A

Seminar report

On

Risk Management

Submitted in partial fulfillment of the requirement for the award of degree
Of MBA

SUBMITTED TO:

www.studymafia.org

SUBMITTED BY:

www.studymafia.org

Preface

I have made this report file on the topic **Risk Management**; I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to ……..who assisting me throughout the preparation of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

Acknowledgement

I would like to thank respected Mr…….. and Mr. ……..for giving me such a wonderful opportunity to expand my knowledge for my own branch and giving me guidelines to present a seminar report. It helped me a lot to realize of what we study for.

Secondly, I would like to thank my parents who patiently helped me as i went through my work and helped to modify and eliminate some of the irrelevant or un-necessary stuffs.

Thirdly, I would like to thank my friends who helped me to make my work more organized and well-stacked till the end.

Next, I would thank Microsoft for developing such a wonderful tool like MS Word. It helped my work a lot to remain error-free.

Last but clearly not the least, I would thank The Almighty for giving me strength to complete my report on time.

Content

Introduction

In ideal risk management, a prioritization process is followed whereby the risks with the greatest loss (or impact) and the greatest probability of occurring are handled first, and risks with lower probability of occurrence and lower loss are handled in descending order. In practice the process of assessing overall risk can be difficult, and balancing resources used to mitigate between risks with a high probability of occurrence but lower loss versus a risk with high loss but lower probability of occurrence can often be mishandled.

> Intangible risk management identifies a new type of a risk that has a 100% probability of occurring but is ignored by the organization due to a lack of identification ability. For example, when deficient knowledge is applied to a situation, a knowledge risk materializes. Relationship risk appears when ineffective collaboration occurs. Process-engagement risk may be an issue when ineffective operational procedures are applied. These risks directly reduce the productivity of knowledge workers, decrease cost-effectiveness, profitability, service, quality, reputation, brand value, and earnings quality. Intangible risk management allows risk management to create immediate value from the identification and reduction of risks that reduce productivity.

Risk management also faces difficulties in allocating resources. This is the idea of opportunity cost. Resources spent on risk management could have been spent on more profitable activities. Again, ideal risk management minimizes spending (or manpower or other resources) and also minimizes the negative effects of risks.

Why do Risk Management?

The purpose of risk management is to:

- Identify possible risks.
- Reduce or allocate risks.
- Provide a rational basis for better decision making in regards to all risks.
- Plan.

Assessing and managing risks is the best weapon you have against project catastrophes. By evaluating your plan for potential problems and developing strategies to address them, you'll improve your chances of a successful, if not perfect, project.

Additionally, continuous risk management will:

- Ensure that high priority risks are aggressively managed and that all risks are cost-effectively managed throughout the project.

- Provide management at all levels with the information required to make informed decisions on issues critical to project success.

If you don't actively attack risks, they will actively attack you!!

How to do Risk Management

First we need to look at the various sources of risks. There are many sources and this list is not meant to be inclusive, but rather, a guide for the initial brainstorming of all risks. By referencing this list, it helps the team determine all possible sources of risk.

Various sources of risk include:

Project Management

- Top management not recognizing this activity as a project
- Too many projects going on at one time
- Impossible schedule commitments
- No functional input into the planning phase
- No one person responsible for the total project
- Poor control of design changes
- Problems with team members.
- Poor control of customer changes
- Poor understanding of the project manager's job
- Wrong person assigned as project manager
- No integrated planning and control
- Organization's resources are overcommitted
- Unrealistic planning and scheduling
- No project cost accounting ability
- Conflicting project priorities
- Poorly organized project office

- **External**
  - Unpredictable
    - Unforeseen regulatory requirements
    - Natural disasters
    - Vandalism, sabotage or unpredicted side effects
  - Predictable
    - Market or operational risk
    - Social
    - Environmental
    - Inflation
    - Currency rate fluctuations
    - Media
  - Technical
    - Technology changes
    - Risks stemming from design process
  - Legal
    - Violating trade marks and licenses
    - Sued for breach of contract
    - Labour or workplace problem
    - Litigation due to tort law
    - Legislation

