Table of contents

Research Methodology 3

Introduction:

Literature Review

What is Enterprise Risk Management? 5

Enterprise Risk Management Framework: Objectives and components.....11

Enterprise Risk Management Implementation Plan Keys – Initiation Process 15

Enterprise Risk Management Policy Implementation 22

Scope and Purposes 22

In what and where should Enterprise Risk Management be implemented? 24

Updates on Enterprise risk management practices 24

ERM Integration into risk registers process 25

Responsibilities & Accountabilities 26

Risk Categories 27

Likelihood and Impact Scale 28

Risk Register 29

Risk Assessment 29

Evaluate Risks 33

Risk Response / Treatment 36

Risk Transfer and Risk Response Transfer 41

Risks Mitigations 42

Control Activities 43

Communication & Information 44

Monitoring & Reviewing 45

Terms of ERM implementation process 47

Limitations of Enterprise Risk Management Policy 49

Survey Results **50**
Conclusion **54**
Appendix **56**
Bibliography **70**

Research Methodology

The research was conducted in a form of survey which was developed to describe the status of enterprise risk management in SME's manufacturing organizations in the United Arab Emirates and evaluate the existing resources in those organizations to measure the ability of start implementing a risk management system to be able to identify, quantify and mitigate various kinds of risks that may affect achieving the strategic objectives of the organization and shareholder's value as well.

The survey was directed mostly to the managers amongst well-established private manufacturing firms of the sample taken which hold the positions of Deputy Managing Directors, Chief Finance Officers, Internal Audit Managers, Finance Managers and Chief Accounting staff which present the opinion from senior officers' point of view**.**

The survey was established and designed by using the questionnaire forms on SurveyMonkey website (www.surveymonkey.com) and the total number of responses collected is 122; where 115 responses were complete answers and the rest were incomplete and excluded when research has been analyzed. In addition, some interviews have been conducted after collecting the responses to strengthen the feedback on the survey questions.

The questionnaire prepared contains of ten multiple choice questions and other six rating questions. The first three questions were about introducing the respondent and his organization investment structure, and seven questions prepared to describe the status of risk management in the organization and its implementation process considering the challenges and inhibitors to implement ERM, besides the benefits expected when having a functional risk management system in place.

The rating questions prepared to get the feedback on the knowledge of the organization's staff in risk management area and the main functions of any existing established firm and respondents' perception of the training needs to ensure the employees ability to accomplish their duties in a risk management system environment.

Literature Review

What is Enterprise Risk Management?

It is difficult to determine a unique meaning of enterprise risk management as it's a broad-wide concept which may vary between organizations that are looking to build a risk management system to be able to control and monitor their exposure to different kinds of risks. However, enterprise risk management has been defined by many firms, institutions and authors in order to set a general concept that could describe clearly the process of identifying, quantifying and mitigating risks of the organization to achieve its strategic goals.

The Committee of Sponsoring Organization of the Treadway Commission (COSO) has defined Enterprise Risk Management as *"A process effected by an entity's board of directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."*

The above definition of ERM provided some fundamental concepts and has a broad purpose of many directions to capture some fundamental concepts on how organizations manage their own risks and focus to enhance the ability to achieve organization's objectives. It was discussed on COSO ERM framework and summarized as follows:

- *"A process, ongoing and flowing through an entity.*
- *Effected by people at every level of an organization.*
- *Applied in strategy-setting.*
- *Applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk.*
- *Designed to identify potential events affecting the entity and manage risk within its risk appetite.*

- *Able to provide reasonable assurance to an entity's management and board.*
- *Geared to the achievement of objectives in one or more separate but overlapping categories".*

Moreover, individual authors interpreted the definition of enterprise risk management like Wang and Faber (2006) view in addition to that of Brodeur and Pritsch (2008), defined the Enterprise Risk Management as:

"An offensive discipline of studying the risk dynamics of the enterprise, the interaction of internal/external players and forces, and how players' actions influence the behaviors of the risk dynamics, with the ultimate goal of improving the performance and resiliency of the system, thus maximize the enterprise value".

Lam (2000) defined Enterprise Risk Management as *"An integrated framework for managing credit risk, market risk, operational risk, economic capital, and risk transfer in order to maximize firm value."*

Makomaski (2008) highlighted that Enterprise Risk Management is *"A decision-making discipline that addresses variation in company goals."*

Alviunessen and Jankensgard (2009) marked out that *"Enterprise Risk Management is concerned about a holistic, company-wide approach in managing risks, and centralized the information according to the risk exposures."* They use the term ―Risk Universe, which is the risk that might affect the future cash flow, profitability and continued operations of a company. In other words, risk universe is the risks that could affect the entity of the company. If risk universe can be identified, the next step is to take an appropriate action such as risk mapping process, accessing the likelihood and impact and curb the risk based on the organizations' objectives.

Other financial institutions have also tried to identify Enterprise Risk Management and put some actions in place to highlight the major concepts of ERM and its implementation

plan like (Andre` Brodeur, Kevin Buehler, Michael Patsalos-Fox and Martin Pergler) in their paper of (A broad Perspective on Enterprise Risk Management – McKinsey 2010) for five dimensions for the best practice of ERM implementation:

- *"Risk Transparency and Insight:*
  (Prioritized risk heat map / Insight into the big bets that really matters / Cascading reports tailored to different management levels).
- *Risk Appetite and Strategy:*
  (Clear definition of risk appetite, with matching operational levers / Strategy informed by risk insights).
- *Risk-related business process and decisions:*
  (Managerial decisions optimized by embedding risk in processes / Strong links between ERM function and k Bus and other functions).
- *Risk organization and governance:*
  (Organizational model tailored to business requirements / Adequate resource levels to manage risks).
- *Risk Culture:*
  (Clear understanding of firm's risk culture gaps / Alignment of culture with the firm's risk strategy)."

Furthermore, Casualty Actuarial Society (2003) or CAS defined Enterprise Risk Management as:

"Disciplines by which an organization in any industry assesses, controls, exploits, finances, and monitors risks from all sources for the purposes of increasing the organization's short- and long-term value to its stakeholders."

In the past, firms used to transfer risks through insurance or other financial products which formed a mean of treating risks. However, CAS (2003) has discussed that there are a number of driving forces lead to practice enterprise risk management through the general evolution toward ERM:

- *More –and more complicated- Risks*

Due to the advance of technology, the accelerating pace of business, globalization and the increase of financial sophistication, organization started to recognize the importance of managing all risks and the interactions of them not only the clear types of risks or normal ones. Besides that, the business environment has been changed as Hazard Risks such as stoppage in the production line or losing an area of sales have been managed actively in the former ages of risk management.

- *External Pressure*

There is a lot of pressure on the organizations' senior management to implement and adopt Enterprise risk management and take greater responsibilities for managing risks on an enterprise-wide scale. This pressure may arise from regulators, rating agencies, institutional investors and corporate governance oversight bodies. In public firms, ERM drives the shareholders to believe more in having stable and predictable returns as it's one of the main objectives of enterprise risk management implementation for many firms.

- *Portfolio Point of View*

It is inefficient to manage risks in 'Silos' rather than being managed within the total organization which can be counter-productive for many divisions or subsidiaries to provide a collective risk framework to be implemented amongst the whole organization. Some principals should be thought of like; the portfolio risk is not the simple sum of silos risks as correlation will take place between the factors of those risks. Although, it is essential to understand each silo's risks to be able to understand and analyze all kinds of portfolio risk which is relevant to the key risk decisions facing the organization.

- *Quantification*

Tendency to quantify exposure to all kind of risks has been grown through years using different kinds of models by the advance of technology as expertise put in place more identification tools to quantify frequent risks and further to infrequent and unpredictable

risks that are historically been complicated to be quantified. In contrast, it is much more difficult to quantify the portfolio risks from only the results of quantifying individual's risks unless interactions between individual's risk elements take place.

- *Boundaryless Benchmarking*

Although there are general rules and concepts that are recognized and employed by the organizations throughout the world, different firms can develop their own variations of enterprise risk management model to be employed and embedded within the business structure of that certain firm. Some areas of implementing enterprise risk management in the organization are directly related to its business activity and may differ from organization to another such as licenses for drugs companies and approvals of new products and health authority's authentication of food and beverage companies. Moreover, the boundaries and limitations are different from one country to another even for the same organization or same products where different rules and regulations must be followed with respect to that country's law.

- *Risk as Opportunity*

In the past, Organizations were taking a defensive position towards risks by viewing them as situations to be mitigated or avoided. On the other hand, the organization can employ an aggressive way towards risks if the management knows that it can switch to defensive stance quickly when needed. In addition, opportunities can be pursued and found when the management believes that it has the ability to exploit some risks that are selected to increase the diversification of the organization for a better return. In fact, there is a realization that risks are not completely avoidable but in essence informed risk taking is a way to competitive advantage and sustain the growth of the organization.

In addition to the researches about the implementation of ERM and determine the key elements to identify and assess risks, a paper of KPMG issued in 2001 concluded that enterprise risk management can becomes a mean of helping the organization shifts its

focus away from crises response and compliance, and a strategic competitive advantage to set up specific actions to enhance the organization performance and optimize its risk which will result in improving the shareholders value. The paper outlined some questions to be considered by the board of directors to identify and assess different types of risks from an ERM point of view:

"Strategic Risk

- *Are the critical strategies appropriate to enable the organization to meet its business objectives?*
- *What are the risks inherent in those strategies, and how might the organization identify, quantify and manage these risks?*
- *How much risk is the organization willing to take?*

Operational Risk

- *What are the risks inherent in the processes that have been chosen to implement the strategies?*
- *How does the organization identify, quantify and manage these risks given its appetite for risk? How does it adapt its activities as strategies and processes change?*

Reputation Risk

- *What are the risks to reputation inherent in how the organization executes its strategies?*

Regulatory or Contractual Risk

- *What are the risks related to compliance with regulations or contractual agreements - not are those that are financially based?*

Financial Risk

- *Have operating processes put financial resources at undue risk?*
- *Has the organization incurred reasonable liabilities to support operating processes?*
- *Has the organization succeeded in meeting measurable business objectives?*

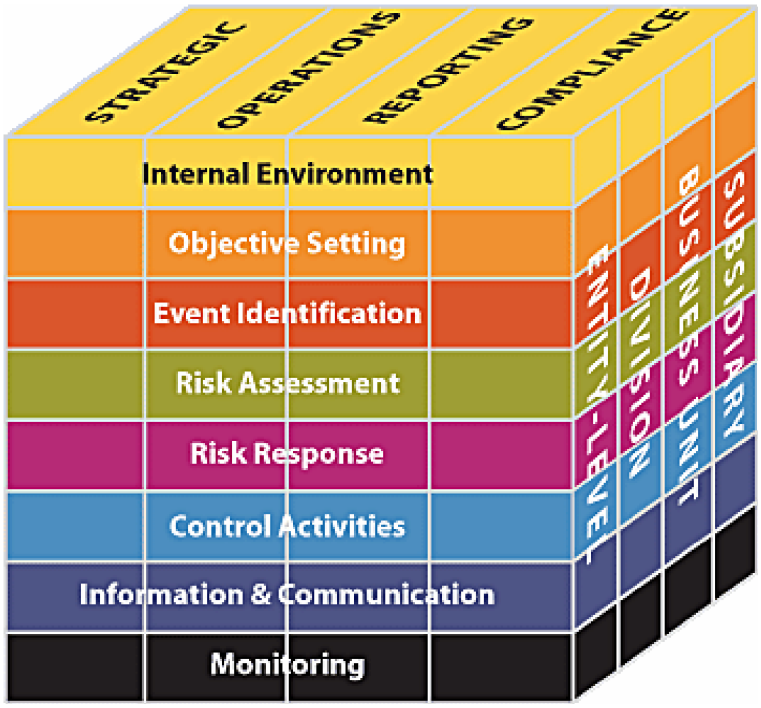
Information Risk

- *Is our data/information/knowledge reliable, relevant and timely?*
- *Are our information systems reliable?*

New Risks

- *What risks have yet to develop?*

Enterprise Risk Management Framework: Objectives and components



When an organization decides to implement Enterprise Risk Management, it should establish the strategic objectives which have been set in four categories by The Committee of Sponsoring Organizations of the Treadway Commission in its framework as follows:

1. *Strategic – high-level goals, aligned with and supporting its mission.*
2. *Operations – effective and efficient use of its resources.*
3. *Reporting – reliability of reporting.*
4. *Compliance – compliance with applicable laws and regulations.*

On the other side of the framework cube, there are eight interrelated components which are derived from the way management runs the organization and are integrated within the management process. As per COSO framework, these eight components are:

1. *Internal Environment* – The first component of the COSO ERM Framework is the internal environment which represents the management philosophy of risk and its appetite toward risk exposures, which reflects the shareholders and board of director's tone on the major decisions on the organization's structure, foundation, policies, integrity and ethical values that are determining the operation path of the organization.
2. *Objective Setting* – The organization's Objectives should be formed to support the mission of the organization and to ensure that the vision can be achieved through the chosen objectives taking into consideration the entity's risk appetite with implementing Enterprise Risk Management.
3. *Event Identification* – Assessment of internal and external events that may affect the achievement of the organization's strategic objectives. The events might be identified as positive ones such as opportunities or might be evaluated as risks (negative events) which can be transferred to a positive action if management decides that there is an opportunity behind this risk(s).
4. *Risk Assessment* – Analyzing risks through the likelihood and the impact of these risks and they must be treated by qualitative or quantitative methods since risks are likely to affect the organization's objectives over a period of time.
5. *Risk Response* – the way that management decides to react against any risks, whether accepting, avoiding, mitigating or sharing them through some actions which fall within the risk appetite of the organization.
6. *Control Activities* – implement internal policies and procedures to ensure that risk response is managed actively.

