Reviews of Literature
Impact Factor : 1.4716 (UIF)
Volume 2 , Issue 5 / Dec 2014 ISSN:-2347-2723

RISK MANAGEMENT

J. K. Khetiya

Principal, Shri M. J. Goriya College, Jam-Khambhaliya

Abstract:

Risk management is recognized as an essential tool tackle the inevitable uncertainty associated with business and projects at all levels. But it frequently fails to meet expectations, with projects continuing o un late, over budget under or under performing, and business not gaining the expected benefitsThe evident discount which often occurs between strategic vision and tactical project delivery typically arises from poorly defined project objectives and inadequate attention to the proactive management of risks that could affect those objectives, one of the main failings in the traditional approach to risk management arises from a narrow focus on the downside, restricted to the technical or operational field, addressing tactical threats to processes, performance or people.

This shortcoming can be overcome by widening the scope of risk management to encompass both strategy risks and upside opportunities, creating an integrated approach which can bridge the gap between strategy and tactics.

Integrated risk management addresses risks across a variety of levels in the organization, including strategy and tactics, and covering both opportunity and threat. Effective implementation of integrated risk management can produce a number of benefits to the organization which are not available from the typical limited-scope risk process.

This paper explores how to expand risk management to deliver strategic advantage while retaining its use as a tactical tool.

Keywords; Risk management , organization, including strategy and tactics.

1. Introduction

Risk management is a rapidly developing discipline and there are many and varied views and descriptions of what risk management involves, how it should be conducted and what it is for. Some form of standard is needed to ensure that there is an agreed:

- Terminology related to the woods used
- Process by which risk management can be carried out
- Organization structure for risk management
- Objective for risk management

Importantly, the standard recognizes that risk has both an upside and a downside.

Risk management is not just something for corporations or public organizations, but for any activity whether short or long term. The benefits and opportunities should be viewed not just in the context of the activity itself but in relation to the many and varied stakeholders who can be affected.

There are many ways of achieving the objectives of risk management and it would be impossible to try to set them all out in a single document. Therefore it was never intended to produce a prescriptive standard which would have led to a box ticking approach nor to establish a certifiable process. By meeting the various component parts of this standard , albeit in different ways, organizations will be in a position to report that they are in compliance. The standard represents best practice against which organizations can measure themselves.

2 Definition of 'Risk Management

Definition: In the world , risk management refers to the practice of identifying potential risks in advance, analyzing them and taking precautionary steps to reduce/curb the risk.

Description: When an entity makes an investment decision, it exposes itself to a number of financial risks. The quantum of such risks depends on the type of financial instrument. These financial risks might be in the form of high inflation, volatility in capital markets, recession, bankruptcy, etc.

So, in order to minimize and control the exposure of investment to such risks, fund managers and investors practice risk management. Not giving due importance to risk management while making investment decisions might wreak havoc on investment in times of financial turmoil in an economy. Different levels of risk come attached with different categories of asset classes.

For example, a fixed deposit is considered a less risky investment. On the other hand, investment in equity is considered a risky venture. While practicing risk management, equity investors and fund managers tend to diversify their portfolio so as to minimize the exposure to risk.

The identification, analysis, assessment, control, and avoidance, minimization, or elimination of unacceptable risks. An organization may use risk assumption, risk avoidance, risk retention, risk transfer, or any other strategy (or combination of strategies) in proper management of future events

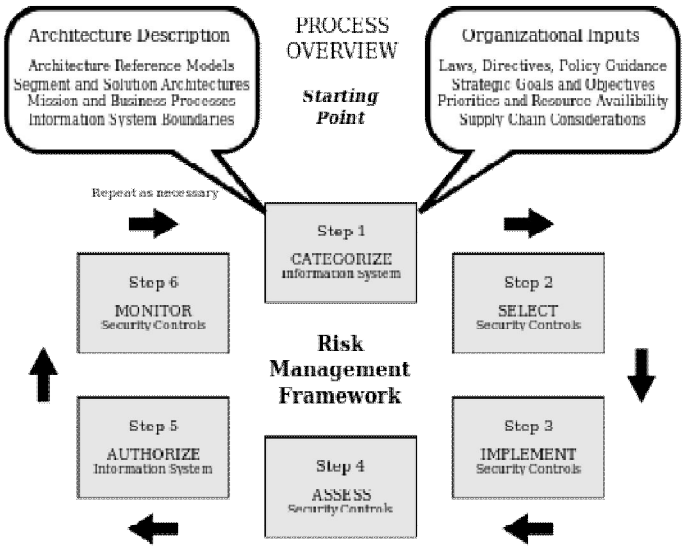
He process of identification, analysis and either acceptance or mitigation of uncertainty in investment decision-making. Essentially, risk management occurs anytime an investor or fund manager analyzes and attempts to quantify the potential for losses in an investment and then takes the appropriate action (or inaction) given their investment objectives and risk tolerance. Inadequate risk management can result in severe consequences for companies as well as individuals. For example, the recession that began in 2008 was largely caused by the loose credit risk management of financial firms.

