CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter provides a comprehensive literature foundation and discussion on which the research is situated. The review is organized conceptually or thematically, which establishes the framework for the research investigation.

2.2 Definition of Risk

Žigiene et al. (2019) defined risk as one of the negative factors that decrease and destroy the competitiveness of any business. According to International Electrotechnical Commission (IEC), risk is defined as the combination of the probability of occurrence of harm and the severity of that harm. ISO 31000: 2018 (subsequently referred to as ISO 31000) define risk as the effect of uncertainty on objectives. It focuses on the effects of incomplete knowledge of events or circumstances on an organization's decision making. COSO's Enterprise Risk Management – Integrating with Strategy and Performance (COSO ERM Framework) defined risk as the possibility that events will occur and affect the achievement of strategy and business objective. The effects include both positive and negative effects. Risk is inherent in all business functions and in every kind of activity (Gorzeń-Mitka, 2015).

2.3 Risk Management

Risk management is the task of identifying risks, assessing risks, measuring the probability and the possible impacts of events, and treating risks, eliminating, or

reducing their effects with the minimum investment of resources (Baranoff et al., 2009; Ekwere, 2016; Md. Sum & Hamir, 2019; Verbano & Venturini, 2013). Project Management Institute (PMI) defined risk management as the systematic process of identifying, analysing, and responding to project risk (Project Management Institute, 2013). Risk management is a systematic process that involves everyone in the organization to maximize the probability and consequences of positive events, and minimize the probability and consequences of negative events to project objectives. Mansor (2017) defined risk management as a process of determining the maximum acceptable level of overall risk for engaging in business activities. As stated by Zoghi (2017), different types of business will need different tools and techniques to manage risks. Hence, there is no certain tool or technique or steps for managing risks.

According to Ekwere (2016), risk management needs to be integrated with a few items. The items are business planning, occupational health and safety, human resources management, compliance, financial management, client-customer relationship management, contract management and quality assurance. Risk management starts with identifying possible threats and then implement processes to minimize or negate them (Panigrahi, 2012). The whole risk management involves communication and consultation, establishing the internal and external context of the business, problems and issues identification, risk identification, risk evaluation and scoring, risk treatment, and monitoring and review.

Risk management includes hazard management, control management, and opportunity management. An essential element in the process of risk management is to assess the opportunities arising from risk management (Ivascu & Cioca, 2014). Bekefi et al. (2008) give an example of how a risk can be turned to a potential opportunity. A car manufacturing company may face innovation risks where market demands for core

product diminishes. Car manufacturers can use this opportunity to project the future and think about where the industry is heading and compete in advance. For example, Toyota develops a hybrid petrol-electric car years before competition. Organizations enhance their performance by managing risks and exploiting the opportunities better (Park et al., 2015). However, Ashby et al. (2020) finds that board directors struggle to find the balance in seeing risk as opportunity and as threat. Furthermore, an imperfect information on risks further complicates the board directors' struggles. Therefore, it is crucial for organizations to properly assess risks that are associated with opportunity to determine if the opportunity is really favourable (Ivascu & Cioca, 2014).

2.3.1 Risk Management Benefits

Risk management aims to prepare stakeholders for potential problems that may occur (Srinivas, 2019). A good risk management decision comes from a decision-making process that involve the views of those affected by the decision, so that a different technical assessments, public values, knowledge, and perceptions are considered (Jardine et al., 2003). Risk management aims to prevent direct and indirect costs of potentially occurring events, favouring the sustainability of the company in the long-term and assuring the achievement of the expected business value (Ferreira de Araújo Lima et al., 2020).

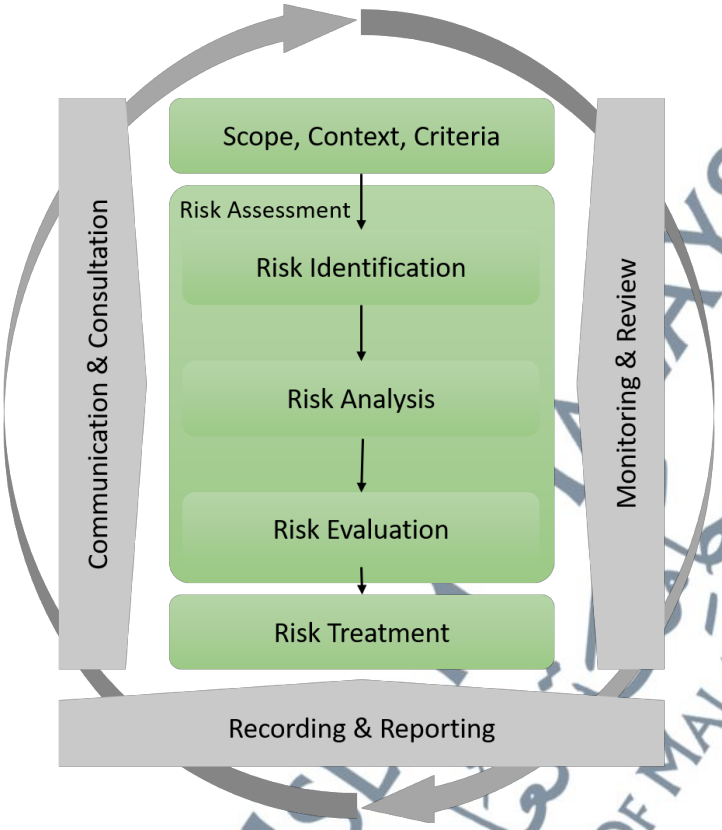
Duong (2009) stated risk management emphasizes the capabilities of a business to anticipate changes while managing risk without avoiding risks. Abu Bakar (2019) states the implementation of risk management is important to reduce volatility in the effects of risk by emphasizing the capabilities of a business to grow by managing risks, not avoiding them (Duong, 2009). Khameneh et al. (2016) agree that risk management is the key function for project-based organizations who want to create value to

corporation. Khosla (2009) adds risk management enables a business to identify threats and challenges ahead and help the business to face the risks in a more capable manner. A risk strategy should be based on the objectives of the risk management, which should include necessary preparation with respect to defined approach, tasks, and tools (Jayathilake, 2012).

2.4 ISO 31000: 2018 – Risk Management Guidelines

The International Organization for Standardization (ISO) is a worldwide federation of national standard bodies (Department of Standards Malaysia, 2010). ISO management standards typically provides a structured framework intended to meet the needs of any type of organization or situation, hence, the proposed approach in the standard is fundamentally intended to be generic and rational (Lalonde & Boiral, 2012).

The risk management process developed by ISO is as presented in Figure 2.1. The details on each step of the process are explained in the followings.



Source: ISO 31000: 2018 Risk management – Guidelines

Figure 2.1:Risk management process developed by ISO 31000: 2018.

Step 1 – Scope, context, and criteria. The first step is to establish the scope, context, and criteria of the organization. ISO 31000 states the purpose of this step is to ensure the risk management process is fit tailor made for the organization. Organization must define the scope of its risk management process because risk management may be applied at various levels of activities.

Organizations may consider a few items when defining the scope of its risk management activities. The considerations include objectives and decisions that need to be made; expected outcomes from the steps to be taken in the process; time, locations, specific inclusions and exclusions; appropriate risk assessment tools and techniques;

required resources, responsibilities, and records to be kept; and relationships with other projects, processes, and activities.

The term context as defined by ISO 31000 in clause 6.3.3 is the "environment in which the organization seeks to define and achieve its objectives". The context of the risk management process must be established from the understanding of the internal and external environment in which the organization operates. External context can be the complexity of networks and dependencies, and contractual relationships and commitments of the organization. Meanwhile, internal context can be the vision, mission, values, and culture of an organization. The context should reflect the specific environment of the business activity where risk management process will be applied. ISO 31000 emphasizes the importance for organizations to understand the business context. The importance or business context are as follows:

1. Risk management takes place in the context of the objectives and activities of the organization.
2. Organizational factors can be a source of risk.
3. The purpose and the scope of the risk management process can be interrelated with the objectives of the organization

In addition, ISO 31000 also states there are a few criteria that need to be set by the organization which are risk criteria and evaluation criteria. Defining risk criteria is to define in specific the amount and type of risk that an organization may or may not take (Institute of Risk Management, 2018). Risk criteria should be aligned with the risk management framework and must fit the purpose and scope of the activity that will go through risk management process. The risk criteria are to reflect the values of the organization, its objectives, and resources. ISO 31000 has lined out a few items to consider when setting risk criteria that are the nature and type of uncertainties that can

affect business outcomes and objectives, how to define and measure risk impacts and likelihood, time-related factors, how to determine the risk level, how to manage combinations and sequences of multiple risks, and the organization's capacity.

Step 2 – Risk assessment. The second step in the risk management process developed by ISO 31000 is risk assessment. Risk assessment is divided into three parts that are risk identification, risk analysis, and risk evaluation. Risk assessment is meant to be conducted systematically, iteratively, and collaboratively, considering the knowledge and views of stakeholder, using the best available information.

Step 2(a) – Risk identification. ISO Guide 73 defines risk identification as the "process of finding, recognizing, and describing risks". Organizations will require relevant, appropriate, and up-to-date information to identify risks. Risk identification can be done using various methods and techniques like documentation reviews, information gathering techniques, brainstorming, Delphi technique, interviewing, root-cause analysis, SWOT analysis (strength, weakness, opportunity, threat), and checklist analysis; retrospectively or prospectively.

In addition, organizations must consider a few factors, and the relationship between them when identifying risk. The factors are tangible and intangible sources of risk; causes and events; threats and opportunities; vulnerabilities and capabilities; changes in the external and internal context; indicators of emerging risks; the nature and value of assets and resources; consequences and their impact on objectives; limitations of knowledge and information reliability; time-related factors; and biases, assumptions and beliefs of the people involved. Risks are to be identified regardless of the risk source, either it is controllable or uncontrollable.

Step 2(b) – Risk analysis. Risk analysis is defined as the "process to comprehend the nature of risk and to determine the level of risk" in ISO Guide 73. Risk analysis includes a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls, and controls effectiveness.

The purpose of analysis, availability and reliability of information, and available resources can vary the detail and complexity of risk analysis process. Organizations can use qualitative, quantitative, or combination of both techniques to analyse risks. It is important for organizations to consider factors like the probability of risk events and impacts; the nature and magnitude of impacts; complexity and connectivity; time-related factors and volatility; the effectiveness of existing controls; and the sensitivity and confidence levels.

In addition, ISO 31000 suggests organizations to consider any opinions, biases, perceptions of risks, and judgements. Any influences during risk analysis process must be considered, documented, and communicated to decision makers or top management. The outcomes from risk analysis provide input for risk evaluation. Results from risk analysis help to decide whether risks need to be treated or not, and how risks should be treated using the most appropriate risk treatment strategy and methods. The results from risk analysis also provide insights for decisions where choices are made involving different types and levels of risk.

Step 2(c) – Risk evaluation. The last part of risk assessment is risk evaluation. Risk evaluation is defined as the "process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable" in the ISO Guide 73. Risk evaluation aims to support decisions by comparing the results

of risk analysis with the established risk criteria. Risk evaluation helps to figure out whether additional action is required.

After evaluating risks, the organization may do nothing further towards the risk; consider risk treatment options; undertake deeper analysis to better understand the risk; maintain existing controls; and/or reconsider objectives. However, decisions made must consider the wider context and the actual impacts to external and internal stakeholders. ISO 31000 stresses that output from risk evaluation process should be recorded, communicated, and later confirmed at appropriate levels of the organization.

Step 3 – Risk treatment. The third step in risk management process developed by ISO is risk treatment. ISO Guide 73 defined risk treatment as a process to modify risk. Risk treatment aims to select and implement options to address risk. The process to modify risk includes an iterative different process such as formulating and selecting risk treatment options; planning and implementing risk treatment; assessing the effectiveness of that treatment; deciding whether the remaining risk is acceptable; and what to do if the remaining risk is unacceptable.

It is important for organizations to choose the most suitable risk treatment options. Organizations have broad options to treat risks such as avoiding risks by not starting or continuing with activities that cause risk to happen; taking the risk to pursue an opportunity; changing the likelihood and/or impacts; sharing the risks through contracts; or retaining the risk by informed decision. If treatment options are unavailable or insufficient to modify the risks, the risks should be recorded and kept under ongoing review.