7. *Information and Communication* – the flow of information between employees themselves and with other parties should be done in a time frame, thus each employee carry out his responsibilities through effective communication which occurs in a broader sense, flowing down, across, and up the entity.
8. *Monitoring* – Monitoring is accomplished through ongoing management activities, Internal Audit, separate evaluations, or both and modifications on the process are made as necessary.

The Committee of Sponsoring Organizations of the Treadway Commission COSO outlined that the Enterprise Risk Management framework shows that there is a relationship between the three sides of the framework cube; it indicates that for any organization needs to achieve the set of objectives, it must implement the eight components with respect to the organization structure and requirements.

INTERNAL ENVIRONMENT Risk Management Philosophy – Risk Appetite – Board of Directors – Integrity and Ethical Values – Commitment to Competence – Organizational Structure – Assignment of Authority and Responsibility – Human Resource Standards
OBJECTIVE SETTING Strategic Objectives – Related Objectives – Selected Objectives – Risk Appetite – Risk Tolerances
EVENT IDENTIFICATION Events – Influencing Factors – Event Identification Techniques – Event Interdependencies – Event Categories – Distinguishing Risks and Opportunities
RISK ASSESSMENT Inherent and Residual Risk – Establishing Likelihood and Impact – Data Sources – Assessment Techniques – Event Relationships
RISK RESPONSE Evaluating Possible Responses – Selected Responses – Portfolio View
CONTROL ACTIVITIES Integration with Risk Response – Types of Control Activities – Policies and Procedures – Controls Over Information Systems – Entity Specific
INFORMATION AND COMMUNICATION Information – Communication
MONITORING Ongoing Monitoring Activities – Separate Evaluations – Reporting Deficiencies

Source: COSO, *Enterprise Risk Management—Integrated Framework: Executive Summary*, AICPA, New York, 2004, p. 2.

Enterprise Risk Management Implementation Plan Keys – Initiation Process

In different types of organizations; it is difficult to initiate the first step in the process of implementing ERM throughout the organization. I have listed below some steps which provide a useful base for the initiation action and can help shareholders and senior management especially to identify the limitations and barriers in each area of the organization and ease the resistance in the areas of action to make it happen and have ERM implementation process easily started.

Shareholders and Board of Directors support

Although the board of directors are not directly responsible for implementing the risk management approach in the organization, but they have to supervise the management to lead the process and to ensure that the right path of the risk appetite is considered through this wide process amongst the organizations' departments. The board of director's support must be effective to participate in the process as an enhancement tool of reviewing and evaluating the management's performance for the initiatives taken for ERM to manage and control the main and top risks exposures. Moreover, the board of directors must set up a channel of communication which should be clear and understood by the management to devote the right concentration and most useful techniques to extract more outcomes from existing resources in the organization.

To begin and spread the practical insights of boards through the organization, some questions should be directed to the management which put in place the tone of risk philosophy besides sending a message to the management that the board is aware about the weaknesses of facing top risks in the way of managing the organization and maintain an effective risk management process, like; "What are the main risks exposures and How much they will affect the firm?", "What is the time frame to implement ERM and where to start?".

Select ERM Leader and ERM committee

The leader of the organization's risk committee can be chosen from the existing staff -at least at the beginning of the implementation process- to benefit from his built experience in the same field and his relationships with other departments' managers.
These responsibilities can be given to a senior manager who has a rich knowledge of the organization's strategic objectives besides its risks; he can be the head of internal audit or the chief financial officer for instance and the main attributes of ERM Leader would be:

- Excellent Knowledge of the business nature, objectives and organization's risks.
- Strong relationships with the board of directors and senior management.
- Excellent communication and management skills.
- Wide acceptance and credibility across the organization.

The board of directors should be comfortable with the leader assigned by management to be in-charge for the implementation process and ensure that he understands his responsibilities to achieve the main goals and set up the working schedule of each personnel in this process as well as continue his supervision overall the organization units.
Although this leader can be assigned from the existing staff, thus, he will not necessarily be responsible of ERM for a long term and can be assigned to get the initiative started and moving ERM to the next levels of implementation.

On the other hand, a risk committee must be established to enable the assigned leader to direct the implementation process to the committee which might include other departments' managers to help the ERM leader to engage the concerned employees in each business unit to ensure success of their ERM practices efforts and embedded across the organization's business activities.

Determine Risk Appetite

Once the leader of the risk committee is assigned with respect to the board's approval, the management will have to present its risk management philosophy by studying the options of how the risks must be reported and seeks how to establish a growth perspective towards facing different kind of identified and unidentified risks. It is unlikely the right path to develop the organization's performance and growth opportunities if the management decides to deal with all kind of risks -no matter the size of it and its probability of occurrence-, but it has to set the top risks exposures and focus on the ones that fall within its risk appetite and control them accordingly. The whole process of ERM implementation is manifested in the organization's risk appetite, which provides a clear picture on how many risks can the entity handle and their volumes given the capabilities of human resources and technologies which are main factors of the amount of risks that the company can accept and should fall within the shareholders expectations.

Although the decisions are taken by the management to determine the risk appetite structure and its workflow based on the boards' vision, but the risk appetite must influence the culture of the organization and its operation management style, in other words; it is a broad entity-wide concept.

Take incremental steps base in building ERM

It is difficult to launch ERM overall the organization as one complete step where all of its components should be implemented through different divisions in the organization at the same time, and the main reasons are the complicity and high costs especially in the small and medium enterprises in order to bring a tangible value to the organization as an expected outcome from having risk management system in place. The third key to achieve ERM successes and the benefits out of it is by using incremental steps base to implement it among the organization.

The leader of the process can gain a lot of experience while using the incremental base from the difficulties faced in one area and how they were solved to the following area of implementation because of many repeated issues might occurred which will have a major impact on saving a lot of time and efforts of every employee who is responsible for a part of implementation schedule. Besides that, the same employee can be assigned to handle certain steps in different departments.

The incremental steps base can be started with identifying the key practices by listing some action steps to be shared with the board of directors to point out the identified risks and follow it with more details of risk assessing modules that can be used to further research on other risks that the organization is currently facing or might be exposed to them in future. In addition, using incremental steps provides an opportunity to the top management and line managers to make additional requests to widen the ERM activities through each department in the organization and evaluate the results of those requests separately to see what benefits have been generated and the value derived from each one of them. On the other side, it is an efficient control tool for the board of directors to oversee the management's performance at the initial steps and measure their capabilities in implementing ERM in the organization on each step taken to have ERM in place. Using incremental steps base has two faces in term of value for the organization, one of them is an efficient way of building ERM by the top management and the other one is a sustain performance evaluation tool in the board of directors hands to ensure that the management is employing all resources to develop the risk management system in the organization.

Begin with limited focus on minimum numbers of top risks

To start implementing a risk management system effectively, it is better to first determine the minimum number of critical risks that can be identified easily and controlled by ERM team on the initial steps and then start building further the system in the respective departments.

Controlling the smaller number of critical risks might be enough for some companies if the management achieved the main objectives of its business plan as those risks are taking the big share of impacting the company's performance. On the other hand, it is more efficient to develop the ERM process based on manageable determined risks in monitoring and reporting, and it is an added value in term of taking the incremental steps path to initiate ERM. Also, the management might decide to manage top risks in one department only, and then drive the success from that unit to others in the organization. This limited focus on major risks and their exposures on the organization could be used to develop ERM initial process to formulate it after that to other departments.

Use existing resources and activities in building ERM system

The management should review the existing resources in the organization prior initiating the process of implementing ERM like existing staff and their experience in the same filed besides the existing data related to the process instead of hiring new expertise or engage other parties to help in collecting the information about the impact of major risks. The best practice of undertaking the ERM project is to search through existing tools of technology or human resources and leverage risk management resources which can be used to move ahead with ERM. The management will most likely discover that they already have the knowledgeable personnel who is capable to move forward in ERM process and have the sufficient experience in monitoring top risks as they are doing basically while running the business during the previous periods.

Any running organization has some form of activities related to the risk management done by the internal audit staff or finance team such as; existing credit policies, risk assessment reports and financial statements analysis. It would not be marked as ERM form before starting the implementation process, nevertheless; the organization already has an unidentified reporting system with respect to Enterprise Risk Management.

Although it makes sense to initiate enterprise risk management system upon existing risk related activities, however it should be started with the recognition that the existing activities are not forming a risk management system that would generate benefits to the organization and achieving business plans targets. ERM requires risk management processes that are ultimately applied across the organization and represent an entity-wide view of risks, which is not usually derived from the existing resources.

Embed ERM into the business activities and units

Enterprise risk management is a process that is applied across every department of the organization as defined in COSO framework, so it involves all employees at all levels in the organization to ensure its effectiveness. Although there should be a separate unit that its core role in the organization to sustain the implementation of ERM, nevertheless this process cannot be viewed or implemented as a stand-alone function unit that is operating the practices and ERM activities without having conjunction activities with other departments especially at the beginning of implementation in the Small-Medium enterprises.

In all cases, whether the organization decided to have a dedicated department for the implementation of ERM or not, the ERM should be embedded into the core business processes of the organization being integrated into periodic budget/forecast plans by identifying the top risks and what are the management response activities towards these risks.

Inventory existing risk treatment practices

While the management progresses in the implementation process of ERM, it is important to keep records of the practices took place in areas where risks have been reported, assessed and treated. This will allow management to identify areas of strength to go through and weakness points to be highlighted hence these data will be the base structure for further assessment of other risks that might be faced in future or enhancing the treatment practices of current risks. Also, it helps management develop progress and the benefits of implementing enterprise risk management by serving as a point of comparison as the practices mature.

Continuous monitoring on ERM Updates

ERM should not be presented and viewed as one-time event as the practices of ERM continue to improve by time when implementation process starts. Therefore, it is important for senior managers to ensure that ERM process continue the incremental approach to achieve ERM benefits, and all departments maintain updates on reporting system to reinforce and nurture the risk management culture in the organization besides extending the understanding of current status of ERM and what needs to be achieved in the next steps. The primary objective is to maintain the momentum running and to continue to improve, expand and deepen the organization's risk management capabilities.

Enterprise Risk Management Policy Implementation

Scope and Purposes

The enterprise risk management policy must define the overall practices among the organization; it should contain individual and functional responsibilities that are required to achieve the organization's business objectives and further to realize its vision. Enterprise Risk Management must be established as a policy to provide practical guidance enabling organization's employees to incorporate risk management into daily management practices.

To be most effective, risk management should become part of the organization culture. It should be integrated into organization philosophy, strategy, business plan, and daily practices rather than be viewed or practiced as a separate program where each employee in the organization has to play a role in the identification and management of risks through the risk management processes being integrated in all key processes and embedded in all management activities. Furthermore, all employees have a role to play in achieving organization objectives, setting risk priorities and use ERM policy in their day-to-day working environment. Sound risk management practices will help ensure that the organization takes advantage of opportunities and respond to threats on its strategic objectives. When this is achieved, risk management becomes the business of everyone in the organization.

The purpose of any ERM policy is to explain the organization's underlying approach to risks and risk management philosophy by relating to the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse affects within the organization's environment.

Risk is uncertainty and it is inherent in everything we do. So, when examining the risks associated with achieving the goals and objectives of any organization, it is essential to

ask, "*How do the existing legislation, regulations, policies and practice guide how we do business?*" and "*What other uncertainties might exist that could have an impact (positive or negative) on the organization's goals and objectives?*"

Risk Management helps answer these questions and provides a process by which anyone can identify and assess the risks, evaluate them, develop prevention and mitigation, recovery strategies and result in achieve organization's goals and objectives most efficiently.

It is necessary to build and maintain an ERM framework to provide practical guidance and process enabling employees to incorporate and standardize risk management into daily management practices as risk management is about analyzing and responding to those risks which could prevent the organization from achieving its strategic objectives. When this also involves developing and executing risk management plans, it becomes ERM.

