ignou
THE PEOPLE'S
UNIVERSITY

Indira Gandhi National Open University
School of Vocational Education and Training

MSEI-026
BCP, DR PLANNING AUDIT

Risk Analysis

1

''शिक्षा मानव को बन्धनों से मुक्त करती है और आज के युग में तो यह लोकतंत्र की भावना का आधार भी है। जन्म तथा अन्य कारणों से उत्पन्न जाति एवं वर्गगत विषमताओं को दूर करते हुए मनुष्य को इन सबसे ऊपर उठाती है।''

— इन्दिरा गांधी

"Education is a liberating force, and in our age it is also a democratising force, cutting across the barriers of caste and class, smoothing out inequalities imposed by birth and other circumstances."

– Indira Gandhi

ignou
THE PEOPLE'S
UNIVERSITY

Indira Gandhi National Open University
School of Vocational Education and Training

MSEI-026
BCP, DR Planning and Audit

Block

1

RISK ANALYSIS

Programme Expert/Design Committee of Post Graduate Diploma in Information Security (PGDIS)

Prof. K.R. Srivathsan
Pro Vice-Chancellor, IGNOU

Mr. B.J. Srinath, Sr. Director & Scientist 'G',CERT-In, Department of Information Technology, Ministry of Communication and Information Technology, Govt of India

Mr. A.S.A Krishnan, Director, Department of Information Technology, Cyber-Laws and E-Security Group, Ministry of Communication and Information Technology, Govt of India

Mr. S. Balasubramony, Dy. Superintendent of Police, CBI, Cyber Crime Investigation Cell Delhi

Mr. B.V.C. Rao, Technical Director, National Informatics Centre, Ministry of Communication and Information Technology

Prof. M.N. Doja, Professor, Department of Computer Engineering, Jamia Milia Islamia New Delhi

Dr. D.K. Lobiyal, Associate Professor, School of Computer and Systems Sciences, JNU New Delhi

Mr. Omveer Singh, Scientist, CERT-In Department of Information Technology, Cyber-Laws and E-Security Group, Ministry of Communication and Information Technology Govt of India

Dr. Vivek Mudgil, Director, Eninov Systems Noida

Mr. V.V.Subrahmanyam, Assistant Professor School of Computer and Information Science IGNOU

Mr. Anup Girdhar, CEO, Sedulity Solutions & Technologies, New Delhi

Prof. A.K. Saini, Professor, University School of Management Studies, Guru Gobind Singh Indraprastha University, Delhi

Mr. C.S. Rao, Technical Director in Cyber Security Division, National Informatics Centre Ministry of Communication and Information Technology

Prof. C.G. Naidu, Director, School of Vocational Education & Training, IGNOU

Prof. Manohar Lal, Director, School of Compute and Information Science, IGNOU

Prof. K. Subramanian, Director, ACIIL, IGNOU Former Deputy Director General, National Informatics Centre, Ministry of Communication and Information Technology, Govt of India

Prof. K. Elumalai, Director, School of Law IGNOU

Dr. A. Murali M Rao, Joint Director, Computer Division, IGNOU

Mr. P.V. Suresh, Sr. Assistant Professor School of Computer and Information Science IGNOU

Ms. Mansi Sharma, Assistant Professor, School of Law, IGNOU

Ms. Urshla Kant
Assistant Professor, School of Vocational Education & Training, IGNOU
Programme Coordinator

Block Preparation

Unit Writer	Block Editor	Proof Reading
Mr. Prince Amjad Khan Technical Architect- External Consultant, Kirk Communications Pvt. Ltd New Delhi (Unit 1, 2, 3 & 4)	Ms. Urshla Kant Assistant Professor, School of Vocational Education & Training IGNOU	Ms. Urshla Kant Assistant Professor School of Vocational Education & Training IGNOU

Production

Mr. B. Natrajan Dy. Registrar (Pub.) MPDD, IGNOU, New Delhi	Mr. Jitender Sethi Asstt. Registrar (Pub.) MPDD, IGNOU, New Delhi	Mr. Hemant Parida Proof Reader MPDD, IGNOU, New Delhi

November, 2011

Indira Gandhi National Open University, 2011

ISBN: 978-81-266-5713-1

Further information about the School of Vocational Education and Training and the Indira Gandhi National Open University courses may be obtained from the University's office at Maidan Garhi, New Delhi-110068. or the website of IGNOU www.ignou.ac.in

Printed and published on behalf of the Indira Gandhi National Open University, New Delhi, by the Registrar, MPDD

Laser typeset by Mctronics Printographics, 27/3 Ward No. 1, Opp. Mother Dairy, Mehrauli, New Delhi-30

Printed at : Young Printing Press, 2626, Gali No.7, Bihari Colony, Shahdara, [illegible] – 11 00 32.

BLOCK INTRODUCTION

This block deals with the risk analysis. In the business world, risk analysis is one of the primary tools used in the process of risk management. Within this setting, the business looks at how various operations, campaigns, and expansions are likely to impact the financial stability of the company. When the risk analysis indicates that all or most of the factors are favorable, the company moves forward with the product launch. When it comes to growing a business, risk analysis is an important part of any constructive business planning. The business assessment often includes understanding both the risks of maintaining the company in its current state as well as determining what could happen if new policies, procedures or product lines were introduced into the corporate culture. This block comprises of four units and is designed in the following way;

The **Unit one** is an effort towards answering some of the fundamental queries about Risk Analysis. The risk analysis process is an important aspect of business recovery planning. The probability of a disaster occurring in an organization is highly uncertain. Organizations should also develop written, comprehensive business recovery plans that address all the critical operations and functions of the business. The plan should include documented and tested procedures, which, if followed, will ensure the ongoing availability of critical resources and continuity of operations. A business recovery plan, however, is similar to liability insurance.

The **Unit two** provides an overview of the risk assessment which can take different approaches. It can be quantitative; i.e. it can assign numeric values to probabilities and consequences; it can be qualitative; or it can be some combination of the two. The distinction is important when it comes to applying financial analysis to decisions and priorities.

The **Unit three** covers various risk analysis techniques and methodologies which is a systematic approach to determine specific risk events and their consequences. The behavioral aspects of risk management are considered to support innovation and help to develop business. The personal bias in risk management depends on a person with his or her experience, culture, value, as well as education. The schedule risks estimates have good knowledge on sources of estimates and determine the high risk dependencies. The resource risks are determined as these risks effects the development of the project and the early identification helps to meet the project objectives on time.

The **Unit four** covers risk mitigation. Risk Mitigation is all about forecasting the possible problems that might arise in future and finding out ways to prevent it from occurring or do alternate ways to avoid the problems from happening. It also covers types of risk mitigation and also discussed different strategies for risk mitigation and to monitor the risks.

Hope you benefit from this block.

ACKNOWLEDGEMENT

The material we have used is purely for educational purposes. Every effort has been made to trace the copyright holders of material reproduced in this book. Should any infringement have occurred, the publishers and editors apologize and will be pleased to make the necessary corrections in future editions of this book.

UNIT 1 INTRODUCTION TO RISK ANALYSIS

Structure

1.0 INTRODUCTION

Risk analysis is a broad term that is used in a number of different settings. In each instance, the term refers to the evaluation of the potential risk inherent in an upcoming transaction and the identification of several different options in how to proceed. Often, these options are designed to minimize the risk while obtaining the most benefit or at least finding ways to protect you while taking the risk.

In the business world, risk analysis is one of the primary tools used in the process of risk management. Within this setting, the business looks at how various operations, campaigns and expansions are likely to impact the financial stability of the company. When the risk analysis indicates that all or most of the factors are favorable, the company moves forward with the product launch.

When it comes to growing a business, risk analysis is an important part of any constructive business planning. The business assessment often includes understanding both the risks of maintaining the company in its current state as well as determining what could happen if new policies, procedures or product lines were introduced into the corporate culture.

1.1 OBJECTIVES

After studying this unit, you should be able to:

- define risk analysis;
- explain the importance of risk analysis;
- explain types of risk analysis;
- perform risk analysis;
- conduct risk analysis; and
- describe golden rules of risk analysis.

1.2 WHAT IS RISK ANALYSIS?

Risk analysis is the process of systematically identifying and assessing the potential risks and uncertainties that occur when trying to achieve a certain goal (like reaching a target income or finishing a project) and then finding a feasible strategy for most efficiently controlling those risks.

1.2.1 Brief History

Risk Analysis is a relatively new section of the American Statistical Association. The section grew out of an ASA committee, advisory to the U.S. Nuclear Regulatory Commission. A prime mover in the establishment of the Section is **Professor Bernard Harris** (University of Wisconsin). Bernie was the first Chairman of the Section (and is currently the Section's Representative to the ASA Council of Sections). Other members of the initial Executive Committee included Lee R. Abramson (U.S. Nuclear Regulatory Commission), Robert F. Bordley (General Motors Research Laboratories), Harry F. Martz (Los Alamos National Laboratory), Lisa Weissfeld (University of Pittsburgh) and Stanley L. Sclove (University of Illinois at Chicago).

At JSM97/Anaheim, the Section hosted three sessions, two Invited Sessions (including "The Many Faces of Risk in the 21st Century", in keeping with the theme of JSM97, "Shaping Statistics for Success in the 21st Century") and one Contributed Paper Session and sponsored or co-sponsored six other sessions (including "Applications of Decision Analysis in the Pharmaceutical Industry").

1.2.2 Mission

The principal objectives of the Risk Analysis Section are:

- To study and develop the methodology of risk analysis and risk assessment
- To develop their applications to various subject matter areas.

Specific activities of the Section shall include, but not be limited to:

- conducting workshops
- sponsoring joint meetings with other professional societies

- sponsoring sessions at meetings of other professional societies publishing newsletters and scientific articles
- establishing committees and advisory groups for government agencies and other nonprofit bodies.

A Risk Analysis is:

- "Systematic use of available information to identify hazards and to estimate the risk to individuals or populations, property or the environment" – IEC 60300-3-9
- "A systematic approach for describing and/or calculating risk. Risk analysis involves the identification of undesired (accidental) event and the causes and consequences of these events" – NS 5814

1.2.3 Risk Concepts and Definitions

Risk Estimation

This is the process used to produce a measure of the level of health, property or environmental risks being analyzed. Risk estimation contains the followings steps: frequency analysis, consequence analysis and their integration.

Risk Analysis

It is the use of available information to estimate the risk to individuals or populations, property or the environment, from hazards. Risk analysis generally contains the following steps: scope definition, hazard identification and risk estimation.

Risk Evaluation

The stage at which values and judgments enter the decision process, explicitly or implicitly, by including consideration of the importance of the estimated risks and the associated social, environmental and economic consequences, in order to identify arrange of alternatives for managing the risks.

Risk Assessment

It is a process of risk analysis and risks evaluation.

Risk Control or Risk Treatment

The process of decision making for managing risks and the implementation or enforcement of risk mitigation measures and the re-evaluation of its effectiveness from time to time, using the results of risk assessment as one input.

Risk Management

It is a complete process of risk assessment and risk control (or risk treatment).

1.3 WHY RISK ANALYSIS IS DONE?

In business and government one faces having to make decisions with uncertain outcome all the time. Understanding the uncertainty can help us make a much better decision.

Imagine that you are a national health care provider considering which of two vaccines to purchase. The two vaccines have the same reported level of efficacy (60%), but further study reveals that there is a difference in confidence attached to these two performance measure: one is twice as uncertain as the other.

All else being equal, the health care provider would purchase the vaccine with the smallest uncertainty about its performance: vaccine A.

Replace vaccine by investment and efficacy by profit and we have a problem in business, for which the answer is the same: pick the investment with the smallest uncertainty, all else being equal (investment A). The principal problem is determining that uncertainty which is the central focus of risk analysis.

We can think of two forms of uncertainty that we have to deal with in risk analysis.

The first is a general sense that the quantity we are trying to estimate has some uncertainty attached to it.

Then we have risk events, which are random events that may or may not occur and for which there is some impact of interest to us.

We can distinguish between two types of events.

A **Risk** and **Opportunity** can be considered the opposite sides of the same coin. It is usually easiest to consider a potential event to be a risk if it would have a negative impact and its probability is less than 50% and if the risk had a probability in excess of 50%, to include it in a base plan and then consider the opportunity of it not occurring.

1.3.1 Risk and Opportunity

A risk is an event that may possibly occur and if it did occur would have a negative impact on the goals of the organization. Thus a risk is composed of three elements:

- The scenario.
- Its probability of occurrence.
- The size of its impact if it did occur (either a fixed value or a distribution).

An opportunity is an event that may possibly occur and if it did occur would have a positive impact on the goals of the organization. Thus an opportunity is composed of the same three elements as a risk.

The management of an opportunity is essentially the opposite of managing a risk, i.e. one attempt to maximize the probability of an opportunity occurring and to position oneself to enjoy the greatest benefit should the event occur.

1.3.2 Purpose of Risk Analysis

The purpose of a risk analysis is to provide information to help make better decisions in an uncertain world. A decision maker has to work with the risk analyst to precisely define the questions that need answering. You should consider a number of things:

- Rank the questions that need answering from 'critical' down to 'interesting'.
- Discuss with the risk analyst the form of the answer.
- Explain what arguments will be based on these outputs.
- Explain whether the risk analysis has to sit within a framework.
- Explain the target audience.
- Discuss any possible hostile reactions.
- Figure out a timeline.
- Figure out the priority level.
- Decide on how regularly the decision maker and risk analyst will meet.

In order to plan a risk analysis properly you'll need to answer a few questions:

- What do you want to know and why?
- What assumptions are acceptable?
- What is the timing?
- Who is going to do the risk analysis?

1.3.3 Determine the Assumptions that are Acceptable or Required

If a risk analysis is to sit within a certain framework, discussed above, it may well have to comply with a set of common assumptions to allow meaningful comparisons between each risk analysis' results. Sometimes it is better not to revise some assumptions for a new analysis because it makes it impossible to compare. You can often see a similar problem with historic data, e.g. calculating crime or unemployment statistics. It seems that the basis for these statistics keeps changing making it impossible to know whether the problem is getting better or worse.

In a corporate environment there will be certain base assumptions used for things like interest and exchange rates, production capacity and energy price. The same assumptions should be used in all models. In a risk analysis world these should be probabilistic forecasts but they are nonetheless often fixed point values. Oil companies, for example, have the challenging job of figuring out what the oil price might be in the future. They can get it very wrong so often take a low price for planning purposes: e.g. $16 a barrel which in 2007 might seem rather unlikely for the future. The risk analyst working hard on getting everything else really precise could find such an assumption irritating, but it allow consistency between analyses where assigning distributions of uncertainty to oil price forecasts would be so large as to mask the differences between investment opportunities.

Some assumptions we make are conservative meaning that if, for example, we need a certain percentile of the output to be above X before we accept the risk as acceptable and then a conservative assumption will bias the output to lower values. Thus, if the output still gives numbers that say the risk is acceptable we know we are on pretty safe ground. Conservative assumptions are most useful as a sensitivity tool to demonstrate that one has not taken an unacceptable risk, but they are to be avoided whenever possible because they run counter to the principle of risk analysis which is to give an unbiased report of uncertainty.

1.3.4 Time and Timing

Risk analysis is an integral part of the planning of a project, not an add-on at the end. One of the prime reasons for doing risk analyses are to identify risks and risk management strategies so the decision-makers can decide how the risks can be managed which could well involve a revision of the project plan. That can save a lot of time and money on a project: if risk analysis is added on at the end, you lose all that potential benefit.

The data collection efforts required to produce a fixed-value model of a project are little different from the efforts required for a risk analysis, so adding a risk analysis on at the end is inefficient and delays a project as the risk analyst has to go back over previous work.

We advocate that a risk analyst writing the report as the model develops. It helps keep a track of what one is doing and makes it easier to meet the report submission deadline at the end. I also like to write down my thinking because it helps me spot any mistakes early.

Finally, try to allow the risk analyst enough time to check the model for errors and get it reviewed.

Clearly Stated Questions

In order for a risk analysis to help the manager determine which options are to be preferred, the manager must provide a clear question stated in terms of a quantitative estimate. For example:

"What is the risk of AIDS?"

It is insufficient. The manager would need to specify.

The risk to whom?

The population in general or a sub-group.

In what units?

The measure of impact is the analyst to evaluate a person living with AIDS the same as a person suffering symptoms, the same as a person who dies from the virus. Perhaps all three values are needed.

Over what period?

There has to be a unit of exposure. For example, per random person per year or per lifetime. Perhaps the exposure is required per sexual contact with an AIDS sufferer, per new sexual partner or birth (for transfer to children) etc.

How is the Answer to be Enumerated?

The choice of numerical representation can be very important. For example, the risk from some exposure or activity X in a country of 50 million population could be expressed as follows:

1) 1 in a million chance of death per person per year
2) 1 in a million chance of death per statistical person per year
3) An expected 50 deaths per year
4) 10-6 risk of death per person per year
5) 0.000 001 risk of death per person per year
6) 0.000 1% risk of death per person per year
7) Same risk as dying from Y (where Y is some recreational activity)

If these explanations of risk are presented to the population, they may engender quite different reactions. For example:

1) 'Yes, but I'll be the "1". It's too risky'
2) 'Not so risky'
3) 'Completely unacceptable to condemn 50 people to death each year'
4) 'What does 10-6 mean? They're trying to blind us with science'
5) 'That's a lot of zero. Not a problem'
6) 'Doesn't look that small to me'
7) 'How dare you impose a risk on me that I didn't ask for'

It is common and, in our view, very practical for analysts and managers to spend some time debating the questions that can be answered and the process is iterative: the collection of available data will often lead to a change or refinement to the question and the asking of additional questions.

Check Your Progress 1

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) What is Risk Analysis and what are different concepts and definitions of risk?

.....

.....

.....

.....

2) Explain the Purpose of Risk Analysis.

.....

.....

.....

.....

3) Describe how the risk could be analyzed.

.....

.....

.....

.....

4) Define Opportunity? Differentiate Risk & Opportunity.

.....

.....

.....

.....

1.4 PROJECT RISK

Project Risk is always in the Future. Risk is an uncertain event or condition that, if it occurs, has an effect on at least one project objective. Objectives can include scope, schedule, cost and quality. A Risk may have one or more causes and, if it occurs, if may have one or more impacts. A cause may be a requirement, assumption, constraint or condition that creates the possibility of negative or positive outcomes. For example, causes could include the requirement of an environment of an environmental permit to do work or having limited personnel assigned to design the project.

The risk event is that the permitting agency may take longer than planned to issue a permit or in the case of an Opportunity, limited design personnel available and assigned may still be able to get the job done on time, thereby accomplishing

work with less resource utilization. If either of these uncertain events occurs, there may be an impact on the *Project cost, Schedule or Performance*. Risk conditions could include aspects of the Project's or Organization's environment that may contribute to project risk, such as immature project management practices, lack of integrated management systems, concurrent multiple projects or dependency on external participants who cannot be controlled.

Project risk has its origins in the uncertainty present in all projects. Known risks are those that have been identified and analyzed, making it possible to plan responses for those risks. Specific unknown risks cannot be managed proactively, which suggests that the project team should create a contingency plan. A project risk that has occurred can also be considered an issue.

Organization perceives risk as the effect of uncertainty on their project and Organizational objectives. Organizations and stakeholders are willing to accept varying degrees of risk. This is called Risk Tolerance.

