society of Actuaries, Schaumburg, IL.[Google Scholar]*.

Buhr, R., Nel, A., & dos Santos, M. (2006, September). Enterprise Risk Management: A New Philosophy. In *2006 IEEE International Engineering Management Conference* (pp. 351-355). IEEE. https://doi.org/10.1109/IEMC.2006.4279884

COSO. (2004). *COSO Enterprise Risk Management - Integrated Framework.*

Deloitte Canada. (2012). Dico webinar: The five components of an effective ERM framework. [Online]Available:http://www.deloitte.com/view/en_CA/ca/services/enterprise-risk/governance-risk/ 2e2e85606be88310VgnVCM1000001956f00aRCRD.html

Fraser, J., & Simkins, B. (Eds.). (2010). *Enterprise risk management: Today's leading*

research and best practices for tomorrow's executives (Vol. 3). John Wiley & Sons.

Hoyt, R., & Liebenberg, A. (2011). The Value of Enterprise Risk Management. *The Journal of Risk and Insurance, 78*(4), 795-822. https://doi.org/10.1111/j.1539-6975.2011.01413.x

Walker, P. L. (2007). Enterprise Risk Management: Tools and Techniques for Effective Implementation. *Montvale, New Jersey, USA: Institute of Management Accountants*, 4-14.

Lam, J. (2000). Enterprise-wide risk management and the role of the chief risk officer. *white paper, ERisk. com, March*, *25*.

Masuan, M. (2013). *Implementing enterprise risk management in XYZ company: A way forward.* Unpublished Master Thesis, Multimedia University.

McShane, M. K., Nair, A., & Rustambekov, E. (2011). Does enterprise risk management increase firm value?. *Journal of Accounting, Auditing & Finance*, *26*(4), 641-658. https://doi.org/10.1177/0148558X11409160

Mikes, A. (2005). Enterprise risk management in action. *Discussion paper published by the Center of Analysis of Risk and Regulation at London School of Economics and Political Science*.

Purdy, G. (2010). ISO 31000: 2009—setting a new standard for risk management. *Risk Analysis: An International Journal*, *30*(6), 881-886. https://doi.org/10.1111/j.1539-6924.2010.01442.x

Quon, T. K., Zeghal, D., & Maingot, M. (2012). Enterprise risk management and firm performance. *Procedia-Social and Behavioral Sciences*, *62*, 263-267. https://doi.org/10.1016/j.sbspro.2012.09.042

Dos Santos, M. P. F., Clarke, W. A., & Nel, A. L. (2007, September). Enhancing telecommunications business operations and service level agreements by incorporating operational risk management. In *AFRICON 2007* (pp. 1-7). IEEE. https://doi.org/10.1109/AFRCON.2007.4401613

Schiller, F., & Prpich, G. (2014). Learning to organise risk management in organisations: what future for enterprise risk management? *Journal of Risk Research, 17*(8), 999-1017. https://doi.org/10.1080/13669877.2013.841725

Shenkir, W., & Walker, P. (2006). Enterprise risk management: Framework, elements and integration. *Institute of Management Accounting*.

Stoh, P. (2005). Enterprise risk management at United Health Group. *Strategic Finance, 87*(7), 26-35.

The Institute of Internal Auditors (IIA). (2009). *IIA Position Paper: The Role of Internal Auditing in Enterprise-Wide Risk Management*, U.S.A, the IIA.

Yazid, A., & Muda, M. (2005). The role of foreign exchange risk management in Malaysia.

Irish Journal of Management, 26(2), 45-68.

Yazid, A., Hussin, M., & Wan Daud, W. (2011). An examination of enterprise risk management (ERM) practices among the government-linked companies (GLCs) in Malaysia. *International Business Research, 4*(4), 94-103. https://doi.org/10.5539/ibr.v4n4p94

Yazid, A., Razali, A., & Hussin, M. (2012). Determinants of enterprise risk management (ERM): A proposed framework for Malaysian public listed companies. *International Business Research, 5*(1), 80-86. https://doi.org/10.5539/ibr.v5n1p80

Zikmund, W., Babin, B., Carr, J., & Griffin, M. (2013). *Business Research Methods* (9 ed.). Canada: South-Western Cengage Learning.

Copyright