In what and where should Enterprise Risk Management be implemented?

ERM practices should be integrated and applied at department level into the following areas:

- Organization's objectives.
- Activities.
- Management systems.
- Strategic and Business planning.
- Policies development.
- Project management.
- Day-to-day decision making.

It is important to indicate here that funds should be used efficiently and effectively to control risk. Specifically, the costs and benefits of controlling risks should be considered to make the best use of resources especially the limited ones. The formal consideration of ERM provides a framework for using professional judgment and skill in the planning and evaluation of the organization's activities.

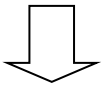
Updates on Enterprise risk management practices

ERM should be a part of the normal planning process at the onset of any functional planning period, significant program or project. In addition, it should be revisited whenever the organization's senior management is aware of any significant change to the circumstances or risks for the function, program / project / activity.

ERM Integration into risk registers process

Unpredictable risks

Residual risks / Failure / Lack of Mitigation



Crises Management

Responsibilities & Accountabilities

The ERM implementation structure provides a mechanism for communication, oversight and guidance on all ERM issues. It is critical for the coordinated response to specific risks within the Sections and Departments, while providing the framework for the flow of risk information to aggregate within the central ERM department. Considering that there will be a complexity of operations usually in most of the organizations, the risk structure will provide the appropriate channels in which risk data can flow through the organization by determining the responsibilities of every one involved in the implementation plan and has a role to achieve the strategic objectives of the organization which can be summarized as follow:

- **Board of Directors and Chief Executive Officer:** To establish an ERM Policy and make the necessary resources available to meet ERM objectives and targets besides review and approve the ERM Policy, risk appetite, risk governance model and risk documentation such as risk tolerances, impact and likelihood scales and risk rating boundaries.

- **ERM Leader:** to oversee, develop and administer the ERM policy / Function and ensure that all activities are carried out consistently with the ERM Policy. Also, to ensure accurate and timely reporting of risks raised by the ERM Function to the Board of Directors and CEO. On the other side, ERM Leader must act as independently audit personnel and present to department managers any significant risks not already identified by their departments.

- **ERM Team:** to coordinate meetings within other departments to identify inter-departmental risks and risk response approach on department level. Besides that, to escalate risks in case of High or very High Risk which has been identified and

cannot wait until the submission of the risk registers and send escalation report to ERM Leader for approval and further process.

Moreover, the team is responsible to deploy and maintain tools that assist in estimating the likelihood and severity of risk events.

- **Risk Owners (Departments Managers who own the risks):** to be responsible for identifying, assessing, mitigating, reviewing and monitoring all foreseeable risks that fall within the scope of the department's activities, processes and remit and identify risk treatment options, perform cost-benefit analysis and develop recommendations and risk treatment plans.

  Eventually, it is all staff responsibility to identify any new risk and send the new identified risk to the ERM Team. ERM Team will allocate the risk to the department that can bear the risk the best according to each Department's responsibilities.

Risk Categories

Risk categories can be defined as risk groupings that helps organize consistent identification, assessment, measurement and monitoring across risks. Using consistent risk categories across an organization enables risks to be aggregated to determine their overall impact on the organization.

Organizations can adopt the risk categories for risks like Environmental Risk, Financial Risk, Human Resources Risk, Operational Risk, Reputation Risk and Systems and Technology Risk. Thus, in case the organization faces any risk which has more than one category, it can be used at the most relevant category for the risk assessment and link the risk to other departments where the other risk categories are related to.

Likelihood and Impact Scale

Key Risks must be categorized to fit with the defined risks in the organization's ERM policy to express its degree of risk appetite, then assess those risks according to the approved impact and Likelihood scale, a sample is shown below can be used as a scale of annual frequency and a risk map to place risks as they can be shown based on risks assessment process, before taking the decision to treat each type of risks.

Description	Annual Frequency
Almost Certain	The risk event is expected to occur more than 20 times per year.
Common	The risk event is expected to occur less than 20 times per year.
Likely	The risk event is expected to occur once per year, up to once in 3 years.
Rare	The risk event is expected to occur once in 10 years, up to once in 20 years.
Remote	The risk event is not expected to occur more than once in 30 years.

Consequence	Impact of risk
Major	Huge consequences – major effect
Moderate	Moderate level of risk impact
Minor	Minor effects

High Impact *Low Likelihood*	*High Impact* *High Likelihood*
Low Impact *Low Likelihood*	*Low Impact* *High Likelihood*

Risk Register

The Risk Registers in any firm is the product of a risk session of any list of risks with rankings and summary treatments arrived at by consensus, to inform an improved business plan. All risk registers should be updated in the ERM Software to be reviewed by the ERM Leader.

Risk Assessment

Risk assessment is an overall process of risk identification, risk analysis and risk evaluation.

Identify Risks

The Identify Risks process seeks to identify risks that may prevent the organization from achieving its objectives using the common classification, criteria and processes developed in ERM Policy. When identifying risks it is important to understand and document the factors that could trigger risk events, as well as possible consequences. Identifying risks and possible triggers and consequences is a first step in understanding organization's overall risk exposure.

The Identify Risks process seeks to identify the risks to be managed using a well structured and systematic process.

At this stage in the overall framework, the primary concern is to identify as many risks to achieve the organization objectives, the sources of the risks and the impacts. This list should subject to further qualification and refinement as part of the Analyze Risks process. The idea is to cast a wide net at the start in Identify Risks, and then to progressively narrow the list to the most critical using the qualitative and quantitative techniques in Analyze Risks.

It is important that all risks are captured in ERM regardless of whom the owners are and its impact or likelihood. Thus, the scope of Risk Identification and Analysis shall include but not limited to the department's Strategic Objectives, Initiatives, Operational Plan, Projects, Procedures and Activities.

Stating risk involves considering its three elements: event, causes and impacts. By acting on one of the elements of risk occurrence; the risk can be affected when removing one element which prevents this certain risk. Since risk will be defined as "the effect of uncertainty on objectives", it is helpful to link the organization's objectives to the risk identification.

On the other hand, events must be defined as something that could prevent achievement of an objective, milestone or target or create an opportunity to exceed them. From there, the causes and impacts become easier to identify as:

- Identify a risk event related to an in-scope objective without stating general unfavorable conditions, in and of themselves, as risk events.
- List the potential causes of such an event. There are often multiple causes for a given risk event. Ask yourself "*Why"* the event might happen.
- Identify the impacts of the event, should it happen. Ask yourself, "*So what"* if the event were to occur. Keep asking "*so what"* to the chain of impacts until realistically potential impacts are identified.

Analyze Risks

The Analyze Risks process seeks to understand the magnitude of both the positive and the negative consequences of a risk event, as well as the likelihood of those consequences occurring. Assessing the magnitude and likelihood of possible consequences will enable the organization to prioritize and aggregate its risks, and enhance its risk treatments in a way that focuses on those risks that pose the greatest threat to achieving objectives.

Risk Rating:

Risk Rating is the process of calculating the Likelihood of an event and its Impact if it occurred. The product of these two variables is the *Risk Rating*.

Risk Rating = Likelihood x Impact

Each risk will be identified during the Identify Risks process should be subjected to a qualitative evaluation of its likelihood and impact risks scales. The list of risks is then narrowed and refined based on the criticality of the risk. Risks can be assessed in terms of many different impact categories, such as Financial, Operational, Reputation and Safety & Health, etc. The Risk Rating is based on the probability multiplied by the highest of the impact category scores, therefore taking into account the worst case scenario where a risk has a High impact even though the impact against cost is low.

Likelihood: is the chance that the risk event identified will actually occur. When available, statistical data can support estimates of likelihood and severity. In practice, historical data might not exist. Instead, ERM team can rely on the experience of those around the table; therefore, likelihood rarely implies mathematical certainty rather it is a subjective estimate.

Consequence: is the severity of effect upon goals, objectives or values.

Risk Rating Terms

The terms associated with the levels or ratings of risks vary across the risk management discipline; therefore, some clarification is required. Inherent Risk, Initial Risk, Residual Risk and Current Risk are common terms used.

Inherent risk: involves rating the exposure in the absence of existing controls. When seeking to understand inherent risk, considering a hypothetical condition free of all controls should take place like locks, rules, procedures, ethics and so forth. This can be difficult to imagine. However, there is value in assessing risk this way as it can identify if whether an exposure is over or under controlled. This is of particular interest to auditors. Strategic risk assessments -of an organization business plan- for example, often benefit from an assessment of inherent risk.

Initial risk: involves rating the exposure within its current control environment. In addition, initial risk is a baseline against which the organization can measure progress. Reviews of loss histories, reviews of similar sectors' loss histories and consultation with stakeholders can support the assessment process.

Residual risk: involves rating the exposure after the development of additional mitigation/treatment strategies. It is important to establish a residual risk rating because it is a prediction of the efficacy of proposed mitigations. It also serves as a start point for an informed discussion of acceptable risk with senior decision-makers.

Current risk: is a measure of progress. Regular updates on the progress of risk mitigation strategies can be valuable in helping to demonstrate progress or to secure additional resources for stalled mitigation efforts. The tracking of current risk over time allows efficient shifting of resources to problem areas or to areas of opportunity. In addition,

tracking the progress of current risk can help demonstrate the effectiveness of the organization risk management program.

Evaluate Risks

The Evaluate Risks process seeks to prioritize risks for treatment by evaluating them against pre-established risk appetite and tolerance criteria. By understanding the level of risk exposure relative to the organization's risk appetite and tolerance, decisions about treatment can be made that optimize risk taking and maximize the likelihood of achieving objectives.

The Evaluate Risks process uses the understanding of risk obtained by risk analysis to rank and prioritize risks in order to make decisions about risk treatment. It is too expensive or ineffective to treat all risks. Senior manager needs to know which of their risks are most critical and prioritize accordingly. Usually, it is found that the treatment of a few critical risks results in dramatic reductions in residual risk, whereas the treatment of each following risk results in nominal incremental reductions in residual risk. Ranking the risks to facilitate this analysis in the Treat Risks Process is important.

At this stage, senior managers have a large amount of enterprise-wide information about their risks that may not have been available earlier during Identify Risks process when tolerance levels were being set and risks were being mapped to strategic objectives.

Prioritize Risk: after deciding which risks to accept, the risks need to be prioritized. To ensure objectivity and transparency, they should be prioritized against agreed criteria. Prioritizing the risks against agreed criteria is efficient because the results may give a different outcome from the initial thinking:

- Risk Rating - what is the risk rating of the risk?
- Trend - what is the trend of the risk occurring? Rating is going up or down? What is the progress of the implementation of the mitigation measure? How many risks with same risk description have been identified in other departments?
- Impact - what is the financial impact if the risk does occur? What is the operation impact (in terms of time) if the risk does occur? What is the reputation impact if the risk does occur? What is the impact on employees if the risk does occur? What is the regulatory impact if the risk does occur?
- Likelihood - what is the likelihood of the risk occurring?

Aggregate Risk: risk aggregation is the roll-up of low-level risks to higher levels.
This technique relies on qualitative judgment to summarize risks at the critical risk area and process level in terms of likelihood and consequence. The risks identified by each department are first grouped according to critical risk areas/processes and listed in priority sequence. Within each area/process the individual risks are evaluated against a set of established criteria to determine the overall aggregate risk rating for the area/process.
The aggregation criteria are the same as the aforementioned prioritizing criteria as well as the ERM Team will aggregate the department's risks to an organization level, and then the organization's top 10 risks can be defined. Risk evaluation also consists of considering the ranked risk in relation to its existing controls. There are three considerations when evaluating existing controls:

1. Characterize, in qualitative terms, the existing controls (i.e., describe the process, policy, device, practice or other action already in place that mitigates the risk in question?) Non-existent, Inadequate, Adequate, Robust and Excessive (this latter indicates over-controlling and so possibly overspending).

2. Characterize the risk in relation to the organization's degree of tolerance: Unacceptable / Acceptable with treatment / Acceptable. It is possible to have "zero" tolerance for certain risks (assuming one can avoid them).

A risk may be "Acceptable" either because it is inevitable and too prohibitive to treat, or because it is immaterial and not worthwhile to treat. Over time, the organization can develop risk criteria or measures of risk tolerance and risk thresholds. Expressing tolerance for an unexpected financial loss over a certain percentage of operating budgets as "unacceptable" might be one way that a senior manager can quantify their tolerance of certain risks.

3. Decide on consequent action, based on steps 1 and 2: Avoid/ Treat/ Monitor. A risk may be avoided altogether, if unacceptable, by not doing the action that would incur it in the first place. ERM team can tolerate and monitor risk when treatment is impracticable or prohibitive. Monitor risks that are inconsequential, but whose status might change.

Risk Response / Treatment

The Treat Risks process seeks to identify, assess and implement treatment options to respond to risks. Risk treatment not only seeks to minimize potential downside but also maximize the potential upside of opportunities.