The treatment options may affect the balance between the potential benefits derived to achieve objectives, against costs, effort, or disadvantage of implementation.

Therefore, organizations must select the best treatment options that fit the organization's objectives, risk criteria, available resources, and involvement of stakeholders. However, the risk treatments may not produce the expected outcomes. Some risk treatments might produce unwanted consequences and introduce new risks that need to be managed. ISO suggested monitoring and review to be an integral part of risk treatment implementation to ensure the effectiveness to the treatments implemented. Monitoring, review, and documentation of the remaining risk is important, so the decision makers and stakeholders are aware of the nature and extent of the residual risk after risk treatment.

Organizations will need risk treatment plans to implement risk treatment. Risk treatment plans aim to specify how the chosen ~~the chosen~~ treatment options will be implemented. The specifications in risk treatment plan are to ensure the progress of the plan can be monitored and the arrangements of the plan understood by everyone involved. The treatment plans should be integrated into the organization's management plans and its processes and consulted with stakeholders. There is a few information that must be included in the treatment plans. The information includes the rationale for the treatment options selected and the expected gains from the option; who should be accountable and responsible for approving and implementing the plan; the proposed actions; the required resources; how to measure performances after implementation; the constraints; the required reporting and monitoring; and the time-related factors.

Step 4 – Monitoring and review. The fourth step in the risk management process developed by ISO is monitoring and review. ISO Guide 73 defined monitoring as "continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected". Review is defined

as “activity undertaken to determine stability, adequacy, and effectiveness of the subject matter to achieve established objectives”.

Monitoring and review aim to assure and improve the quality and effectiveness of process design, implementation, and outcomes. In earlier plan of risk management process, ongoing monitoring and periodic review and the outcomes from both activities should be included with a clearly defined responsibility. Monitoring and review should take place in all stages and processes of risk management. The process of monitoring and review includes activities like planning, gathering and analysing information, recording results, and providing feedbacks. The outcome of monitoring and review is to be incorporated along in the organization’s performance management, measurement, and reporting activities.

Communication and consultation. The purpose of communication and consultation is to aid relevant stakeholders to understand risk, the basis in decision making, and why particular actions are needed. Communication and consultation aim to

(i) bring different areas of expertise together for each step of the risk management process.

(ii) ensure different views are appropriately considered when defining risk criteria and when evaluating risks.

(iii) provide ample information to help oversees risk and in decision-making.

(iv) build a sense of inclusiveness and ownership among stakeholders that are affected by risk.

Recording and reporting. ISO Guide 73 defines risk reporting as “a form of communication intended to inform particular internal or external stakeholders by

providing information regarding the current state of risk and its management". The purpose of recording and reporting is to improve risk management activities, and to assist interaction with stakeholders, including those with responsibility and accountability for risk management activities. An organization may include decisions concerning the creation, retention, and handling of documented information when recording and reporting risk management process.

Reporting is also an integral part of an organization's governance. Risk reporting should further improve the quality of dialogue with stakeholders, apart from supporting top management and oversight bodies to accomplish their responsibilities. A few factors that can be considered by organizations when reporting may include the method, cost, frequency, and timeliness of reporting.

2.5 Risk Management Processes by Previous Studies

The following discusses risk management steps based on previous research. The discussion explains in detail the steps included in the process.

The risk management process by (Baranoff et al., 2009).

Baranoff et al. (2009) stated that for each risk exposure, the risk management process is similar across firms. The risk management process developed by Baranoff et al. (2009) is presented in Figure 2.2 and explained in the following paragraphs.

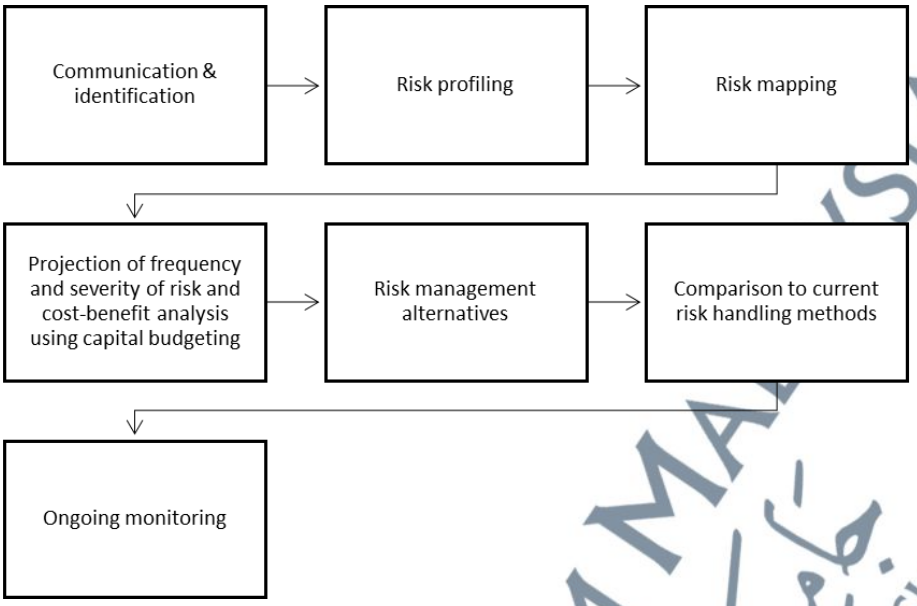


Figure 2.2: Risk management process developed by Baranoff et al. (2009).

Step 1 – Communication and identification. Baranoff et al. (2009) starts risk management process with communication and identification. Firms must have a tool to communicate the risk management process. The tool can be risk management policy or company mission statements, or risk management manuals. Firms are strongly suggested to prepare a risk management guideline. The guideline aims to help in setting the process of identification, monitoring, assessment, evaluation, and adjustments. The risk management guidelines may include crucial items like:

- writing a mission statement for risk management in the firm
- communication with every section of the business to promote safe behaviour
- identifying risk management policy and processes
- pinpointing all risk exposures
- assessing risk management and financing alternatives, and external conditions in the insurance markets
- allocating costs

- negotiating insurance terms
- adjusting claims adjustments in self-insuring firms
- keeping accurate records.

According to Baranoff et al. (2009), identifying risks is an important and detailed process. Apart from the step being a critical element in risk management process, risk managers must involve every company stakeholder and understand the firm's supply chain of movement of merchandise. It is crucial for risk managers to ensure the firm is not ignoring risks since the risks may destroy the firm.

Step 2 – Risk profiling. The second step is risk profiling. Risk profiling is a process of evaluating all risks in the firm where risk managers measure the frequency and severity of each risk. At this stage, risk managers need to learn and understand the firm's risk tolerance where they discover the risks, assess the risks, and explore the relationships of every risk with each other. Since different firms have different types of risk exposures, the risk evaluation process can differ vastly across different industries.

Step 3 – Risk mapping. To ease the risk management process, Baranoff et al. (2009) proposes to use risk mapping model as a tool for risk management. Risk mapping can be useful to identify risks and choosing the best approach to mitigate them. The technique aims to:

- aid with identification of risks and their interrelations
- provide mechanism to clearly see the best risk management strategy to undertake
- compare and evaluate the firm's risk handling

- aid in selection of appropriate strategies
- show the residual risk after risk mitigations actions are in place
- see how risks are clustered
- understand the relationship among risks
- to easily communicate risk management strategy to management and employees.

A risk map graph is divided into the four quadrants of the classic risk management matrix. Risk map is the output of risk profiling step, where the risks are charted as an entire spectrum of risk, and not individual risk (silo). Using risk map, risk managers can assess risk by displaying the risks according to their severity and frequency. An example of a holistic risk map by Baranoff et al. (2009) is presented in Figure 2.3. Figure 2.3 presented an example of a set of risks identified in a firm. The location of each data point reflects an additional risk exposure for the firm. The risks presented in the risk map can be seen holistically, hence risk manager can clearly identify all of the firm's loss exposures, estimate, and forecast the frequency and severity of each risk.

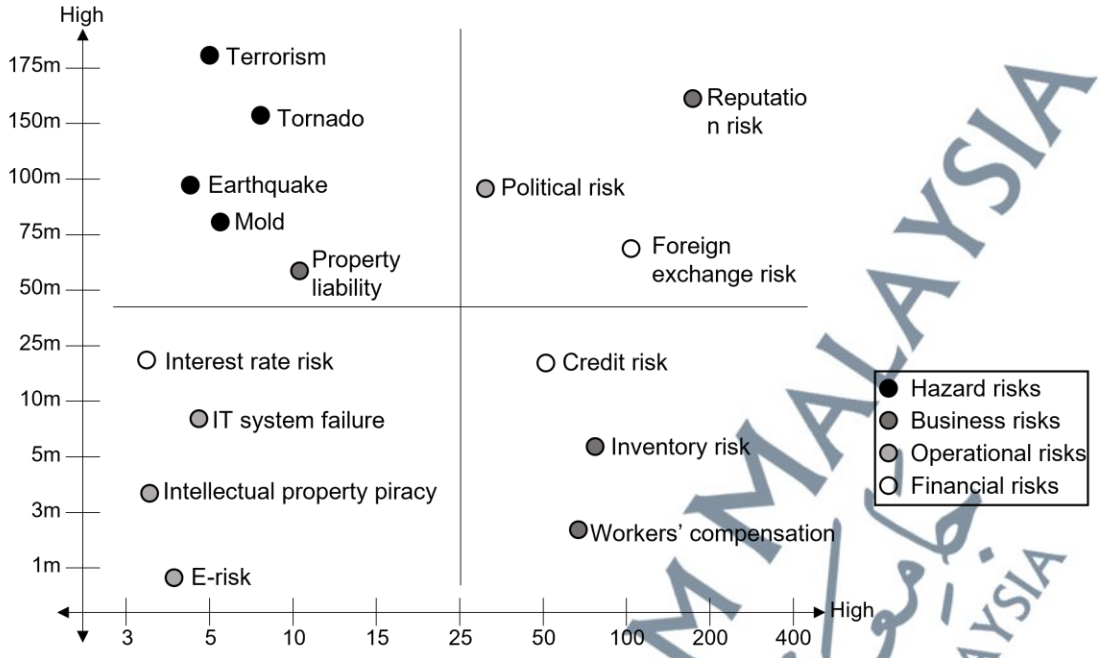


Figure 2.3: Risk map example by Baranoff et al. (2009)

Step 4 – Projection of frequency and severity of risk and cost-benefit analysis using capital budgeting. The fourth step of risk management process developed by Baranoff et al. (2009) is to project the frequency and severity of risk, and to do cost-benefit analysis using capital budgeting techniques. Baranoff et al. (2009) state forecasting involves projecting the frequency and severity of losses into the future based on current data and statistical assumption.

Given a case of investing a new research and development (R&D) project for an existing product to reduce the risk of injury among consumers, a cost-benefit analysis can be done by examining the cost of the R&D project compared to the compensation the company have to pay later. A risk manager must convince the firm that investing in the R&D project now will reduce the amount of compensation that need to be paid later. The cost of investing for R&D project is lower compared to the amount of compensation to be paid.

For this step to be done and to come out with a decision, risk managers require data and depends on analysis techniques. Baranoff et al. (2009) suggested for firm to develop an appropriate data system to allow risk managers to quantify the firm's loss history. The data system should include the type of losses, number of losses, circumstances surrounding each loss, dates, and other relevant facts. A good data warehouse allows risk managers to easily forecast using mathematical methods, do easier capital budgeting, and helps to establish a probability distribution and trend analysis.

Step 5 – Risk management alternatives. The fifth step is to find the alternatives available to manage risk based on the frequency and severity of the risk. Baranoff et al. (2009) proposed to use the risk management matrix to aid in finding alternatives to manage risks. A matrix is different from risk map. A risk management matrix includes one axis for categories of relative frequency (high and low), and one axis for categories of relative severity (high and low).

The simplest risk management matrix is as presented in Figure 2.4. There are four alternatives suggested in the risk management matrix.

