Student: Houssam Hajar_____ ID:_UM4666BBA10498

# financial risk management

**Risk management** is the human activity which integrates recognition of risk, risk assessment, developing strategies to manage it, and mitigation of risk using managerial resources.

The strategies include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk.

Some traditional risk managements are focused on risks stemming from physical or legal causes (e.g. natural disasters or fires, accidents, death and lawsuits). Financial risk management, on the other hand, focuses on risks that can be managed using traded financial instruments.

Objective of *risk management* is to reduce different risks related to a pre-selected domain to the level accepted by society. It may refer to numerous types of threats caused by environment, technology, humans, organizations and politics. On the other hand it involves all means available for humans, or in particular, for a risk management entity (person, staff, organization).

# Contents

## Some Explanations

In ideal risk management, a prioritization process is followed whereby the risks with the greatest loss 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 can be very difficult, and balancing 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 risk - 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 materialises. 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 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 while maximizing the reduction of the negative effects of risks.

# Steps in the risk management process

### Establish the context

Establishing the context involves

0. Identification of risk in a selected domain of interest

1. **Planning** the remainder of the process.

2. **Mapping out** the following: the social scope of risk management, the identity and objectives of stakeholders, and the basis upon which risks will be evaluated, constraints.

3. **Defining a framework** for the activity and an agenda for identification.

4. **Developing an analysis** of risks involved in the process.

5. Mitigation 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. Hence, risk identification can start with the source of problems, or with the problem itself.

- **Source analysis** Risk sources may be internal or external to the system that is the target of risk management. 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 privacy information or the threat of 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; privacy information may be stolen by employees even within a closed network; lightning striking a Boeing 747 during takeoff may make all people onboard 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. Objective-based risk identification is at the basis of COSO's Enterprise Risk Management - Integrated Framework
- **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. Taxonomy-based risk identification in software industry can be found in CMU/SEI-93-TR-6.
- **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. An example of known risks in the software industry is the Common Vulnerability and Exposures list found at http://cve.mitre.org.
- **Risk Charting** This method combines the above approaches by listing Resources at risk, Threats to those resources Modifying Factors which may increase or reduce 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

Once risks have been identified, they must then be assessed as to their potential severity of 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 guesses possible in order to properly prioritize the implementation of the risk management plan.

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 immaterial 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 of occurrence** multiplied by the **impact of the event** equals **risk**

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 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 (annualised 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: (Dorfman, 1997) (remember as 4 T's)

- **Tolerate** (aka **retention**)
- **Treat** (aka **mitigation**)
- **Terminate** (aka **elimination**)
- **Transfer** (aka **buying insurance**)

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 Defense Acquisition University, calls this ACAT, for Accept, Control, Avoid, and Transfer. The ACAT acronym is reminiscent of the term ACAT (for Acquisition Category) used in US Defense industry procurements.

### Risk avoidance

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 liability that comes with it. Another would be not flying in order to not 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.

**Risk reduction**

Involves methods that reduce the severity of the loss. Examples include sprinklers 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.

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. A current trend in software development, spearheaded by the Extreme Programming community, is to reduce the size of iterations to the smallest size possible, sometimes as little as one week is allocated to an iteration.

**Risk retention**

Involves accepting the loss 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 transfer**

Means causing another party to accept the risk, typically by contract or by hedging. Insurance is one type of risk transfer that uses contracts. Other times it may involve contract language that transfers a risk to another party without the payment of an insurance premium. Liability among construction or other contractors is very often transferred this way. On the other hand, taking offsetting positions in derivatives is typically how firms use hedging to financially manage risk.

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.

Outsourcing is another example of Risk transfer where companies outsource IT,BPO,KPO etc. In IT, some companies will outsource only development work and product is made at offshore locations where as business requirements are handled at onshore/client site. This way, companies can concentrate more on business development rather than managing large group of IT development team.

### Create a risk mitigation plan

Select appropriate controls or countermeasures to measure each risk. Risk mitigation needs to be approved by the appropriate level of management. For example, 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 anti virus 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

Follow 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, and
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.

## Limitations

If risks are improperly assessed and prioritized, time can be wasted in dealing with risk of losses that are not likely to occur. Spending too much time assessing and

managing unlikely risks can divert resources that could be used more profitably. Unlikely events do occur but if the risk is unlikely enough to occur it may be better to simply retain the risk and deal with the result if the loss does in fact occur.

Prioritizing too highly the *risk management processes* could keep an organization from ever completing a project or even getting started. This is especially true if other work is suspended until the risk management process is considered complete.

It is also important to keep in mind the distinction between risk and uncertainty. Risk can be measured by impacts x probability.

# Areas of risk management

As applied to corporate finance, **risk management** is the technique for measuring, monitoring and controlling the financial or operational risk on a firm's balance sheet. See value at risk.

The Basel II framework breaks risks into market risk (price risk), credit risk and operational risk and also specifies methods for calculating capital requirements for each of these components.