3 Principles of risk management:

- 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
- 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

4 Process of risk management

Risk Management Framework



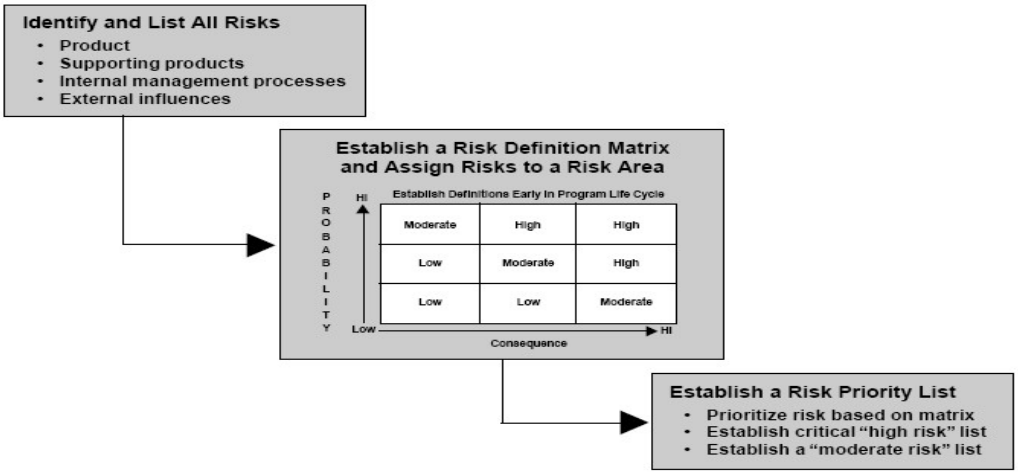
4.1 Establishing the context

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.

4.2 Identification

Risk 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 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.

4.3 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

5 Risk management strategy

A risk management strategy provides a structured and coherent approach to identifying, assessing and managing risk. It builds in a process for regularly updating and reviewing the assessment based on new developments or actions taken. A risk management strategy can be developed and implemented by even the smallest of groups or projects or built into a complex strategy for a multi-site international organization.

The process of identifying and reviewing the risks that you face is known as risk assessment. By assessing risks you are able to be actively aware of where uncertainty surrounding events or outcomes exists and identifying steps that can be taken to protect the organization, people and assets concerned. How this is achieved and the level of detail which is considered can vary between organizations. In many circumstances, where staff or volunteers have a more hands-on role in the organization, the Management Committee may not carry out the risk assessment themselves.

Example 1:
Implementing a risk management strategy in a small organization

Lone Fathers Action Group set aside one committee meeting per year to review the major risks faced by the group. One committee member has responsibility for risk management and facilitates the discussion. They ensure that the discussion is documented and use subsequent meetings to check progress against actions are then followed up in subsequent meetings. Every 6 months this committee member reports to the committee on any changes in the levels of risk faced.

Example 2:
Implementing a risk management strategy in a large organization

In Tree Conservation International, risk management is one of the key responsibilities of the Assistant Director. They provide training for each manager within the organization to ensure that risk assessment is built into their working practices and to enable them to carry out annual

risk assessments of each project, using the organization's templates. These are then collated by the Assistant Director to enable Senior Managers to discuss and assess the overall risks to the organization. A prioritized profile of the top 30 risks is then presented to the Management Committee for their consideration to ensure they are happy to accept the risks to the organization and approve the actions being taken. This process usually takes 2 months. Progress is reviewed after 6 months with a report sent to the Management Committee. Risks are reassessed annually.

6 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.

7 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

7.1 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.

7.2 Create a 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.

7.3 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.

7.4 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.

8 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.

8.1 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, liquidity risk, market risk, and operational risk.

- 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 is 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.

8.2 Risk management activities as applied to project management

Planning how risk will be managed in the particular project. Plans 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 the possibility to report risks that he/she 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 whom 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 spent for the risk management.

8.3 Risk management for mega projects

Mega projects (sometimes also called "major programs") are extremely large-scale investment projects, typically costing more than US$1 billion per project. Mega projects include bridges, tunnels, highways, railways, airports, seaports, power plants, dams, wastewater projects, coastal flood protection schemes, oil and natural gas extraction projects, public buildings, information technology systems, aerospace projects, and defense systems. Mega projects have been shown to be particularly risky in terms of finance, safety, and social and environmental impacts Risk management is therefore particularly pertinent for mega projects and special methods and special education have been developed for such risk management.