- **Risk transfer**. The first alternative is risk transfer or insurance, suggested for risks with low frequency and high severity. Risk transfer is a displacement of risk to a third, unrelated party. Firms will pay someone else to bear some or all of the risk of certain financial losses that cannot be avoided, assumed, or reduced to acceptable levels.
- **Risk assumption**. The second alternative is risk assumption. Risk assumption is for risks with low frequency and low severity. Firms may retain the risk by self-insuring the risks. Risk managers can retain the risks

when the firm is willing to bear and withstand the financial losses from claims. However, risk retention depends on the accuracy of loss predictions and the arrangements made for loss payment. Some large firms use captives as insurance. Captive method is when large firms use their subsidiaries that are controlled by them, to handle risk exposures. Meanwhile, for smaller firms, they have their own risk retention group. Risk retention group is a group self-insurance, where these small firms provide risk management and retention to a few players in the same industry who are too small to act on their own.

- **Risk reduction**. The third alternative is risk reduction. Risk reduction is for risks with high frequency and low severity. Risk reduction aims to prevent losses where if losses are of low value, the loss may be easily paid out using the firm's or individual's own funds. Risk reduction is usually used to finance highly frequent, predictable losses. There are two types of risk reductions that are loss prevention and loss reduction. Loss prevention is any action taken to reduce the probability of risk occurring. Loss reduction is any action taken to reduce the severity of loss.
- **Risk avoidance.** The final alternative is risk avoidance. Risk avoidance is for risks with high frequency and high severity. Firms must avoid any situation falling in this category if possible. However, not all avoidance necessarily results in 'no losses. Avoiding a risk may lead to create other risks.

PURE RISK SOLUTIONS		
	Low frequency of losses	High frequency of losses
Low severity of losses	Retention – self insurance	Retention with loss control – risk reduction
High severity of losses	Transfer – insurance	Avoidance

Figure 2.4: The traditional risk management matrix (for one risk)

Source: Baranoff et al. (2009)

Step 6 – Comparison to current risk-handling methods. The sixth step is to create separate graphs to show how the firm is handling each risk. An example of current risk handling map is presented in Figure 2.5. When both Figure 2.4 and Figure 2.5 are overlaid, some current risk handling is different from the traditional risk management matrix. Therefore, risk managers can see that some current risk handling might not be appropriate.

Risk managers can also create another risk map to show the residual risk after implementing a risk management strategy on risks with the highest severity. This map can be created especially if the insurance coverage is lower than the expected loss. Holistic risk mapping helps risk managers to present a clear and easy-to-read presentation on firm's overall level of risks and the residual risk after implementation of risk mitigation strategies. A holistic risk map lets firm to notice risks that are still unbearable, difficult to bear, or relatively unimportant, after risk mitigation efforts are made.

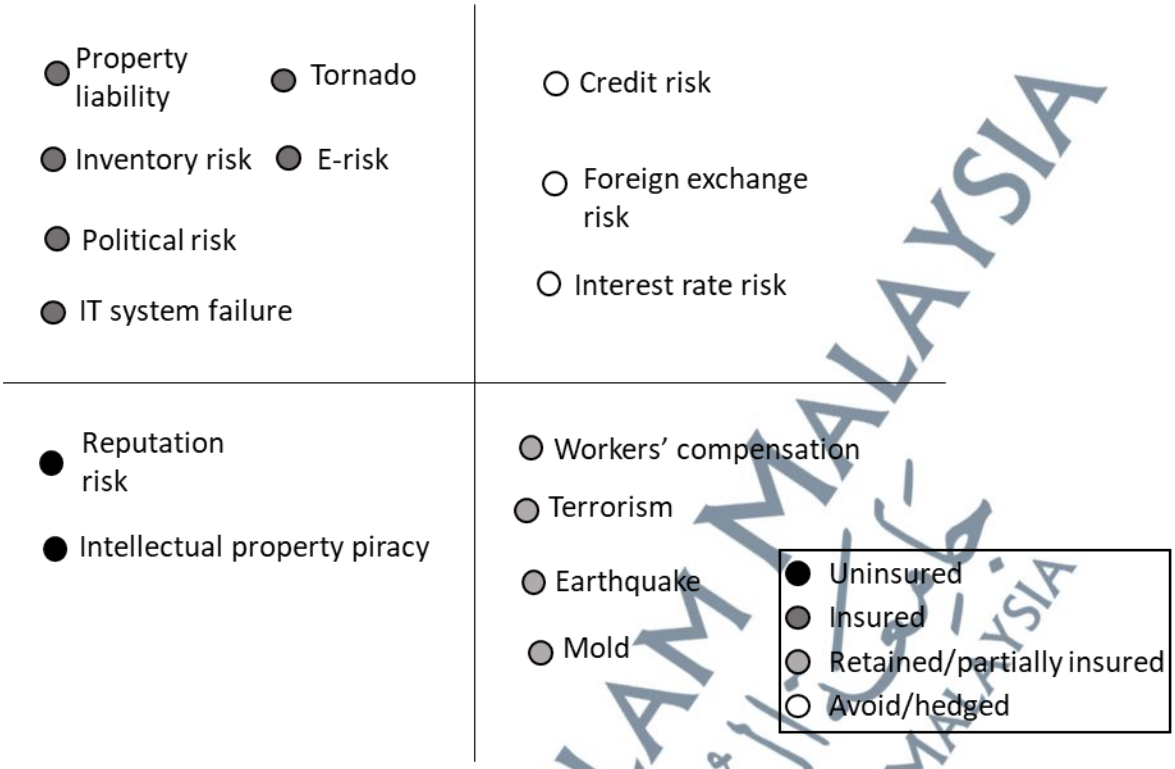


Figure 2.5: An example of current risk handling in a firm by Baranoff et al. (2009).

Step 7 – Ongoing monitoring. Risk management is continuous and requires constant monitoring. Regular and constant monitoring is important to ensure (i) the decisions implemented were correct and have been correctly implemented; and (ii) the underlying problems have not changed so much as to require revised plans for managing them. When any of the two situations (i) and (ii) exists, the risk management process returns to the step of identifying the risks. The risk management tools, and cycle will repeat.

Risk management planning for agricultural risk by Crane et al. (2013).

In 2013, Crane et al. (2013) published a handbook on risk management skills. The handbook aims to improve the risk management skills of American farmers and ranchers. The handbook helps farmers to gain knowledge on different risk management tools and how to use them. The handbook aims to build the confidence of crop and

livestock producers when dealing with risk. Crane et al. (2013) develop a nine-step risk management process. The steps are presented in the Figure 2.6.

Figure 2.6: Risk management process for agricultural sector.

Step 1 – Identify risks. Crane et al. (2013) suggest farmers to begin managing their risks by identifying and classifying prospective risks. The research identifies five main sources of risk in agricultural sector. The sources are production risk, marketing risk, financial risk, legal risk, and human risk. The research sets examples for each source of risk. For example, for production risk, the research defines production risk as any production related activity or event that has a range of possible outcomes. The farmers can oversee their risks from the major sources of production risks like weather, climate changes, pests, diseases, technology, and machinery efficiency.

Step 2 – Measure risks. Crane et al. (2013) proposes to use probabilities to express the chance of the risks occurring. The probabilities values can be obtained objectively by observation or subjectively estimated by the decision maker. Apart from that, the impact of the risk will also be measured. According to the research, riskier situations normally have greater variability of outcomes. The research suggests farmers to look for the range

of values of the possible outcomes combined with the average of the impact of the risk to their activities. These combined values may provide some information about the variability of the risks. For example, the larger the crop field, the higher the net income for the farmers. Measuring risks will involve the assessment of the probabilities to enlarge the crop field, and the impact of enlarging the crop field.

Step 3 – Assess risk bearing capacity. The third step suggested by Crane et al. (2013) is to assess an individual's capacity to bear risk. The focus is on financial capability. Farm owners can consider their obligations for cash costs, taxes, loan repayment, and family expenses that must be met every year. The higher the obligations, the less able the business is to assume risk. Therefore, it is crucial for farm owners to maintain farms' production and marketing information to assist in assessing the business capacity. The records may be supplemented by external sources. However, there is no replacement for actual historical data. If the business does not keep any financial record, they will not be able to assess their risk bearing capacity.

Step 4 – Evaluate risk tolerance or preferences. The fourth step in risk management developed by Crane et al. (2013) is to evaluate the risk tolerance or preferences of the farmers. Crane et al. (2013) divides risk tolerance of farm owners to three categories that are risk averse producers, risk neutral producers, and risk preferring producers.

- Risk averse producers are those who prefers to maintain the stability of their business, rather that exploring opportunity for higher returns. They are the most cautious risk takers.

- Risk neutral producers gather and analyse information before deciding to take any action to maximize income. They understand that there is a certain level of risks in every situation.
- Risk preferring producers view risks as something challenging and exciting. They look for the chance to take risk and enjoy adventuring into the market. Crane et al. (2013) finds that some farmers may be risk preferring individuals with respect to their marketing plan, though they might not plan to face market risk. Typically, risk preferring individuals are pure speculators.

Step 5 – Set risk management goals. Crane et al. (2013) defines meaningful goal as something specific, measurable, attainable, challenging but realistic, time specific, written, and performance based. Goals are meant to be achieved. However, if the farm cannot achieve the measurable goals, the research suggests doing objective analysis and adjust improve the likelihood of success. Farmers should focus to set goals over areas that can be well controlled. For example, if farmers can best control the skills that need to be acquired, then goals are set on skills to be acquired, and the control over achievement of skills is maintained.

Step 6 – Identify effective risk management tools. The sixth step suggested by Crane et al. (2013) is to identify the effective risk management tools. A complete strategy that integrates different responses to risks is necessary for effective risk management. This is because risks can be from different multiple sources. However, there is no limit on how farm managers combine different tools to mitigate risks. The combination of strategies may depend on the farmer's situations, types of risk faced, and the risk attitudes or preferences. The tools may vary but have the same objective that is to reduce

the probability of risk happening, and to provide protection against the adverse consequences of risk.

Step 7 – Select professional assistance. Crane et al. (2013) strongly suggest farmers to look for professionals and other growers and stakeholders if they struggle in risk management. Crane et al. (2013) proposes farmers to find educators, insurance agents, consultants, attorneys and any others that are available and qualified to help with risk management planning, depending on their specific needs.

Step 8 – Make a decision and implement the plan. Crane et al. (2013) agrees that implementing a plan is the hardest part on any decision-making process. Therefore, farm owners are suggested to be confident in following the steps and numerical measurements in implementing any plans that best fits the situation.

Step 9 – Evaluate the results. The final step suggested by Crane et al. (2013) is to evaluate the results after implementing controls on risks. Farm owners can use a mechanism to collect the results from the plans implemented. The results will then be compared with expected outcomes. The farmers may use the evaluation to make plans for any adjustments, and for future decision cycles if necessary.

Crane et al. (2013) also includes an overall risk management plan checklist as a guide for the intended users. The checklist is as follows:

- Have the primary sources of risk been identified and classified?
- Have the outcomes and their likelihood or probability of occurring been estimated?
- Has the financial capacity of the business or ability to bear risk been evaluated?

- Are risk goals written and are they specific, measurable, attainable, relevant, and timed?
- Have the goals been shared with everyone involved in the business?
- Have risk tools and strategies been identified to help manage risks which could prevent achieving established goals?
- Has a confident relationship been established with a team of risk management advisors, so they can help assess and manage business and personal risk exposure?

Risk-based thinking framework developed by Ramly & Osman (2018).

Ramly & Osman (2018) apply the risk management developed by ISO 31000 on three organizations to determine issues in the implementation of risk-based thinking (RBT). The issues determined are (i) too many and complicated RBT approaches; (ii) no integration between RBT with strategic and operation; and (iii) communication and awareness of RBT. To solve these issues, Ramly & Osman (2018) modifies risk management process by ISO based on the issues addressed by participants of the research. The developed risk management process is as presented in Figure 2.7.

Figure 2.7: Risk management Risk Based Thinking Process developed by Ramly & Osman (2018).

Step 1 – Determine the purpose. The first step recommended by Ramly & Osman (2018) is the same as the step 'Scope, context and criteria' by ISO. Ramly & Osman (2018) modifies the name of the step to 'Determine the purpose' because the research participants are unable to explain the needs to link risk with context of organization. Ramly & Osman (2018) solves this issue by suggesting context of organization funnelling process for organizations to come out with risk management scope and criteria. The funnelling process proposes organizations to include and consider external issues, internal issues, and organization strategies and objectives.