Risks that are threats to the project may be accepted if the risks are within tolerances and are in balance with the rewards that may be gained by taking the risks.

Individuals and groups adopt attitude towards risk that influence the way they respond. These risk attitudes are driven by Perception, Tolerances and other biases.

1.5 TYPES OF RISK ANALYSIS

Risk analysis is a complex science and a procedure to identify threats & vulnerabilities, analyze them to ascertain the exposures and highlight how the impact can be eliminated or reduced.

In other definition, a process to determine what security is appropriate for a system or environment.

In a bottom line, the security you implement should be commensurate with the risks applicable. Risk Analysis should enable you to achieve this goal.

It should also help you establish where to invest your security budget for the best return.

1.5.1 Quantitative Risk Analysis

Quantitative Risk Assessment (QRA) provides a quantitative estimate of the risks posed as well as enabling risk mitigation methods to be evaluated so that risk can be reduced to acceptable levels. It is simpler and widely used. QRA helps in the identification of the assets and resources at risk, vulnerabilities that might allow the threats to be realized, safeguards already in place and those which may be implemented to achieve an acceptable level of risk and increase overall awareness.

Quantitative analysis does this as well as identifies the specific envelope in which the losses and safeguards exist. It does, however, present its results in a management-friendly form of monetary values, percentages and probabilities.

Perform Quantitative Risk Analysis

Perform Quantitative Risk Analysis is performed on Risks that have been prioritized by Perform Qualitative Risk Analysis process as potential and substantially impacting the project's competing demands. The perform Quantitative Risk Analysis process analyzes the effect of those risk events. It may be used to assign a numerical rating to those risks individually or to evaluate the aggregate effect of all risks affecting the project. It also presents a quantitative approach to making decisions in the presence of uncertainty.

Perform Quantitative Risk Analysis generally follows Qualitative Risk Analysis process. In some cases, Perform Quantitative Risk Analysis may not be required to develop effective Risk Responses. Availability of time and budget and the need for qualitative or quantitative statements about risk and impacts, will determine which methods to use on any particular project.

Tools and Techniques

1) **Data Gathering and Representation Techniques**

- **Interviewing** – Interviewing Techniques draw an experience and historical data to quantify the probability and impact of risks on project objectives. The information needed depends upon the type of probability distribution that will be used. For e.g. information would be gathered on the optimistic(low), pessimistic(high) and most likely scenarios for some commonly used distributions.
- **Probability Distribution**

WBS Element	Low	Most Likely	High
Design	$4M	$6M	$10M
Build	$16M	$20M	$35M
Test	$11M	$15M	$23M
Total Project	$31M	$41M	$68M

Fig. 1

Continuous Probability distribution used extensively in modeling and simulation represent the uncertainty in values such as durations of schedule activities & costs of Project Components. Two examples of widely used continuous distributions are shown in Figure below. Beta and Triangular distributions are frequently used in quantitative risk analysis.

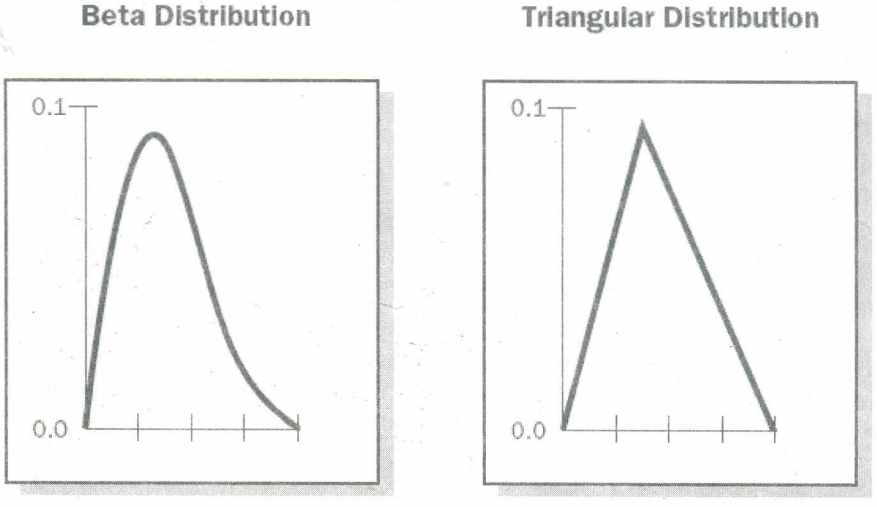


Fig. 2

2) **Quantitative Risk Analysis & Modeling Techniques**

Commonly used techniques include both event-driven and project-oriented analysis approaches including:

- **Sensitivity Analysis**

  It helps to determine which risks have the most potential impact on the project and examines the extent to which the uncertainty of each project element affects the objective being examined when all other uncertain elements held at their baseline values.

- **Expected monetary value analysis (EMV)**

  EMV analysis is a statistical concept that calculates the average outcome when the future includes scenario that may or may not happen. EMV of a project is calculated by multiplying the value of each possible outcome by its probability of occurrence and adding the products together.

- **Modeling and Simulation**

  A project Simulation uses a model that translates the specified detailed uncertainties of the project into their potential impact on project objectives. In a simulation, the project model is computed any times (iterated), with the input values chosen at random for each iteration from the probability distributions of these variables.

  For cost risk analysis, simulation uses cost estimates.

  For schedule risk analysis, the schedule network diagram and duration estimates are used.

3) **Expert Judgment**

Expert Judgment (ideally using experts with relevant, recent experience) is required to identify the potential cost and schedule impacts, to evaluate the probability and to define inputs (such as probability distribution) into the tools.

It also comes into play in the interpretation of the data. Experts should be able to identify the weaknesses of the tools as well as their relative strengths. Experts may determine when a specific tool may or may not be more appropriate given the organization's capabilities and culture.

As the analysis is repeated, a trend may become apparent that leads to conclusions affecting risk responses. Organizational historical information on project schedule, cost, quality and performance should reflect new insights gained through QAR process. Such history may take the form of a quantitative risk analysis report.

1.5.2 Qualitative Risk Analysis

Qualitative Risk Analysis improves the awareness of Information System security problems and posture of the system being analyzed. It helps in the identification of the assets and resources at risk, vulnerabilities that might allow the threats to be realized, safeguards already in place and those which may be implemented to achieve an acceptable level of risk and increase overall awareness. This analysis uses simple calculations and uses procedure in which it is not necessary to determine the dollar value of all assets and the threat frequencies or the implementation costs of the controls.

Performing Qualitative Risk analysis is the process of prioritizing risks for further analysis or action by accessing and combining their probability of occurrence and impact. Organizations can improve the project's performance by focusing on high-priority risks. It assess the priority of identified risks using their relative probability

or likelihood of occurrence, the corresponding impact on project objectives if the risks occur, as well as other factors such as the time frame for response and the organization's risk tolerance associated with the project constraints of cost, schedule, scope and quality. Such assessments reflect the attitude of the project team and other stakeholders to risk, Effective assessments therefore requires explicit identification and management of the risk attitudes of key participants in the Perform Qualitative Risk Analysis process. Where these risk attitudes introduce bias into the assessment of identified risks, attention should be paid to evaluating bias and correcting for it.

Establishing definitions of the levels of probability and impact can reduce the influence of bias. The time criticality of risk related actions may magnify the importance of a risk. An evaluation of the quality of the available information on project risks also helps clarify the assessment of the risk's importance to the project.

Tools and Techniques

1) **Risk Probability and Impact Assessment**

It investigates the likelihood that specific risk will occur. Risk impact assessment investigates the potential effect on a project objective such as schedule, cost, quality or performance, including negative effects for Threats and Positive effects for Opportunities.

The level of probability for each risk and its impact on each objective is evaluated during the interview or meeting. Explanatory details, including assumptions justifying the levels assigned, is also recorded. They are rated according to the definitions.

2) **Risk Data Quality Assessment**

A qualitative Risk analysis requires accurate and unbiased data if it is to be credible. Analysis of the quality of risk data is a technique to evaluate the degree to which the data about the risks are useful for Risk Management. It involves examining the degree to which the risk is understood and the accuracy, quality, reliability and integrity of the data regarding the risk. If data quality is unacceptable, it may be necessary to gather higher-quality data.

3) **Risk Categorization**

Risk to the project can be categorized by sources of risk, the area of project affected or other useful category to determine areas of the project most exposed to the effects of uncertainty. Grouping risks by common root causes can lead to developing effective risk responses.

This is by far the most widely used approach to risk analysis. Probability data is not required and only estimated potential loss is used. Most qualitative risk analysis methodologies make use of a number of interrelated elements:

Threats

These are things that can go wrong or that can 'attack' the system. Examples might include fire or fraud. Threats are ever present for every system.

Vulnerabilities

These make a system more prone to attack by a threat or make an attack more likely to have some success or impact. For example, for fire vulnerability would be the presence of inflammable materials (e.g. paper).

Controls

These are the countermeasures for vulnerabilities. There are four types:

1) Deterrent controls reduce the likelihood of a deliberate attack.

2) Preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact.

3) Corrective controls reduce the effect of an attack.

4) Detective controls discover attacks and trigger preventative or corrective controls.

These elements can be illustrated by a simple relational model:

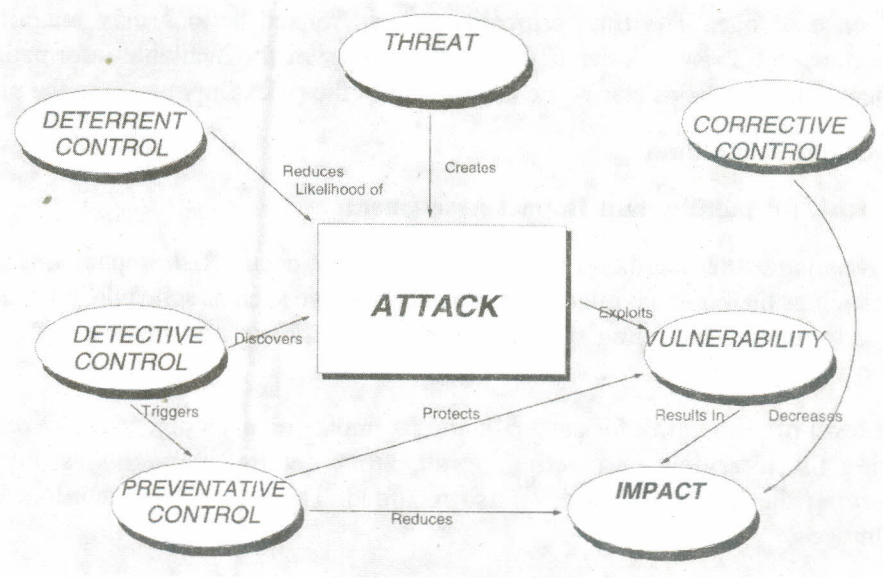


Fig. 3

Check Your Progress 2

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) Explain the term Risk Analysis.

.....

.....

.....

.....

2) Define Qualitative Risk Analysis? What are tools and techniques to perform.

.....

.....

.....

.....

3) Define Quantitative Risk Analysis. What are tools and techniques to perform.

.....

.....

.....

.....

1.6 PERFORMING A RISK ANALYSIS

Performing a risk assessment analysis includes identifying potential threats. Project managers decide how likely it is that these problems will occur and then develop strategies to prevent or minimize any impact on the project. An initial risk analysis occurs at the beginning of the project and the team should monitor any potential vulnerability throughout each phase to avoid problems that might affect the project's schedule, costs or quality output.

1.6.1 Gather Information

The project manager must first obtain all documentation related to the policies, procedures and standards that will be used during the project. He should have a thorough understanding of the operational tasks required in the business environment. Details about personnel assigned to the project, vendor or supplier contracts and other pertinent information need to be scrutinized too. If available, metrics and output from risk assessment analysis from precious projects of a similar type and scope should be located. A risk assessment analysis should identify all facets of the project that need to be protected.

1.6.2 Analyze Data

Once the project manager has assembled all the relevant information and identified potential risks, he needs to classify and rank these events based on how likely they are to occur. Classifying the problems allows the manager to focus his efforts on controlling problems in consistent manner. Additionally, if problems arise that haven't been previously identified, by classifying the new problem as similar to a known issue can streamline the time it takes to respond with a mitigating action. The team should analyze the potential damage a risk might have during different phases of the project. For example, the costs associated with fixing problems increases as the project progresses, resulting in lost productivity, financial losses and missed deadlines. Using quantitative methods to identify the numbers associated with any threat and qualitative methods such as industry information, the project team determines the potential severity and loss.

1.6.3 Create a Plan to Monitor and Control Risk

Project managers control and manage risk by establishing preventive, detective or corrective actions. They also define technical and administrative responses to problems that might occur. By monitoring the project, the manager can ensure policies and procedures are followed. If vulnerabilities get exploited, the team can respond quickly and effectively to handle the problem before it impacts the milestones. Risks rated with a "high" level of probability typically need to be monitored daily. Project managers tend to monitor potential problems rated as "medium" or "low" on a less frequent basis.

Evaluating risks requires involvement of the entire project team. Utilizing their skills, knowledge and experience, they can identify threats, rank the likelihood of occurrence and control problems should they arise. Performing a risk assessment analysis helps coordinate a systematic response, ensure standardization and maximize project performance.

Risk analysis is a process used to identify and assess factors that may jeopardize the success of a project or achieving a goal. Another term for this process is project impact analysis (PIA). It will require an in-depth cost-benefit analysis to be conducted. The process gives organization management the opportunity to examine and assess a proposal before it becomes a live project. This examination should not only determine whether the project should be approved but it should also establish key objectives or impacts.

The risk analysis process is conducted in the analysis phase of the SDLC. Here the interested parties are charged with building their case and presenting the proposal to the management review committee for approval and initial funding.

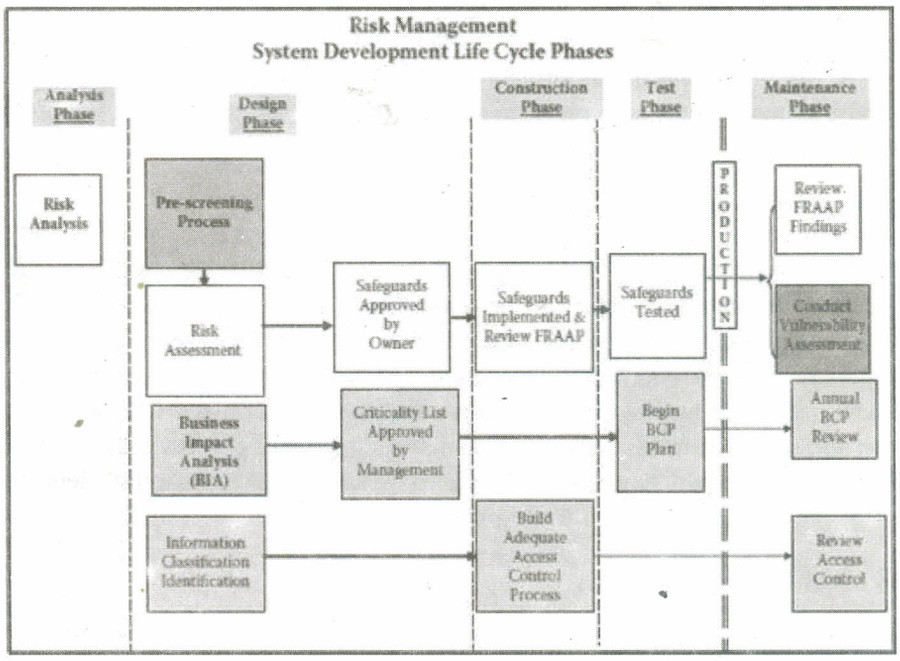


Fig. 4

The goal of the risk analysis process is to present to the management approval team the business reasons the proposal should become a project and then become part of the production environment. In addition to the pros and cons of accepting the proposal, the risk analysis will allow the team to establish the project goals and objectives, the risks and critical success factors and the organization and implementation of the approved project.

The risk analysis process can take as little as a week or may take several months to complete depending on the size and scope of the project. Early on, the project proposal team will want to identify all the stakeholders or those individuals with a vested interest in the project. These individuals will help the proposal team examine and meet the risk analysis objectives.

Once the risk analysis is complete, the champion and the project lead take the document to the executive committee that reviews and approves new projects. This process could take more than one meeting with the committee. If the committee turns the proposal down, this process must be documented and the report filed away. Unsuccessful proposal reports should be kept for a period of five to seven years. The retention period will depend on the requirements identified by the records-management program of the organization.

If the proposal is successful, the champion and the project lead next visit the project management office to register the project. Part of this process will be the requirement to complete the pre-screening process. The pre-screening process asks a few questions that will help determine whether this project will require a full risk assessment or business impact analysis. The only other element required early on in the SDLC is for the project team to classify the data to be found and used with the project.

1.7 ELEMENTS OF RISK ANALYSIS

Part of the risk analysis will examine the costs of the project. When researching costs, the team will establish any costs for procurement of the project and any

development costs. Although these costs are important, they do not represent the actual or total cost of the project. In your project proposal, it will be beneficial to have a chart similar to the one shown in Table 1.

Table 1: Risk Analysis Table

S.No.	Description	Hours	Cost
1.	Product Procurement Cost		
2.	Enhancements to code (contract)	82 hrs. @ $75 per	$6,150
3.	Deployment and Configuration Management	40 Hours	
4.	Conversation/migration costs		
5.	Daily Operation Costs (added staff requirements) 1 additional headcount		
6.	Maintenance(monthly/yearly)		$10K Annual
7.	Infrastructure Training	4 hrs per employee	
8.	User Training and Documentation	1 hr training per user	
9.	Upgrades	TBD	

Probably the lowest part of the overall cost for any project is the actual procurement or development costs. The costs that I find have the most impact include operations and maintenance. In the mid-1990s, as companies began to deploy to the Internet, the need for security was reinforced in the risk assessment process. One of the solutions was to implement a firewall. One electrical utility began the implementation in August 1995. The head of information security was told that there would be a need for a firewall to protect the organization as it connected to the Internet. The security professional was not initially concerned because the firewall was hardware and as such was a capital expenditure, which would be part of the Operations department's budget. That part of the implementation was true; however, what he didn't know about was the need for a firewall administrator. This added cost was compounded when the total number of firewalls was going to be fifteen and that administration was a 24/7 operation, so there was going to be a need for more than one administrator.

When working through the risk analysis process, it is always important to consider the impact of converting to a new process or having to migrate processes or data over to the new structure. During a recent class on risk management, a fellow security professional shared with the class that a former PeopleSoft company had just converted to SAP. We decided to use this project to walk through the components of the risk analysis process. We discussed the nine key components examined in the risk analysis table (Table 1). When we got to the discussion on conversion and migration, the discussion took a scary turn. It was related to the class that the conversion process was a most-formidable exercise. The process took over a year and many employees, including IT, financial and HR, worked long hours. We discussed where one could go to find such information on conversion impact. We thought about user groups or asking fellow professionals or the vendor. We did a quick search of the Internet and found a number of articles that helped the class fill in the needed figures.

During our investigation, we found the following in a very interesting article, "The Great PeopleSoft Migration" by Joab Jackson in Government Computing News, March 7, 2005.