Principles of risk management

The International Organization for Standardization (ISO) identifies the following principles of risk management:

Risk management should:

- create value – resources expended to mitigate risk should be less than the consequence of inaction, or (as in value engineering), the gain should exceed the pain
- be an integral part of organizational processes
- be part of decision making process
- explicitly address uncertainty and assumptions
- be systematic and structured process
- be based on the best available information
- be tailorable
- take human factors into account
- be transparent and inclusive
- be dynamic, iterative and responsive to change
- be capable of continual improvement and enhancement
- be continually or periodically re-assessed

Process

According to the standard ISO 31000 "Risk management – Principles and guidelines on implementation,"[4] the process of risk management consists of several steps as follows:

Establishing the context

This involves:

1. identification of risk in a selected domain of interest
2. planning the remainder of the process
3. mapping out the following:
    - the social scope of risk management
    - the identity and objectives of stakeholders
    - the basis upon which risks will be evaluated, constraints.
4. defining a framework for the activity and an agenda for identification
5. developing an analysis of risks involved in the process
6. mitigation or solution of risks using available technological, human and organizational resources.

Identification

After establishing the context, the next step in the process of managing risk is to identify potential risks. Risks are about events that, when triggered, cause problems or benefits. Hence, risk identification can start with the source of our problems and those of our competitors (benefit), or with the problem itself.

- Source analysis[*citation needed*] - Risk sources may be internal or external to the system that is the target of risk management (use mitigation instead of management since by its own definition risk deals with factors of decision-making that cannot be managed).

Examples of risk sources are: stakeholders of a project, employees of a company or the weather over an airport.

- Problem analysis- Risks are related to identified threats. For example: the threat of losing money, the threat of abuse of confidential information or the threat of human errors, accidents and casualties. The threats may exist with various entities, most important with shareholders, customers and legislative bodies such as the government.

When either source or problem is known, the events that a source may trigger or the events that can lead to a problem can be investigated. For example: stakeholders withdrawing during a project may endanger funding of the project; confidential information may be stolen by employees even within a closed network; lightning striking an aircraft during takeoff may make all people on board immediate casualties.

The chosen method of identifying risks may depend on culture, industry practice and compliance. The identification methods are formed by templates or the development of templates for identifying source, problem or event. Common risk identification methods are:

- Objectives-based risk identification- Organizations and project teams have objectives. Any event that may endanger achieving an objective partly or completely is identified as risk.
- Scenario-based risk identification - In scenario analysis different scenarios are created. The scenarios may be the alternative ways to achieve an objective, or an analysis of the interaction of forces in, for example, a market or battle. Any event that triggers an undesired scenario alternative is identified as risk – see Futures Studies for methodology used by Futurists.
- Taxonomy-based risk identification - The taxonomy in taxonomy-based risk identification is a breakdown of possible risk sources. Based on the taxonomy and knowledge of best practices, a questionnaire is compiled. The answers to the questions reveal risks.
- Common-risk checking- In several industries, lists with known risks are available. Each risk in the list can be checked for application to a particular situation.
- Risk charting - This method combines the above approaches by listing resources at risk, threats to those resources, modifying factors which may increase or decrease the risk and consequences it is wished to avoid. Creating a matrix under these headings enables a variety of approaches. One can begin with resources and consider the threats they are exposed to and the consequences of each. Alternatively one can start with the threats and examine which resources they would affect, or one can begin with the consequences and determine which combination of threats and resources would be involved to bring them about.

Assessment

Main article: risk assessment

Once risks have been identified, they must then be assessed as to their potential severity of impact (generally a negative impact, such as damage or loss) and to the probability of occurrence. These quantities can be either simple to measure, in the case of the value of a lost building, or impossible to know for sure in the case of the probability of an unlikely event occurring. Therefore, in the assessment process it is critical to make the best educated decisions in order to properly prioritize the implementation of the risk management plan.