Step 2 – Determine the issues. The second step recommended by Ramly & Osman (2018) is to determine the issues in the organization. Ramly & Osman (2018) finds organizations are confused when defining issues and risks. Therefore, organizations must clearly define the terms used for risk management process. Issue can be defined as key drivers which may impact objectives of the organization. Organizations can begin with referring context of organization as the external or internal environment in which the organization seeks to achieve its objectives. Ramly & Osman (2018) suggests organizations to use Balance Scorecard (BSC) where the categories in the BSC can be further derive organizations' issues in term of objectives or key performance indicator. The term risk defined in this research follows the definition by ISO that is "the effect of uncertainty on objectives".

Step 3 – Determine the consequences criteria. The third step recommended by Ramly & Osman (2018) is to determine the consequences criteria. Risk consequences criteria can be determined from the issues found from Step 2. Brainstorming of the possible impacts from the determined issues can help in this step. Risk consequences criteria set up can include qualitative description such as high or low, and quantitative description through scores or scale. The scores or scales represent the level of impacts of the risks.

Step 4 – Risk identification. The fourth step is risk identification. Ramly & Osman (2018) suggests organizations to describe risks in detail when identifying risks. The risk description may include risk sources, potential events, the consequences, and the likelihood of the risks. Risk source is any element that have potential to increase the likelihood of risk event to happen. Potential event is defined as how risk event may

occur and should be described in terms of something that can be controlled or corrected. The aim is to assign a proper risk treatment for the risk cause.

Step 5 – Risk assessment.The fifth step is risk assessment. Risk assessment aims to determine whether the risk level is acceptable when compared to risk appetite of an organization. Risk level can be determined by combining the consequences and likelihood of risks. Consequences is the outcome of a risk event which affects organization's objectives. The effects can be certain or uncertain, positive or negative, and direct or indirect. Meanwhile, likelihood is the chance of an event to happen. Likelihood can be described objectively or subjectively, using general or mathematical terms. Both likelihood and consequences can be expressed quantitatively or qualitatively. The participants of the research use methods such as risk mapping, risk priority number, and force field analysis for risk assessment.

Step 6 – Determine risk appetite. The sixth step is to determine risk appetite. Ramly & Osman (2018) adopts definition of risk appetite as the amount of risk that one is prepared to accept, tolerate, or be exposed to at any point in time. Only one out of three research participants in the research have a properly defined risk appetite and risk tolerance in their organization. The other two organizations used colour coding in risk matrix and risk priority number threshold as the benchmark to define their risk tolerance.

Step 7 – Determine risk treatment. The final step is to determine risk treatment. Ramly & Osman (2018) adopts the risk treatment step in the risk management process developed by ISO. The term and definition of risk treatment in ISO was replaced with

risk control. Risk control is a measure that maintains and/or modifies risk. Modified risk is known as residual risk, the remaining risk after the efforts to mitigate and eliminate risk are put in place. The residual risk may be known but not completely controllable. Ramly & Osman (2018) also suggests risk treatment methods or actions as suggested by ISO. Ramly & Osman (2018) reports the participants do not have specific methods to determine risk treatment.

Operational risk management framework developed for SMEs by Naude & Chiweshe (2017).

Naude & Chiweshe (2017) develop an operational risk management framework for SMEs. The risk management framework can be used by SMEs to identify and analyse risks in their operations and taking corrective actions to mitigate the risks. Naude & Chiweshe (2017) uses a conceptual analysis approach on relevant literature sources to formulate the developed framework. The framework is as presented in Figure 2.8. Naude & Chiweshe (2017) assumes SMEs to have several employees with functional responsibilities. The targeted risk manager is not relative to highly skilled functional department heads, but rather individuals who know the business and its functions, and those who understand the risks that an operation face.

Step 1 – Risk identification. The first step proposed by Naude & Chiweshe (2017) is risk identification. This step aims to identify and understand the possible risk sources. The risk identification step is divided into three sub-columns that are objective, description of risk, and responsible person. The possible risk category listed by the research on the left column of the proposed risk management framework are suggestions. The categories differ depending on the size and type of the business.

To identify the risk category, Naude & Chiweshe (2017) suggests SMEs to form a cross-functional team to discuss the objectives of the SME operations and identify potential operational risks. For example, for marketing risk, the team can start by identifying a key potential business or marketing issues that can negatively impact the business operation. The team can investigate this issue from an objective perspective, or desired outcome perspective. From this, the team can create a positive statement that the business wants to achieve in the operational area. The team can ask questions regarding the likelihood of the objective to be achieved, and types of issues that causes the objective to be non-achievable. The details of this issues that causes objectives to be unachievable will then be written in the next column, description of risk.

The final step of risk identification is to nominate the responsible person. For example, for problems relating to transporting goods to customer, the name of the person in charge to transport the goods can be written in the responsible person column. In short, businesses will have the desired objective in the first column, the actual risk detail in the second column, and the person who will be responsible to manage and monitor the risk.

Risk identification			Risk assessment							Risk response – Mitigation strategy	Risk monitoring and control
Objective	Description of risk	Responsible person	Severity rating (scale of 1-10)					Probability rating	Risk score		
			Financial	Health and safety	Natural environment	Reputation/ media	Legal				
Operational risks: - - -											
Market risks: - - -											
Technical risks: - - -											
Financial risks: - - -											

Source: Naude & Chiweshe (2017)

Figure 2.8: Operational risk management framework for SMEs developed by Naude & Chiweshe (2017).

Step 2 – Risk assessment. The second step is risk assessment. There are three main columns under risk assessment. The first column is for severity rating of identified risk. The impacts of the risks are subcategorized to different aspects of the business. Then, the risks are ranked from 1 to 10 with 10 being the highest severity. The ratings are then combined. For example, if a risk has a severity score of financial (4), natural environment (2), and legal (3). The ratings will be: 4 + 2 + 3 = 9.

The second column is for probability rating given to identified risk. Like severity, the scale for risk probability is also 1 to 10 with 10 being the highest probability of a risk event to occur. For example, if the cross-functional team decides that 40% of the time the marketing procedure to look for potential customers is disrupted, the probability scale will be 4.

The third column in risk assessment is risk score. The risk score can be obtained by multiplying the severity risk rating by the probability rating. From the mentioned

example, the risk score will be 9 × 4 = 36. The risk score is 36. The research concludes the higher the risk score, the higher the perception that the risk will happen and impact the business.

Step 3 – Risk response – mitigation strategy. The third step is risk response – mitigation strategy. The aim of this step is so the cross-functional team can look over the existing controls and the added measures needed to mitigate more severe risks. Therefore, after obtaining risk scores, the risks must be ranked top to bottom according to the scores. This way, the cross-functional team can deal with risks that have highest risk score, or the most severe risk. A discussion can be held between the cross-functional team with the person assigned in responsible person column. The responsible person will need to share their input or the risk mitigation strategy to mitigate the risk.

Naude & Chiweshe (2017) also proposed risk mitigation to be divided into three steps.

- Step 1: Alerting stakeholders relating to the risk.
- Step 2: Doing check and balance of the process causing risk event to happen. Check and balance, and audit can help identify and address any system or process weaknesses.
- Step 3: Take action to mitigate risks and ensure the risk or problems will not happen again in the future. It is crucial for the person responsible to satisfy the cross-functional team with the mitigation actions taken against the identified risk.

Step 4 – Risk monitoring and control. The final step is risk monitoring and control. Risk monitoring and control can provide early warning of increasing risk levels.

Implementing this step may help organization to buy time to react to changes and formulate new approach to mitigate the risk. In this column, the results of mitigation actions taken to mitigate risks is written. This process is done only after mitigation actions are implemented, and the feedbacks and evidence of the mitigation actions implementation are provided to the cross-functional team.

Naude & Chiweshe (2017) recommends cross-functional team to meet at least twice a year to ensure responsible person have ample time to complete the mitigation action steps. The next meeting should be a follow-up review of the risks. The team will need to re-evaluate, rescore, and overwrite the original values of each identified risk. The original risk score will also be noted in this column to monitor and confirm the progress of the risk strategies. This last process is the key to closing the risk management cycle and to ensure forward progress and momentum.

Enterprise risk management system for SMEs by Bensaada & Taghezout (2019).

Bensaada & Taghezout (2019) intends to help SMEs to engage in enterprise risk management (ERM). The developed risk management system uses the general ERM pattern which is constituted by five key components imbedded in a multicycle iterative process as shown in Figure 2.9. The five key components are communication and information, foundations and context, modelling and assessment, response and treatment, and monitor and review.

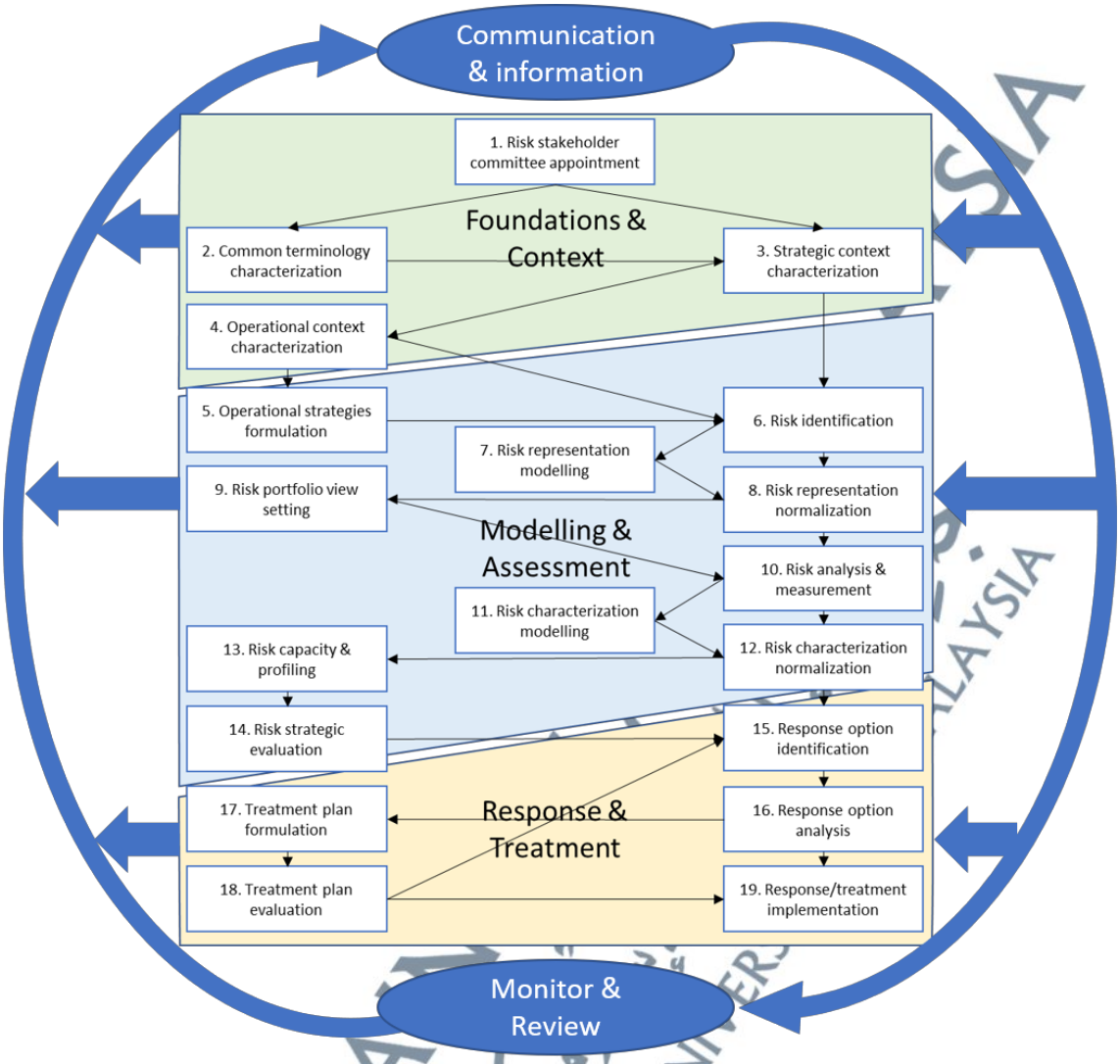


Figure 2.9: Modular, optional and sequential (MOS) framework corresponding to the core synthetized ERM process developed by Bensaada & Taghezout (2019).