If all goes according to schedule, the Defense Department will complete the Defense Integrated Military Human Resources System – estimated to be the world's largest human resources program – in 2013. Unfortunately, 2013 is also the year DIMHRS will become a legacy system, because that's the year Oracle Corp. plans to end support for PeopleSoft applications, the platform DIMHRS will run on.

Last December, when database vendor Oracle purchased PeopleSoft Inc., agency heads faced a tough decision. Should they stick with Oracle as the company migrated PeopleSoft users over to its own e-business platform? Or would the upgrade be so arduous, the new features so underwhelming, that making the switch would be untenable?

Spending all of that time to implement a process only to discover that it will be running a non-supported legacy system is an issue that should have been uncovered in the risk analysis process.

1.8 IMPORTANCE OF RISK ANALYSIS

Risk analysis is an important and vital part of project management. A good risk analysis takes place during the project planning phase. These are things we know. What sometimes isn't clear is exactly how that risk analysis should take place. Sometimes the hardest part of undertaking a project is getting things started. In this unit, we take you through the steps of risk analysis in a salient way. For our risk analysis example, we will be using the example of remodeling an unused office to become a break room for employees. Through working through the risk analysis with a simple example, you can become familiar with the process before you need to use it in a project.

1.8.1 Identifying Project Steps

Many guides on risk analysis will start by having you jump into the risk analysis process by having you identify project risks. I want you to stop before you do this and first identify important project steps. The reason you want to make sure you've already performed decomposition and come up with a rough work breakdown structure is that you will know the steps that are involved in your project. In our example, there might be the following project steps:

- Remove current office furniture, wall furnishings, etc.
- Hire a contractor to insert a sink (let's say the office was next to a restroom) and some cabinets
- Paint
- Upgrade flooring
- Purchase refrigerator
- Purchase microwave
- Purchase tables and chairs
- Purchase bookshelves (in case you have literary employees, it is nice to have reading material in the break room)

Complete this list on your own. Imagine that you are able to construct the ultimate employee break room. What features would you want? Don't move on to step two

until you've compiled your list of possible project steps, but don't take too long compiling this list either.

1.8.2 Identifying Potential Threats

Now that you have a rudimentary list of action items for your remodeling project, it is time to identify potential threats. According to a MindTools article covering project risk analysis, there are many types of threats to a project, including:

- **Human** – These are risks stemming from risk to individuals. Perhaps you remodel the break room and the employees don"t like it or the new carpeting causes some employees to become ill.
- **Operational** – These are risks that have to do with distribution, obtaining supplies necessary, etc. In the remodeling example, perhaps there is no possibility of installing a sink or the sink installation winds up being a larger chore than necessary.
- **Reputation** – Loss of confidence from employees or damage to the reputation of the company. Perhaps remodeling takes longer than expected and thus the employees lose faith in the fact that the break room will ever be finished. Alternatively, it could be that the public thinks the funds are being mis-spent.
- **Procedural** – These are risks associated with fraud, loss of productivity, etc. The remodeling may cause a disruption in work due to the noise level generated by the contractors.
- **Project** – Project risks have to do with over-runs, jobs taking too long, etc. When remodeling, as we know from remodeling homes, often the project takes much longer than estimated.
- **Financial** – Anything that has to do with the financial health of the project and company. The break room may wind up costing much more than budgeted for.
- **Technical** – This has to do with failed technology. What might go wrong with the break room example that is technical?
- **Natural** – Threats from weather, disease, etc. Perhaps while remodeling, there is an earthquake that destroys the progress made. What other natural risks might occur in a remodeling project?
- **Political** – Changes in government policy, taxes, etc. Perhaps local policy will change governing the requirements for employee break rooms.
- **Others** – You get the idea. Come up with your own list of potential threats based upon the list you created. Don't continue to the next page until you've identified potential threats for the break room example.

1.8.3 Estimate the Level of Risk

Here is where risk analysis begins to get tricky. You've thought out the steps of the project and you've even identified potential threats to the project. Now you need to estimate how likely each of those threats are to occur. For example, it is much more likely that the remodeling project will run overtime than it is that a tsunami will hit your office (unless, of course, your office is in a tsunami zone!). Nonetheless, it's time to take that list you made of potential threats. First you will go through each threat and give it a number between one and ten, with one being highly unlikely and ten being most likely. Your list might look like this:

- Remodeling takes longer than expected – 10
- Remodeling goes over budget – 10
- Tsunami hits building making remodel obsolete – 1

- Earthquake strikes – 2
- Contractors cannot get sink installed – 7

Once you have assigned a number to each of your potential risks, go back through the items. Now, you will assign a cost to each of those risks. The cost you will assign is the amount of money it would take in order to fix whatever went wrong. For example, perhaps someone drops the microwave on the way up the stairs to the office and it breaks. It might cost $100 to repair this. Continue to assign a value to each of the items until all values have been assigned. Finally, before moving to the next step of completing a risk analysis, multiply the likelihood of an event occurring by the amount of money that event would set you back. This will give you the value of each risk.

1.9 RISK ANALYSIS TECHNIQUES

There may be some terminology and definition differences related to risk analysis, risk assessment and business impact analysis. Although several definitions are possible and can overlap, for purposes of this article, please consider the following definitions:

- A risk analysis involves identifying the most probable threats to an organization and analyzing the related vulnerabilities of the organization to these threats.
- A risk assessment involves evaluating existing physical and environmental security and controls and assessing their adequacy relative to the potential threats of the organization.
- A business impact analysis involves identifying the critical business functions within the organization and determining the impact of not performing the business function beyond the maximum acceptable outage. Types of criteria that can be used to evaluate the impact include: customer service, internal operations, legal/statutory and financial.

Most businesses depend heavily on technology and automated systems and their disruption for even a few days could cause severe financial loss and threaten survival. The continued operations of an organization depend on management's awareness of potential disasters, their ability to develop a plan to minimize disruptions of mission critical functions and the capability to recover operations expediently and successfully. The risk analysis process provides the foundation for the entire recovery planning effort.

A primary objective of business recovery planning is to protect the organization in the event that all or part of its operations and/or computer services is rendered unusable. Each functional area of the organization should be analyzed to determine the potential risk and impact related to various disaster threats

Check Your Progress 3

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) What is Project Monitoring and Controlling? How to monitor and control Risk.

.....

.....

.....

.....

2) What is the importance of Risk Analysis?

.....

.....

.....

.....

3) What is Potential Threat? What are those? Explain them.

.....

.....

.....

.....

1.10 WHEN TO CONDUCT RISK ANALYSIS?

Although it is important to consider all of the elements of cost in deciding to move forward, the outlay of capital expenditures is just part of the risk analysis process. What must also be considered is the cost of not moving forward with a project. What would be the impact to the enterprise if it was decided to delay or not approve the project? How would not moving forward impact the competitive advantage of the organization? How would this decision impact the ability to meet the mission of the enterprise? How would strategic business partners, suppliers, vendors and other stakeholders be impacted?

In the late 1980s, many big organizations decided to convert from a paper-based order entry system to an e-commerce process. This foray into electronic data interchange (EDI) caught a number of suppliers off guard. EDI is the process of using telecommunications to exchange documents between companies. Orders, purchase agreements, shippers and the like were going to be converted to electronic format. These small suppliers were concerned that they would not be able to meet the aggressive implementation deadline established by the big vendors. One manufacturer established a compromise for the handling of paper-based documents. They vendor would charge the supplier a one-dollar-per-page handling fee for each sheet of paper submitted. This handling fee would be automatically deducted from the amount owed the supplier.

When conducting a risk analysis, it is vital that as many factors as possible be uncovered. This is why the risk analysis should have access to the stakeholders and those with a vested interest in the project. Asking questions and exploring options is vitally important.

Another important factor to consider in this process is the impact of regulatory compliance issues. The new project should, whenever possible, enhance regulatory requirements. Gap analysis, provides the organization with the ability to identify all of the regulatory laws and regulations and map them against the industry standards that the organization is using as its baseline security controls. The organization then maps their policies, procedures and standards to the all-inclusive set of standards. This allows the organization to identify any areas where it needs to improve for regulatory compliance.

Any time a risk analysis is preformed, it will be important to review the gap analysis to ensure that the new project does not impact the compliance issues.

Sometimes a new idea or concept is drafted by a department such as marketing and it gains support and then management acceptance before the infrastructure, budget or security personnel have an opportunity to perform a formal risk analysis. A number of years ago we were hired to perform a network vulnerability assessment on a utility company located in the Southwest. The technical team was running a port scan of the firewall and my technician came running in to inform us that there were some ports open that were major security issues. We went to the firewall administrator and asked why the ports were open. The firewall administrator told us senior management had requested that they be opened so that local high school students could have access to the Internet. Our investigation discovered that marketing had approached the utility's management and indicated that it would be a good public service to provide Internet access to the students. When we presented the security hole to management, we were informed that no one was told what ports were opened, so there should be no security risk!

Once when performing a physical security review, we found a UNIX server located in an office area. We could not find the server on any list of hardware provided by the IT department. We went back to the user department with the lead IT auditor and the information security officer. When we asked about the server, we were informed that it had been purchased as "filing" equipment and a contractor had been hired to develop a new bill-paying program for them. They had tested the program and were just getting ready to contact IT to have their server connected to the network.

The tangible way to measure success is to see a lower bottom line for cost. Risk assessment can assist in this process by identifying only those controls that are needed to be implemented. Organizations are not implementing controls because they think they are needed. Only those actions that are actually required are being implemented. For risk analysis, the metric is that only those projects that show a true business need are being implemented.

Another way that the success of a risk analysis and risk assessment is measured is if there is a time when management decisions are called into review. By having a formal process in place that demonstrates the due diligence of management in the decision-making process, this kind of inquiry will be dealt with quickly and successfully.

Whenever money or resources are to be spent, a risk analysis should be conducted. This process will provide the business reasons that should be used to justify the decision to move forward with a new project or capital expenditure. The documentation of this process can be used by management to demonstrate that they have been performing their due diligence responsibilities.

Typically, the output from a risk analysis will be used twice. The first time will be when the organization decides whether or not to move forward with a development or capital project. The other and often the most important time is when the organization is being examined by some third party and they are looking to management to find out why the project was approved. This documented process will provide the necessary material to defend any decision.

1.11 SAMPLE RISK ANALYSIS

For risk analysis and project impact analysis, the need to demonstrate due diligence is an important output of the process. However, the overriding reason to conduct these processes is that it makes good business sense. The organization proceeds on certain paths based on need and the ability of the organization to meet those specific business or mission needs. The risk analysis process provides management

with a consistent tool to be used to determine where the organization's limited resources will provide the best return on investment.

It is important to establish a set of questions that will help the team present the best set of options for the approval process. When we are working on putting together such a report, we examine each of these questions with the champion and the project lead to ensure that the objectives are firmly established in business need. It will be necessary to include all of those individuals with a vested interest in the project or stakeholders.

PROJECT IMPACT ANALYSIS QUESTIONAIRE

S.No.	Issue	Applicable (Y/N)	Comments
1)	Identify any existing requirements in the baseline that conflict with the proposed change		
2)	Identify any other pending requirement changes that conflict with the proposed changes		
3)	What are the consequences of not making the change?		
4)	What are the possible adverse side effects or other risks of making the proposed changes?		
5)	Will the proposed change adversely affect performance requirements or other quality attributes?		
6)	Will the change affect any system component that affects critical properties such as safety and security or involve in product change that triggers recertification of any kind?		
7)	Is the proposed change feasible within known technical constraints and current staff skills?		
8)	Will the proposed change place unacceptable demands on any computer resources required for the development, test or operating environments?		
9)	Must any tools be acquired to implement and test the change?		
10)	How will the proposed change affect the sequence, dependencies, effort or duration of any tasks currently in the project plan?		
11)	Will prototyping or other user input be required to verify the proposed change?		

12)	How much effort that has already been invested in the project will be lost if this change is accepted?		
13)	Will the proposed change cause an increase in product unit cost such as by increasing third party product licensing fees?		
14)	Will the change affect any marketing manufacturing, training or customer support plans?		
15)	Identify any existing requirements in the baseline that conflicts with the proposed change.		

Check Your Progress 4

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) What is the best time to conduct Risk Analysis?

.....

.....

.....

.....

2) Explain the difference between Threat and Opportunity.

.....

.....

.....

.....

3) Write down any five Questions arises while doing Risk Analysis?

.....

.....

.....

.....

1.12 LET US SUM UP

This unit is an effort towards answering some of the fundamental queries about Risk Analysis. The risk analysis process is an important aspect of business recovery planning. The probability of a disaster occurring in an organization is highly uncertain. Organizations should also develop written, comprehensive business recovery plans that address all the critical operations and functions of the business.

The plan should include documented and tested procedures, which, if followed, will ensure the ongoing availability of critical resources and continuity of operations.

A business recovery plan, however, is similar to liability insurance. It provides a certain level of comfort in knowing that if a major catastrophe occurs, it will not result in financial disaster for the organization.

Insurance, by itself, does not provide the means to ensure continuity of the organization's operations and may not compensate for the incalculable loss of business during the interruption or the business that never returns.

1.13 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) Risk analysis is the process of systematically identifying and assessing the potential risks and uncertainties that occur when trying to achieve a certain goal and then finding a feasible strategy for most efficiently controlling those risks. Risk Concepts and Definitions:

   a) Risk Estimation

   b) Risk Analysis

   c) Risk Evaluation

   d) Risk Assessment

   e) Risk Control

   f) Risk Management

2) In business and government one faces having to make decisions with uncertain outcome all the time. Understanding the uncertainty can help us make a much better decision. Imagine that you are a national health care provider considering which of two vaccines to purchase. The two vaccines have the same reported level of efficacy (60%), but further study reveals that there is a difference in confidence attached to these two performance measure: one is twice as uncertain as the other.

) Here we define risk as 'the perceived extent of possible loss'. Different people will have different views of the impact of a particular risk – what may be a small risk for one person may destroy the livelihood of someone else.

   One way of putting figures to risk is to calculate a value for it as:

   Risk = probability of event x cost of event

   To carry out a risk analysis, follow these steps:

   a) Identify Threats

   b) Estimate Risk

   c) Manage Risk

   d) Review

4) A risk is an event that may possibly occur and if it did occur would have a negative impact on the goals of the organization. Thus a risk is composed of three elements:

   a) The scenario.

b) Its probability of occurrence.

c) The size of its impact if it did occur (either a fixed value or a distribution).

An opportunity is an event that may possibly occur and if it did occur would have a positive impact on the goals of the organization. Thus an opportunity is composed of the same three elements as a risk.

Check Your Progress 2

1) Risk analysis is a technique to identify and assess factors that may jeopardize the success of a project or achieving a goal. This technique also helps to define preventive measures to reduce the probability of these factors from occurring and identify countermeasures to successfully deal with these constraints when they develop to avert possible negative effects on the competitiveness of the company. Reference class forecasting was developed to increase accuracy in risk analysis. One of the more popular methods to perform a risk analysis in the computer field is called Facilitated Risk Analysis Process (FRAP).

2) Qualitative Risk Analysis improves the awareness of Information System security problems and posture of the system being analyzed. It helps in the identification of the assets and resources at risk, vulnerabilities that might allow the threats to be realized, safeguards already in place and those which may be implemented to achieve an acceptable level of risk and increase overall awareness. This analysis uses simple calculations and uses procedure in which it is not necessary to determine the dollar value of all assets and the threat frequencies or the implementation costs of the controls.

3) Quantitative risk analysis makes use of a single figure produced from these elements. This is called the 'Annual Loss Expectancy (ALE)' or the 'Estimated Annual Cost (EAC)'. This is calculated for an event by simply multiplying the potential loss by the probability. It is thus theoretically possible to rank events in order of risk (ALE) and to make decisions based upon this. The problems with this type of risk analysis are usually associated with the unreliability and inaccuracy of the data. Probability can rarely be precise and can, in some cases, promote complacency. In addition, controls and countermeasures often tackle a number of potential events and the events themselves are frequently interrelated. Notwithstanding the drawbacks, a number of organizations have successfully adopted quantitative risk analysis.

Tools and Techniques

- Interviewing
- Probability Distribution
- Expert Judgments

Check Your Progress 3

1) Project managers control and manage risk by establishing preventive, detective or corrective actions. They also define technical and administrative responses to problems that might occur. By monitoring the project, the manager can ensure policies and procedures are followed. If vulnerabilities get exploited, the team can respond quickly and effectively to handle the problem before it impacts the milestones. Risks rated with a "high" level of probability typically need to be monitored daily. Project managers tend to monitor potential problems rated as "medium" or "low" on a less frequent basis.

2) Risks exist in every dimension of business, but project management efforts are particularly sensitive to identifying and minimizing risk potential so that project completion is not jeopardized.

Project management teams usually develop risk management plans that serve to identify risks, strategize ways to minimize or avoid those risks and develop contingency plans in case risks occur and hinder a project's completion. Some project management teams hire risk managers or consultants to help them identify risks to their projects. It can help to have an outside perspective to ensure a risk assessment is comprehensive and factors everything in.

3) According to a MindTools article covering project risk analysis, there are many types of threats to a project, including:

   a) Human

   b) Operational

   c) Reputation

   d) Procedural

   e) Project

   f) Finance

   g) Technical

   h) Natural

   i) Political

Check Your Progress 4

1) When conducting a risk analysis, it is vital that as many factors as possible be uncovered. This is why the risk analysis should have access to the stakeholders and those with a vested interest in the project. Asking questions and exploring options is vitally important. Any time a risk a analysis is performed, it will be important to review the gap analysis to ensure that the new project does not impact the compliance issues.

2) SWOT analysis is a strategic planning method used to evaluate the Strengths, Weaknesses, Opportunities and Threats involved in a project or in a business venture. It involves specifying the objective of the business venture or project and identifying the internal and external factors that are favorable and unfavorable to achieve that objective. The technique is credited to Albert Humphrey, who led a convention at Stanford University in the 1960s and 1970s using data from Fortune 500 companies.

   A SWOT analysis must first start with defining a desired end state or objective. A SWOT analysis may be incorporated into the strategic planning model.

   Strategic Planning has been the subject of much research.

   a) Strengths: characteristics of the business or team that give it an advantage over others in the industry.

   b) Weaknesses: are characteristics that place the firm at a disadvantage relative to others.

   c) Opportunities: external chances to make greater sales or profits in the environment.

   d) Threats: external elements in the environment that could cause trouble for the business.

3) Following are the Questions:

   a) Is it worth running this risk to an end I have set?

b) How can I reduce the risk as much as possible?

c) What information do I need before taking the risk?

d) What human resources and other assistance would be possible to reduce risk and achieve the objective?

e) Is this a major risk?

f) What are my fears about this risk?

g) Am I really ready to spare no efforts to achieve the objective?

h) What you'll get if I run this risk?

i) What preparations should I do before taking the risk?

j) How can I determine in quantitative terms if I've reached my goal?

k) What are the main obstacles to achieve my goals?

1.14 SUGGESTED READINGS

- Risk Assessment Guidance for Superfund: Volume I: Human Health Evaluation Manual, Part A.[EPA/9285.7-01/FS, NTIS PB90-273830INX.] Office of Emergency and Remedial Response, Washington, DC. April 1990. Dr. Larry Leng (2004), Computer Fundamental, Wiley Dreamtech Publication.
- Risk Assessment Guidance for Superfund: Volume II: Environmental Evaluation Manual, Interim Final. [EPA/540/1-89/001]Office of Emergency and Remedial Response, Washington, DC. March 1989.http://www.eiu.edu.