Even a short-term positive improvement can have long-term negative impacts. Take the "turnpike" example. A highway is widened to allow more traffic. More traffic capacity leads to greater development in the areas surrounding the improved traffic capacity. Over time, traffic thereby increases to fill available capacity. Turnpikes thereby need to be expanded in a seemingly endless cycles. There are many other engineering examples where expanded capacity (to do any function) is soon filled by increased demand. Since expansion comes at a cost, the resulting growth could become unsustainable without forecasting and management.

The fundamental difficulty in risk assessment is determining the rate of occurrence since statistical information is not available on all kinds of past incidents. Furthermore, evaluating the severity of the consequences (impact) is often quite difficult for intangible assets. Asset valuation is another question that needs to be addressed. Thus, best educated opinions and available statistics are the primary sources of information. Nevertheless, risk assessment should produce such information for the management of the organization that the primary risks are easy to understand and that the risk management decisions may be prioritized. Thus, there have been several theories and attempts to quantify risks. Numerous different risk formulae exist, but perhaps the most widely accepted formula for risk quantification is:

> Rate (or probability) of occurrence multiplied by the impact of the event equals risk magnitude.

Composite risk index

The above formula can also be re-written in terms of a Composite Risk Index, as follows:

Composite Risk Index = Impact of Risk event x Probability of Occurrence

The impact of the risk event is commonly assessed on a scale of 1 to 5, where 1 and 5 represent the minimum and maximum possible impact of an occurrence of a risk (usually in terms of financial losses). However, the 1 to 5 scale can be arbitrary and need not be on a linear scale.

The probability of occurrence is likewise commonly assessed on a scale from 1 to 5, where 1 represents a very low probability of the risk event actually occurring while 5 represents a very high probability of occurrence. This axis may be expressed in either mathematical terms (event occurs once a year, once in ten years, once in 100 years etc.) or may be expressed in "plain English" (event has occurred here very often; event has been known to occur here; event has been known to occur in the industry etc.). Again, the 1 to 5 scale can be arbitrary or non-linear depending on decisions by subject-matter experts.

The Composite Index thus can take values ranging (typically) from 1 through 25, and this range is usually arbitrarily divided into three sub-ranges. The overall risk assessment is then Low, Medium or High, depending on the sub-range containing the calculated value of the Composite Index. For instance, the three sub-ranges could be defined as 1 to 8, 9 to 16 and 17 to 25.

Note that the probability of risk occurrence is difficult to estimate, since the past data on frequencies are not readily available, as mentioned above. After all, probability does not imply certainty.

Likewise, the impact of the risk is not easy to estimate since it is often difficult to estimate the potential loss in the event of risk occurrence.

Further, both the above factors can change in magnitude depending on the adequacy of risk avoidance and prevention measures taken and due to changes in the external business environment. Hence it is absolutely necessary to periodically re-assess risks and intensify/relax mitigation measures, or as necessary. Changes in procedures, technology, schedules, budgets, market conditions, political environment, or other factors typically require re-assessment of risks.

Risk options

Risk mitigation measures are usually formulated according to one or more of the following major risk options, which are:

1. Design a new business process with adequate built-in risk control and containment measures from the start.
2. Periodically re-assess risks that are accepted in ongoing processes as a normal feature of business operations and modify mitigation measures.
3. Transfer risks to an external agency (e.g. an insurance company)

4. Avoid risks altogether (e.g. by closing down a particular high-risk business area)

Later research has shown that the financial benefits of risk management are less dependent on the formula used but are more dependent on the frequency and how risk assessment is performed.

In business it is imperative to be able to present the findings of risk assessments in financial, market, or schedule terms. Robert Courtney Jr. (IBM, 1970) proposed a formula for presenting risks in financial terms. The Courtney formula was accepted as the official risk analysis method for the US governmental agencies. The formula proposes calculation of ALE (annualized loss expectancy) and compares the expected loss value to the security control implementation costs (cost-benefit analysis).

Potential risk treatments

Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories.