Key component 1 - Foundation and context.

The first key is foundation and context (F&C). F&C deals on one hand with risk management benefits and consulting the internal and external stakeholders to involve them effectively. Apart from that, F&C also plan, define, and set the external context, internal context, and risk contexts in which the risk management process will take place. F&C can be considered as a modelling of the organization and its environment to simplify and clarify business complexity. These contexts are crucial to be understood

so that ERM can be designed and integrated to complement, and do not conflict with the organizational culture, processes, structures, strategies, and objectives. There are five modules under the first key component. The modules are risk stakeholder committee appointment, common terminology characterization, strategi context characterization, and operational context characterization. Each module is explained in the next part.

Module 1 – Risk stakeholder committee appointment. The first module consists of determining who should participate in the ERM process, and their tasks, responsibilities, and accountabilities. To set up ERM, a standardized risk management governance structure should be formed involving two stages. The first stage requires collaborators to take care of the control aspect, fix the objectives and scope all core modules, and operate the F&C component. The first stage will involve managers who supervise the organization main functions.

The second stage is involving assistants of appointed key operating staff because they are considered the most knowledgeable in their work areas. These people should be the one who runs the core modules, but only starting from risk identification. Module one is designed to be ran without help from any expert. However, the committee may call for an expertise in case there is a need for it.

Module 2 – Common terminology characterization. The second module aims to adopt key terminology for targeted organization. The terms are to be used as a standardized markers so the activities in the upcoming modules will be more straightforward and coherent. Usage of common language helps in information recording and retrieval, widens, and structures thinking perspectives. For example, the

term ‘employee’ should describe all types of employees including top management, operational staffs, and so on.

Module 3 – Strategic context characterization. At this step, the main strategic features of the organization must be understood, defined, expressed in a meaningful and actionable way to ensure decisions about risks are put in place in the later steps. Items for strategic context like business core values, objectives, model, and risk appetite policies must be clarified. These items are then formulated as strategic parameters like reputation, corporate responsibility, laws and norms compliance, and production and distribution capabilities. The attitude of the organization towards the strategic parameters must be analysed and appreciated with measurable criteria like the organization’s intended growth, desired risk-taking attitude, and criticality. Setting strategic parameters also helps organization to optimizer resources allocation for risk management process, especially in ‘Modelling and assessment’ & ‘Response and treatment’.

Module 4 – Operational context characterization. This stage is to ensure a proper understanding of inner workings and the actual and potential operational strategies. Module four aims for prioritization of the areas in the organization which are targeted as focus drivers in terms of devoted resources and efforts. The end goal is to classify various actual or potential ERM target by order of importance within each type.

At this stage, these identified ERM targets are referred as risk units (RU). There are four steps that need to be performed on RU to achieve the desired goal. The first step is to define the operational parameters on each RU that is going to be evaluated. The parameters can be important score, independency score, and time frames. The

second step is to identify different RU from the most global type to the most specific, according to a top-down approach, defining by the way vertical illusion ties (parent-child).

The next step is to evaluate each RU with the operational parameters. The output is the priority scores for each RU. The fourth and last step is to classify RU according to their types and scores. The organization now have a list of ranked global RU and its children. RU allows automatic integration of project ins ERM.

Module 5 – Operational strategies formulation. This module is about defining and expressing the operational plan for contexts identified in module four. Some organizations use the existing performance benchmark. However, new performance measurements might be created when needed. At this stage, each performance indicator will have their own target value and deviation tolerance threshold. The values are based on the current enterprise operational and strategic contexts. Organizations can explore alternative strategies by applying different settings for RU. For example, adding different activities for the same project.

Key component 2 - Modelling and Assessment

The second key component in the developed risk management process is Modelling and Assessment (M&A). There are nine modules for this stage continual from the previous stage. The modules are explained as the followings.

Module 6 – Risk identification. The aim of this module is to identify all possible risks of the organization. Organization can use any methods or techniques to identify risks, but they must consider the output of the preceding modules. At this stage, organizations

are expected to identify the maximum number of risks. The research suggests two tools which are meant to suit non-experts and are complement to each other. The tools suggested is highly compatible with the risk representation model provided in module seven.

The first tool is by finding out the main event that can affect each one of the strategic parameters. From that, organization can look for the event factors and causes, and the possible effects of the event. The second tool is rather deductive. The organization may begin with a given RU, with the uncovered and listed main agents, their types, and states. Organization may also consider different events that happen due to the same factors as the RU given. Organization can identify their mutual interactions and impacts on the strategic parameters. The more refined the RUs, the easier it is to identify the agents and consequent risk events precisely.

Module 7 – Risk representation modelling. This module aims to integrate all risk management components used in the previous modules. These components must be translated into risk description tool that can be understood even by the non-experts. The risk representation developed and proposed at this stage provide a formulation with two levels to grasp and describe risk, namely high and low. High level links to less refined and structured risk information, and low level linked to highly refined and structured risk information. The information from both levels is used differently. Each risk is associated with textual description, main factors, possible outcomes, its current state, existing control mechanisms, first impression evaluation, accountable person, and events reporter.

The high-level description aims to provide a loose, unconstrained, and sketched expression of a risk. The input format is easy to handle. The high-level description is

meant to cluster the low-level description elements. The low-level description is a detailed and well-structures view. The deeper description may include causes and consequences of chain, and deeper understanding of the risk and its dependencies, according to the wanted depth of modelling-scope.

The low-level description causes a linear network of nodes of the risks. There are three types of nodes distinguished namely cause, consequence, and cause-consequence. A cause node is defined as three properties that are the agent or the cause itself, its type, and state. Consequence node is by looking at the directly impacted strategic parameter by risk event, the impact form whether positive or negative, and indicators like the measurement criteria impacted by the risk event. Lastly, the cause-consequence node is the combination of the first two nodes. It is crucial for the organization to understand that a risk event might constituted by one or more cause nodes, but only have one consequence node. This means the consequence node can represent the main risk event, while cause nodes represent the circumstances for its occurring. The research suggests organizations to document the risk representation in templates that are easy to fill and managed.

Figure 2.10: Risk analysis according to risk representation templates from Module 7.

Module 8 – Risk representation normalisation. The objective of this module is to familiarize with risk description because identified risks could be represented in various ways. The risks identified in Module 6 must be analysed following the risk representation template from Module 7. The aim is to standardize the risk description because some risks might be represented in various ways.

A simplified steps to analyse risk is presented in Figure 2.10. In step 3 represented in Figure 2.10, a basic set of rules must be applied. The rules are (i) main factor event agents are instantiated as cause nodes; (ii) main outcome event agents are instantiated as cause-consequence nodes; and (iii) impacted strategic parameters are

either instantiated as consequence nodes or should be integrated in corresponding cause-consequence nodes. The result of this stage is to produce an updated risk event register.

Module 9 – Risk portfolio view setting. This module aims to build a tailored flexible categorization for the organization. In this module, risks are sorted out from the whole risk pool. The sorting is done within the frame of risk representation model according to similarities of tags related to a given property. Risk sorting can be done through the analysis of tag-data correlations.

Module 10 – Risk analysis and measurement. The module aims to analyse and measure risks. Identified risks may need further refinements to present related risks. Organizations can use qualitative or quantitative method to analyse the risks, depending on type of the risks and the analysis depth-scope wanted.

Module 11 – Risk characterization modelling. This module includes the process of consistently integrating the risk management components used with risk characterization tool that meets non-expert needs. The outcome from Module 11 combined with risk representation model yields the full entity-wide risk definition.

Module 12 – Risk characterization normalisation. This process is in conformity with the previous formulation in Module 11. At this stage, analysis and measurement of risks should be reconsidered to the organization's global scale. The purpose of this module is to make the whole process independent towards risk analysis tools. This will later provide a universal and coherent risk characterization for the organization.

Module 13 – Risk capacity and profiling. This module appraises risk capacity of the organization against available resources. The risk capacity set up must be within how much organization resources can withstand the risks before a state of no-recovery occurs. The organization must appreciate the level of risk distribution across risk portfolios. This level of risk distribution is to be expressed in terms of impact of the risks on strategic level, which leads to the establishment of the organization risk profile.

Module 14 – Risk strategic evaluation. The measured risk level obtained in Module 12 is used in this module. Module 14 aims to determine the level of organization exposure to each risk. Hence, the risk level obtained in Module 12 will be used with respect to the strategic global preference of the organization, especially the risk appetite components. The output from this module is a refined classification and prioritization of risks that require adequate risk response.

Key component 3 – Response and Treatment. The last key component in the developed risk management process is response and treatment. There are five modules in this stage continual from the previous stage. The five modules are explained as the followings.

Module 15 – Response option identification. At this stage, organizations can identify the possible responses to risks, either individually or in portfolios. There are three main options of types of risk responses that are avoidance, reduction, and acceptance. Accepting risks means exploiting the risks for organizations benefit; or monitor the risks for early warnings.

Module 16 – Response option analysis. This module is meant as the analysis of the response options what should be performed with respect to feasibility of the organization and the cost/benefit criteria. At this stage, the adequate option can be selected. The responses are not necessarily mutually exclusive. Hence, organizations will have multiple response options to choose for each risk.

Module 17 – Treatment plan formulation. In this module, organizations will describe how the selected response options will be carried out. The descriptions should be detailed in a form of comprehensive plan. There can be one or more plans consisting of different combinations of response options.

Module 18 – Treatment plan evaluation. At this stage, the different ERM targets acquired as treatment plans should all be processes through M&A modules. If the deduced remaining risk exposure estimate is not acceptable, the organization must return to Module 15. Otherwise, the incremental best plan should be selected.

Module 19 – Response/treatment implementation. The final phase is solely for the execution of the response options or treatment plans selected.

The following modules are meant to be implemented throughout the risk management steps. The first two modules are included in monitor and review. Module 22 and 23 is for communication and information.

Module 20 – Monitor. This module deals with what should be monitored. Organization should check the effectiveness of its activity, and any external factors varying over time

that might change or invalidate the previous assumptions. Organizations will have to define how the review is going to be done.

Module 21 – Review. This module concerns the definition of the review modalities like module performance indicators. This module will also observe and assess any substantial change concerning the monitored entities whose impacts should be considered.

Module 22 – Communication. In this module, organization should define the methodologies for diffusion and exchange of information elements, and interaction between individuals. Different tools can be used to different modules such as emails, document sharing, meetings, and trainings.

Module 23 – Information. The research suggests organizations to use the hardware and software of information technology structure to serve as exploitation leverage. Information can be articulated around three basic items that are gathering, storage framing, and visualization and exploration.

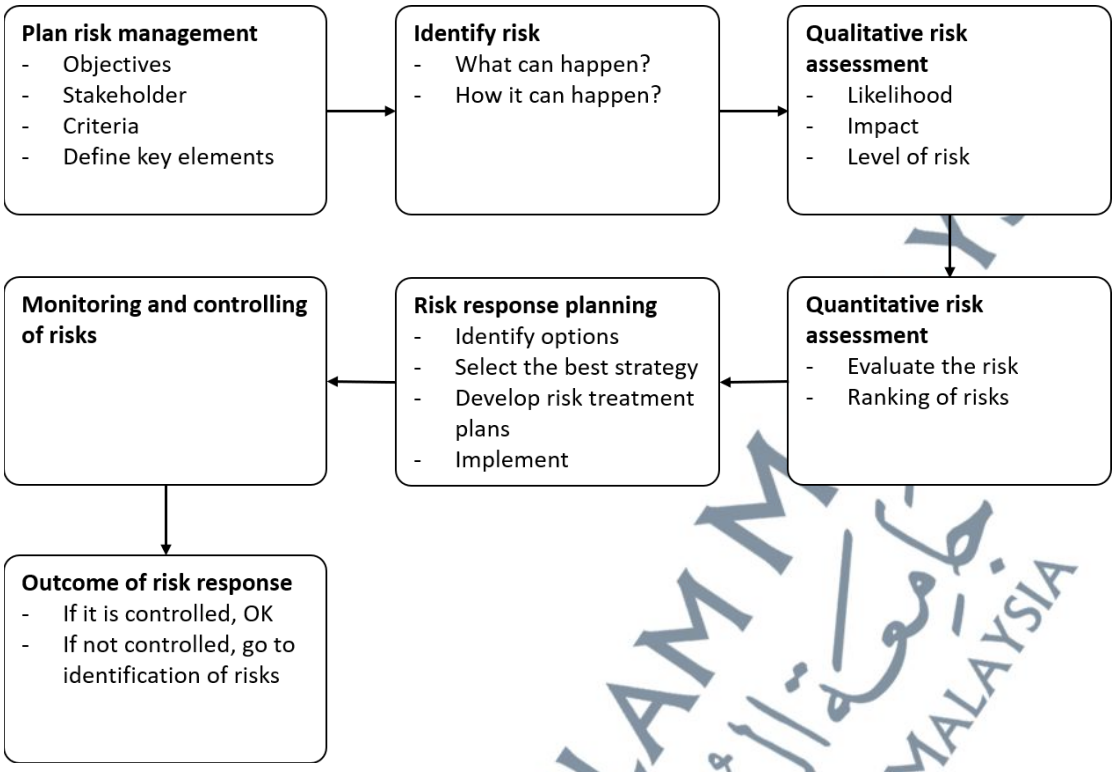
Module 24 – Culture diffusion. The final module aims to diffuse risk culture in the organization. The individual contribution to ERM can be enhanced by the reduction of change resistance, spreading of risk awareness, and motivation through culture diffusion mechanisms like ERM explanation trainings and workshops.