UNIT 2 RISK ASSESSMENT

Structure

2.0 INTRODUCTION

Risk Assessment

Owners of a business are legally required to assess the risks of injury and ill health affecting employees. Risk assessment is the careful examination of the diverse factors that can bring about these risks. Risk assessment should also make sure that enough precautions are implemented in order to prevent harm coming to an

employee. Ill health and accidents can have a very serious affect on business. They can ruin lives and damage business output. They can also lead to costly court cases and increased insurance costs. Risk assessment procedures should help to dispense with the above and make the workplace a safer environment for employees.

In risk assessment, the most important factor is to decide what a hazard in the workplace is. If the risk is determined to be significant enough, precautions should be put into place so that the risk is minimized or dispensed with altogether. For example, electricity in the workplace is hazardous, but provided that all proper protection is in place, the risk to employees becomes insignificant.

There are five steps that should be undertaken when conducting a thorough risk assessment. The first step is to look for hazards. Take a tour of the workplace and check for potential dangers. Concentrate on anything with the potential to cause serious harm to employees. Also ask for employee opinions on the subject. Accident and ill-health records are a good way of revealing why and how accidents have occurred in the past.

The second step is to decide who might be harmed and how. Decide who might be particularly at risk. Trainees, young workers or expectant mothers may be high on this list. Members of the public who are not familiar with the workplace or anyone who is not in the workplace full time and may not be familiar with the layout may also be at risk.

With the third step, you must calculate whether there have been enough precautions put into place to counter the hazard. For each risk you find, a decision should be made whether you have established enough precautions to reduce the risk. Has your risk assessment procedure taken into accounted all the health and safety aspects required by law? Is there anything further you can do to reduce the risk, such as issuing protective clothing or preventing access with guardrails?

The next step is to record your findings. Your risk assessment check must show that you have dealt with all the obvious hazard areas. It should also show that you have checked with employees who might be affected and that any hazards that remain have been dealt with and are now reasonably low.

The final step is to review your risk assessment procedures and make revisions if necessary. In the future, new machinery, substances and work procedures could be implemented in the workplace. This is when your revision should take place to ensure that the work environment is risk fee and will continue to be so in the future.

Risk Likelihood

It is the probability that a risk can occur. The factors that should be taken into account in the determination of likelihood are: the source of the threat, capability of the source, nature of the vulnerability and existence and effectiveness of current controls. Likelihood can be described as high, medium and low.

- **High:** An event is expected to occur in most circumstances
- **Medium:** An event will probably occur in many circumstances
- **Low:** An event may occur at some time

2.1 OBJECTIVES

After studying this unit, you should be able to:

- explain the purpose of risk assessment;

- explain the procedure of risk assessment;
- describe various elements of risk assessment;
- conduct risk assessment; and
- explain general guidelines of risk assessment.

2.2 PURPOSE OF RISK ASSESSMENT

Employers in each workplace have a general duty to ensure the safety and health of workers in every aspect related to their work. The purpose of carrying out a risk assessment is to enable the employer to take the measures necessary for the safety and health protection of workers.

These measures include:

- prevention of occupational risks;
- providing information to workers;
- providing training to workers;
- Providing the organization and means to implement the necessary measures.

Whilst the purpose of risk assessment includes the prevention of occupational risks and this should always be goal, it will not always be achievable in practice. Where elimination of risks is not possible, the risks should be reduced and the residual risk controlled. At a later stage, as part of a review programmed, such residual risk will be reassessed and the possibility of elimination of the risk, perhaps in the light of new knowledge, can be reconsidered.

The risk assessment should be structured and applied so as to help employers to:

- identify the hazards created at work and evaluate the risks associated with these hazards, to determine what measures they should take to protect the health and safety of their employees and other workers, having due regard to legislative requirements;
- evaluate the risks in order to make the best informed selection of work equipment, chemical substances or preparations used, the fitting out of the workplace and the organization of work;
- check whether the measures in place are adequate;
- priorities action if further measures are found to be necessary as a result of the assessment;
- demonstrate to themselves, the competent authorities, workers and their representatives that all factors pertinent to the work have been considered and that an informed valid judgment has been made about the risks and the measures necessary to safeguard health and safety;
- Ensure that the preventive measures and the working and production methods, which are considered to be necessary and implemented following a risk assessment, provide an improvement in the level of worker protection.

Risk management includes the systematic use of the risk assessment results to make decisions regarding the best practicable strategy that will be used to protect workers from harm.

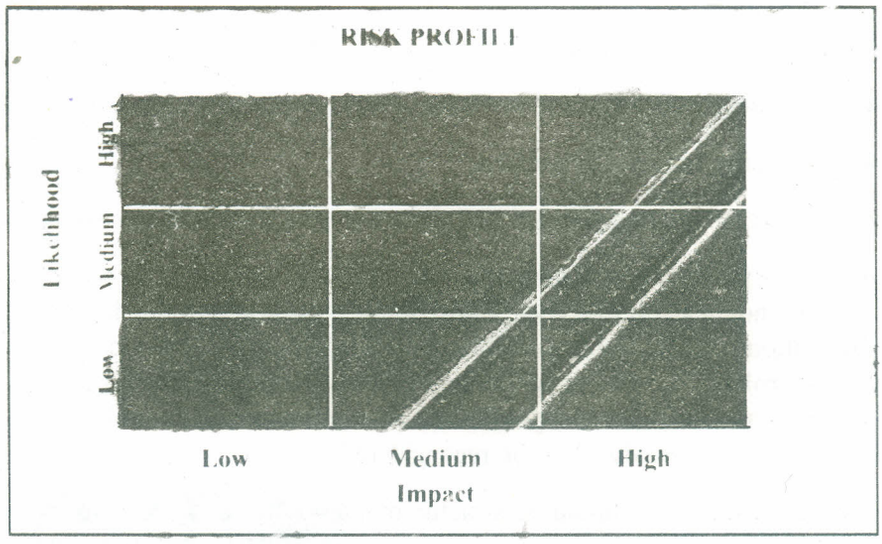
Safety management is the system used to ensure that the risk levels achieved during the risk assessment process are maintained.

Risk Impact

It is the potential effect that a risk could have on the organization if it arises. It is worth mentioning that not all threats will have the same impact as each system in the organization is worth differently. The magnitude of impact also can be categorized as high, medium and low.

- High: Serious impact on operation, reputation or funding status
- Medium: Significant impact on operations, reputation or funding status
- Low: Less significant impact on operations, reputation or funding status

The combination of likelihood and impact gives us the value for each risk factor



Risk Assessment Process

It is the process of identifying and analyzing inherent and residual risks to the achievement of an organization's objectives.

2.3 RISK ASSESSMENT PROCEDURE

During the Risk Assessment, risks to the business will be identified and evaluated. The vulnerability of the business to these risks will be rated. You will also:

1) Identify what prevention practices are being used.
2) Define and implement safeguards to mitigate risks.
3) Conclude the overall risk to the business.
4) Build a case for strategy selections.

Once the assessment is completed, a business can make decisions regarding methods of mitigating risks. By completing a Risk Assessment and Business Impact Analysis, a business can implement the best strategies for Contingency Planning.

Despite the prevention practices utilized, potential hazards that are existent and could result in a loss to the business need to be considered. Even though the exact nature of these exposures and their consequences are tough to determine, it is valuable to conduct a risk assessment of all threats that can logically happen.

All locations and facilities should be included in the risk assessment. Surrounding businesses, local fire, police and community utilities should also be included in the assessment. Any vendor provided service that is provided to the business should also be evaluated.

2.3.1 Steps to Follow

The following steps are necessary for completing a Risk Assessment.

1) Identify Threats/Risk and Vulnerabilities.

2) Analyze risks and determine vulnerability.

3) Identify mitigation and recovery options.

4) Evaluate and Choose Options.

There are additional steps that need to take place during this process. Some of those actions are:

1) Review Internal Plans and Policies.

2) Meet with Outside Groups.

3) Identify Assets.

4) Conduct an Insurance Review.

2.3.2 Assessing Your Risk

The process of identifying risks/threats, probability of occurrence, the vulnerability to each risk/threat and the potential impact that could be caused, is necessary to prepare preventative measures and create recovery strategies. Risk identification also provides a number of other advantages including:

1) Exposes previously overlooked vulnerabilities that need to be addressed by plans and procedures.

2) Identifies where preventative measures are lacking or need reevaluated.

3) Can point out the importance of contingency planning to get staff and management on board.

4) Will assist in documenting interdependencies between departments and increase communication between internal groups.

For the ease of this process, categories of risk should be created to focus the thought process. In the Risk Assessment Survey, the main categories include, Natural Risks, Man-Made (Human) Risks and Environmental Risks. These are certainly not requirements and should not be considered to be constraining.

The nature of a risk/threat should be determined, regardless of the type. Factors to consider should include (but not limited to):

1) Geographic Location.

2) Weather Patterns for the Area and Surrounding Areas.

3) Internal Hazards (HVAC, Facility Security, Access etc).

4) Proximity to Local Response/Support Units.

5) External Hazards (neighboring Highways, Plants etc).

Potential exposures may be classified as:

1) Natural Threats.

2) Man-made (human) Threats.

3) Environmental Threats.

Other steps in conducting Risk Assessment are to review following points:

1) Probability of Occurrence.

2) Vulnerability to Risk.

3) Potential Impact.

4) Preventative Measures in Place.

5) Insurance Coverage.

6) Past Experiences.

2.3.3 Analyzing the Results

Once the Risk Assessment Survey and face to face interviews have been conducted, the next step is to analyze and present the results so that Executive Management can get most use of the data. Analysis can be a time-consuming and tedious process, especially with an enormous amount of data, but it is critical to the RA process.

The analysis will be the foundation for planning recommendations to senior management. The recovery strategies that need to be developed should be based on the findings of the Risk Assessment Survey and interviews, as well as the Business Impact Analysis findings.

2.3.4 Final Report and Presentation

Begin your final report with an executive overview of the Risk Assessment Project. This will explain the objectives of the project, what was in scope and what approach was used. Then provide a summary review of potential hazards.

2.3.5 Creation of Executive Report

The findings from the Risk Assessment will form the basis for the final report. The purpose is to provide senior management with enough information to make them comfortable in endorsing the recommending strategies, actions, budgets or to accept the level of risk by not implementing recovery strategies. The report should include graphs, which visually demonstrate the findings. Do not overuse the graphs. Too many graphs and reports can make reviewing the information confusing. Provide graphs for overall information on the departments, financial impact etc.

The final report should include:

1) Previous Disruption History

2) Risks and Vulnerabilities

3) Preventative Measures

4) Presenting the Results

5) Next Steps

The Risk Assessment process is an essential phase of Continuity Planning. The possibility of a disaster impacting a business is unpredictable. The business should implement a comprehensive Continuity Planning Program and develop recovery plans that encompass all critical operations and functions of the business.

2.4 ELEMENTS OF RISK ASSESSMENT

Risk Assessment is only completed when the Assessors and Project Manager are satisfied that any undetected risks are now insignificant.

2.4.1 Identify Uncertainties (and Constraints)

Explore the entire project plans and look for areas of uncertainty or constraints. It is not possible to stress too often that "The project will be late." is not a risk, it is an impact. We need to crawl over the plans to search for things which could make the project late. The risk could be expressed as "We have underestimated the likely duration of task xxx."

Some examples of areas of uncertainty are

- Failure to understand who the project is for
- Failure to appoint an executive user responsible for sponsoring the project
- Failure to appoint a fully qualified and supported project manager
- Failure to define the objectives of the project
- Failure to secure commitments from people who are needed to assist with the project
- Failure to estimate costs accurately
- Failure to specify very precisely the end users' requirements
- Failure to provide a good working environment for the project
- Failure to tie in all the people involved in the project with contracts or Documents of Understanding

Elements of Risks Assessment

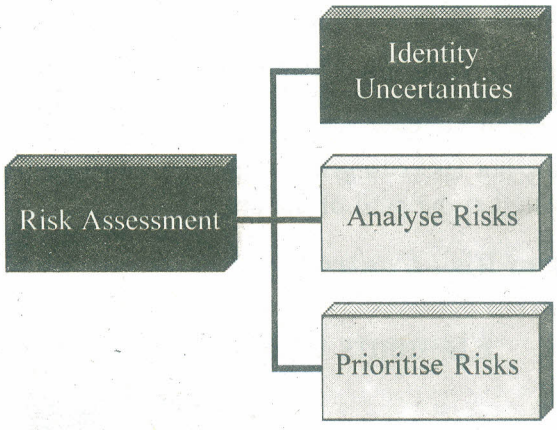


Fig. 2

2.4.2 Classify Risk

The chart plots Probability of occurrence of a risk, which is another way of saying how uncertain the success of the task would be, against the Impact. By Impact we mean the severity of the effect on the budget, the timeliness of project completion or the ability of the project to meet the users' requirements. Whether the severity of Impact or the Probability is high or low is a matter for the judgment of the Risk Assessor and the Project Manager – even with rational method involved we are still talking of an art!

Classifying Risks

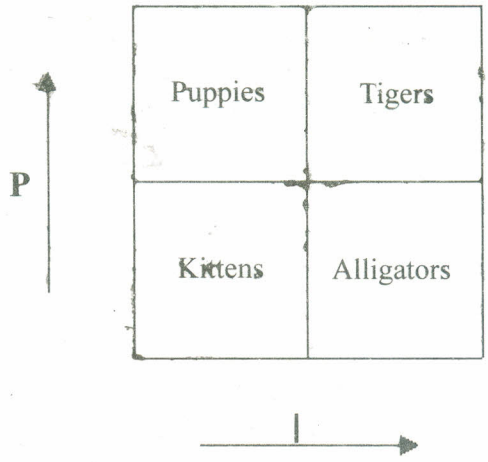


Fig. 3

We have classified the four sectors of the graph, perhaps whimsically, as:

- Tigers – High Probability, High Impact. These are dangerous animals and must be neutralized as soon as possible.
- Alligators – Low Probability, High Impact. These are dangerous animals which can be avoided with care. However, we all remember the old joke that it is difficult to remember when one is up to the arise in alligators that the original objective was to drain the swamp.
- Puppies – High Probability, Low Impact. We all know that delightful pup will grow into an animal which damage, but a little training can do will ensure that not too much trouble ensures.
- Kittens – Low Probability, Low Impact. The largest cat is rarely the source of trouble, but on the other hand a lot of effort can be wasted on training it!

Prioritize Risks

By now you have really done this. Tigers have to be neutralized i.e. the risks must be mitigated early on. Alligators have to be watched and there must be an action plan in place to stop them from interfering with the project. Puppies similarly have to be watched, but less stringently and with less urgent containment plans. Kittens can be ignored at the peril of the project manager.

2.4.3 Elements of Risk Control

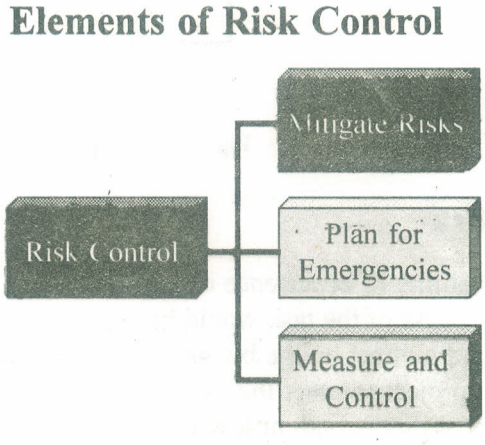


Fig. 4

We can mitigate risks by reducing either the probability or the impact. Remember that we identified the risk by seeking uncertainty in the project. The probability can be reduced by action up front to ensure that a particular risk is reduced. An example is to employ a team to run some testing on a particular data base or data structure to ensure that it will work when the remainder of the project is put together around it. The technique of building a pilot phase of the project is an example of risk mitigation. Unfortunately it often fails, because the team works closely with the pilot user group and then thinks that all the problems are solved for the roll out. This is rarely the case.

Plan for Emergencies

By performing the risk assessment, we know the most likely areas of the project which will go wrong. So the project risk plan should include, against each identified risk, an emergency plan to recover from the risk. As a minimum, this plan will name the person accountable for recovery from the risk, the nature of the risk and the action to be taken to resolve it and the method by which the risk can be spotted. A risk which has been mitigated may still be a significant and dangerous risk – it is rare for a tiger to be converted to a kitten by action before the event. These will require emergency plans as well as alligators and puppies. Kittens can probably be allowed to play at will; provided we are satisfied they really are kittens!

Check Your Progress 1

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) Why perform a Risk Assessment?

.....

.....

.....

.....

2) What is the difference between Risk Assessment and Safety Audit?

.....

.....

.....

.....

3) What is difference between a Risk Management and Safety Management?

.....

.....

.....

.....

4) What is risk and why carry out Risk Assessments?

.....

.....

.....

.....

2.5 CONDUCTING RISK ASSESSMENT

A Risk Assessment is identifying, analyzing and weighing all the potential risks, threats and hazards to the business's internal and external environment. It discovers if a facility (building) is vulnerable to weather related events, HVAC failure, Internal/External Security vulnerabilities and local area hazards. It allows a business to document what mitigating actions have been taken to manage these exposures. By identifying the threats that currently are being mitigated verses threats that are not, a business can compile a list of recommendations for improvement.

To be successful, any risk assessment has to concentrate on the local identifiable issues relating to the business. Before exploring other concerns, concentrate on the most realistic risks and threats that currently exist in the business environment. This can include factors such as:

1) The Nature of the Business.
2) Surrounding Area of Facility.
3) The Construction of the Facility.
4) Common Weather Patterns.
5) Technology Dependencies.

2.5.1 Risk Assessment Process

Despite the prevention practices utilized, potential hazards that are existent and could result in a loss to the business need to be considered. Even though the exact nature of these exposures and their consequences are tough to determine, it is valuable to conduct a risk assessment of all threats that can logically happen.

All locations and facilities should be included in the risk assessment. Surrounding businesses, local fire, police and community utilities should also be included in the assessment. Any vendor provided service that is provided to the business should also be evaluated.

Steps to Follow

The following steps are necessary for completing a Risk Assessment.

1) Identify Threats/Risk and Vulnerabilities.
2) Analyze Risks and determine Vulnerability.
3) Identify mitigation and recovery options.
4) Evaluate and Choose options.

There are additional steps that need to take place during this process. Some of those actions are:

1) Review Internal Plans and Policies.
2) Meet with Outside Groups.
3) Identify Assets
4) Conduct an Insurance Review

2.5.2 Risk

Three elements determine Risk:

1) The causes which may initiate and contribute to a failure.

2) The particular potentially hazardous condition or failure which may result from the cause.

3) The consequences which may derive from the particular potentially hazardous condition or failure.

The sequence of events or scenario, leading to a consequence of concern can be characterized by two parameters: its likelihood, measured as a probability or a frequency and the impact of the consequences, measured as personnel, property and environmental and/or economic loss.

Fig. 5 show how the risk associated with a scenario is a function of the likelihood and the impact magnitude and is usually taken as the product of both variables, thus measuring the expected value of the loss.