- Avoidance (eliminate, withdraw from or not become involved)
- Reduction (optimize – mitigate)
- Sharing (transfer – outsource or insure)
- Retention (accept and budget)

Ideal use of these strategies may not be possible. Some of them may involve trade-offs that are not acceptable to the organization or person making the risk management decisions. Another source, from the US Department of Defense (see link), Defense Acquisition University, calls these categories ACAT, for Avoid, Control, Accept, or Transfer. This use of the ACAT acronym is reminiscent of another ACAT (for Acquisition Category) used in US Defense industry procurements, in which Risk Management figures prominently in decision making and planning.

Risk avoidance

This includes not performing an activity that could carry risk. An example would be not buying a property or business in order to not take on the legal liability that comes with it. Another would be not flying in order not to take the risk that the airplane were to be hijacked. Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed. Not entering a business to avoid the risk of loss also avoids the possibility of earning profits. Increasing risk regulation in hospitals has led to avoidance of treating higher risk conditions, in favor of patients presenting with lower risk.

Hazard prevention

Main article: Hazard prevention

Hazard prevention refers to the prevention of risks in an emergency. The first and most effective stage of hazard prevention is the elimination of hazards. If this takes too long, is too costly, or is otherwise impractical, the second stage is mitigation.

Risk reduction

Risk reduction or "optimization" involves reducing the severity of the loss or the likelihood of the loss from occurring. For example, sprinklers are designed to put out a fire to reduce the risk of loss by fire. This method may cause a greater loss by water damage and therefore may not be suitable. Halon fire suppression systems may mitigate that risk, but the cost may be prohibitive as a strategy.

Acknowledging that risks can be positive or negative, optimizing risks means finding a balance between negative risk and the benefit of the operation or activity; and between risk reduction and

effort applied. By an offshore drilling contractor effectively applying HSE Management in its organization, it can optimize risk to achieve levels of residual risk that are tolerable.

Modern software development methodologies reduce risk by developing and delivering software incrementally. Early methodologies suffered from the fact that they only delivered software in the final phase of development; any problems encountered in earlier phases meant costly rework and often jeopardized the whole project. By developing in iterations, software projects can limit effort wasted to a single iteration.

Outsourcing could be an example of risk reduction if the outsourcer can demonstrate higher capability at managing or reducing risks. For example, a company may outsource only its software development, the manufacturing of hard goods, or customer support needs to another company, while handling the business management itself. This way, the company can concentrate more on business development without having to worry as much about the manufacturing process, managing the development team, or finding a physical location for a call center.

Risk sharing

Briefly defined as "sharing with another party the burden of loss or the benefit of gain, from a risk, and the measures to reduce a risk."

The term of 'risk transfer' is often used in place of risk sharing in the mistaken belief that you can transfer a risk to a third party through insurance or outsourcing. In practice if the insurance company or contractor go bankrupt or end up in court, the original risk is likely to still revert to the first party. As such in the terminology of practitioners and scholars alike, the purchase of an insurance contract is often described as a "transfer of risk." However, technically speaking, the buyer of the contract generally retains legal responsibility for the losses "transferred", meaning that insurance may be described more accurately as a post-event compensatory mechanism. For example, a personal injuries insurance policy does not transfer the risk of a car accident to the insurance company. The risk still lies with the policy holder namely the person who has been in the accident. The insurance policy simply provides that if an accident (the event) occurs involving the policy holder then some compensation may be payable to the policy holder that is commensurate with the suffering/damage.

Some ways of managing risk fall into multiple categories. Risk retention pools are technically retaining the risk for the group, but spreading it over the whole group involves transfer among individual members of the group. This is different from traditional insurance, in that no premium is exchanged between members of the group up front, but instead losses are assessed to all members of the group.

Risk retention

Involves accepting the loss, or benefit of gain, from a risk when it occurs. True self insurance falls in this category. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not

avoided or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible. War is an example since most property and risks are not insured against war, so the loss attributed by war is retained by the insured. Also any amounts of potential loss (risk) over the amount insured is retained risk. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

Risk management plan

Main article: Risk management plan

Select appropriate controls or countermeasures to measure each risk. Risk mitigation needs to be approved by the appropriate level of management. For instance, a risk concerning the image of the organization should have top management decision behind it whereas IT management would have the authority to decide on computer virus risks.