## Enterprise risk management

In enterprise risk management, a risk is defined as a possible event or circumstance that can have negative influences on the Enterprise in question. Its impact can be on the very existence, the resources (human and capital), the products and services, or the customers of the enterprise, as well as external impacts on society, markets, or the environment. In a financial institution, enterprise risk management is normally thought of as the combination of credit risk, interest rate risk or asset liability management, market risk, and operational risk.

In the more general case, every probable risk can have a pre-formulated plan to deal with its possible consequences (to ensure *contingency* if the risk becomes a *liability*).

From the information above and the average cost per employee over time, or cost accrual ratio, a project manager can estimate

- the cost associated with the risk if it arises, estimated by multiplying employee costs per unit time by the estimated time lost (*cost impact, C* where *C* = *cost accrual ratio* * *S*).
- the probable increase in time associated with a risk (*schedule variance due to risk, Rs* where Rs = P * S):
    - Sorting on this value puts the highest risks to the schedule first. This is intended to cause the greatest risks to the project to be attempted first so that risk is minimized as quickly as possible.

    - This is slightly misleading as *schedule variances* with a large P and small S and vice versa are not equivalent. (The risk of the RMS *Titanic* sinking vs. the passengers' meals being served at slightly the wrong time).
- the probable increase in cost associated with a risk (*cost variance due to risk*, *Rc* where Rc = P*C = P*CAR*S = P*S*CAR)
    - sorting on this value puts the highest risks to the budget first.
    - see concerns about *schedule variance* as this is a function of it, as illustrated in the equation above.

Risk in a project or process can be due either to Special Cause Variation or Common Cause Variation and requires appropriate treatment. That is to re-iterate the concern about extremal cases not being equivalent in the list immediately above.

## Risk management activities as applied to project management

In project management, risk management includes the following activities:

- Planning how risk management will be held in the particular project. Plan should include risk management tasks, responsibilities, activities and budget.
- Assigning a risk officer - a team member other than a project manager who is responsible for foreseeing potential project problems. Typical characteristic of risk officer is a healthy skepticism.
- Maintaining live project risk database. Each risk should have the following attributes: opening date, title, short description, probability and importance. Optionally a risk may have an assigned person responsible for its resolution and a date by which the risk must be resolved.
- Creating anonymous risk reporting channel. Each team member should have possibility to report risk that he foresees in the project.
- Preparing mitigation plans for risks that are chosen to be mitigated. The purpose of the mitigation plan is to describe how this particular risk will be handled – what, when, by who and how will it be done to avoid it or minimize consequences if it becomes a liability.
- Summarizing planned and faced risks, effectiveness of mitigation activities and effort spend for the risk management

# Risk management and business continuity

Risk management is simply a practice of systematically selecting cost effective approaches for minimising the effect of threat realization to the organization. All risks can never be fully avoided or mitigated simply because of financial and practical limitations. Therefore all organizations have to accept some level of residual risks.

Whereas risk management tends to be pre-emptive, business continuity planning (BCP) was invented to deal with the consequences of realised residual risks. The necessity to have BCP in place arises because even very unlikely events will occur if given enough time. Risk management and BCP are often mistakenly seen as rivals or overlapping practices. In fact these processes are so tightly tied together that such separation seems artificial. For example, the risk management process creates important inputs for the BCP (assets, impact assessments, cost estimates etc). Risk management also proposes applicable controls for the observed risks. Therefore, risk management covers several areas that are vital for the BCP process. However, the BCP process goes beyond risk management's pre-emptive approach and moves on from the assumption that the disaster **will** realize at some point.

# financial risk management

Finance theory (i.e. financial economics) prescribes that a firm should take on a project when it increases shareholder value. Finance theory also shows that firm managers cannot create value for shareholders, also called its investors, by taking on project that shareholders could do for themselves at the same cost. When applied to financial risk management, this implies that firm managers should not hedge risks that investors can hedge for themselves at the same cost. This notion is captured by the hedging irrelevance proposition: *In a perfect market, the firm cannot create value by hedging a risk when the price of bearing that risk within the firm is the same as the price of bearing it outside of the firm.* In practice, financial markets are not likely to be perfect markets. This suggests that firm managers likely have many opportunities to create value for shareholders using financial risk management. The trick is to determine which risks are cheaper for the firm to manage than the shareholders. A general rule of thumb, however, is that market risks that result in unique risks for the firm are the best candidates for financial risk management.

# References


- Crockford, Neil (1986). *An Introduction to Risk Management (2nd ed.)*. Woodhead-Faulkner. 0-85941-332-2.
- Lam, James (2003). *Enterprise Risk Management: From Incentives to Controls*. John Wiley. ISBN-13 978-0471430001.

- van Deventer, Donald R., Kenji Imai and Mark Mesler (2004). *Advanced Financial Risk Management: Tools and Techniques for Integrated Credit Risk and Interest Rate Risk Management*. John Wiley. ISBN-13: 978-0470821268