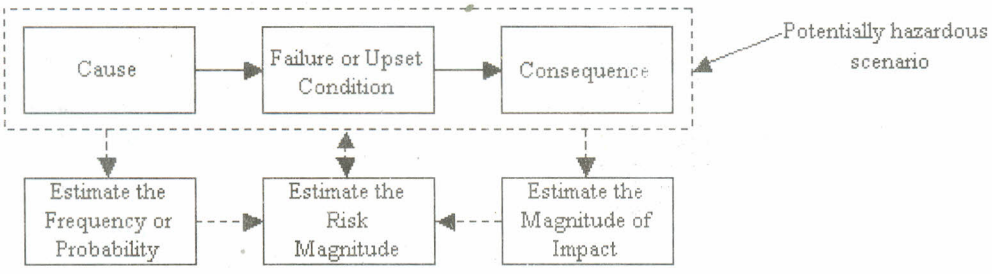


Fig. 5: Risk

2.5.3 Measuring or Estimating Risk

The risk associated with a given event is a function of both the likelihood and impact of such an event. The usual definition of risk is: Risk = likelihood x impact. Risks are often plotted on a logarithmic scale, thus:

Log (Risk) = Log (Likelihood) + Log (Impact magnitude)

In a log-log diagram, the constant risk loci given by the above equation become straight lines, as shown in Fig. 6. Since it is not always possible or convenient to develop quantitative models for both probability and consequences, you can estimate their respective magnitudes, for example in scales from 1 to 4 and assign levels of risk to the different combinations, as shown in Fig. 7.

The high likelihood and high magnitude position corresponds to the highest risk (IV). Risk levels are defined for each situation. The disaster demonstrates the relationships of probability and consequences.

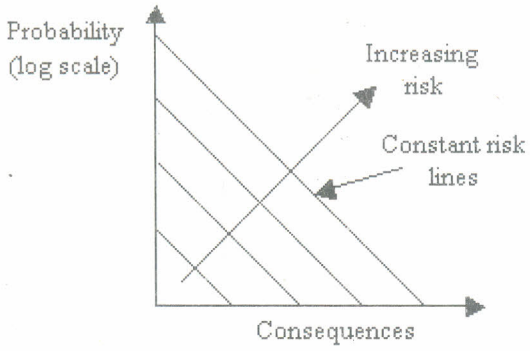


Fig. 6: Risk Plots

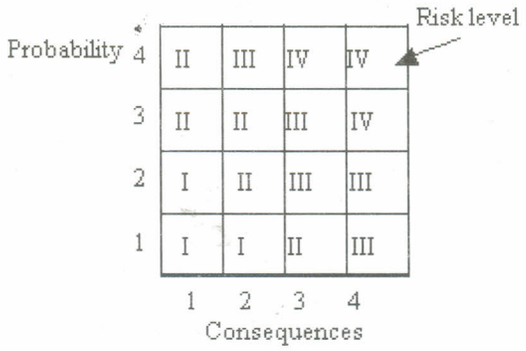


Fig. 7: Risk Matrix

Once the Risk Assessment Survey and face to face interviews have been conducted, the next step is to analyze and present the results so that Executive Management can get most use of the data. Analysis can be a time-consuming and tedious process, especially with an enormous amount of data, but it is critical to the RA process.

The analysis will be the foundation for planning recommendations to senior management. The recovery strategies that need to be developed should be based on the findings of the Risk Assessment Survey and interviews, as well as the Business Impact Analysis findings.

The Risk Assessment process is an essential phase of Continuity Planning. The possibility of a disaster impacting a business is unpredictable. The business should implement a comprehensive Continuity Planning Program and develop recovery plans that encompass all critical operations and functions of the business.

2.6 RISK ASSESSMENT MANAGEMENT

2.6.1 Risk Assessment Management Framework and Process

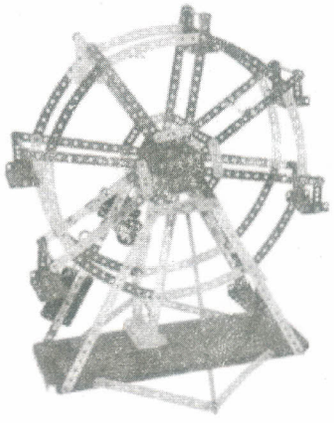


Fig. 8

A Framework is:

a) A structure for supporting or enclosing something else, especially a skeletal support used as the basis for something being constructed.

b) A set of assumptions, concepts, values and practices that constitutes a way of viewing reality.

c) A Risk Management Framework provides guidance to adopt a more holistic approach to managing risk.

d) The application of the Framework is expected to provide employees and organizations a better understanding of the nature of risk and to manage it more systematically.

e) The Risk Management process steps are a generic guide for any entity, regardless of the type of business, activity or function.

f) There are seven steps in the risk management process

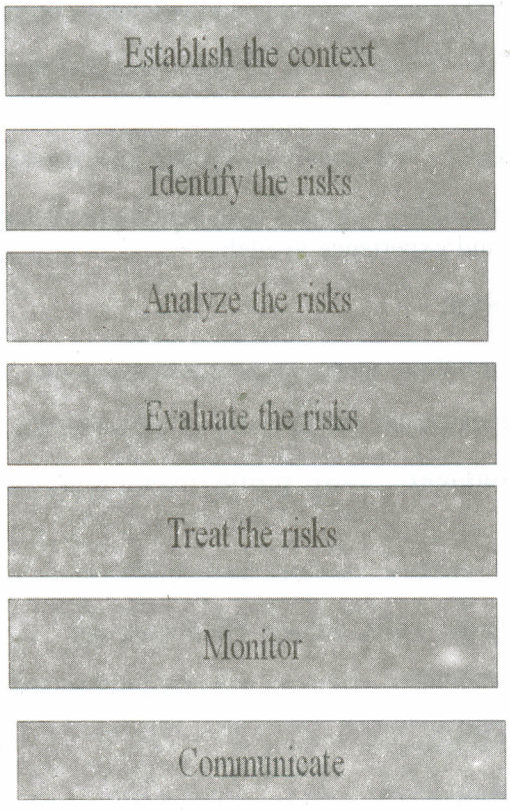


Fig. 9

2.6.2 Established the Context

- Establish the strategic and organizational context in which risk management will take place
- Objectives have to be aligned with the entity's risk appetite, which drives risk tolerance levels for the entity
- **Risk appetite** – A broad boundary of how much risk an entity is prepared to accept
- **Risk tolerance** – The acceptable levels of variation relative to the achievement of objectives
- Objectives can be viewed in the context of four categories:
  - Strategic
  - Operations
  - Reporting
  - Compliance

2.6.3 Identify the Risk

- An event can have a positive or negative impact.
- Events that may have a negative impact represent risks.
- Events may have a positive impact (opportunities), which management may channel back to strategy setting.

- Risks from internal or external sources have to be identified.
- Risk identification can start with the source of the problems or the problem itself.
- Internal and external factors combine and interact to influence the risk profile
  - **Known Risks** – These are the obvious risks that jump out quickly at the beginning of every project
  - **Unknown Risks** – Are usually a result of inexperience in particular areas
  - **Unknowable Risks** – Are risks that can't be predicted even with the best information and experience available.

2.6.4 Sources of Risk

- **Products** – configuration, technology, requirements etc.
- **Procedures** – development and operational processes etc.
- **Business environment** – cost, profit, regulations, competition, market fluctuations etc.
- **Projects** – scope, schedule, resource availability etc.
- **People** – human error, skills, culture, blind spots etc.
- **External** – public opinion, economy, natural disasters etc.

2.6.5 Analyze the Risk

- How likely is the risk event to happen? (Probability and frequency)
- What would be the impact, cost or consequences of that event occurring? (Economic, political, social)

Impact vs. Probability

Risk Ranking				
		Probability		
		High	Medium	Low
Impact Exposure	High	1	2	4
	Medium	3	5	7
	Low	6	8	9

Fig. 10

Evaluate the Risk

- Employ a combination of both qualitative and quantitative risk assessment methodologies
- Assess risk on both an inherent and a residual basis

Techniques of Assessment

a) **Qualitative Techniques**

- Questionnaire
- Survey
- Interviews

b) **Quantitative techniques**

- Probability based techniques
- Back testing
- Non. Probabilistic Techniques
- Sensitivity Analysis
- Scenario Analysis
- Stress Testing
- Bench Marking

Treat The Risks

- Identify and evaluat possible responses to risk.
- Evaluate the options in relation to entity's risk appetite, cost vs. benefit of potential risk responses and degree to which a response will reduce impact and/or likelihood.
- Select and execute response based on evaluation of the portfolio of risks and responses

Risk Responses

a) **Risk avoidance**

- Disposing off a business unit, product line, geographical segment.
- Deciding not to engage in new initiatives/activities that would give rise to the risks

b) **Risk sharing/transfer**

- Insuring significant expected losses.
- Entering into Joint venture/Partnership.
- Entering into syndication agreements.
- Hedging risks.
- Outsourcing Business processes.
- Sharing risks through contractual agreements.

c) **Risk mitigation**

- Diversifying product offerings.
- Establishing operational limits.
- Establishing effective business processes.
- Enhancing mgt. involvement in decision-making,monitoring.
- Rebalancing portfolio of assets to reduce exposure to losses.
- Reallocating capital among operating units.

d) **Risk acceptance**

- "Self-insuring" against loss.

- Relying on natural offsets within a portfolio.
- Accepting risk as already conforming to risk tolerances "if it happens, it happens and we'll deal with it"

Monitor

- Monitor activities and processes to determine the accuracy of planning assumptions and the effectiveness of the measures taken to treat the risk.
- Methods can include data evaluation, audit, compliance measurement.

Communicate

Information is needed at all levels of organization.

Multiple strategies can be used per risk event and strategies may change with time

Cheek Your Progress 2

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) What am I hoping to achieve by performing a Risk Assessment?

.....

.....

.....

.....

2) Why is Risk Assessment Important?

.....

.....

.....

.....

3) What are the techniques of Risk Assessment?

.....

.....

.....

.....

4) What are Risk Responses?

.....

.....

.....

.....

2.7 SUCCESSFUL ASSESSMENT MANAGEMENT

Successful risk assessments require full support of senior management and must

be conducted by teams that include both functional managers and information technology administrators. As business operations, workflow or technologies change, periodic reviews must be conducted to analyze these changes, to account for new threats and vulnerabilities created by these changes and to determine the effectiveness of existing controls.

Departments whose units handle or manage information assets or electronic resources should conduct formal risk assessments. A risk assessment is a process by which to determine what information resources exist that require protection and to understand and document potential risks from IT security failures that may cause loss of information confidentiality, integrity or availability. The purpose of a risk assessment is to help management create appropriate strategies and controls for stewardship of information assets.

The risk assessment tool may be used to identify assets as well as the risks to those assets, to estimate the likelihood of security failures and to identify appropriate controls for protecting assets and resources. Management should evaluate the outcome of the risk assessment to prioritize solutions for potential problems, taking into account the severity of likely ramifications and the expense of implementing cost-effective and reasonable safeguards or controls.

2.7.1 Components of a Risk Assessment

2.7.1.1 Administrative Safeguards

These include, but are not limited to, those control measures that ensure

- classification of data handled by the unit and determination of controls to protect those assets;
- documentation of procedures, standards and recommended practices to ensure that applicable policies and controls are implemented appropriately for a given business process;
- identification of personnel who are authorized to access systems;
- assurance that appropriate authorization controls are implemented;
- security awareness training and education for all personnel; and
- background checks prior to the selection and hiring of new personnel into critical positions.

2.7.1.2 Logical Safeguards

These encompass the range of technical controls that

- ensure access by only authorized users and session termination when finished;
- enforce secure password management;
- manage tracking of development, maintenance and changes to application software and information systems;
- manage access to the network; and
- ensure event logging.

2.7.1.3 Physical Safeguards

These protect physical resources through controls that

- allow access by only authorized individuals, through the use of physical means, such as locks, badge readers or access cards;

- ensure the prevention, detection, early warning of and recovery from emergency disruptions, such as flooding, power failures or earthquakes; and
- Govern the receipt and removal of hardware and electronic media, including equipment reassignment and final disposition of equipment.

The risk assessment measurement criteria detailed below were developed based on professional advisory guidance published by the IIA and Information Systems Assurance and Control Association (ISACA).

2.8 RISK ASSESSMENT METHODOLOGY

Many different approaches to risk assessment have been developed. These following guidelines provide a simple step-by-step process. Additional resources and methodologies are linked under Resources to help you establish an approach appropriate to your business environment.

2.8.1 General Guidelines for a Risk Assessment

1) **Establish the risk assessment team.** The risk assessment team will be responsible for the collection, analysis and reporting of the assessment results to management. It is important that all aspects of the activity work flow be represented on the team, including human resources, administrative processes, automated systems and physical security.

2) **Set the scope of the project**. The assessment team should identify at the outset the objective of the assessment project, department or functional area to be assessed, the responsibilities of the members of the team, the personnel to be interviewed, the standards to be used, documentation to be reviewed and operations to be observed.

3) **Identify assets covered by the assessment**. Assets may include, but are not limited to, personnel, hardware, software, data (including classification of sensitivity and criticality), facilities and current controls that safeguard those assets. It is key to identify all assets associated with the assessment project determined in the scope.

4) **Categorize potential losses.** Identify the losses that could result from any type of damage to an asset. Losses may result from physical damage, denial of service, modification, unauthorized access or disclosure. Losses may be intangible, such as the loss of the organizations' credibility.

5) **Identify threats and vulnerabilities.** A threat is an event, process, activity or action that exploits a vulnerability to attack an asset. Include natural threats, accidental threats, human accidental threats and human malicious threats. These could include power failure, biological contamination or hazardous chemical spills, acts of nature or hardware/software failure, data destruction or loss of integrity, sabotage or theft or vandalism. A vulnerability is a weakness which a threat will exploit to attack the assets. Vulnerabilities can be identified by addressing the following in your data collection process: physical security, environment, system security, communications security, personnel security, plans, policies, procedures, management, support etc.

6) **Identify existing controls.** Controls are safeguards that reduce the probability that a threat will exploit a vulnerability to successfully attack an asset. Identify those safeguards that are currently implemented and determine their effectiveness in the context of the current analysis.

7) **Analyze the data.** In this phase, all the collected information will be used to determine the actual risks to the assets under consideration. A technique to

analyze data includes preparing a list of assets and showing corresponding threats, type of loss and vulnerability. Analysis of this data should include an assessment of the possible frequency of the potential loss.

8) **Determine cost-effective safeguards.** Include in this assessment the implementation cost of the safeguard, the annual cost to operate the safeguard and the life cycle of the safeguard.

9) **Report.** The type of report to make depends on the audience to whom it is submitted. Typically, a simple report that is easy to read and supported by detailed analysis, is more easily understood by individuals who may not be familiar with your organization. The report should include findings; a list of assets, threats and vulnerabilities; a risk determination, recommended safeguards and a cost benefit analysis.

2.8.2 Information Security Risk Assessment

Introduction

A risk assessment is an important part of any information security process. A risk assessment is used to understand the scale of a threat to the security of information and the probability for the threat to be realized. The result of a risk assessment can be used to prioritize efforts to counteract the threats. The following scenarios illustrate how a risk assessment will assist in making information security decisions.

Scenarios

1) A printed list of all Harvard employees with their names, addresses and social security numbers is left in a public place for a courier to pick up on a weekly basis.

2) A printed list of HUIDs, with no names or any other information, is intended for an external consultant and dropped into a mailbox.

Risks

Risks are present in both scenarios; the first scenario presents a far greater risk than the second. In the first scenario, detailed information suitable for identity theft on many people would be exposed if someone were to steal the printout. It would be easy to do so since it is left in a public place for pickup.

In the second scenario, only a few confidential HUIDs, not easily used for identity theft, might be exposed. The US mail system is quite secure so it would be difficult for someone to steal the letter. In the first scenario the scale of the threat is high and the threat probability is also high. In the second scenario the risk and threat probabilities are both low.

Recommendations

Efforts should be focused on mitigating risks such as that in the first scenario. These efforts may include reducing the information that is transported, (for example by only sending information about new hires using HUIDs to identify individuals) or by securing the transport, through use of an encrypted file transfer for example.

In some cases the risk may outweigh the value of the function and the best solution is to stop the function.

Only after significant threats are mitigated should users focus on any low risk situations. In some cases the risk of exposure or exploitation will be low enough that the cost of mitigation outweighs the risk.

Performing a risk assessment will help determine where to focus resources, when to think about modifying functions and when to stop using that function as the risks may not warrant corrective action.

2.9 FINANCIAL RISK ASSESSMENT

Successful business growth requires timely and sufficient financing. Capital and cash availability, interest rates, creditworthiness and securities' and derivatives' price volatility are some of the risks that organizations have to face on their way to expansion.

Risk Assessment as used by investors, business managers and bankers, is the process of determining the likelihood that a specific or particular negative event will occur. Armed with this statistical probability, the decision maker attempts to undertake a particular venture or investment fully aware of the inherent risks in the event of a particular loss.

Risks in markets can come from uncertainty in financial markets, project failures, legal liabilities, credit risk, accidents, natural causes, disasters and indeed regulatory inertia and gross incompetence as well as deliberate attacks from an adversary.

Several risk management standards exist in business and finance universe because some of the risks faced by institutions and operatives in the market may be multiple in nature and may not be amenable to a single or one directional solution.

Effective risk management strategies must include sound value judgment and will certainly include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, accepting some or all of the consequences of a particular risk and creating a risk value system where certain risks are aggregated and pooled for operational core knowledge and skill acquisitions within the institutional environment.

Portfolio and fund managers traditionally use Conditional Value at Risk (cVaR) to gauge and reduce the risks associated with the potential of incurring large losses to their portfolios. Mortgage lenders in competitive and properly regulated markets use Loan_to_Value Ratios to evaluate the risks associated with lending funds to purchase a particular property in particular neighborhoods, regions, markets etc. Bankers and other financial institutions use Credit Analysis to gauge a potential borrower's financial data, ability to repay the loan and eventually at what interest rate to lend money within regulatory guidelines.

For institutions such as banks and investment and portfolio managers, risk assessment is a step in a procedure. It is the determination of quantitative and or qualitative value of risks related to a concrete situation and a known threat.

The quantitative approach calls for calculations of the Risk and the magnitude of the Loss. A third component requires estimation of the Probability that the Loss will occur. A calculation with high probability of occurring will definitely be treated differently from one with a low probability of occurring.

Risks with high and low probabilities of occurring may be given equal priority and weight theoretically, however, in practice, it is very difficult to manage when economic conditions such as scare resources, time, know how etc. are taken into consideration.

In Finance, banking, insurance, pharmaceutical and health, aviation and transportation, energy, natural resource extractions, national security and management of the national economy, risk assessments and efficient risk management are the hallmarks of an effective regime.

In each of these and more, efficient risk management require a prioritization process where the risks with the greatest loss and the highest probability and certainty of occurring are dealt with first and those with lower probability and lower loss are handled in descending order.

In a competitive free market economic environment such as Nigeria, private and government market participants face the enormous task of understanding and effecting the highest and the most value oriented risk balancing act. Balancing between risks with high probability of occurrence but lower loss versus risk with high loss but lower probability of occurrence is very difficult and is susceptible to being mishandled.