Treating risks is just as much about seizing opportunities as it is about minimizing downside. Too much treatment is as undesirable as too little. The objective is to find the right balance to optimize returns to the business by maximizing gains from opportunities while minimizing losses from risks. Evaluation of downside risk involves the consideration of non-financial as well as financial impacts. For example, the risk of enterprise reputation may override purely financial considerations when selecting risk treatment options.

This process delivers qualitative and quantitative information about residual risk to the Develop and Manage Strategy processes to complete then. In this way, the organization can make informed strategic decisions about how to allocate resources to its various lines of business and projects.

Risk Treatment

Once risks have been classified and evaluated, the organization will determine treatment options for each risk rating. On a very rare basis, exceptions may be noted. Exceptions rated as "Very High," which cannot be eliminated or risks rated as "High" will be handled on a case by case basis by the Board of Directors through escalation by the ERM Leader. Therefore, the maximum timeframe to address a risk response and to implement its mitigation measures depends on the risk.

To facilitate all departments, the organization can determine a timeframe for defining Risk Treatment Response. All departments shall adhere to the timeframe defined unless any department can justify why the risk response and mitigation should have a timeframe beyond the pre defined limits.

Risk Treatment Options

Develop an overall risk treatment strategy. Treatment of individual risks seldom occurs in isolation. Having a clear understanding of a complete treatment strategy is important to ensure that critical dependencies and linkages are not compromised. For this reason, the development of an overall treatment strategy should be a top-down process, driven jointly by the need to achieve the organization's objectives while controlling uncertainty to the extent that is desirable. Many treatments need to be acceptable to stakeholders or those involved in implementation if they are to be effective and sustainable.

Risk treatment options can be examined by costs-benefits analysis, and to advise the risk treatment strategy to the department's manager for review and approval, and for budget not within the Operations Plan, nevertheless the department shall seek budget approval through the organization's policies and procedures.

A costs-benefits analysis is a systematic process for calculating and comparing benefits and costs of a project for two purposes:

- To determine if it is a sound investment (justification / feasibility).
- To see how it compares with alternate projects (ranking / priority assignment).

It involves comparing the total expected cost of each option against the total expected benefits, to see whether the benefits outweigh the costs, and by how much.

Risk Treatment Plan

Treatments (risk mitigation) can consist of virtually any sort of administrative action, as well as the application of specialized disciplines – where a separate analysis may be required; e.g., emergency planning, business continuity planning, security planning, risk financing, financial controls and human resources management. Grouping risks in categories can help in the design of cost-effective treatments.

Develop a detailed risk treatment action plan including the person responsible for implementing the risk treatment, the primary activities, required resources, schedule, budget, reviewer and status. Treatments are new measures undertaken to mitigate identified risks. However, participants may fall into familiar thought patterns and merely repeat the list of existing controls and say there is nothing more to be done. Alternatively, they may say that the implementation of their planned program activities constitutes mitigation of risk. It is just here where the Risk Team may add value:

- Risk Team can lead off by asking (either simple or well-informed) questions about possible treatments and stimulate discussion;
- Risk Team can draw attention to the ranking of the risk – if Participants are reminded that it is high or extreme and threatens the viability of the department's objectives, they will feel less inclined to leave the matter unattended.
- Risk Team can introduce categories of implementation risk (well- documented, common reasons for program failure) to inform the analysis.
- The necessity to study the issue and develop treatments "off-line" or in a separate session can be flagged.
- The possibility of inviting expertise from outside the organization can be raised.
- At a minimum, the action of documenting the risk and bringing it to the attention of a higher authority or other organization constitutes an improvement in the management of the risk.

Implement Risk Treatment Plans

Suggested treatments (mitigation of either a risk likelihood or degree of consequence) are subject to cost-benefit analysis. The Risk Champion must challenge the participants to commit to acting upon mitigation strategies. If the risk management initiative is an enhancement tool to existing processes, then the treatments must become new items in the list of project tasks or business plan strategies. Assigning an individual by name to the development of a mitigation strategy and identifying a specific deliverable.

The Risk Owner will be responsible for securing the budget to implement the risk treatment plan as per the organization Budget.

Once budget is secured, implementation of the risk treatment should be initiated. The identified Risk Response Owner responsible for implementation should take the actions outlined in the treatment plan by reporting progress to the Risk Owner and other identified personnel, and manages implementation within the agreed budget and schedule. Once the implementation is complete, the Risk Owner and the ERM Team should be informed.

Risk Treatment Plan Implementation & Monitor

The Risk Treatment Plan Implementation and monitor can be done through implementing the following steps:

- Update the organization risk register with the approved risk treatment plans.
- Update information in the risk management software regarding risk treatment progress.
- Update information regarding the root causes and impacts of the risks including frequencies, probabilities, impacts and existing treatment strategies and controls where applicable.

- Monitor the status of risk treatment plans against agreed milestones as recorded in the risk management software and alert responsible party if deadlines are likely to be or have been missed.
- Determine and implementing corrective actions such as reassigning work, identifying additional resources to assist with the activity or communicating with a direct supervisor to reassign work so that the responsible person has an appropriate limit of time to devote to assigned risk management activities.
- If a deadline is missed, communication must be established with the responsible party to document the reason whereas the corrective action should be taken to determine a revised milestone date.

Risk Transfer and Risk Response Transfer

Risk Transfer

A risk can be transferred to another department in case the responsibility has been reallocated by Management as the Original Risk Owner can transfer the risk (after Department Manager approval) and send to the ERM Team then to the ERM Leader final approval. Once the risk is accepted by the Proposed Risk Owner, the risk shall be incorporated in their Risk Register and closed in the risk register of the Original Risk Owner.

If there will be any dispute in risk ownership transfer / allocation, the ERM Leader should get involved where required to mediate between the two parties.

Risk Response Transfer

If the risk response owner is not the risk owner then the risk response should be transferred to the department where the risk will be mitigated on behalf of the risk owner. To transfer the "risk response" of a risk to another department if the department is not intended to be used for requesting extra budget or resources and if any new risks rated as Very High or High, that are unplanned in Operations Plan / Budget, then the respective department can request the required resources directly from the subject department.

For risk response transfer between departments; both departments must agree on the risk response(s), benefit(s), response cost, response time frame or dead line of implementation quarterly progress and monitoring report of the risk response by the risk response owner.

Risk Monitoring and Progress Report

In order to monitor the implementation progress of a risk response on department level the implementation progress of risk response for High and Very High risks should be monitored as often as needed according to the timeframe provided by the ERM Team and set the expectation that deadlines will be met and expected residual risk levels can be achieved.

Risk Treatment Effectiveness

Upon implementation of a risk treatment plan, assessment of whether the reduced probabilities or impacts or other expected benefits have been realized by making adjustments as necessary to reflect actual conditions, by comparing the expected benefits and costs of risk treatment to the actual, and calculating the residual risk to compare it with the risk tolerance levels to determine if additional risk treatment will be necessary.

Risks Mitigations

Once the risk is clearly identified detailing event, causes and impacts, it is important to identify existing mitigations. It is important to ask what measures are currently in place (if any) to mitigate this risk. Only those mitigations that already exist should be listed and to identify additional proposed mitigations after the ERM Team has evaluated the adequacy of existing mitigations and the significance of the risk.

Control Activities

Organizations that decide to reduce risks need to identify control activities that can be used to effectively reduce risks or the costs associated with them noting that control activities under the COSO ERM framework expand beyond what have traditionally been considered control activities under the notion of internal control, according to the new COSO Internal Control Framework 2011 article 488: "*Enterprise Risk Management is broader than Internal Control, expanding and elaborating on Internal Control and focusing more fully on risk. Internal Control is an integral part of Enterprise Risk Management. The Enterprise Risk Management – Integrated Framework remains in place for entities and others looking more broadly at Enterprise Risk Management.*"

A control activity consists of any initiative or activity that reduces the likelihood / probability / frequency of any risk or reduces the associated impact cost. What has been traditionally considered "internal control" is a subset of possible control activities and applies to those activities that specifically manage financial reporting risks. The next aspect of control activities is determining the cost of risk reduction activities.

Communication & Information

Although described as a separate component in the COSO cube, the component of information and communication is less a separate set of risk-related processes than a set of tools and processes linking other components. The Communicate and Consult or information process must be an integral part of creating a positive risk management culture within the organization.

By taking a consultative approach to risk management rather than a one way flow of information, shareholders will understand the rationale behind decision making as well as their importance to manage the organization's risks.

Furthermore, engaging in multilateral dialogue with shareholders ensures the comprehensiveness and robustness of each step in the risk management process. Communication and consultation are intrinsic to the process of ERM and should be considered at each step of the framework.

Involving others, or at least looking at things from another point of view, is an essential ingredient of an effective approach to ERM. Engagement with shareholders makes risk management explicit and more soundly based, and adds value to the organization. It is particularly important where shareholders may:

- Have an impact on the effectiveness of the proposed risk treatments.
- Be affected in risk incidents.
- Add value in the assessment of risks.
- Incur additional costs; or be constrained by future risk controls.

Monitoring & Reviewing

The Monitor and Review process seeks to continuously evaluate the effectiveness and relevance of the organization's ERM program. By continuing to monitor risks and the effectiveness of their treatments, the organization will be able to refine its ERM program to evolve with the dynamic circumstances in which it operates.

The Monitor and Review process involves the on-going review which ensures that the ERM program remains relevant and effective. Factors that may affect the likelihood and consequences of an outcome may change, as the factors that affect the suitability or cost of the treatment options. Therefore it is necessary to repeat the ERM cycle regularly.

On the other side, actual progress against risk treatment plans provide an important performance measure and should be incorporated into the organization's performance management, measurement and reporting system. Monitoring and review also involves learning lessons from the risk management process by reviewing events, treatment plans and their outcomes.

Moreover, monitoring provides routine surveillance of actual performance for comparison with expected or required performance. Review involves periodic investigation of the current situation, usually with a specific focus.

Monitoring and review is an essential and integral part of managing risk and is one of the most important steps of the risk management process organizationally. It is necessary to monitor risks, the effectiveness and appropriateness of the strategies and management systems set up to implement risk treatments and the risk management plan and system as a whole.

Ultimately, assurance and monitoring processes should be continuous and dynamic as it is not sufficient to rely only on periodic audits reports.

For the Monitor and Review process, the following activities must be completed:

- **Monitor Regular Management of Risk Information**

Monitoring take place when managing risks information as a regular practice. Risks themselves undergo change and can require revision in terms of their description and ranking. Therefore A periodic update of risk information using the risk register generated from the ERM Database as a management tool will enhance the regular monitoring. Also, using the risk register to track the implementation of mitigation strategies and the resultant impact on risk ratings where the risk register becomes a valuable communication tool by informing executive on the progress, or lack thereof, and any additional resources required.

- **Review Historical Risk Information**

In a mature practice of risk management, a growing body of information can inform analysis of the risks themselves, their most common sources, their frequency and impacts/costs of actual occurrence, the efficacy of treatments and the occurrence of unforeseen events. All of this serves to better manage risks and inform planning. Audits, complaints investigations, legal judgments and retrospective cost/benefit analysis are some sources of historical risk information and this information must be recorded for knowledge sharing and also for identifying potential risks for management.

Terms of ERM implementation process

Implementation process of ERM must have some terms and conditions to limit the roles and responsibilities of employees throughout the organization in order to achieve the strategic objectives like:

- The board of directors and executive officers are committed to adopt and implement ERM to minimize various risks to meet the organization's objectives.
- The board of directors and executive officers are committed to deal with any conflict of interest in respect of risks within the organization or with external parties.
- The organization ERM policy is aligned with and in compliance with the current government's statutes, Laws, and policies. The ERM program seeks to provide a benefit to the shareholders as the firm emerges as a benchmark for ERM best practice in its business field.
- Through its ERM policy, the organization defines and analyses its capacity to retain, reduce, avoid, or transfer risks. The definition is aligned with and in support of the organization overall strategic objectives, risk tolerance and risk appetite.
- The senior management is committed to provide the tools and resources that are necessary to encourage and enable employees to fully capitalized on risk-related opportunities and minimize risk downside by providing ERM information throughout the organization, monitoring and measuring ERM performance.
- Each department or risk owner is responsible for identifying, prioritizing, evaluating, treating and monitoring risks within the scope and responsibilities of the department. The organization endeavors to follow the risk governance model and ERM framework to which the organization identify and adopt.
- Department policies, processes and procedures' risk-related aspects must be developed constantly, and in alignment with the organization overall ERM policy.