The risk management plan should propose applicable and effective security controls for managing the risks. For example, an observed high risk of computer viruses could be mitigated by acquiring and implementing antivirus software. A good risk management plan should contain a schedule for control implementation and responsible persons for those actions.

According to ISO/IEC 27001, the stage immediately after completion of the risk assessment phase consists of preparing a Risk Treatment Plan, which should document the decisions about how each of the identified risks should be handled. Mitigation of risks often means selection of security controls, which should be documented in a Statement of Applicability, which identifies which particular control objectives and controls from the standard have been selected, and why.

Implementation

Implementation follows all of the planned methods for mitigating the effect of the risks. Purchase insurance policies for the risks that have been decided to be transferred to an insurer, avoid all risks that can be avoided without sacrificing the entity's goals, reduce others, and retain the rest.

Review and evaluation of the plan

Initial risk management plans will never be perfect. Practice, experience, and actual loss results will necessitate changes in the plan and contribute information to allow possible different decisions to be made in dealing with the risks being faced.

Risk analysis results and management plans should be updated periodically. There are two primary reasons for this:

1. to evaluate whether the previously selected security controls are still applicable and effective

2. to evaluate the possible risk level changes in the business environment. For example, information risks are a good example of rapidly changing business environment.

Types

Enterprise Risk

Enterprise risk management (ERM) is a framework to reduce earnings volatility through a robust risk governance structure and strong risk culture, supported by sound risk management capabilities. It is the organization's enterprise risk competence—the ability to understand, control, and articulate the nature and level of risks taken in pursuit of business strategies—coupled with accountability for risks taken and activities engaged in, which contributes to increased confidence shown by stakeholders.

Credit Risk

In the past, managing the credit portfolio was considered good risk management. But in today's broader, more complex environment, best-practice institutions understand that they need to measure and manage risk across the entire enterprise. We recognize that managing credit risk is essential to enterprise-wide risk management, so we offer products and services to institutions and individuals involved in retail, commercial, and corporate credit risk. RMA is the premier provider of commercial credit education and information.

Market Risk

RMA serves market risk practitioners at both the larger-institution and smaller-institution levels.

For larger institutions—where market risk management and its related technologies are well known and mature—RMA provides peer sharing and professional development opportunities through round tables in North America and Europe. RMA also undertakes surveys, benchmarking studies, and best practice papers.

For smaller institutions—where the market risk function is part of the asset/liability management process—RMA offers beneficial training through both open-enrollment and Web-based courses. The RMA Journal® also regularly carries articles on market-risk-related topics.

Operational Risk

Operational risks exist in every financial organization, regardless of its size, in any number of forms including hurricanes, blackouts, computer hacking, and organized fraud. Managing those risks—however big or small—is critical to an organization's success.

Advantages of Risk Management

- First: **the awareness of possible threats.** This also includes identification of possible loss of assets. In that way, the company can have back up funds in case they lose an asset.
- The manager can also highlight how easier it will be to determine if a system can still operate in case these threats occur.
- Risk management can also transform threats into a **threshold to new opportunities**.
- When a threat occurs, it's important for all departments to come together and deal with it. **Risk management prevents a department from isolation.** Everyone is involved because everyone is aware. Imagine the impact a company will have to their clients if they show oneness in the midst of perplexity.

Disadvantages of Risk Management

- **Cost.** This module will shell out cash from the company funds. Companies will have to improve their cash generating tactics in order to provide means for training and maintenance for something that hasn't happened yet.
- **Training.** The time spent for development and research will have to be allocated for training to ensure proper execution of risk management.
- **Motivation.** Employees that are already accustomed to their mundane activities need to adjust to new measures.

References

- www.google.com
- www.wikipedia.com
- www.studymafia.org