8.4 Risk management regarding natural disasters

It is important to assess risk in regard to natural disasters like floods, earthquakes, and so on. Outcomes of natural disaster risk assessment are valuable when considering future repair costs, business interruption losses and other downtime, effects on the environment, insurance costs, and the proposed costs of reducing the risk.[14] There are regular conferences in Davos to deal with integral risk management.

8.5 Risk management of information technology

Information technology is increasingly pervasive in modern life in every sector. IT risk is a risk related to information technology. This is a relatively new term due to an increasing awareness that information security is simply one facet of a multitude of risks that are relevant to IT and the real world processes it supports.

8.6 Risk management techniques in petroleum and natural gas

For the offshore oil and gas industry, operational risk management is regulated by the safety case regime in many countries. Hazard identification and risk assessment tools and techniques are described in the international standard ISO 17776:2000, and organizations such as the IADC (International Association of Drilling Contractors) publish guidelines for HSE Case development which are based on the ISO standard. Further, diagrammatic representations of hazardous events are often expected by governmental regulators as part of risk management in safety case submissions; these are known as **bow-tie** diagrams. The technique is also used by organizations and regulators in mining, aviation, health, defense, industrial and finance.[18]

8.7 Risk management as applied to the pharmaceutical sector

The principles and tools for quality risk management are increasingly being applied to different aspects of pharmaceutical quality systems. These aspects include development, manufacturing, distribution, inspection, and submission/review processes throughout the lifecycle of drug substances, drug products, biological and biotechnological products (including the use of raw materials, solvents, recipients, packaging and labeling materials in drug products,

biological and biotechnological products). Risk management is also applied to the assessment of microbiological contamination in relation to pharmaceutical products and clean room manufacturing environments.

9.Conclusion

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.

Reference:-

1. **Jump up** ^ Crockford, Neil (1986). *An Introduction to Risk Management* (2 ed.). Cambridge, UK: Woodhead-Faulkner. p. 18. ISBN 0-85941-332-2.
2. **Jump up** ^ Dorfman, Mark S. (2007). *Introduction to Risk Management and Insurance* (9 ed.). Englewood Cliffs, N.J: Prentice Hall. ISBN 0-13-224227-3.
3. **Jump up** ^ McGivern, Gerry; Fischer, Michael D. (1 February 2012). "Reactivity and reactions to regulatory transparency in medicine, psychotherapy and counselling". *Social Science & Medicine* **74** (3): 289–296. doi:10.1016/j.socscimed.2011.09.035.
4. **Jump up** ^ IADC HSE Case Guidelines for MODUs 3.2, section 4.7
5. **Jump up** ^ Roehrig, P (2006). "Bet On Governance To Manage Outsourcing Risk". *Business Trends Quarterly*.
6. **Jump up** ^ Flyvbjerg, Bent (2003). *Megaprojects and Risk: An Anatomy of Ambition*. Cambridge University Press. ISBN 0521804205.
7. **Jump up** ^ Oxford BT Centre for Major Programme Management
8. **Jump up** ^ Craig Taylor and Erik VanMarcke, ed. (2002). *Acceptable Risk Processes: Lifelines and Natural Hazards*. Reston, VA: ASCE, TCLEE. ISBN 9780784406236.
9. **Jump up** ^ Cortada, James W. (2003-12-04). *The Digital Hand: How Computers Changed the Work of American Manufacturing, Transportation, and Retail Industries*. USA: Oxford University Press. p. 512. ISBN 0-19-516588-8.
10. **Jump up** ^ Cortada, James W. (2005-11-03). *The Digital Hand: Volume II: How Computers Changed the Work of American Financial, Telecommunications, Media, and Entertainment Industries*. USA: Oxford University Press. ISBN 978-0-19-516587-6.
11. **Jump up** ^ Cortada, James W. (2007-11-06). *The Digital Hand, Vol 3: How Computers Changed the Work of American Public Sector Industries*. USA: Oxford University Press. p. 496. ISBN 978-0-19-516586-9.
12. **Jump up** ^ RPS HSE & Risk Management. BowtieXP. Retrieved on 2012-04-17.
13. **Jump up** ^ Saghee M, Sandle T, Tidswell E (editors) (2011). *Microbiology and Sterility Assurance in Pharmaceuticals and Medical Devices* (1st ed.). Business Horizons. ISBN 978-8190646741.

14. **Jump up** ^ John Adams, RISK, Routledge 1995
15. **Jump up** ^ David Hillson; Ruth Murray-Webster (30 March 2007). *Understanding and Managing Risk Attitude*. Gower Publishing, Ltd. ISBN 978-0-566-08798-1. Retrieved 17 April 2012.

J. K. Khetiya
Principal, Shri M. J. Goriya College, Jam-Khambhaliya