When deficient knowledge is applied to a risk management situation, even risks with 100% occurrence rate can be misunderstood and ignored. These intangible risks, a failure of the ability to identify or appreciate risks, when carried out at the economy_wide macro levels morphs into a knowledge deficiency risk which may lead into ineffective collaborations across specific units at the macro levels.

The cascading consequences of these risk appreciation failures are the emergence of relationship risks and ineffective operational procedures.

In both micro and macro-economic units of our free market systems, poor relationship risks and ineffective operational procedures reduce the productivity of all knowledge workers, decrease cost effectiveness, profitability, quality of services, reputation, brand values, quality of earnings etc.

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. More than three centuries of economic thought has shown that an ideal risk management regime minimizes spending and minimizes the negative effects of risks and maximizes positive returns on invested capital.

2.10 ENVIRONMENTAL RISK ASSESSMENT

In order to understand what is meant by environmental risk assessment it is important to be familiar with the concepts of hazard and risk. These terms have different meanings and are not interchangeable. The following definitions are used here.

Hazard: is the inherent potential for something to cause harm.

Hazards can include substances, machines, energy forms or the way work is carried out.

Risk: is the likelihood that harm will actually be done by the realisation of the hazard during the work being carried out or by the way something is used.

Risk = Hazard × Exposure.

In general, the term environmental covers the physical surroundings that are common to everybody including air, water, land, plants and wildlife. The definition used in the Environmental Protection Act 1990 is that the environment '... consists of all or any, of the following media, namely the air, water and land'.

Thus environmental risk assessment covers the risk to all ecosystems, including humans, exposed via or impacted via, these media. The term environmental risk assessment does not normally cover the risks to individuals or the general public at large from consumer products or from exposure in the work place, where other specific legislation applies.

Stages in carrying out an environmental risk assessment

Environmental risk assessment can be thought of as containing the following key stages:

1) Hazard identification. This would typically include identification of the property or situation that could lead to harm. This step is sometimes also known as problem formulation.

2) Identification of consequences if the hazard was to occur. This step is sometimes also known as hazard identification.

3) Estimation of the magnitude of the consequences. This can include consideration of the spatial and temporal scale of the consequences and the time to onset of the consequences. When considering chemicals, this step can sometimes be termed release assessment.

4) Estimation of the probability of the consequences. There are three components to this, the presence of the hazard, the probability of the receptors being exposed to the hazard and the probability of harm resulting from exposure to the hazard. This step can sometimes be called exposure assessment or consequence assessment.

5) Evaluating the significance of a risk (often termed risk characterization or risk estimation) is the product of the likelihood of the hazard being realised and the severity of the consequences.

A concept frequently used in environmental risk assessment is that of the source - pathway – receptor. In this model the pathway between a hazard source (for example a source of contamination) and a receptor (for example a particular ecosystem) is investigated. The pathway is the linkage by which the receptor

could come into contact with the source (a number of pathways often need to be considered). If no pathway exists then no risk exists. If a pathway exists linking the source to the receptor then the consequences of this is determined. This approach is used in the assessment of contaminated land, but can be and is, applied to many other areas. An EHSC note is available on the assessment of contaminated land.

Example Sources	Example Pathways	Example Receptors
Contaminated soils	Air	People
Contaminated water	Water	Domestic and commercial property
Leaking drums	Soil	Infrastructure
Industrial process releases	Food chain	Ecosystems
		Animals
		Plants
		Controlled waters

At the end of the risk assessment process, existing controls should be recorded and further measures may need to be considered to reduce or eliminate the risks identified. Detailed consideration of risk management is beyond the scope of this paper but, in general terms, risk management can be achieved by reducing or modifying the source, by managing or breaking the pathway and/or modifying the receptor.

The final stage is the evaluation of the significance of the risk which involves placing it in a context for example with respect environmental standard or other criterion defined in legislation, statutory or good practice guidance.

The amount of effort and detail required in assessing each risk can vary widely, but is generally proportionate to its priority and complexity. Thus environmental risk assessments can be carried out on several levels. An example of a relatively common, simplistic, approach based on a risk ranking matrix is shown below. The meanings of high, medium, low and very low can be determined in various ways, for example using a descriptive or numerical scale or often based on expert judgement. Once risks have been identified, the matrix allows the relative importance to be easily determined and the risk can then be prioritized and an appropriate risk management strategy or plan can be implemented. Other relatively simple approaches include the use of assessment sheets whereby the materials and activities are listed and any potential impacts for the environment are described.

Uses of Environmental Risk Assessment

There are a wide range of uses of environmental risk assessment and, although the specific methodology and the responsibility for carrying out the assessment may vary, the core principles and the key stages of the process are fundamentally the same in each case. There is a wide range of legislation that encompasses the principles of environmental risk assessment in relation to chemicals. The European Environment Agency (1999) publication lists some of these but the area is rapidly changing and it is impractical to provide a complete list here. Specific guidance is often available for each piece of legislation. The principles of environmental risk assessment are also applied in a number of other areas, for example flood protection, noise pollution and planning. Some examples of the use of environmental risk assessment are given below:

- Assessing the impacts of chemicals used at existing sites (for example for the Control of Major Accident Hazards (COMAH) Regulations (1999), Environmental Permitting Regulations (2007) and other similar legislation).
- Assessing the impacts of products generated by individual companies/sites due to their use or transport etc.
- Assessing potential impacts of new developments, new sites or new processes as part of the planning procedure (for example in relation to the Town and Country Planning Regulations (1999) (as amended). This is often known as Environmental Impact Assessment or EIA.
- Assessing the impacts of products, processes or services over their life cycle (life cycle assessment or LCA). An EHSC note on LCA is available (see bibliography).
- Consideration of risks to the environment in a company's environmental management system.

(EMS) or eco-management and audit scheme (EMAS). Such schemes are based on continual environmental improvement in which risk assessment plays an important part.

Environmental risk assessment is a key component of determining the safe use of chemicals under this legislation. An EHSC note is available on individual legal and ethical responsibilities for environmental safety.

Check Your Progress 3

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) What is Successful Risk Assessment? What are the components of Risk Assessment?

.....

.....

.....

.....

2) What are general guidelines of Risk Methodology?

.....

.....

.....

.....

3) Explain Financial Risk Assessment.

.....

.....

.....

.....

4) What is environmental Risk Assessment? And what are the stages of it?

.....

.....

.....

.....

.....

2.11 LET US SUM UP

Risk Assessment can take different approaches. It can be quantitative; i.e. it can assign numeric values to probabilities and consequences; it can be qualitative; or it can be some combination of the two. The distinction is important when it comes to applying financial analysis to decisions and priorities. While fully quantitative risk analysis is expensive, costing up to 10 times as much as a qualitative analysis, it provides the best bet for optimizing product or plant performance and corporate value.

Increasingly, industry uses risk analysis tools, such as fault tree analyses or failure modes and effects analysis, to cut costs and to improve safety and reliability. For example, fault tree analysis requires keeping records of how often components or pipes, vessels and instruments fail and require calculating the chances that people will make certain critical mistakes. The same information can be used for controlling costs.

Risk assessment has proven to be a useful tool in making industries safer and more reliable. Experience shows it can also improve a company's bottom line.

2.12 CHECK YOUR PROGRESS : THE KEY

Check Your Progress 1

1) By performing a comprehensive risk assessment we are trying to achieve the following:

   - Measure the likelihood of a person being injured if risk reduction measures are not employed.
   - Measure the impact of risk reduction measures (guarding) on the original risk estimation.
   - Measure the likelihood of a machine control system failing to perform a safety function.
   - Measure the overall performance of all risk reduction measures.
   - Compare the residual risk to the risk level that exists on machines that present similar hazards.
   - The demonstration of due diligence.

2) A risk assessment is a process that is used to evaluate the likelihood of harm occurring and the severity of that harm. The results of the risk assessment can then be used to determine if the work can be performed safely. If the risk is not accepted, decisions must be made regarding additional protective measure that that will help to keep workers safe.

   A safety audit is a process that is used to verify whether or not the risk reduction strategy is consistent with the results of the decisions made during the risk reduction portion of the risk assessment process. Each risk reduction measure is validated in order to ensure that the work is being performed is accordance with the decisions made during the risk assessment.

3) Risk management includes the systematic use of the risk assessment results to make decisions regarding the best practicable strategy that will be used to protect workers from harm.

   Safety management is the system used to ensure that the risk levels achieved during the risk assessment process are maintained.

5) Risk is the possibility or probability that something undesirable (or bad) will happen.

   If you do not perform a risk assessment, you will not know whether risk is present or whether you need to do more to control, reduce or eliminate the risk or whether you can live with the risk

Check Your Progress 2

1) The aim of the risk assessment process is to remove a hazard or reduce the level of its risk by adding precautions or control measures, as necessary. By doing so, you have created a safer and healthier environement.

2) Risk assessments are important as they reduce the risks of accidents and ill health to you and your employees that could be very costly both physically and financially.

Risk assessments are very important as they form an integral part of a good occupational health and safety management plan. They help to:

- Create awareness of hazards and risks.
- Identify who may be at risk (employees, cleaners, visitors, contractors, the public etc).
- Determine if existing control measures are adequate or if more should be done.
- Prevent injuries or illnesses when done at the design or planning stage.
- Prioritize hazards and control measures.

3) a) **Qualitative Techniques**

- Questionnaire
- Survey
- Interviews

b) **Quantitative techniques**

- Probability based techniques
- Back testing
- Non. Probabilistic Techniques
- Sensitivity Analysis
- Scenario Analysis
- Stress Testing
- Bench Marking

4) a) Risk Avoidance

b) Risk Sharing/Transfer

c) Risk Mitigation

d) Risk Acceptance

Check Your Progress 3

1) Successful risk assessments require full support of senior management and must be conducted by teams that include both functional managers and information technology administrators. As business operations, workflow or technologies change, periodic reviews must be conducted to analyze these changes, to account for new threats and vulnerabilities created by these changes and to determine the effectiveness of existing controls. Components are:

a) Administrative Safeguards

b) Logical Safeguards

c) Physical Safeguards

2) General Guidelines are as follows:

a) Establish the risk assessment team.

b) Set the scope of the project.

c) Identify assets covered by the assessment.

d) Categorize potential losses

e) Identify threats and vulnerabilities.

f) Identify existing controls.

g) Analyze the data.

h) Determine cost-effective safeguards

I) Report

3) In terms of the cash you keep on deposit at a bank of building society, the risk is inflation. The capital remains the same, if you take the interest, but inflation eats into the purchasing power over a period of time. If the interest is left in the account, then it needs to be the same as inflation just to keep parity. If the interest you get net is say, 2% and inflation is running at 3% then your purchasing power is reduced by 1% pa over a period of one year. The risk in this case is the financial security of the bank or building society.

   Investment risk depends on many factors, including inflation, interest rates, legislation and the stock market in general.

   How much risk you are able to accept depends on even more factors:

   - The amount of money you are investing against your overall liquid assets
   - The amount of loss you are willing to accept on a set time-line, against the amount of profit you wish to gain through making the investment. The permutations are endless.

4) In general, the term environmental covers the physical surroundings that are common to everybody including air, water, land, plants and wildlife. The definition used in the Environmental Protection Act 1990 is that the environment 'consists of all or any, of the following media, namely the air, water and land'.

   Thus environmental risk assessment covers the risk to all ecosystems, including humans, exposed via or impacted via, these media. The term environmental risk assessment does not normally cover the risks to individuals or the general public at large from consumer products or from exposure in the work place, where other specific legislation applies.

2.13 SUGGESTED READINGS

- Good Practice in Assessing Risk: Current Knowledge, Issues and Approaches (Good Practice in Health, Social Care and Criminal Justice) by Hazel Kemshall and Bernadette Wilkinson.
- Good Practice in Risk Assessment and Risk Management (Good Practice Series) by Hazel Kemshall and Jacki Pritchard.
- Risk Assessment Guidance for Superfund, Volume OSWER. EPA 540-1-89-002. December.
- Risk Assessment: Practitioner's Guide to Predicting Harmful Behaviour by Bryony Moore.
- Torchwood: Risk Assessment by James Goss.

UNIT 3 RISK ANALYSIS TECHNIQUES AND METHODOLOGIES

Structure

3.0 INTRODUCTION

There may be some terminology and definition differences related to risk analysis, risk assessment and business impact analysis. Although several definitions are possible and can overlap, for purposes of this article, please consider the following definitions:

- A risk analysis involves identifying the most probable threats to an organization and analyzing the related vulnerabilities of the organization to these threats.
- A risk assessment involves evaluating existing physical and environmental security and controls and assessing their adequacy relative to the potential threats of the organization.
- A business impact analysis involves identifying the critical business functions within the organization and determining the impact of not performing the business function beyond the maximum acceptable outage. Types of criteria that can be used to evaluate the impact include: customer service, internal operations, legal/statutory and financial.

Most businesses depend heavily on technology and automated systems, and their disruption for even a few days could cause severe financial loss and threaten survival. The continued operations of an organization depend on management's awareness of potential disasters, their ability to develop a plan to minimize disruptions of mission critical functions, and the capability to recover operations expediently and successfully. The risk analysis process provides the foundation for the entire recovery planning effort.

A primary objective of business recovery planning is to protect the organization in the event that all or part of its operations and/or computer services is rendered unusable. Each functional area of the organization should be analyzed to determine the potential risk and impact related to various disaster threats.

3.1 OBJECTIVES

After studying this unit, you should be able to:

- define risk analysis;
- how to analyse risk?
- describe the methodologies to assess/analyse risk; and
- identify risks and its methodologies.

3.2 RISK ANALYSIS

Regardless of the prevention techniques employed, possible threats that could arise inside or outside the organization need to be assessed. Although the exact nature of potential disasters or their resulting consequences are difficult to determine, it is beneficial to perform a comprehensive risk assessment of all threats that can realistically occur to the organization. Regardless of the type of threat, the goals of business recovery planning are to ensure the safety of customers, employees and other personnel during and following a disaster.

The relative probability of a disaster occurring should be determined. Items to consider in determining the probability of a specific disaster should include, but not be limited to: geographic location, topography of the area, proximity to major sources of power, bodies of water and airports, degree of accessibility to facilities within the organization, history of local utility companies in providing uninterrupted services, history of the area's susceptibility to natural threats, proximity to major highways which transport hazardous waste and combustible products.

Potential exposures may be classified as natural, technical or human threats. Examples include:

Natural Threats: internal flooding, external flooding, internal fire, external fire, seismic activity, high winds, snow and ice storms, volcanic eruption, tornado, hurricane, epidemic, tidal wave, typhoon.

Technical Threats: power failure/fluctuation, heating, ventilation or air conditioning failure, malfunction or failure of CPU, failure of system software, failure of application software, telecommunications failure, gas leaks, communications failure, nuclear fallout.

Human Threats: robbery, bomb threats, embezzlement, extortion, burglary, vandalism, terrorism, civil disorder, chemical spill, sabotage, explosion, war, biological contamination, radiation contamination, hazardous waste, vehicle crash, airport proximity, work stoppage (Internal/External), computer crime.

All locations and facilities should be included in the risk analysis. Rather than attempting to determine exact probabilities of each disaster, a general relational rating system of high, medium and low can be used initially to identify the probability of the threat occurring.

The risk analysis also should determine the impact of each type of potential threat on various functions or departments within the organization. A Risk Analysis Form, found here (PDF Format), can facilitate the process. The functions or departments will vary by type of organization.

The planning process should identify and measure the likelihood of all potential risks and the impact on the organization if that threat occurred. To do this, each department should be analyzed separately. Although the main computer system may be the single greatest risk, it is not the only important concern. Even in the most automated organizations, some departments may not be computerized or automated at all. In fully automated departments, important records remain outside the system, such as legal files, PC data, software stored on diskettes or supporting documentation for data entry.

The impact can be rated as: 0 = No impact or interruption in operations, 1 = Noticeable impact, interruption in operations for up to 8 hours, 2 = Damage to equipment and/or facilities, interruption in operations for 8 – 48 hours, 3 = Major damage to the equipment and/or facilities, interruption in operations for more than 48 hours. All main office and/or computer center functions must be relocated.

Certain assumptions may be necessary to uniformly apply ratings to each potential threat. Following are typical assumptions that can be used during the risk assessment process:

1) Although impact ratings could range between 1 and 3 for any facility given a specific set of circumstances, ratings applied should reflect anticipated, likely or expected impact on each area.

2) Each potential threat should be assumed to be "localized" to the facility being rated.

3) Although one potential threat could lead to another potential threat (e.g. a hurricane could spawn tornados), no domino effect should be assumed.

4) If the result of the threat would not warrant movement to an alternate site(s), the impact should be rated no higher than a "2."

5) The risk assessment should be performed by facility.

To measure the potential risks, a weighted point rating system can be used. Each level of probability can be assigned points as follows:

Probability Points

High 10

Medium 5

Low 1

To obtain a weighted risk rating, probability points should be multiplied by the highest impact rating for each facility. For example, if the probability of hurricanes is high (10 points) and the impact rating to a facility is "3" (indicating that a move to alternate facilities would be required), then the weighted risk factor is 30 (10 x 3). Based on this rating method, threats that pose the greatest risk (e.g. 15 points and above) can be identified.

Considerations in analyzing risk include:

1) Investigating the frequency of particular types of disasters (often versus seldom).
2) Determining the degree of predictability of the disaster.
3) Analyzing the speed of onset of the disaster (sudden versus gradual).
4) Determining the amount of forewarning associated with the disaster.
5) Estimating the duration of the disaster.
6) Considering the impact of a disaster based on two scenarios;
    a) Vital records are destroyed
    b) Vital records are not destroyed
7) Identifying the consequences of a disaster, such as;
    a) Personnel availability
    b) Personal injuries
    c) Loss of operating capability
    d) Loss of assets
    e) Facility damage
8) Determining the existing and required redundancy levels throughout the organization to accommodate critical systems and functions, including;
    a) Hardware
    b) Information
    c) Communication
    d) Personnel
    e) Services
9) Estimating potential dollar loss;
    a) Increased operating costs
    b) Loss of business opportunities
    c) Loss of financial management capability
    d) Loss of assets
    e) Negative media coverage
    f) Loss of stockholder confidence
    g) Loss of goodwill
    h) Loss of income

i) Loss of competitive edge

j) Legal actions.

10) Estimating potential losses for each business function based on the financial and service impact and the length of time the organization can operate without this business function. The impact of a disaster related to a business function depends on the type of outage that occurs and the time that elapses before normal operations can be resumed.

11) Determining the cost of contingency planning.

3.3 EVALUATING AND MANAGING RISKS

Almost everything we do in today's business world involves a risk of some kind: customer habits change, new competitors appear, and factors outside your control could delay your project. But formal risk analysis and risk management can help you to assess these risks and decide what actions to take to minimize disruptions to your plans. They will also help you to decide whether the strategies you could use to control risk are cost-effective.

Here we define risk as 'the perceived extent of possible loss'. Different people will have different views of the impact of a particular risk – what may be a small risk for one person may destroy the livelihood of someone else.

One way of putting figures to risk is to calculate a value for it as:

Risk = probability of event × cost of event

Doing this allows you to compare risks objectively. We use this approach formally in decision making with Decision Trees.