- Each section and department is responsible for adopting and following the organization ERM framework defined in the policy. All employees shall provide a coordinated response on specific risks - when providing risk information – to ensure risks are properly aggregated across the organization.
- Each department and risk personnel is responsible for conducting regular reviews and reporting of their risk registers in accordance with ERM policy depending on their risk appetite and in their own business context, which includes individual strategic objectives and the external environment in which they operate.
- Risk management performance must be measured on (Quarter - Semiannual – Annual) basis based on the defined ERM scoring criteria, which is linked to the department KPI's.
- All employees should be empowered to lead and support a culture of risk transparency and open dialogue. The ERM function must support and help to facilitate regular risk discussions, risk-related organizational change management, corporate communication and risk awareness with ongoing risk education and training for ERM coordinators.
- The organization ERM policy should be reviewed at least annually to ensure that it remains in alignment with best interest of all shareholders. The organization executive management carries the ultimate responsibility of ensuring the commitments within ERM policy are current and continuously executed.

Limitations of Enterprise Risk Management Policy

It is essential to recognize that risk management does not mean risk avoidance. Even with the best risk management environment, mistakes will happen. However, it is important to take a professional considered judgment on the potential risks and the costs of organization's response. For example, in some circumstances, the best approach is to accept a risk, if all potential response strategies are too costly or have other disadvantages. Sound risk management helps to make defensible decisions in such cases.

Survey Results

The first part of the survey consisted of ten multiple choice questions which can be analyzed as follow:

The first question in the survey aimed to show the sample's business type. Despite of different structures indicated in the answer options, but the target was to approach respondents with a manufacturing background which has reached almost 96% of the responses collected and the remaining 4% percent were answered by employees work in consultancy firms. Also, it is important to indicate that there was no feedback collected from employees work in trading and contracting companies, therefore, the survey may not describe the current status of those organizations in term of Enterprise Risk Management.

The results showed that more than 99% of the respondents were from the private sector and less than 1% was from public and no participants from government or non-profit organizations. In addition, the survey results showed that more than 86% of respondents were handling senior positions which reflect the opinion of the main decision makers of their organizations. On the other side, middle and junior level employees' responses reached to 12.3% and 1.6% respectively.

Furthermore, respondents indicated that most of the influence to implement risk management system is exerted by the organization's internal auditors and senior management officers due to their role in managing the organization's risks as it is an essential part of their key responsibilities. Fewer numbers of employees think that Shareholders, Board of Directors and middle management employees and less than 1% thinks that Finance department have main influence on management to put risk management process in place.

The challenges towards implementing risk management system were questioned in the survey; as a result, above 85% of the respondents think that Board of Directors vision,

integration of risk management within the nature of business, difficulty in translating risks into figures and lack of risk assessment tools are the main challenges besides that 70% of them think that building a risk management system can be achieved with incurring high initial costs. Other answers indicated that there is another challenge like; "Achieve a common understanding on the process and its integration as a part of the operational business".

Only about 9% of the respondents think that collection of historical data is a challenge towards implementing risk management system. This is minor due to the extensive use of computer systems to keep historical data and advanced filing system used.

A lot of companies were established in the UAE recently which their core business is to assist and build a risk management system for other companies under many aspects of the risk strategy set up, identification, assessment, mitigation and monitoring risks, however only 5% of respondents indicated that their organizations have engaged an outside party to assist its management in setting up risk management system.

The responsibility of monitoring risks in the organizations of the sample tested belongs to the internal audit department with more than 87% of responses collected through audit findings reports to ensure that all other departments are following the organization's policies and procedures and addressing different kinds of risks which inhibit the organization from achieving its strategic objectives where as 45% think that it is under the responsibility of division managers as they are in line with operations on daily basis and managing the division's overall performance in the absence of independent risk department. The risk strategy of each division manager is presented in his performance by reducing costs and increasing the number of production units to meet the maximum production capacity in manufacturing organizations assuming high market demand.

The main inhibitors to involve risk management personnel in assessing different types of risks exposures are indicated in the respondents' answers are lack of management support due the focus of shareholders more on the production side and immediate returns instead

of spending funds on implementing risk management system considering that perceived cost is much higher that benefits expected. On the other hand, respondents think that inadequate trained staff and lack of IT support and risk management specialized software are main inhibitors as well. Data Unavailability formed 15% of the respondents' opinions and 3% think that there are no inhibitors of risk management personnel involvement in assessing organizations risks. In addition, one answer showed another inhibitor of "Poor qualifications and experience absence by the controller" which can be added to the option of having inadequate trained staff.

The greatest value of addressing different types of risks to the organization was addressed in the respondents' answers mainly in developing overall business strategy, monitor reputational risk caused by quality of products or service provided and improve operational performance. Another opinion was "avoidance of unexpected hits in the bottom line" that presents a part of the operational performance in the form of determining budget plans and achieves forecasted figures. Nevertheless, other respondents indicated that Profit share increase will increase the market share and achieve regulatory compliance is an added value in term of risks identification process success.

Moreover, the status of risk management strategy based on more than 80% of the respondents' opinion stated that it is one of the organization's future plans, which means that currently is not yet started. More studies on the strategy are required to set the initial steps to start with was indicated by about 7% of the sample tested. In contrast, between 2 to 5% think that the strategy is defined and implementation process is completed or still under process, while less than 3% believes that their organizations are not planning to establish a risk management system in future.

The second part of the survey consisted of six rating questions focused on the scale of competency of the organization's staff in different areas of research which play a basic role in the implementation process of enterprise risk management in any organization.

Staff knowledge in term of risk management operations were rated mostly as limited knowledge, despite of 18 to 23% of the sample think that their organization's staff is knowledgeable; however such information can be validated only when the process of risk management policy is tested in full and monitored over a period of time. In addition, more that 85% of the respondents believe that the staff level of competency is not adequate and need improvement in Identifying, classifying and assessing risks besides development on risk management process as well as quality of risks results reporting.

In Audit process, the knowledge of the organization staff was rated as knowledgeable in more than 70% in audit planning and conducting meetings despite of almost half of the sample tested think that staff knowledge is adequate, and the rest believe that they need improvement. For other elements in audit process, the level of competency decreased in respondents opinion as those elements are more complicated and need advance skills than the entry level of audit process and improvement is required for more than of 70% of the sample in the areas of continuous monitoring, data analysis tools, cost reduction and report writing.

Experts in risk management process and audit process were considered as less that 2% which can be examined and verified based on detailed study of the status of risk management process in those organizations.

Similarly, the level of competency for the staff was tested on the operation side of the business like procurement, inventory, production and sales since the enterprise risk management implementation process has to be embedded with the business fabric of the organization in every department, the percentage between having knowledge and limited knowledge were almost equal in those departments amongst the sample tested where as more improvement was required to enhance staff expertise to support the implementation process and ease the flow of information between all departments and achieve the department's strategic objectives.

Conclusion

Enterprise risk management is a broad concept which requires an extensive focus on all kinds of risks to be implemented fully and it is important that any organization identify and manage risks to optimize the organization's resources and achieve its strategic objectives. However, the process can be started gradually in the organization's departments and then embed the concept of risk management practices within the business units by a set of training courses to the employees to be able to spread the culture of risk management work-base environment.

Senior managements might face resistance from employees as they think that implementing any risk management system will result in more workload and extra responsibilities without getting a tangible return. It was found that senior managers and internal audit department are exerting the most to put risk management practices in place, while division managers and supervisors were not; because implementing a risk management system certainly will lead to minimize their authorities and decision making power.

Apparently, it is not efficient for Small-medium manufacturing firms in the United Arab Emirates to fulfill the requirements of COSO to apply Enterprise Risk Management across the firm; however the concept can be redesigned to fit the organization's needs to focus on most key business risks by conducting a risk assessment model then move forward to form a common matrix of well-established risk management system.

On conclusion, senior managements should effectively lift their organizations to a higher standards level of risk management practices by motivating the key staff to increase their level of knowledge when providing a proper training in ERM field. Organizations can benefit from the existing human resources and historical information to build an efficient risk management system without incurring high costs initially.

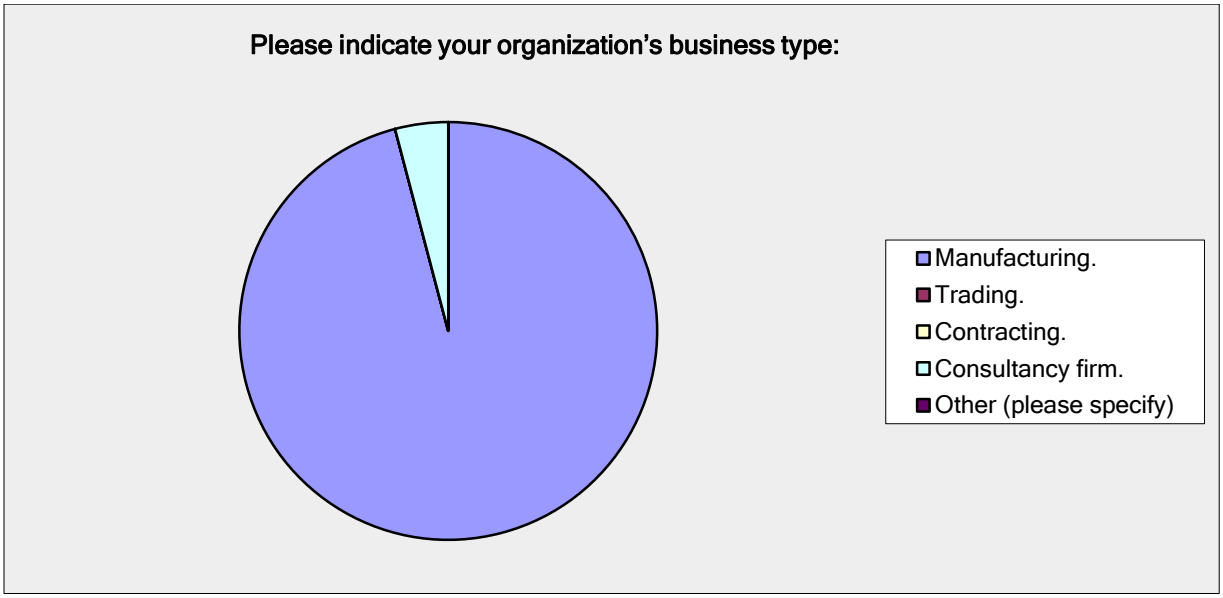
On the whole, ERM implementation process can be eased if it started using the existing resources in the organization which will minimize the implementation cost comparing with establishing a new risk department dedicated only to implement a risk management, thus it is essential to have a shareholders and board of directors support to start the process.

Appendix

Questionnaire - Enterprise Risk Management

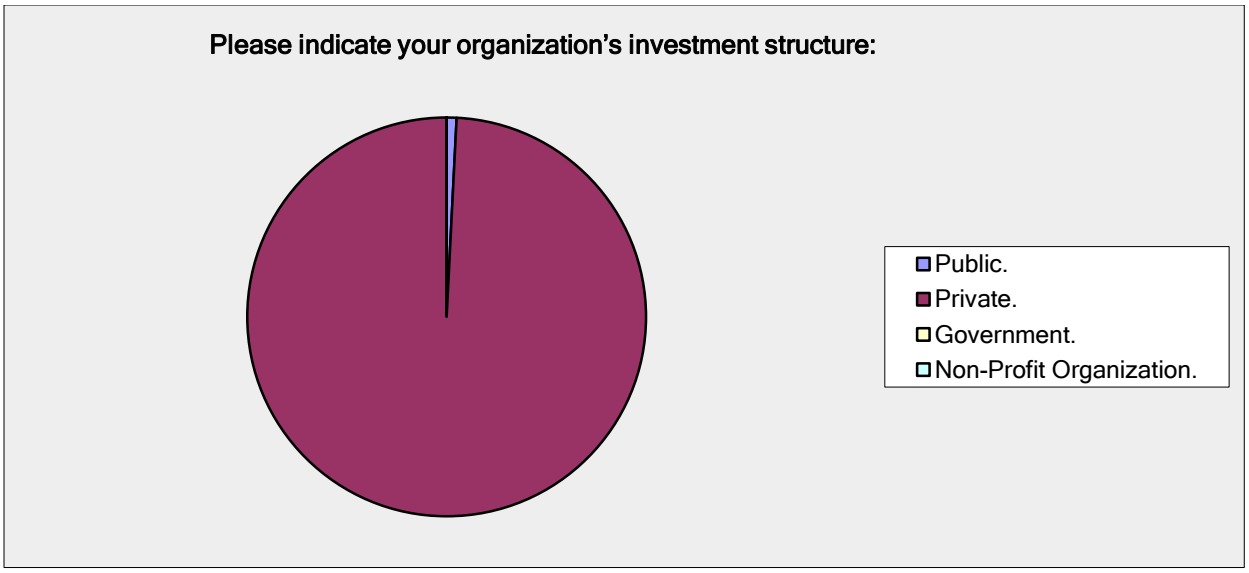
1. Please indicate your organization's business type:

Answer Options	Response Percent	Response Count
Manufacturing	95.9%	117
Trading	0.0%	0
Contracting	0.0%	0
Consultancy firm	4.1%	5
Other (please specify)	0.0%	0
	answered question	122
	skipped question	0



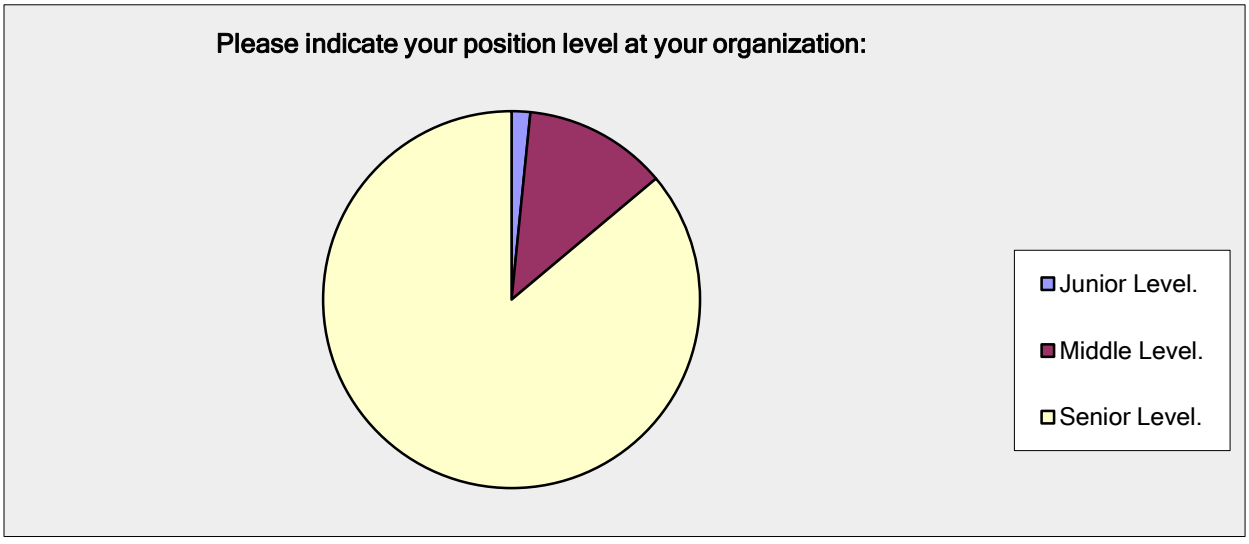
2. Please indicate your organization's investment structure:

Answer Options	Response Percent	Response Count
Public	0.8%	1
Private	99.2%	121
Government	0.0%	0
Non-Profit Organization	0.0%	0
	answered question	122
	skipped question	0



3. Please indicate your position level at your organization:

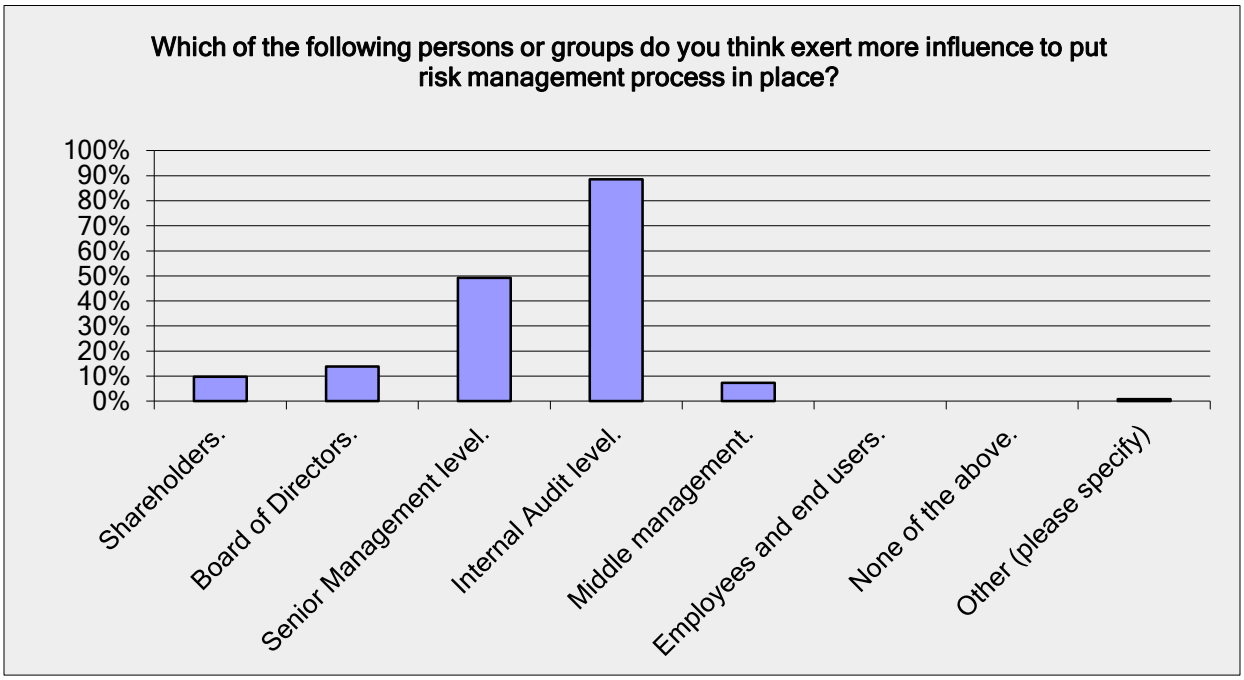
Answer Options	Response Percent	Response Count
Junior Level	1.6%	2
Middle Level	12.3%	15
Senior Level	86.1%	105
	answered question	122
	skipped question	0



4. Which of the following persons or groups do you think exert more influence to put risk management process in place?

Answer Options	Response Percent	Response Count
Shareholders	9.8%	12
Board of Directors	13.9%	17
Senior Management level	49.2%	60
Internal Audit level	88.5%	108
Middle management	7.4%	9
Employees and end users	0.0%	0
None of the above	0.0%	0
Other (please specify)	0.8%	1
	answered question	122
	skipped question	0

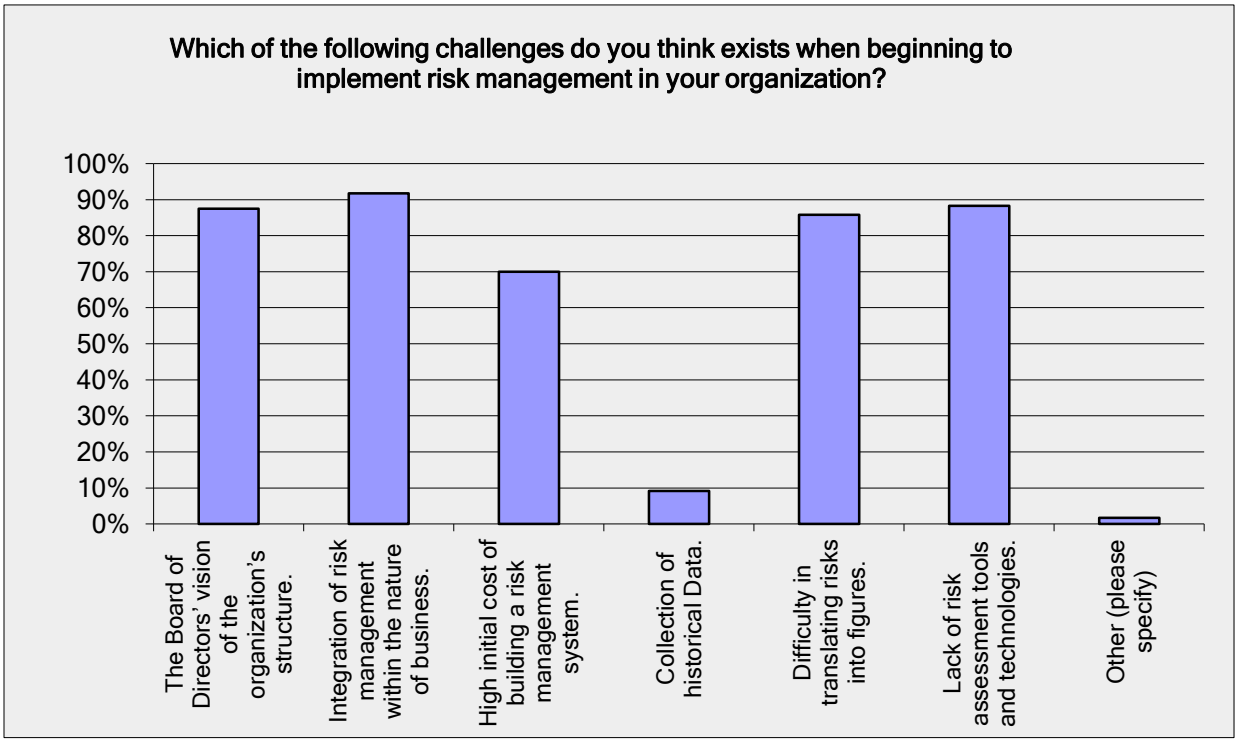
Number	Response Date	Other (please specify)	Categories
1		Finance	



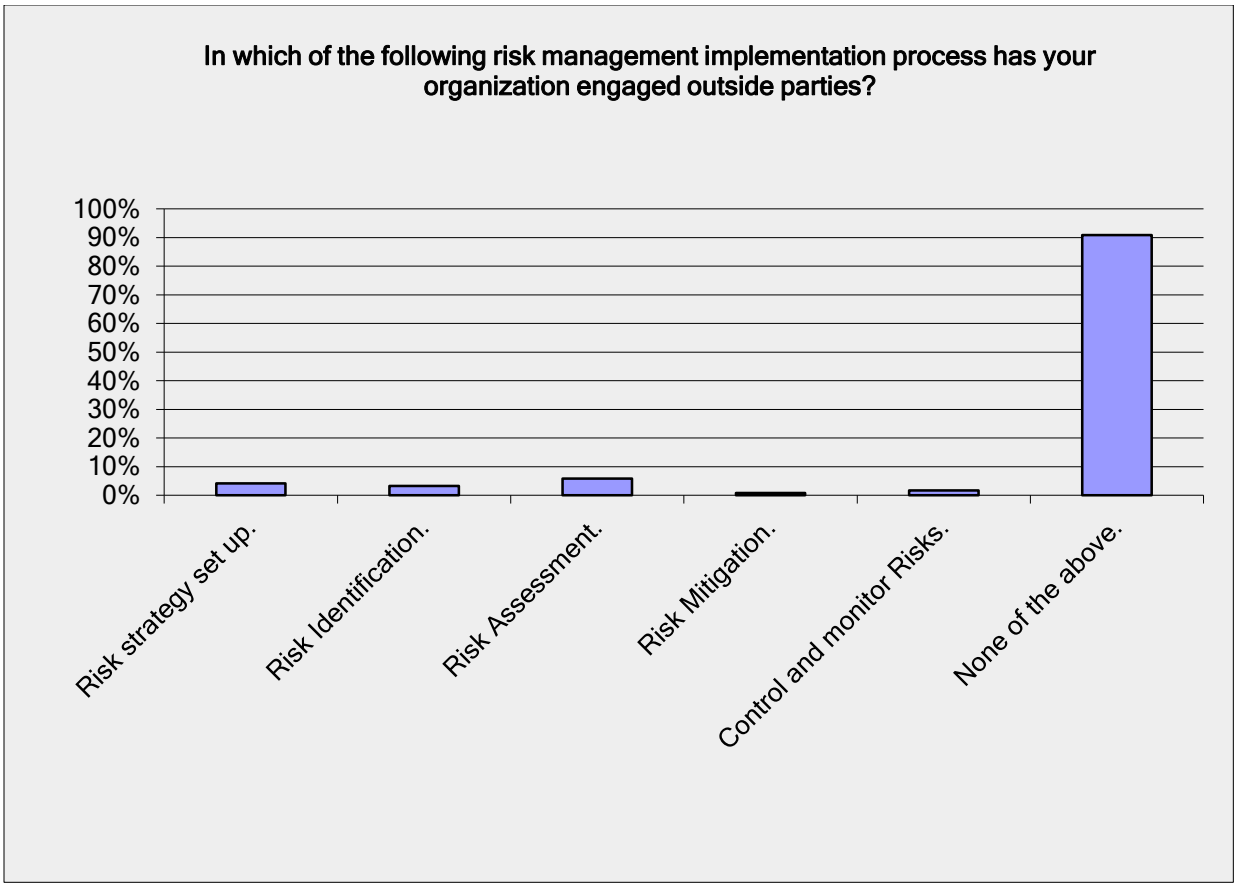
5. Which of the following challenges do you think exists when beginning to implement risk management in your organization?