Project risk management process developed by Srinivas (2019).

A small, unexpected delay in a project is caused by internal and external environments and risk factors that may occurs concurrently. However, the impact of the delay is so huge, that it may cause cost overrun, schedule overrun, the industry where the project is in, and even a country's economy. Therefore, Srinivas (2019) develop a risk management process for construction process. The risk management steps are presented in Figure 2.11.

Step 1 – Identification of risks. The objective of identifying risk is to obtain a list of risks that may impact on the progress of a project. The process to identify risk can be informal. Risk identification can be performed in various ways depends on the organization and the project team. The process typically relies heavily on existing studies and experience. Therefore, organizations may combine different tools and techniques to identify risks in any project.

Srinivas (2019) suggests identifying and allocating the sources of risks too for a more effective risk management. Among the tools that can be utilized to identify risk are by reviewing documents, and gathering information through methods like brainstorming, Delphi techniques, and cause and effect diagram. The organization needs to keep in mind that there are variety of risks faced by them coming from different sectors like financial, legal, environmental, logistics, and quality operational labour.



Source: Srinivas (2019)

Figure 2.11: Risk management process developed for construction projects by Srinivas (2019).

Step 2 – Risk assessment. At this stage, the collected data is analysed for potential risk. Srinivas (2019)defines risk assessment as short listing of risks identified from previous stage and ranking the risks starting from low impact to the highest impact on the project. There are two types of risk assessment that are qualitative risk assessment and quantitative risk assessment.

Qualitative risk assessment involves registration of identified risks. Srinivas (2019) proposes to use a risk register. The risk register may include a few items to formalize the risk assessment process. There are several items that can be included in the risk register. The items are as following:

(i) Classification and reference. Classification aims to assist with identification of risk source. Referencing is defined as to give a reference number for each risk.

(ii) Description of the risk. The description of the risk must be detailed to avoid redundancy when explaining the risk in brief.

(iii) Relationship to other risks. Relationship between risks must be noted since it is rare for any project activities to be independent. Noting the relationship between risks will also help for successful implementation of risk management.

(iv) Potential impact. The research suggests measuring impact of risks on projects in terms on cost and quality. At this stage, risks are classified according to their impacts. Therefore, high impact risks can be given more attention compared to lower impact risks.

(v) Likelihood of occurrence and calculation of risk factor. The research suggests giving a suitable scale of 1 to 10 to the probability (P) and impact (I) of risks, with 1 refers to low probability or impact and 10 refers to highest probability or impact. The values of probability score and impact score is then divided by 10 to change to the scale of 0 to 1. Then, the risk factor (RF) is calculated using the formula $RF = P + I - (P * I)$.

(vi) Risk response/mitigation strategy. The aim of this stage is to reduce, eradicate, or avoid the identified risks. The research suggests allocating the identified risks to respective stakeholders who should be responsible to address the risks. The allocation is based the competency of these stakeholders in managing risks.

Srinivas (2019) uses quantitative risk assessment for risks that are classified as high, critical, or unmanageable. The aim is to find the estimated amount of contingency that is needed for the risks. Therefore, if risk event occurs, the organization will have enough fund to cover the extra expenditure. Quantitative risk assessment requires more in-depth analysis to estimate the impact of risk in a project in terms of scope, time, cost, and quality. Deep analysis suits better for medium to large complex projects, compared to smaller projects.

To estimate the contingencies, Srinivas (2019) suggests two elements that are (i) base estimates for items that are known, and the degree of certainty exists, and (ii) contingency allowance for all other uncertain elements of a project. The outputs from quantitative risk assessment are probabilistic analysis of a project, prioritised list of quantified risk, and trends in quantitative risk analysis results. There are four methods for quantitative risk assessment suggested by the research. The methods are explained in detail in the following.

(i) Scenario technique: Monte Carlo simulation. Monte Carlo method is a statistical method where data is randomly generated within predetermined parameters and produce realistic project outcomes. Organizations or project manager can use historical data from previous projects. The project outcome is forecasted by randomly simulating a combination of values for each risk and repeating the calculation for a few times. The outcomes of these calculations and recorded. The average of the outcomes constitutes the forecast of the risk. However, it is important to identify the accurate parameters to ensure an accurate and realistic project outcome. The data variables are usually represented in pessimistic way or in negative terms, or the other way round, depending on the risks encountered. The result from

this method is usually presented in percentage. The research also suggests using Risk Simulator Palisade Software to perform Monte Carlo simulation.

(ii) Modelling technique: sensitivity analysis. Project managers can use this method to demonstrate the variable impact on the whole project caused by a small change in one or more element or risk. The more uncertain a specific risk is, the more sensitive it is concerning the objectives of the project. The research suggests to us a spider diagram to identify areas in the project that are most sensitive and critical.

(iii) Decision tree. Project managers are suggested to use decision tree when a particular risk has an exceptionally high impact on the two main objectives of the project. Decision tree method is typically used when there is a series of interrelated possible course of actions, and the future outcomes are in terms of time and cost. Project managers can estimate probabilities and values of potential outcomes. These values are later used for quantification to provide a more informed basis in making decision.

(iv) Multiple estimating using risk analysis (MERA). MERA aims to provide a range of estimates. The estimates are presented as risk-free base estimate, average risk estimate (ARE), and maximum likely risk estimate (MLRE). ARE is the total of risk-free base estimate and average risk allowance. Meanwhile, MLRE is the sum of ARE and maximum risk allowance. MLRE is to find a level or probability value of a project to be successful. ARE values can be found by multiplying average allowance by average probability of occurrence. Maximum risk allowance is the product of maximum allowance by maximum probability of occurrence of particular risk.

Step 3 – Risk response planning. Risk response is defined as a form of mitigation by adopting necessary strategies in respect of positive and negative risks. There are four types of risk mitigation strategy suggested by Srinivas (2019). The strategies to mitigate negative risks are risk avoidance, risk transfer, risk reduction, and risk acceptance. The description of the strategies are as follows.

(i) Risk avoidance. This strategy eliminates the threat entirely. It could involve changing the project management plan. Project manager may isolate the project objectives that are in jeopardy.

(ii) Risk transfer. This strategy needs a shifting of some or all negative impact of risks, together with the ownership of the response to a third party. Risks can be transferred to a consultant or insurance company.

(iii) Risk reduction. risk reduction is defined as the reduction of probability and consequence of a particular risk to be within the acceptable threshold limits. The research suggests risk reduction if risk mitigation leads to increase in costs that is less than the potential loss.

(iv) Risk acceptance. Srinivas (2019) proposes risk acceptance when it is impossible to eliminate all risks from a project. There is no action needed to mitigate risks. The project team only need to document the strategy of how to deal with risks if risk events occur.

Srinivas (2019) also suggests risk mitigation strategies for positive risks or opportunities. There are six strategies suggested that are exploitation, share, enhancement, acceptance, contingent response strategies, and expert judgement. The details for each strategy are as follows.

(i) Exploit. Exploitation on positive risks can be implemented if the organization wants to ensure the opportunity is realised. This strategy eliminates any uncertainty relating to particular risk and ensure the opportunity is exploited.

(ii) Share. This strategy involves allocating some or all ownership of the positive risk to a third party. The third party must also be capable to capture the opportunity from the risk. For example, join ventures.

(iii) Enhance. Project managers can use this strategy to increase the positive impact from the positive risks. They can identify and maximise the key driers of the risks to increase the probability of risk event to occur.

(iv) Accept. Organization or project manager accepts a risk by willing to take advantage if the risk come. However, the risks are not chased actively for their advantages.

(v) Contingent response strategies. Contingent response is responses that are planned earlier but only be implemented if risk event occurs. The plans are only executed if there is a sufficient warning for implementation but under certain predefined conditions.

(vi) Expert judgement. Any opinions from knowledgeable individuals pertaining to the actions to be taken on a particular risk.

Step 4 – Monitoring and controlling risk. There are a few parameters that are needed for risk monitoring and control.

- Risk register. The risk register must contain risks identified, risk owners, agreed risk responses, specific mitigation actions. Project manager must also know

signs of any risks, residual risks after risk treatment is implemented, list of low priority risk, and contingency measures in terms of time and cost.

- Main risk management plan. Risk management plan includes risk tolerances, assignment of manpower, bearers of risks, time, and other resources for the project risk management.
- Work performance information. Performance information results must be quantified in term of deliverable status, schedule progress and incurred costs. Finally, the performance reports. Performance reposts are needed for variance analysis, earned value data, and forecasting the likely date for the project to complete.

Srinivas (2019) proposes six tools and techniques for risk monitoring and control. The tools and techniques are risk reassessment, risk audits, earned value analysis, technical performance measurement, reserve analysis, and status meetings. The details of each tool and technique are as follows.

(i) Risk reassessment. Risk monitoring and control includes identification of new risks, reassessment of existing risks, and closing risks that are not threating the project. Therefore, project risk assessment is to be performed regularly. Progresses of the projects relative to objective will determine the frequency and depth of assessment needed.

(ii) Risk audits. Risk audits aim to examine and document the effectiveness of risk responses in dealing with identified risks, their respective causes, and the effectiveness of the risk management process. Risk audits meetings can be help separately or included in project review meetings.

(iii) Earned value analysis. Earned value analysis or variance analysis is done by comparing expected values with actual values. Performance information and values obtained from earned value analysis, deviation from cost and schedule are used to review trends in execution. The values may also indicate potential impact of threat or opportunities.

(iv) Technical performance measurement. This technique measures the technical accomplishments during project execution. The method is expected to help forecasting the degree of success of the project and expose the degree of technical risk faced.

(v) Reserve analysis. Reserve analysis aims to examine whether the available contingencies is sufficient. The amount of contingencies fund is then compared to the risk remaining in the project.

(vi) Status meetings. Project risk management should be included in all status meetings of a project. This is because the time allocated for any item in the project depends on the identified risks, their priority and complexity to respond. Frequent discussions will make stakeholders to be more concern to identify risks and opportunities.

Risk management process for social media risk developed by (Demek et al., 2018).

The use of social media in workplace is quite common. However, there is limited knowledge on how social media risk is managed in an organization. Therefore, Demek et al. (2018) develop a social media risk management model to examine whether the manner in which organizations address social media risk is consistent with a formalized risk management process. The Social Media Risk Management Model (SM-RMM) proposed by Demek et al. (2018) consists of four components and six steps which are

mapped to enterprise risk management integrated framework (ERM-IF). The proposed SM-RMM is presented in Figure 2.12.