To carry out a risk analysis, follow these steps:

3.3.1 Identify Threats

The first stage of a risk analysis is to identify threats facing you. Threats may be:

- **Human** – from individuals or organizations, illness, death etc.
- **Operational** – from disruption to supplies and operations, loss of access to essential assets, failures in distribution etc.
- **Reputational** – from loss of business partner or employee confidence or damage to reputation in the market.
- **Procedural** – from failures of accountability, internal systems and controls, organization, fraud etc.
- **Project** – risks of cost over-runs, jobs taking too long, of insufficient product or service quality etc.
- **Financial** – from business failure, stock market, interest rates, unemployment etc.
- **Technical** – from advances in technology, technical failure etc.
- **Natural** – threats from weather, natural disaster, accident, disease etc.
- **Political** – from changes in tax regimes, public opinion, government policy, foreign influence etc.
- Others

This analysis of threat is important because it is so easy to overlook important threats. One way of trying to capture them all is to use a number of different approaches:

- Firstly, run through a list such as the one above, to see if any apply.
- Secondly, think through the systems, organizations or structures you operate, and analyze risks to any part of those.
- See if you can see any vulnerability within these systems or structures.
- Ask other people, who might have different perspectives.

3.3.2 Estimate Risks

Once you have identified the threats you face, the next step is to work out the likelihood of the threat being realized and to assess its impact.

One approach to this is to make your best estimate of the probability of the event occurring, and to multiply this by the amount it will cost you to set things right if it happens. This gives you a value for the risk.

3.3.3 Manage Risks

Once you have worked out the value of risks you face, you can start to look at ways of managing them. When you are doing this, it is important to choose cost effective approaches – in most cases, there is no point in spending more to eliminating a risk than the cost of the event if it occurs. Often, it may be better to accept the risk than to use excessive resources to eliminate it.

Risk may be managed in a number of ways:

- **By using existing assets**

  Here existing resources can be used to counter risk. This may involve improvements to existing methods and systems, changes in responsibilities, improvements to accountability and internal controls etc.

- **By contingency planning**

  You may decide to accept a risk, but choose to develop a plan to minimize its effects if it happens. A good contingency plan will allow you to take action immediately, with the minimum of project control if you find yourself in a crisis management situation. Contingency plans also form a key part of Business Continuity Planning (BCP) or Business Continuity management (BCM).

- **By investing in new resources**

  Your risk analysis should give you the basis for deciding whether to bring in additional resources to counter the risk. This can also include insuring the risk: Here you pay someone else to carry part of the risk – this is particularly important where the risk is so great as to threaten your or your organization's solvency.

3.3.4 Review

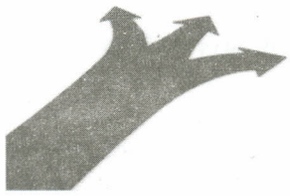
Once you have carried out a risk analysis and management exercise, it may be worth carrying out regular reviews. These might involve formal reviews of the risk analysis or may involve testing systems and plans appropriately.

Risk analysis allows you to examine the risks that you or your organizations face. It is based on a structured approach to thinking through threats, followed by an evaluation of the probability and cost of events occurring.

Risk analysis forms the basis for risk management and crisis prevention. Here the emphasis is on cost effectiveness. Risk management involves adapting the use of existing resources, contingency planning and good use of new resources.

3.4 DECISION TREE

Decision Trees are excellent tools for helping you to choose between several courses of action. They provide a highly effective structure within which you can lay out options and investigate the possible outcomes of choosing those options. They also help you to form a balanced picture of the risks and rewards associated with each possible course of action.



Evaluate all of your options

3.4.1 Drawing a Decision Tree

You start a Decision Tree with a decision that you need to make. Draw a small square to represent this towards the left of a large piece of paper.

From this box draw out lines towards the right for each possible solution and write that solution along the line. Keep the lines apart as far as possible so that you can expand your thoughts.

At the end of each line, consider the results. If the result of taking that decision is uncertain, draw a small circle. If the result is another decision that you need to make, draw another square. Squares represent decisions and circles represent uncertain outcomes. Write the decision or factor above the square or circle. If you have completed the solution at the end of the line, just leave it blank.

Starting from the new decision squares on your diagram, draw out lines representing the options that you could select. From the circles draw lines representing possible outcomes. Again make a brief note on the line saying what it means. Keep on doing this until you have drawn out as many of the possible outcomes and decisions as you can see leading on from the original decisions.

An example of the sort of thing you will end up with is shown in Fig. 1:

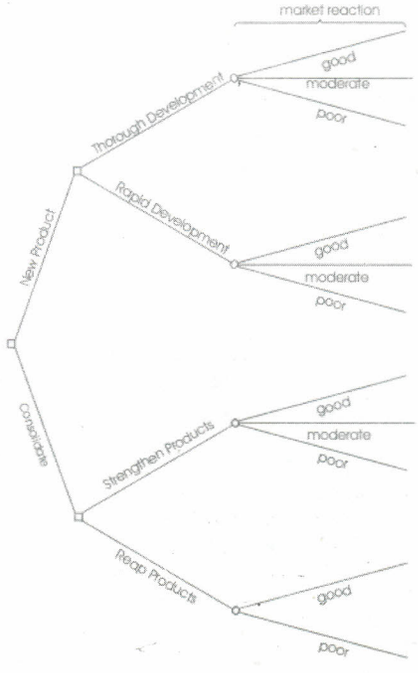


Fig. 1: Example Decision Tree

Once you have done this, review your tree diagram. Challenge each square and circle to see if there are any solutions or outcomes you have not considered. If there are, draw them in. If necessary, redraft your tree if parts of it are too congested or untidy. You should now have a good understanding of the range of possible outcomes of your decisions.

3.4.2 Evaluating Your Decision Tree

Now you are ready to evaluate the decision tree. This is where you can work out which option has the greatest worth to you. Start by assigning a cash value or score to each possible outcome. Estimate how much you think it would be worth to you if that outcome came about.

Next look at each circle (representing an uncertainty point) and estimate the probability of each outcome. If you use percentages, the total must come to 100% at each circle. If you use fractions, these must add up to 1. If you have data on past events you may be able to make rigorous estimates of the probabilities. Otherwise write down your best guess.

This will give you a tree like the one shown in Fig. 2

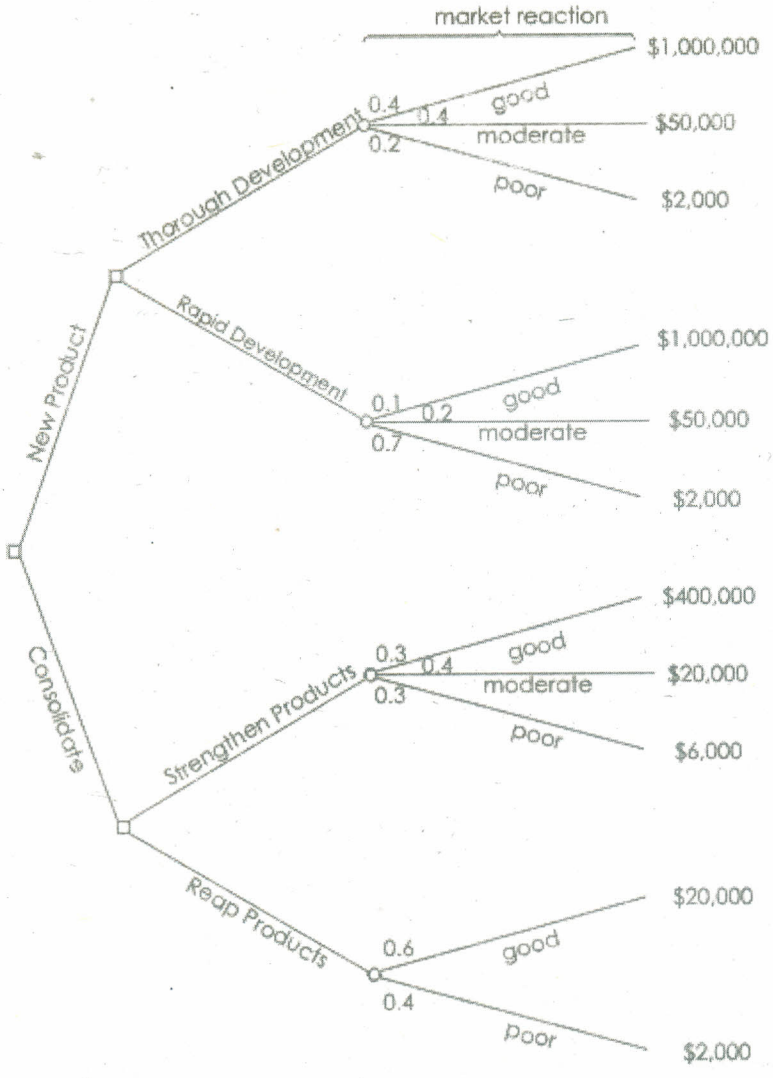


Fig. 2: Example Decision Tree

3.4.3 Calculating Tree Values

Once you have worked out the value of the outcomes and have assessed the probability of the outcomes of uncertainty, it is time to start calculating the values that will help you make your decision.

Start on the right hand side of the decision tree and work back towards the left. As you complete a set of calculations on a node (decision square or uncertainty circle), all you need to do is to record the result. You can ignore all the calculations that lead to that result from then on.

3.4.4 Calculating the Value of Uncertain Outcome Nodes

Where you are calculating the value of uncertain outcomes (circles on the diagram), do this by multiplying the value of the outcomes by their probability. The total for that node of the tree is the total of these values.

In the example in Fig. 2, the value for 'new product, thorough development' is:

0.4 (probability good outcome) x $1,000,000 (value)	=	$400,000
0.4 (probability moderate outcome) x $50,000 (value)	=	$20,000
0.2 (probability poor outcome) x $2,000 (value)	=	$400
		+ $420,400

Fig. 3 shows the calculation of uncertain outcome nodes

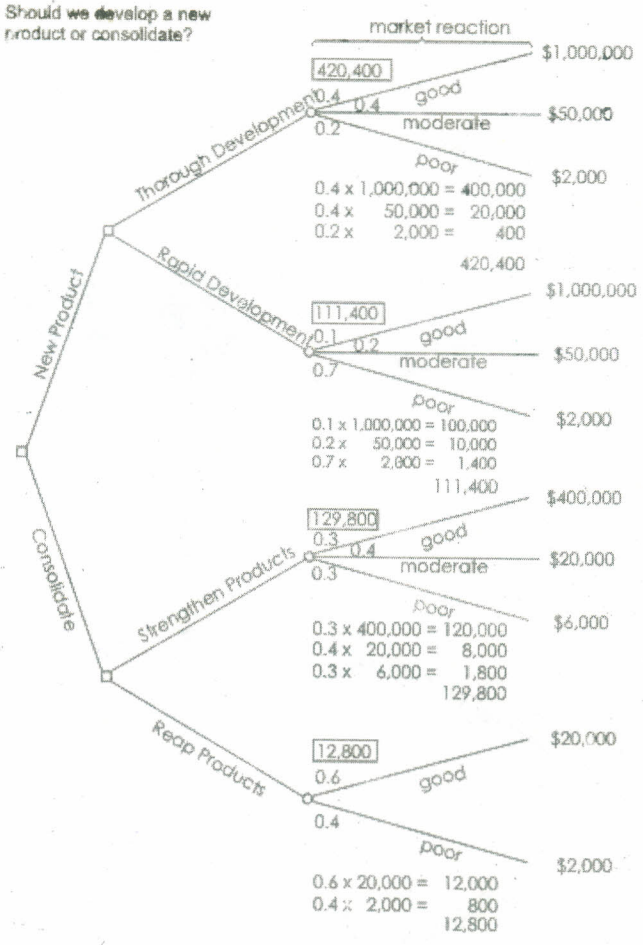


Fig. 3: Example Decision Tree

Note that the values calculated for each node are shown in the boxes.

3.4.5 Calculating the Value of Decision Nodes

When you are evaluating a decision node, write down the cost of each option along each decision line. Then subtract the cost from the outcome value that you have already calculated. This will give you a value that represents the benefit of that decision.

Note that amounts already spent do not count for this analysis – these are 'sunk costs' and (despite emotional counter-arguments) should not be factored into the decision.

When you have calculated these decision benefits, choose the option that has the largest benefit and take that as the decision made. This is the value of that decision node.

Fig. 4 shows this calculation of decision nodes in our example

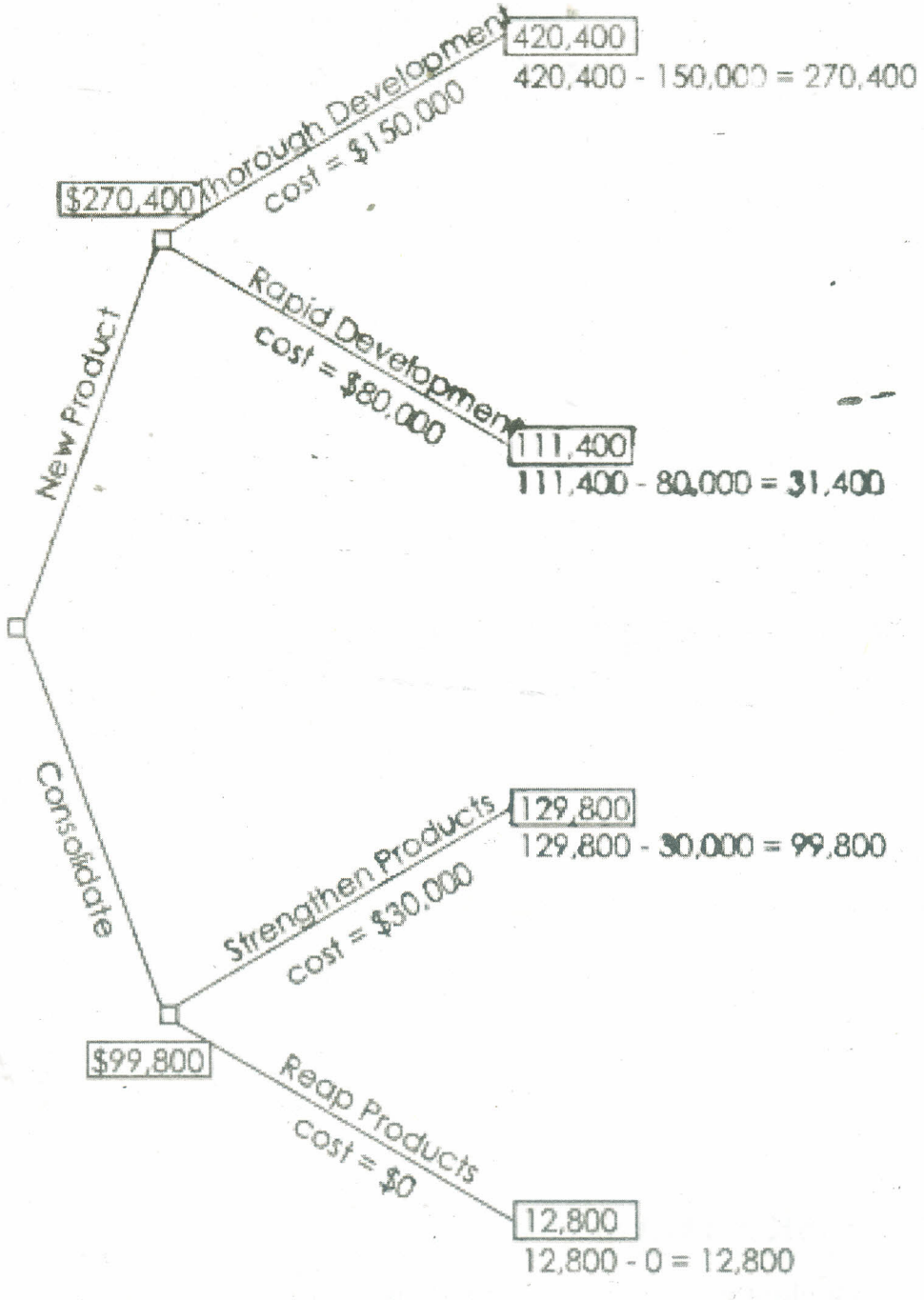


Fig. 4: Example Decision Tree

In this example, the benefit we previously calculated for 'new product, thorough development' was $420,400. We estimate the future cost of this approach as $150,000. This gives a net benefit of $270,400.

The net benefit of 'new product, rapid development' was $31,400. On this branch we therefore choose the most valuable option, 'new product, thorough development' and allocate this value to the decision node.

Result

By applying this technique we can see that the best option is to develop a new product. It is worth much more to us to take our time and get the product right, than to rush the product to market. it is better just to improve our existing products than to botch a new product, even though it costs us less.

Check Your Progress 1

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) What are the steps involved in Risk Analysis Process?

.....

.....

.....

.....

2) Explain the different phases of Risk Assessment Cycle?

.....

.....

.....

.....

3) What are the benefits and drawbacks of Qualitative Risk Analysis?

.....

.....

.....

.....

4) What are the key ideas for identifying Schedule Risks?

.....

.....

.....

.....

3.5 RISK ANALYSIS METHODOLOGIES

3.5.1 Qualitative Risk Analysis Methodologies

In the this section, we will deal with the qualitative methods used in risk analysis namely preliminary risk analysis (PHA), hazard and operability study (HAZOP) and failure mode and effects analysis (FMEA/FMECA).

3.5.1.1 Primary Risk Analysis

- Preliminary Risk Analysis Preliminary risk analysis or hazard analysis is a qualitative technique which involves a disciplined analysis of the event sequences which could transform a potential hazard into an accident. In this

technique, the possible undesirable events are identified first and then analyzed separately. For each undesirable events or hazards, possible improvements or preventive measures are then formulated.

- The result from this methodology provides a basis for determining which categories of hazard should be looked into more closely and which analysis methods are most suitable. Such an analysis also proved valuable in the working environment to which activities lacking safety measures can be readily identified. With the aid of a frequency/consequence diagram, the identified hazards can then be ranked according to risk, allowing measures to be prioritized to prevent accidents

3.5.1.2 Hazard and Operability studies (HAZOP)

- The HAZOP technique was developed in the early 1970s by Imperial Chemical Industries Ltd. HAZOP can be defined as the application of a formal systematic critical examination of the process and engineering intentions of new or existing facilities. To assess the hazard potential that arises from deviation in design specifications and the consequential effects on the facilities as a whole.

- This technique is usually performed using a set of guidewords: NO/NOT, MORE/LESS OF, AS WELL AS, PART OF REVERSE AND OTHER THAN. From these guidewords, scenarios that may result in a hazard or an operational problem are identified. Consider the possible flow problems in a process line, the guide word MORE OF will correspond to high flow rate, while that for LESS THAN, low flow rate. The consequences of the hazard and measures to reduce the frequency with which the hazard will occur are then discussed.

  This technique had gained wide acceptance in process industries as an effective tool for plant safety and operability improvements.

3.5.1.3 Failure Mode and Effects Analysis (FMEA/FMECA)

- This method was developed in the 1950s by reliability engineers to determine problems that could arise from malfunctions of military system. Failure mode and effects analysis is a procedure by which each potential failure mode in a system is analyzed to determine its effect on the system and to classify it according to its severity.