Answer Options	Response Percent	Response Count
The Board of Directors' vision of the organization's structure.	87.5%	105
Integration of risk management within the nature of business.	91.7%	110
High initial cost of building a risk management system.	70.0%	84
Collection of historical Data.	9.2%	11
Difficulty in translating risks into figures.	85.8%	103
Lack of risk assessment tools and technologies.	88.3%	106
Other (please specify)	1.7%	2
	answered question	120
	skipped question	2

Number	Response Date	Other (please specify)	Categories
1		Not aware about the answer.	
2		To achieve a common understanding on the process and its integration as part of the operational business	

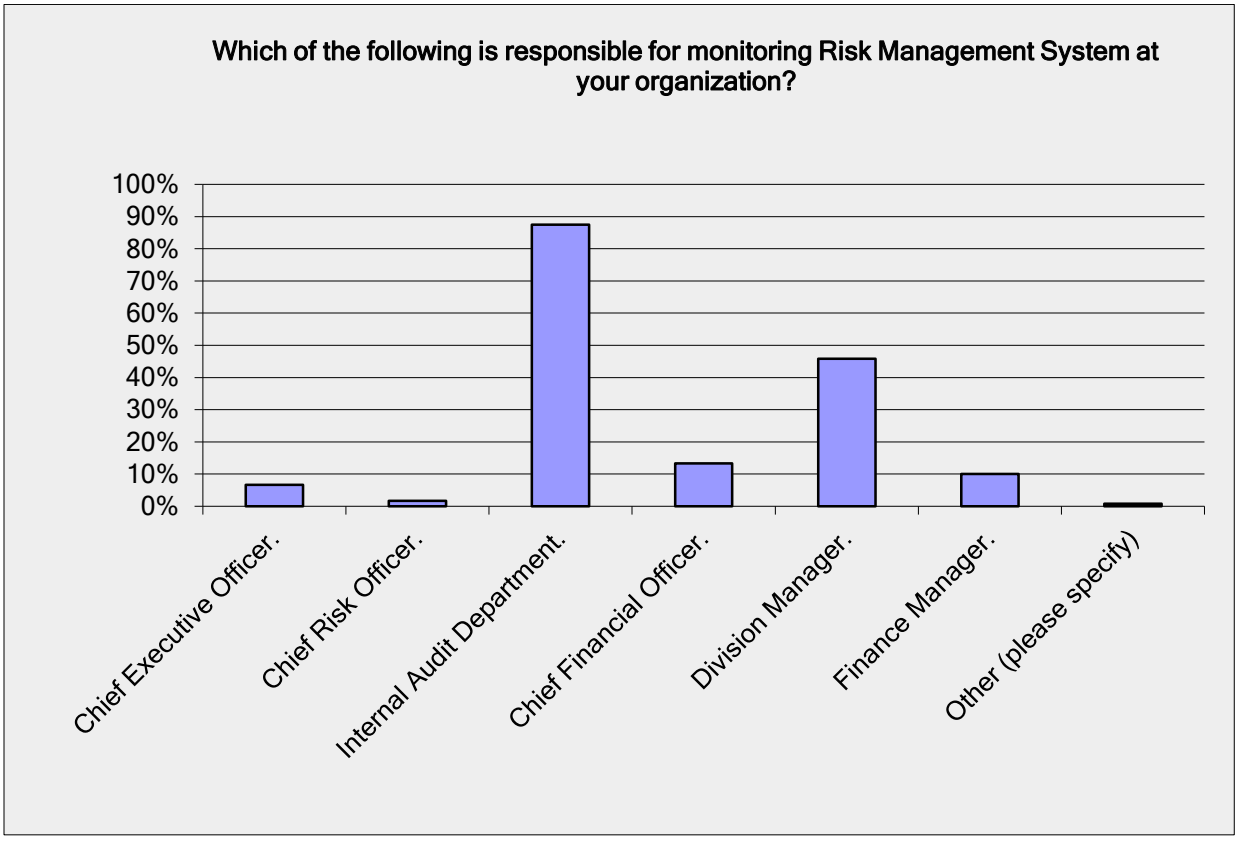


6. In which of the following risk management implementation process has your organization engaged outside parties?		
Answer Options	**Response Percent**	**Response Count**
Risk strategy set up	4.2%	5
Risk Identification	3.3%	4
Risk Assessment	5.8%	7
Risk Mitigation	0.8%	1
Control and monitor Risks	1.7%	2
None of the above	90.8%	109
	answered question	120
	skipped question	2



7. Which of the following is responsible for monitoring Risk Management System at your organization?		
Answer Options	**Response Percent**	**Response Count**
Chief Executive Officer	6.7%	8
Chief Risk Officer	1.7%	2
Internal Audit Department	87.5%	105
Chief Financial Office	13.3%	16
Division Manager	45.8%	55
Finance Manager	10.0%	12
Other (please specify)	0.8%	1
	answered question	120
	skipped question	2

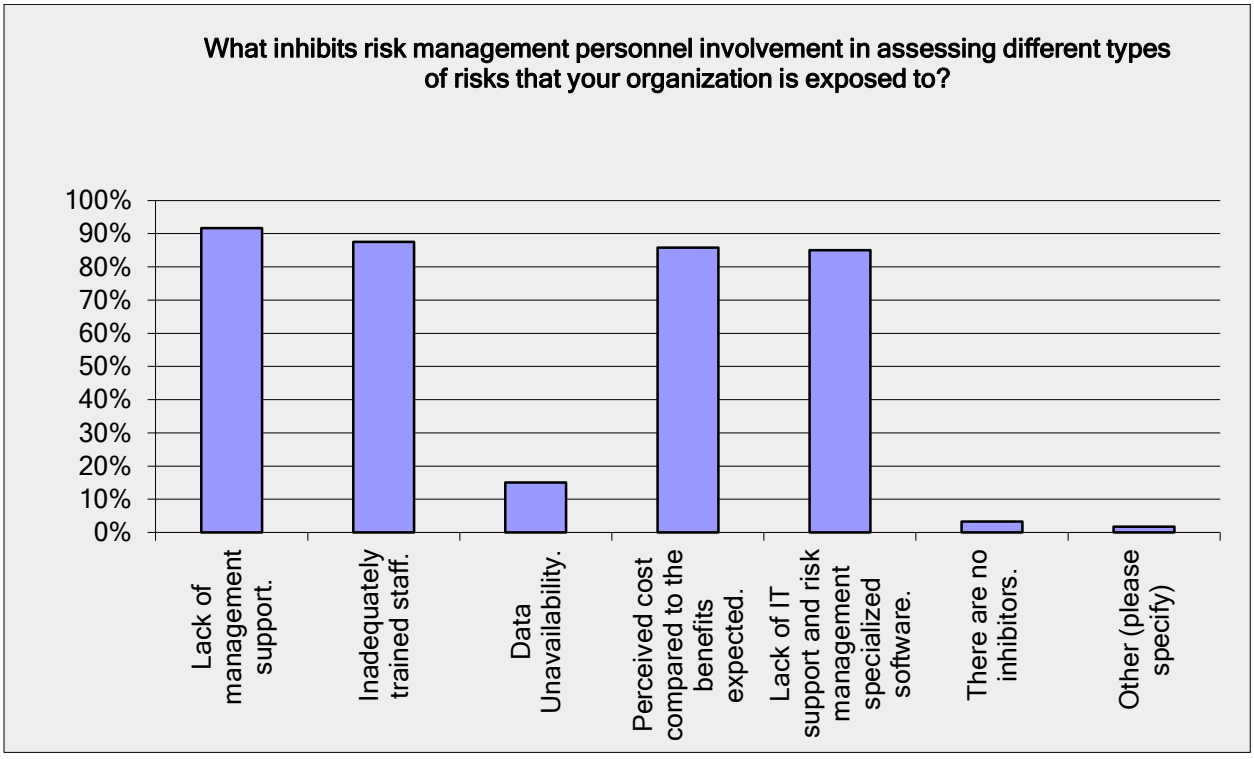
Number	Response Date	Other (please specify)	Categories
1		none	



8. What inhibits risk management personnel involvement in assessing different types of risks that your organization is exposed to?

Answer Options	Response Percent	Response Count
Lack of management support.	91.7%	110
Inadequately trained staff.	87.5%	105
Data Unavailability.	15.0%	18
Perceived cost compared to the benefits expected.	85.8%	103
Lack of IT support and risk management specialized software.	85.0%	102
There are no inhibitors.	3.3%	4
Other (please specify)	1.7%	2
	answered question	120
	skipped question	2

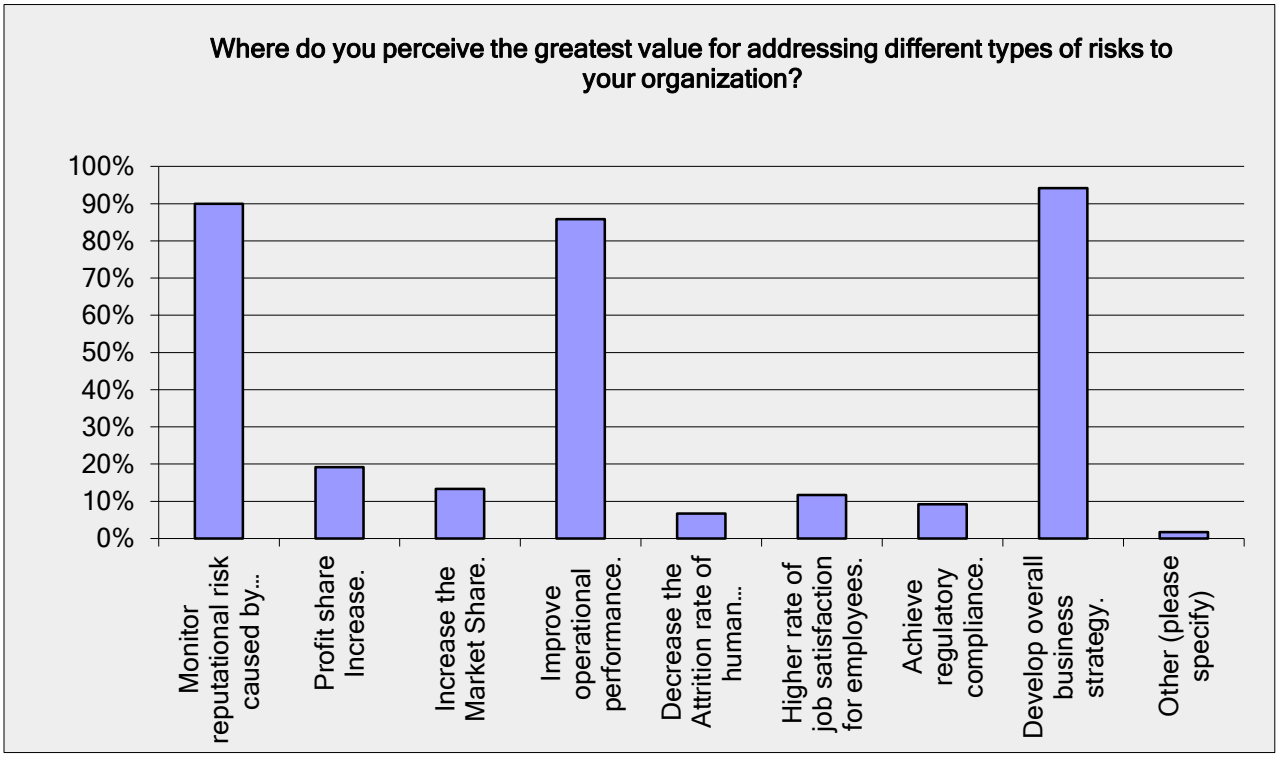
Number	Response Date	Other (please specify)	Categories
1		Poor qualifications and experience absence by the controller	
2		Now aware about the answer.	