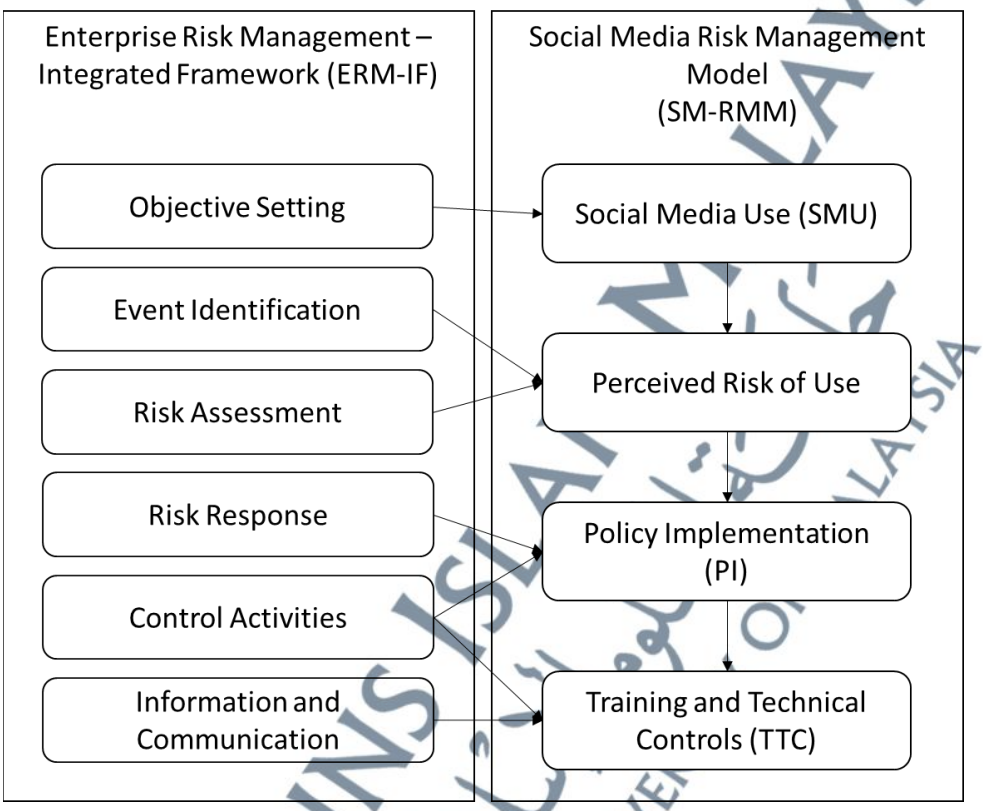


Figure 2.12: Incorporation of ERM-IF into SM-RMM.

Component 1 – Social media use (SMU). Before conducting a formal risk assessment, organizations must understand the objective of using social media within their organization. Organizations use social media to achieve certain goals. Therefore, SMU is mapped to *objective setting* in ERM-IF.

Component 2 – Perceived risk of use. *Event identification* component in ERM-IF is defined as the act of identifying internal and external events that affect the achievement of organization's objectives. The events can be risks or opportunities. After risks are identified, organizations must do *risk assessment*. Risk assessment involves analysis of

likelihood and magnitude of each identified risk. The outcome from the analysis provides basis on how organizations should manage the risks. These two components, event identification and risk assessment, are mapped to perceived risk of use in SM-RMM because they are directly related to identifying the perceived risk of social media use in an organization.

Component 3 – Policy implementation (PI). There are two components from ERM-IF that are directly mapped to policy implementation that are *risk response* and *control activities*. These two components are related to how an organization manages risks. In risk response component, management team of the organization develops a set of actions to be taken to reduce risk. The actions must be within the organization's risk tolerance. The control activities component is defined as the policies and procedures established and implemented by the organization to ensure appropriate risk responses are implemented appropriately.

Component 4 – Training and technical controls (TTC). At this stage, the *control activities* that need to be done by organizations are to implement control. Organizations also need to conduct training for employees to ensure employees know and follow the established policies and procedures of risk management. The component *information and communication* are also mapped to TTC. Information to employees is conveyed through communications in trainings.

Risk management for SMEs in India by Panigrahi (2012).

Panigrahi (2012) investigates risk management practices of small and medium enterprises in India. The research finds the attitudes of business owner managers and

their knowledge towards risks hugely affect how risks are systematically handled. Owner managers must have the capability to expect and prepare for change and react to it, rather than just wait, and do nothing. Therefore, it is important for owner manager to have knowledge and understanding on risks and risk management. Panigrahi (2012) develop a simple risk management process as presented in Figure 2.13.

Risk management begins with identifying the events that could cause loss or disruption to the business. Then, the events are analysed. The analysis aims to find the likelihood of the event occurring, and how serious the consequences are if the event occurs. Owner manager can start simply by assessing each risk using terms like 'very likely', 'moderately likely', or 'very unlikely'. Then, put a dollar value on the risk to prioritize them. For example, how much is needed to replace a machine. After getting a priority risk list, owner manager can attend to risks that have highest likelihood score and the most expensive events first. For each risk, owner manager can develop procedures of treatments for the risks suitable with the risk tolerance the business is willing to accept. After that, the procedure of treatments must be monitored to ensure it is in place and effective to mitigate the risk.

Figure 2.13: Risk management process developed by Panigrahi (2012).

Risk management process for SMEs by Verbano & Venturini (2013).

SMEs have a fundamental role in society from an economic and social point of view. However, the lack of resources and structural features causing SMEs to be vulnerable towards risk. Verbano & Venturini (2013).is motivated by the needs to promote the development of SMEs. The research suggests risk management process following a stage-gate process. Stage-gate system is both a conceptual and an operational model for moving a new product from idea to launch (Cooper, 1990). The risk management process is as presented in Figure 2.14.

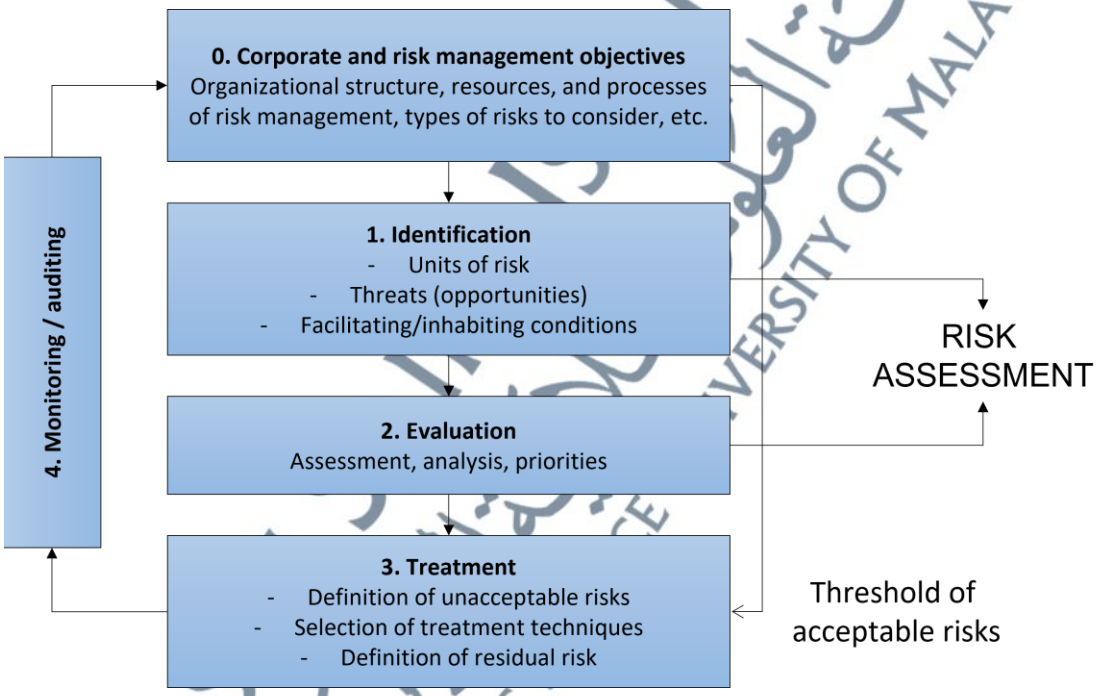


Figure 2.14: Risk management process for SMEs developed by Verbano & Venturini (2013).

Before the first step, a preparatory stage is needed to define risk management plan so it will be consistent with strategic business objectives and when conducting context analysis. The first step is to identify all risks the organization is exposed to. The second step is to assess and analyse risk. The purpose of the second step is to determine

the probability and the expected magnitude related to the occurrence of the damage. Organizations must also set a threshold of acceptability before going to the next step. These first two steps are always known as risk assessment. The threshold depends on the risk appetite of the top management and available resources.

Step three is treatment of unacceptable risks. Treatment of risks is to take actions to reduce risk. The final step is supervision. The implementation of risk management is a long-term, dynamic, and interactive process. It requires continual improvement and integration in the organization's strategic planning.

Risk management model for small business by Ekwere (2016).

Assisting a small business is not only in the form of financial aids. They also need help in terms of management strategies. Ekwere (2016) explore and analyse risk management techniques that are applied on small businesses. There are seven steps recommended by Ekwere (2016) for risk management in small businesses. The steps are as presented in Figure 2.15.

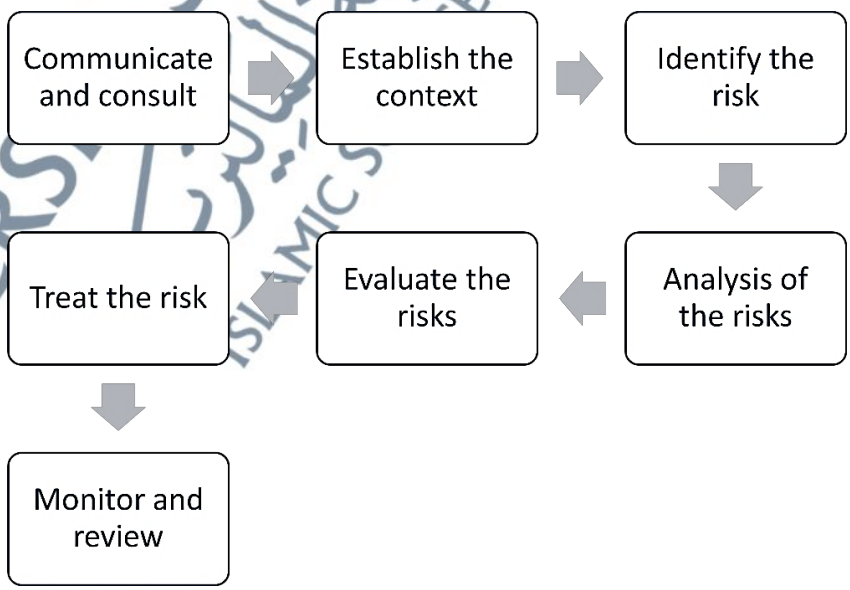


Figure 2.15: Risk management process for SMEs developed by Ekwere (2016).

Step 1 – Communicate and consult. The first step aims to identify who should be involves in risk assessment, risk treatment, risk monitoring, and risk review. Communication and consult also aims to draw out risk information. This step may occur within the organization, or between the organization and its stakeholders. It is important to identify the range of stakeholders who will assist in completing risk information.

Communication and consultation are important to manage stakeholders' perception in managing risk. Stakeholders may have a significant role in decision-making process. Therefore, their perceptions towards risks and benefits should be identified, understood, recorded, and addressed. A communication plan or strategy can be developed for an effective communication. An effective communication leads to identification of internal and external stakeholders and their roles and responsibilities. Ekwere (2016) defines consultation as a two-way process that normally involves talking to a range of relevant groups and exchanging information and views.

Step 2 – Establish the context. Establishment of boundaries to within which risk management will apply in a business is important in small business. Ekwere (2016) refers to Global Risk Alliance (2005) to assist in establishment of context on which risk will be identified.

(i) Establish the internal context. The internal context can be the objectives and goals of the business. It is to ensure all significant risks are understood and the risk decisions to support the broader goals and objectives of the business in the long term. The business can consider the internal culture of the business and capabilities of the business in terms of people, system process, equipment, and other resources, to establish the internal context.

(ii) Establish the external context. Ekwere (2016) defines external context as the overall environment where the business operates. The environment can include the understanding of the clients' or customers' perceptions towards the business. Analysis on these perceptions will help the identification of business strengths, weaknesses, opportunities, and threats in the external environment. Business owners may also consider any regulations that need to be complied with, the type of market the business is in, competitors of the business, and any social or political or cultural issues.