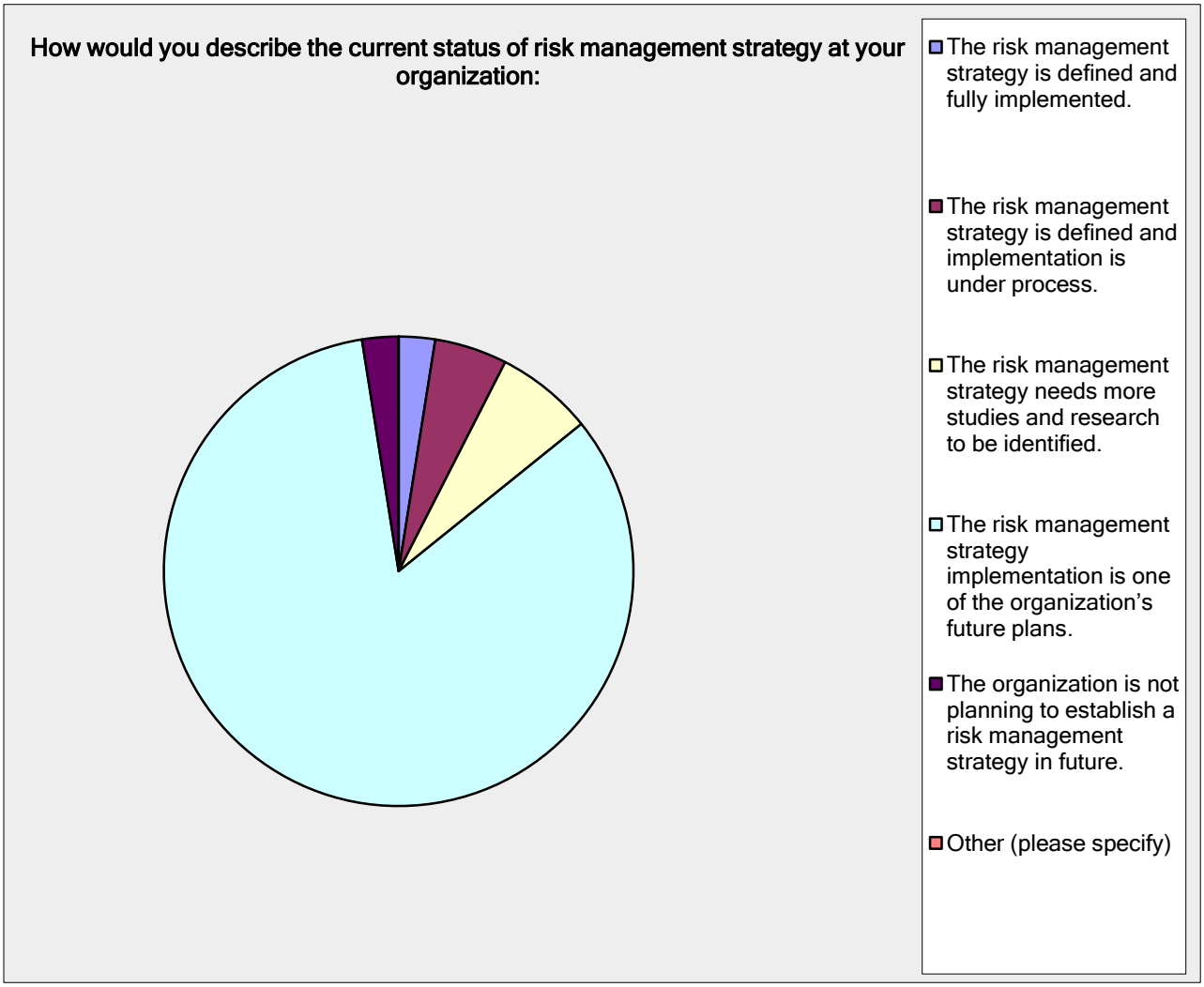
9. Where do you perceive the greatest value for addressing different types of risks to your organization?

Answer Options	Response Percent	Response Count
Monitor reputational risk caused by Quality of products or service provided.	90.0%	108
Profit share Increase.	19.2%	23
Increase the Market Share.	13.3%	16
Improve operational performance.	85.8%	103
Decrease the Attrition rate of human resources.	6.7%	8
Higher rate of job satisfaction for employees.	11.7%	14
Achieve regulatory compliance.	9.2%	11
Develop overall business strategy.	94.2%	113
Other (please specify)	1.7%	2
	answered question	120
	skipped question	2

Number	Response Date	Other (please specify)	Categories
1		Avoidance of unexpected hits in the bottom line	
2		All of the above are essential.	



10. How would you describe the current status of risk management strategy at your organization?		
Answer Options	**Response Percent**	**Response Count**
The risk management strategy is defined and fully implemented.	2.5%	3
The risk management strategy is defined and implementation is under process.	5.0%	6
The risk management strategy needs more studies and research to be identified.	6.7%	8
The risk management strategy implementation is one of the organization's future plans.	83.3%	100
The organization is not planning to establish a risk management strategy in future.	2.5%	3
Other (please specify)	0.0%	0
	answered question	120
	skipped question	2



- Please use the following scale of competency to rate your organization's staff while you answer the following questions:

- 1: No Knowledge
- 2: Limited Knowledge
- 3: Knowledgeable
- 4: Expert
- N/A

* <u>If you are not able to assess your staff level of competency or knowledge in a specific area, please remember to select N/A and proceed to the next question.</u>

11. Risk Management

Level of competency						
Answer Options	**No Knowledge**	**Limited Knowledge**	**Knowledgeable**	**Expert**	**N/A**	**Response Count**
Identifying and Classifying Risks	3	88	23	1	0	115
Assessing Risk: Process, Location, Transaction Level	3	90	20	1	1	115
Risk management structure development	4	90	18	2	0	114
Timelines and quality of risks' results reporting	2	91	20	1	0	114

Based on your role /organization / industry, this knowledge level is:				
Answer Options	**Adequate**	**Need Improvement**	**N/A**	**Response Count**
Identifying and Classifying Risks	13	100	2	115
Assessing Risk: Process, Location, Transaction Level	13	100	2	115
Risk management structure development	12	99	3	114
Timelines and quality of risks' results reporting	11	101	2	114

	Question Totals
answered question	**115**
skipped question	**7**

12. Audit Process						
Level of competency						
Answer Options	**No Knowledge**	**Limited Knowledge**	**Knowledgeable**	**Expert**	**N/A**	**Response Count**
Audit Planning: Entity Level	1	29	83	2	0	115
Conducting Opening / Closing Meetings	0	30	83	2	0	115
Continuous Monitoring	0	47	66	2	0	115
Data Analysis Tools	0	67	45	3	0	115
Operational Auditing: Cost Effectiveness/Cost Reduction	0	66	47	2	0	115
Report Writing	1	58	53	2	1	115

Based on your role /organization / industry, this knowledge level is:				
Answer Options	**Adequate**	**Need Improvement**	**N/A**	**Response Count**
Audit Planning: Entity Level	61	53	1	115
Conducting Opening / Closing Meetings	61	52	2	115
Continuous Monitoring	31	83	1	115
Data Analysis Tools	26	88	1	115
Operational Auditing: Cost Effectiveness/Cost Reduction	25	89	1	115
Report Writing	29	83	2	114

	Question Totals
answered question	**115**
skipped question	**7**

13. Procurement						
Level of competency						
Answer Options	**No Knowledge**	**Limited Knowledge**	**Knowledgeable**	**Expert**	**N/A**	**Response Count**
Contracts and Vendors Management	1	55	54	4	1	115
Receiving and Inspection	0	44	67	3	1	115
Monitoring Supplier Performance	1	55	55	3	1	115
Managing Third-Party Arrangements (e.g. resellers, wholesalers, contract manufacturers, licensees, etc.)	1	54	55	3	2	115
Annual budget reporting	0	59	50	5	1	115

Based on your role /organization / industry, this knowledge level is:				
Answer Options	**Adequate**	**Need Improvement**	**N/A**	**Response Count**
Contracts and Vendors Management	30	83	2	115
Receiving and Inspection	40	73	2	115
Monitoring Supplier Performance	29	84	2	115
Managing Third-Party Arrangements (e.g. resellers, wholesalers, contract manufacturers, licensees, etc.)	30	82	3	115
Annual budget reporting	28	85	2	115

	Question Totals
answered question	**115**
skipped question	**7**

14. Inventory						
Level of competency						
Answer Options	No Knowledge	Limited Knowledge	Knowledgeable	Expert	N/A	Response Count
Inventory Management and Planning (e.g. optimal order quantity, reorder points, etc.)	1	44	65	3	2	115
Scrap and recycling	0	44	67	2	2	115
Valuation (e.g.,FIFO, LIFO, W.A.)	0	55	56	2	2	115

Based on your role /organization / industry, this knowledge level is:				
Answer Options	Adequate	Need Improvement	N/A	Response Count
Inventory Management and Planning (e.g. optimal order quantity, reorder points, etc.)	37	74	3	114
Scrap and recycling	41	71	3	115
Valuation (e.g.,FIFO, LIFO, W.A.)	32	80	3	115

	Question Totals
answered question	115
skipped question	7

15. Production						
Level of competency						
Answer Options	No Knowledge	Limited Knowledge	Knowledgeable	Expert	N/A	Response Count
Cost Reduction Techniques	1	51	59	3	1	115
Production Output Reporting	1	37	74	2	1	115
Efficiency of leading a production line	0	40	71	3	1	115
Quality Standards	0	37	73	4	1	115

Based on your role /organization / industry, this knowledge level is:				
Answer Options	Adequate	Need Improvement	N/A	Response Count
Cost Reduction Techniques	27	86	2	115
Production Output Reporting	38	75	2	115
Efficiency of leading a production line	37	76	2	115
Quality Standards	33	79	2	114

	Question Totals
answered question	115
skipped question	7

16. Sales						
Level of competency						
Answer Options	No Knowledge	Limited Knowledge	Knowledgeable	Expert	N/A	Response Count
Future Sales Forecasting	0	53	57	3	2	115
Areas of items demand	0	51	59	3	2	115
Competitors sales distribution techniques	1	52	57	3	2	115
After-sales services	0	38	71	3	3	115

Based on your role /organization / industry, this knowledge level is:				
Answer Options	Adequate	Need Improvement	N/A	Response Count
Future Sales Forecasting	27	85	3	115
Areas of items demand	28	84	3	115
Competitors sales distribution techniques	28	84	3	115
After-sales services	45	66	4	115

	Question Totals
answered question	115
skipped question	7

Bibliography

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management – Integrated Framework*, September 2004, www.coso.org, New York, NY.

Duncan Galloway and Rick Funston (2000), VOL 8 NO 6 of Deloitte & Touche: The challenges of enterprise risk management.

Steve G. Sutton (2006): Extended-enterprise systems' impact on enterprise risk management.

Andre Brodeur and Gunnar Pritsch (Sep 2008), No 2: Making risk management a value-adding function in the board room.

Priscilla Burnaby and Susan Hass (Jun 2008): Ten steps to enterprise-wide risk management.

Robert Schneier and Jerry Miccolis (1998): Enterprise Risk Management – Strategy & Leadership.

Steve Strongin and Melanie Petsch (1999): The Journal of Risk Finance, Creating Shareholder Value: Turning Risk Management into a Competitive Advantage.

Robert Ceske, Jose V. Hernandez and Luis (2000): The Journal of Risk Finance, Quantifying Event Risk: The Next Convergence.

Michael Power (2004), Vol.5 No. 3: The Risk Management of Everything.

Andre Brodeur, Kevin Buehler, Michael Patsalos-Fox and Martin Pergler (Feb 2010), McKinsey & Company: A Broad Perspective on Enterprise Risk Management.

Committee of Sponsoring Organizations of the Treadway Commission (COSO), Effective Enterprise Risk Management Oversight: The Role of the Board of Directors, 2009.

Patchin Curtis and Mark Carey, Deloitte & Touche (COSO - Oct 2012): Risk Assessment in Practice.

Mark S. Beasley, Bruce C. Branson and Bonnie V. Hancock (COSO - Dec 2010): How Key Risk Indicators can Sharpen Focus on Emerging Risks.
Mark L. Frigo and Richard J. Anderson (COSO - Jan 2011): Practical Approaches for Getting Started.

Protiviti Inc. (Jan 2006): Guide to Enterprise Risk Management.

Donald Pagach and Richard Warr (Aug 2007): An Empirical Investigation of the Characteristics of Firms Adopting Enterprise Risk Management.

Institute of Management Accountants (2011): Enterprise Risk Management: Frameworks, Elements and Integration.

Larry Rittenberg and Frank Martens (COSO - Jan 2012): Understanding and Communicating Risk Appetite.

ICAEW (Oct 2011): Reporting Business Risks: Meeting Expectations.

Institute of Management Accountants (2007): Enterprise Risk Management: Tools and Techniques for Effective Implementation.

Christopher L. Culp, Vol.14, No 4 (2002), Journal of Applied Corporate Finance: The Revolution in Corporate Risk Management: A Decade of Innovations in Process and Products.

KPMG (Nov 2001): Enterprise Risk Management, an Emerging Model for Building Shareholders Value.

Ahmad Rizal Razali and Izah Mohd Tahir, Vol.1, No.5, (Nov 2011): Review of the Literature on Enterprise Risk Management.

Casualty Actuarial Society – Enterprise Risk Management Committee (May 2003): Overview of Enterprise Risk Management.

Australian Transaction Reportsand Analysis Centre (2006), Risk Management:
A tool for small-to-medium sized businesses.

The Institute of Internal Auditors, SARBANES-OXLEY SECTION 404, 2nd Edition, January 2008: A Guide for Management by Internal Controls Practitioners.

Robert E. Hoyt and Andre P. Liebenberg: The Value of Enterprise Risk Management.

Robert J. Chapman Simple Tools and Techniques for Enterprise Risk Management, 2006.

John Fraser and Betty J. Simkins Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives, 2010.