(iii) Establish the risk management context. Organizations must define the limits, objectives, and the scope of activity or issue under examination. Establishment of the parameters and boundaries of the activity or issues can be done by determining the timeframe, required resources, roles and responsibilities, required additional expertise, internal and external relationships, record-keeping requirements, and the required depth analysis. Organizations should also consider the complexity of the activity or issue, the potential consequences, the importance to capturing learned to develop corporate knowledge over associated risk, the importance of the activity and objective achievements, information needed for communication with stakeholders, and types of risks and hazards associated with the activity.

(iv) Develop risk criteria. Risk criteria may include the acceptable level of risk for a specific activity which allows business to clearly define the unacceptable levels of risks. At this stage, risk criteria can be broadly defined and then refined in the next stages.

(v) Define the structure for risk analysis. Structure of risk analysis is equivalent to the categories of risk. Risks can be categorized based on the type of activity or issue, its complexity, and the context of the risks.

Step 3 – Identify the risk. The information from the previous steps can be utilized at this stage to identify as many risks as possible. Risk identification is limited to the experience and knowledge of the person conducting risk analysis. Therefore, organizations can use other reliable sources to help identify risks.

Organization can identify risks in two ways namely retrospectively and prospectively. Retrospective risks are risks that have occurred previously. It is easier to quantify the impact of retrospective risks since the impact has already seen. Sources of retrospective risks includes incident logs, and customer complaints. Prospective risks are risks that have not yet occurred but could occur sometime in the future. The identification process should include all risks, whether it has happened, currently happening, or not yet happen. The rationale of identifying prospective risks is to identify significant risks and monitor the effectiveness of their control. Prospective risks can be identified through methods such as brainstorming and researching the operating environment.

Step 4 – Analysis of the risks. Risk analysis helps organization to determine which risk has greater impact. It is a combination of the possible impact of the risk with the likelihood of it happening. The risk analysis equation to obtain a risk level is "Risk = consequence × likelihood". The result from risk analysis provides a better understanding on the possible impact of a risk or the likelihood of the risk occurring. Risk level also help clarify the resources needed to control the risk.

Risk level can be represented in risk matrix. There are a few elements of risk analysis. The elements are (i) identifying existing strategies and controls that minimize risk and enhance opportunities, (ii) determine the consequence of a positive and negative impact, (iii) determine the likelihood of the positive and negative consequence, (iv) estimate the level of risk by combining consequence and likelihood scores, (v) consider and identify any uncertainties in the estimates, and (vi) analysis techniques.

Risk analysis aims to provide information to business owners for to decide on priorities, treatment options, or balancing costs and benefits. Different tools can be adapted to analyse the risks, depending on the suitability of the risk and business owner. There are three categories of risk analysis namely qualitative, semi-quantitative, and quantitative. The choice of analysis relies heavily on the type or area of the risk. Organization normally use qualitative method since it is simple and easy to use. However, qualitative analysis include intuition and subjective which may lead to bias hence degrading the quality and validity of the result. Qualitative risk analysis can be done by brainstorming and evaluation using multi-disciplinary groups.

Step 5 – Evaluate the risks. Evaluating risks is determining how serious the risks that the business is facing. At this stage, business owner must determine how much risk the business can take. It is a process of comparing risk level from the previous step with previously established risk criteria. Organizations will also have to decide whether the risks require treatment or not. The output from this step is a prioritized list of risk that requires further action. Tolerable risks may be accepted. Accepting risks can be of two reasons which are known as ALARP or 'as low as reasonably practicable'. The first reason is because the risk level is low and the cost to treat the risk will outweigh its benefit. The second reason is there is no reasonable treatment that can be implemented.

Step 6 – Treat the risk. Risk treatment is done for risks that considered as acceptable in the previous step. Risk treatment is an action taken to treat or control risk by reducing or eliminating negative consequences, or to reduce the likelihood of the risk event to occur. Risk treatment also aims to increase positive outcomes. Implementing all risk treatment strategies is not cost effective. Therefore, business owner should choose, prioritize, and implement the most appropriate combination of treatments. Before a risk can be effectively treated, an organization must understand the root cause of the risk. Ekwere (2016) proposes to develop a risk treatment strategy following Global Risk Alliance (2005). There are four risk treatment options suggested that are risk avoidance, changing the consequences, risk sharing, and risk retaining.

(i) Risk avoidance – organizations can avoid risk when there are no controlling measures available, or when the risk cannot be reduced to an acceptable risk level.

(ii) Changing the consequence – this treatment will increase gains and reduce losses of an organization.

(iii) Risk sharing – sharing responsibilities on a risk by transferring the risk to another party.

(iv) Risk retaining – organization may retain or keep certain risks if the risks seem to be on no important harm and are at acceptable level. This treatment option requires organization to choose the appropriate treatment, conduct a cost-benefit analysis, and execute a risk treatment plan and recovery.

After choosing the suitable treatment option, organization must identify whether the risk has been eliminated or not by identifying the residual risk. Residual risk needs

to be evaluated to know whether it is acceptable or not, before implementing treatment options. In addition, organizations must know if the cost of any risk treatment method is justified. They need to consider the number of treatments required, benefit of the treatment, other available treatment options, the reasons of recommending the chosen option, effectiveness of the chosen treatment, total cost of treatment option, how much reduction in residual risk, legislative requirements, and the time frame.

Organization also needs to have a risk treatment plan. A risk treatment plan contains information about the risk identified, level of the risk, the planned strategy, timeframe to implement the strategy, required resources, and the individuals responsible to ensure the strategy is implemented. The risk treatment plan should also include a budget, appropriate objectives, and milestones on the way to achieving the objectives. The last phase is risk recovery. It is possible to predict uncertainty-based risks. Therefore, organizations can always prepare for a significant adverse outcome. Planning a risk recovery can be in different forms such as a crisis or emergency management planning, business continuity planning, and contingency planning.

Step 7 – Monitor and review. Organizations must monitor the risks and review the effectiveness of the treatment plan, strategies, and management system set up to manage risks effectively. It is an essential and integral step in the risk management process. The aim of this step is to ensure the risk priorities do not change even there are changing circumstances in the organization. Normally, very little number of risks will remain unchanged. Therefore, risk management process needs to be regularly repeated to capture new risks and manage them effectively. Ekwere (2016) suggests this step to be included in annual business planning.

Risk management process for SMEs by Falkner & Hiebl (2015).

Falkner & Hiebl (2015) conducted a systematic literature review on risk management in SMEs. The study aims to find vagueness, gaps, and contradictions in available literature. Falkner & Hiebl (2015) identified variety of risks faced by SMEs and demonstrates the importance of risk management processes. Falkner & Hiebl (2015) follows the five-steps risk management process from Hollman & Mohammad-Zadeh (1984). The steps are risk identification, risk analysis, selection of techniques, strategy implementation, and control, as presented in Figure 2.16.

Figure 2.16: Risk management process by Falkner & Hiebl (2015).

Step 1 – Risk identification. The first step in risk management is to identify possible source of loss and risks. This step should be carried out continuously and systematically. There are three methods that can be used to identify risks of loss that are (i) systematic reviews of all data on business asset, activities, and staff; (ii) using financial statements to identify the sources of potential financial losses; and (iii) using flow charts to analyse

all operations or activities of the enterprise. A pre-condition of effective and comprehensive risk identification might be needed. The pre-condition aims to build risk management capacity among employees. Falkner & Hiebl (2015) advice organizations to identify all potential risks.

Step 2 – Risk analysis. Risk analysis involves measuring or estimating the potential frequency of losses and the potential impact of a risk on the company's operation. At this stage, risks can be ranked according to its priority to the company. This stage helps in establishing risk management priorities and providing a starting point for selecting appropriate risk management techniques for each risk. Some employees in a company might be less knowledgeable. Hence, the use of simplified process to analyse risks using variables like "highly likely", "unlikely", "likely" or "highly likely" for the probability of risks, and "negligible", "significant", "major", "catastrophic" for risk impact, might help with the issue.

Step 3 – Selection of techniques. Risks are meant to be managed differently. Falkner & Hiebl (2015) reviews tools and methods from earlier studies that SMEs can use to handle risks. The tools and methods are:

(i) Insurance. Falkner & Hiebl (2015) finds that SMEs owners have knowledge on insurance. SMEs owners know insurance can sometimes be associated with considerable cost and mostly covers unexpected events. SMEs in the United Kingdom typically insure their business against fire, flooding, property damage, and personal injury. Apart from that, insurance also help SMEs in downside risk analysis, legal compliance, and management services, even if the SMEs do not suffer any loss. Therefore, arranging

insurance is advantageous for SMEs because they must examine business risks.

(ii) Weather derivatives. Extreme weather in the United States causing SMEs to hedge their exposure to natural disaster like floods and tornados through weather derivatives. Weather derivatives allows business owners to transfer weather risk to a third party.

(iii) Selection of suppliers. SME owners can mitigate risks by entering a contract with individual suppliers to influence supplier behaviour. Falkner & Hiebl (2015) suggests including a kind of performance guarantee to ensure consistent quality in the contract. Focusing on procurement in local markets is advantageous for western companies because some risks can be avoided like political unrest, customer and currency problems, and risks associated with culture differences. However, the study argues mitigating risks by selection of suppliers requires caution.

Falkner & Hiebl (2015) focuses on previous studies by Ellegaard (2008) and Poba-Nzaou & Raymond (2011) for a deeper search on selection of suppliers. Falkner & Hiebl (2015) concludes there are other factors that must be included because the previous studies rely on relatively small sample sizes. The factors are whether managers from other regions and different contexts can rely only on selection of suppliers to mitigate risks. This is because despite the lower price offered by local suppliers, SMEs managers can try other methods in selecting suppliers like combining market suppliers with global sourcing.

(iv) Overcapacity in production. Having extra capacity in production and warehouse can prevents interruption in production or delivery issues

especially in automotive manufacturing as reported by Thun et al. (2011).. However, SMEs have limited reserves, hence the limited private financial resources and a small stock.

(v) Emergency plan. Companies must establish a continuity or contingency plan. The plans can include several items like how staffs can evacuate the building and the temporary relocation in case of risk event happen. It is reported that SMEs are more likely to lack contingency plans compared to larger companies.

(vi) Networking/cooperative relations. Personal networks and close relationships between SMEs managers and key suppliers can be regard as a successful technique to manage risks like technology, financial, and market risks. Same goes to clients, SMEs managers maintain good relationship with them with the hope to gain more repeat business. Apart from that, networks can be beneficial to attract new customers. Networking with competitors helps in preventing risky transactions because sharing information with competitors results in more information about the creditworthiness of potential customers (Gilmore et al., 2004). It is also crucial for SMEs managers to build on internal networking. Managers need to entrust the senior staffs with responsibility. Entrusting staffs with responsibilities will also requires managers to do internal networking by learning the staffs' personal qualities, skills, and ambitions.

(vii) Asset securitization. Asset securitization can be advantageous to SMEs as it allows them to transfer different types of risks to investors in the capital market at a fair price. Given that SMEs are small, and it is difficult for them to have access to capital, asset securitization allows them to explore

alternatives for external financing. However, the advantageous are only conceptual considerations where a deeper testing and analysing of the asset securitization on SMEs are needed.

Step 4 – Strategy implementation. The fourth step in risk management process is to implement the chosen methods. Falkner & Hiebl (2015) suggests informing all affected employees of the company's risk management objective.

Step 5 – Control. The final step is to consistently review the techniques and measures taken to ensure the SMEs meet the current requirements. SMEs are advised to define a performance benchmark to monitor the risk management process effectively and continuously.

2.6 Summary

From the previous studies, the least number of steps in risk management is four which includes risk identification, risk analysis and evaluation, risk response, and risk monitoring and control. However, there are only two common steps of risk management process in all studies. The common steps are risk identification and risk response.

Risk identification is to identify all risks faced by the organization. The risks identified can be limited to the experience and knowledge of the person who identify the risks. Therefore, organizations can use any other reliable sources to help identify risks. If possible, organizations are to identify the maximum number of possible risks in the organization to avoid any risks left out or unattended.

The second common step in all studies in risk response or mitigation planning or risk treatment or strategy implementation. All risk identified must be treated.

Previous studies have suggested variety of techniques and methods, from exploiting the risk for an opportunity, to avoiding the risk by taking away the root cause of the risk.