- When the **FMEA** is extended by a criticality analysis, the technique is then called **failure mode and effects criticality analysis (FMECA)**. Failure mode and effects analysis has gained wide acceptance by the aerospace and the military industries. In fact, the technique has adapted itself in other form such as misuse mode and effects analysis.

3.5.1.4 Discussion and Conclusion

- The three techniques outlined above require only the employment of "hardware familiar" personnel. However, FMEA tends to be more labor intensive, as the failure of each individual component in the system has to be considered. A point to note is that these qualitative techniques can be used in the design as well as operational stage of a system.

- All the techniques mentioned above have seen wide usage in the nuclear and chemical processing plants. In fact, FMEA, one of the most documented techniques in use; it has been used by "Intel" and "National Semiconductor" to improve the reliability of their products. For the case of preliminary risk analysis, it has seen application in safety analysis in both industry and on offshore platforms. HAZOP, on the other hand, has been widely used in the chemical industries for detailed failure and effect study on the piping and instrumentation layout.

3.5.2 Tree based Techniques

In this section, fault-tree analysis (FTA), event-tree analysis(ETA), cause-consequence analysis(CCA), management oversight risk tree(MORT) and safety management organisation review technique (SMORT) will be discussed.

3.5.2.1 Fault Tree Analysis

The concept of fault tree analysis (FTA) was originated by Bell Telephone Laboratories in 1962 as a technique with which to perform a safety evaluation of the Minutemen Intercontinental Ballistic Missile Launch Control System. A fault tree is a logical diagram which shows the relation between system failure, ie. a specific undesirable event in the system and failures of the components of the system. It is a technique based on deductive logic. An undesirable event is first defined and causal relationships of the failures leading to that event are then identified.

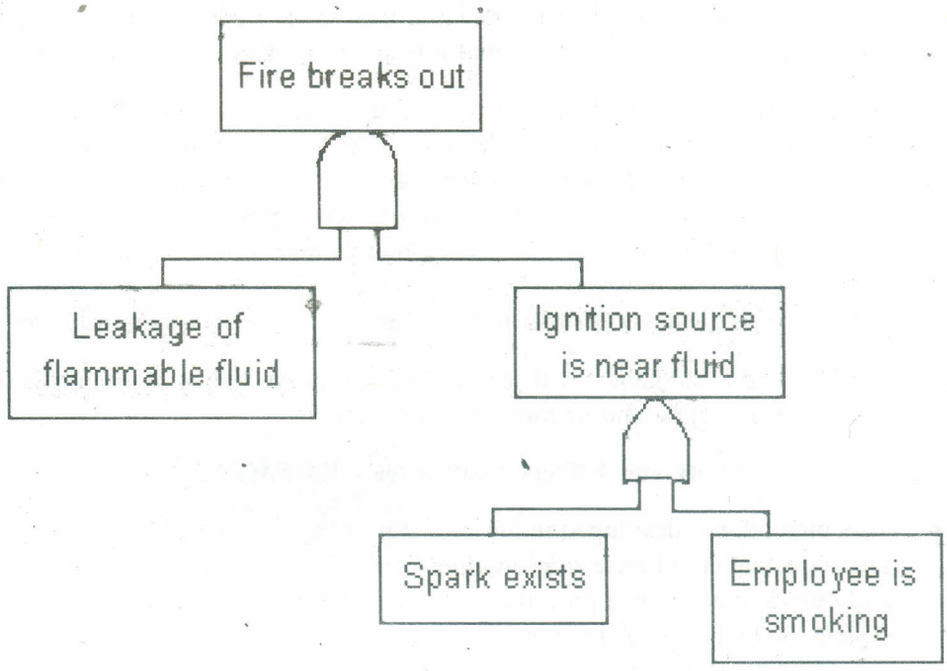


Fig. 5: A fault tree depicting the event "Fire breaks out"

Fault tree can be used in qualitative or quantitative risk analysis. The difference in them is that the qualitative fault tree is looser in structure and does not require use of the same rigorous logic as the formal fault tree. Fig. 5 shows a fault tree with top event "Fire breaks out". This method is used in a wide range of industries and there is extensive support in the form of published literature and software packages, such as CARA. An application of fault tree analysis on causal relations for large vehicle accidents is documented in.

3.5.2.2 Event Tree Analysis

Event tree analysis is a method for illustrating the sequence of outcomes which may arise after the occurrence of a selected initial event. This technique, unlike fault tree uses inductive logic. It is mainly used in consequence analysis for pre-incident and post-incident application. The left side connects with the initiator, the right side with plant damage state; the top defines the systems; nodes (dots) call for branching probabilities obtained from the system analysis. If the path goes up at the node, the system succeeded, if down, it failed.

ETA has seen application in the nuclear industries for operability analysis of nuclear power plant as well as accident sequence in the Three Mile Island-2 reactor's accident.

3.5.2.3 Cause-Consequence Analysis

Cause-consequence analysis (CCA) is a blend of fault tree and event tree analysis . This technique combines cause analysis (described by fault trees) and consequence analysis (described by event trees) and hence deductive and inductive analysis is used. The purpose of CCA is to identify chains of events that can result in undesirable consequences. With the probabilities of the various events in the CCA diagram, the probabilities of the various consequences can be calculated, thus establishing the risk level of the system. Fig. 6 below shows a typical CCA.

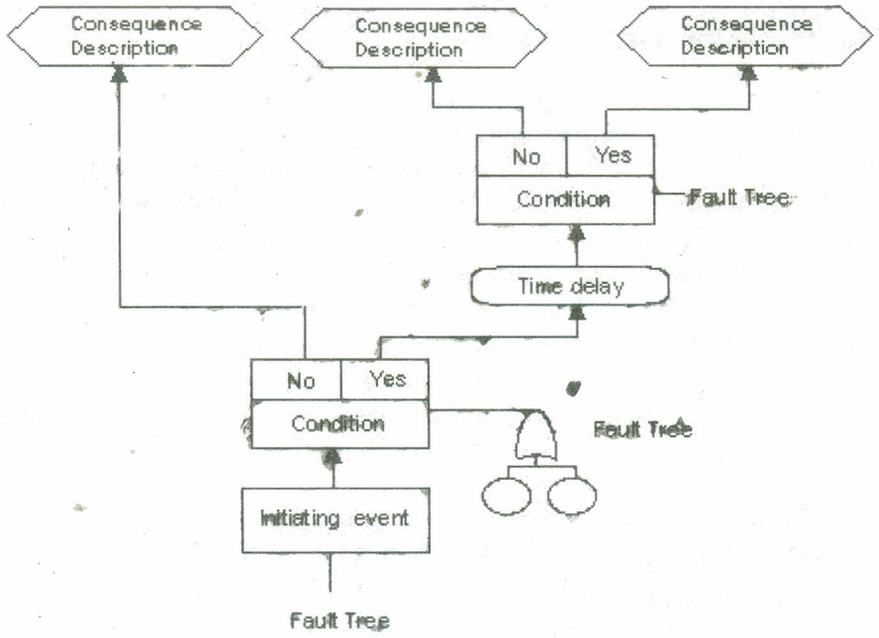


Fig. 6: A typical Cause-Consequence Analysis

This technique was invented by RISO Laboratories in Denmark to be used in risk analysis of nuclear power stations. However, it can also be adapted by the other industries in the estimation of the safety of protective or other systems. Details on how to carry out cause consequence analysis as well as the benefits and restrictions of it are documented in literature.

3.5.2.4 Management Oversight Risk Tree

Management oversight risk tree(MORT) was developed in the early 1970s for the U.S. Energy Research and Development Administration as safety analysis method that would be compatible with complex, goal-oriented management systems. MORT is a diagram which arranges safety program elements in an orderly and logical manner. Its analysis is carried out by means of fault tree, where the top event is "Damage, destruction, other costs, lost production or reduced credibility of the enterprise in the eyes of society". The tree gives an overview of the causes of the top event from management oversights and omissions or from assumed risks or both.

The MORT tree has more than 1500 possible basic events inputed to 100 generic events which have being increasing identified in the fields of accident prevention, administration and management. A generic MORT diagram is included at the end of this report. MORT is used in the analysis or investigation of accidents and events and evaluation of safety programs. Its usefulness was revealed in literature, "normal investigations revealed an average of 18 problems (and recommendations). Complementary investigations with MORT analysis revealed additional 20 contributions per case".

3.5.2.5 Safety Management Organization Review Technique

Safety management organization review technique(SMORT) is a simplified modification of MORT developed in Scandinavia. This technique is structured by means of analysis levels with associated checklists, while MORT is based on a comprehensive tree structure. Owing to its structured analytical process, SMORT is classified as one of the tree based methodologies.

The SMORT analysis includes data collection based on the checklists and their associated questions, in addition to evaluation of results. The information can be collected from interviews, studies of documents and investigations. This technique can be used to perform detailed investigation of accidents and near misses. It also served well as a method for safety audits and planning of safety measures.

3.5.2.6 Discussion and Conclusion

The tree-based methods are mainly used to find cut-sets leading to the undesired events. In fact, event tree and fault tree have been widely used to quantify the probabilities of occurrence of accidents and other undesired events leading to the loss of life or economic losses in probabilistic risk assessment. However, the usage of fault tree and event tree are confined to static, logic modeling of accident scenarios. In giving the same treatment to hardware failures and human errors in fault tree and event tree analysis, the conditions affecting human behavior can not be modeled explicitly. This affects the assessed level of dependency between events. No doubt, there exists techniques such as human cognitive reliability to reconcile such deficiencies in the fault tree analysis; new methodologies that model such responses have emerged.

3.6 QUALITATIVE RISK ANALYSIS METHODOLOGY

Risk analysis can be broken down into two broad methods and these methods are qualitative and quantitative. The qualitative method for risk analysis is designed for the purpose of enhancing one's awareness of potential problems and can assist one in analyzing these risks.

Quantitative risk analysis is designed so that the security measures can be implemented and this will allow the cost envelope to be implemented as well. There is yet a third method for risk analysis which is used and this is referred to as being the hybrid method, since it borrows characteristics from both the quantitative and qualitative risk analysis methods. Of the three approaches, the qualitative analysis is the most simple to use and is therefore used the most often.

Qualitative analysis is useful because it allows one to quickly identify potential risks, as well as assets and resources which are vulnerable to these risks. Not only does qualitative analysis showcase the safety measures that have already been utilized, it will show those which could be useful if they are implemented.

The goal of qualitative risk analysis is to gain a level of risk protection which is acceptable and one which will increase awareness among the necessary members of the organization. This analysis will often make use of calculations which are fairly basic and it is often not necessary to know the value of all the assets in question.

While quantitative analysis does many of the same things which can be found with qualitative analysis, it is also capable of identifying the envelopes for which both safeguards and losses can be found. It is based on a process which is highly subjective and it uses metrics which require it to have a high level of effort put into it.

At the same time, quantitative analysis is capable of presenting data in a manner

which is friendly for management and which expresses percentages, values, as well as probabilities. Now that we've gone over the two primary tools which are used for risk analysis, it is next important to learn a little bit about the methodology which is associated with them.

One piece of methodology that you will want to familiarize yourself with is the scope statement. The scope statement is one statement which is designed to define the things that must be evaluated, as well as state the form of risk analysis that will need to be performed. The scope statement must also be capable of giving the results which have been expected.

The next piece of methodology which is important to learn is called asset pricing. The information system will be defined based on the scope statement and it will be further split into components which may be priced. While you have the option of splitting the system into smaller pieces, some say it is easier to simply take apart the entire unit, leaving on the components which are tangible.

The tangible components tend to be those which are easier to price. One good example of tangible components is the telecommunications tools that the organization uses. These include tools which are internal as well as external. Any device which is used for communication purposes will need to be included in this category.

Some devices which are great examples of this include both modems, routers and telephones, as well as intercom or PA systems. After communication tools have been considered, the next thing which must be taken into consideration is the software devices. This includes any type of software which must be programmed. Operating systems should be the first thing to come to mind.

Once you have incorporated everything related to software and software applications, you will next need to consider the physical equipment. The physical equipment will include things such as monitors, computers and computer terminals.

Any object which is used for the purpose of displaying information must be considered. Printers should be included in this list, along with disk drives and memory cards. Power supplies should be factored in as well. Any systems which are designed for the purpose of holding data, such as error logs, usage logs or info related to schedules, will need to be factored in the system as well.

Check Your Progress 2

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) Mention the steps followed in identification process.

.....

.....

.....

.....

2) Mention any five risk identification methods along with their advantages and disadvantages.

.....

.....

.....

.....

3) Explain the various inputs of the Qualitative Risk Analysis process.

.....

.....

.....

.....

4) What are the techniques used in risk response planning process?

.....

.....

.....

.....

3.7 RISK BREAKDOWN STRUCTURE

When planning a project to meet targets for cost, schedule or quality, it is useful to identify likely risks to the success of the project. A risk is any possible situation that is not planned for, but that, if it occurs, is likely to divert the project from its planned result. For example, an established project team plans for the work to be done by its staff, but there is the risk that an employee may unexpectedly leave the team.

In Project Management, the Risk Management Process has the objectives of identifying, assessing and managing risks, both positive and negative. All too often, project managers focus only on negative risk, however, good things can happen in a project, "things" that were foreseen, but not expressly planned.

The objective of Risk Management is to predict risks, assess their likelihood and impact and to actively plan what should be done ahead of time to best deal with situations when they occur.

The risk management process usually occurs in five distinct steps: risk management planning, risk identification, risk analysis, risk response planning and risk monitoring and control. The central point of risk identification and assessment in risk management is understanding the risk. However, this is also where project managers and risk subject matter experts (SMEs) get the least help from recognized references, best practices or work standards.

Currently, the Project Management Institute (PMIr) has a team of SMEs working on a Practice Standard for Risk Management. This team has identified one very good tool: the Risk Breakdown Structure (RBS). The RBS helps the project manager, the risk manager and almost any stakeholder to understand and therefore be able to identify and assess risk.

3.7.1 What is a Breakdown Structure?

The RBS will prove extremely valuable to better grasp when a project needs to receive special scrutiny, in other words, when risk might happen. The RBS can also help the project manager and the risk manager to better understand recurring risks and concentrations of risk that could lead to issues that affect the status of the project.

Following the concept of the Work Breakdown Structure (WBS), the Risk Breakdown Structure provides a means for the project manager and risk manager to structure the risks being addressed or tracked. Just as PMI defines the Work

Breakdown Structure as a "deliverable-oriented grouping of project elements that organizes and defines the total work scope of the project..." the RBS could be considered as a "[sic] a hierarchically organized depiction of the identified project risks arranged by risk category."

Many project managers and risk managers currently use "home-grown" methods for listing, identifying, assessing and tracking risks in their projects. These methods include: spreadsheets, listing, generic risk taxonomy, based somewhat loosely on various standards and guidelines.

An approach that simply places the risks in a list, a simple table or even in a database does not provide the strength of using a structured, organized method similar to a Work Breakdown Structure. To fully understand the risks and better identify and assess the risk, a "deep-dive" into each risk, recording as many levels of identification as necessary, may be required. The project value of placing risks in a structure such as this lies in the ability of the project manager and risk manager to then quickly and easily identify and assess the risk, identify the potential risk triggers and develop a more robustrisk response plan. If all risks are placed in a hierarchical structure as they are identified and the structure is organized by source, the total risk exposure to the project can be more easily understood and planning for the risk more easily accomplished.

3.7.2 Using the Risk Breakdown Structure

The RBS serves as more than just a "database" for identifying risks to the project. When created, the RBS provides a vehicle for risk analysis and reporting and risk comparison across projects. Most importantly, the RBS is "the" tool for risk identification.

3.7.2.1 Risk Identification

Risk identification will be the first step in determining which risks may affect a project. Identification also provides documentation of the risk characteristics. The first level (Level 1) of the RBS can be used as a sanity check to make certain that all topics that might include risk are covered during the risk identification process. Using the RBS, an iterative process can be initiated that will persist throughout the project life-cycle. The frequency and applicability of this iterative process will be different in each phase of the life-cycle.

Using a risk identification checklist that is focused on the RBS, using Levels 2, 3 and below, assists in identifying specific and generic risks. This checklist can then become a part of the project managers' and risk managers' tool set for future projects.

Risk identification leads to quantitative risk analysis, conducted by the Project Risk Manager. Interestingly, sometimes merely identifying the risk will suggest the proper response, which can be entered into the Risk Response Plan.

3.7.2.2 Risk Analysis (Qualitative Risk Analysis)

Risk analysis is more easily achieved if, after identification, the risks are placed in proper perspective within the RBS by categorizing the risks in the various levels. Risk analysis (quantitative risk analysis) involves the use of techniques for prioritizing the risk, determining the probability of the risk and calculating the impact of the risk. At no point should the project manager or risk manager decide that the total number of identified risks should cause the cancellation of the project. The total number does not take into account the probability with which the risk will occur, nor the impact to the project, should the risk occur. A few risks, with high probabilities and high impact, are far more critical to the overall success of the project than a large number of risks with low probability and minimal impact.

Using the RBS, the project manager and the risk manager should create a "risk score" based on the priority, probability and impact of each risk and with each "group" of risks (according to the appropriate Level of the RBS).

Using the RBS also offers other valuable understanding into the analysis of the identified risks. Some of these new understandings are:

- Risk exposure type
- Dependencies between risks
- Root causality of risks
- Most significant and least significant risks
- Correlations between risks

Another benefit of the RBS is the ability to focus risk responses to the high probability, high impact, high priority risks using the risk topic groupings.

Effective risk management demands that the project manager and risk manager fully understand the risks of a project. A successful risk management process would also require a good knowledge and understanding of the business objectives of the project. During risk identification, a large volume of risks can be identified. Simply listing these risks or putting them in a spreadsheet or database does not provide the in-depth understanding of the identified risks necessary to allow a solid risk response planning task. The RBS provides the tool necessary to assist in identifying risks, analyzing risks and creating a successful risk response plan and it provides a vehicle for "deep-dives" into the complexity of the risk. Using a hierarchical RBS, similar in its design to the WBS, allows the project and risk managers the opportunity to carefully align the risks in proper categories, using as deep an analysis as time and resources would permit

Check Your Progress 3

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) Explain the Concept of Risk Breakdown structure.

.....

.....

.....

.....

2) What are the uses and benefits of RBS?

.....

.....

.....

.....

3) Example of RBS.

.....

.....

.....

.....

3.8 LET US SUM UP

Risk Analysis is a systematic approach to determine specific risk events and their consequences. This approach helps in calculating risks. The risk analysis can further be categorized as qualitative risk analysis and quantitative risk analysis. Risk analysis can be carried out by sequence of steps to provide an appropriate risk treatment.

Risk assessment is considered as the overall process of risk analysis and evaluation. This Risk assessment cycle provides step by step process to deal with risks in a project. This process can further be categorized as quantitative risk assessment and Qualitative risk assessment.

The behavioral aspects of risk management are considered to support innovation and help to develop business. The personal bias in risk management depends on a person with his or her experience, culture, value, as well as education.

The schedule risks estimates have good knowledge on sources of estimates and determine the high risk dependencies. The resource risks are determined as these risks effects the development of the project and the early identification helps to meet the project objectives on time.

3.9 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) Step I : Identify Threat

A risk analysis is performed to determine the nature of the risk and its level of impact. Thus it forms the basis for decision about risk treatments

The following steps are used to carry out the risk analysis process:

a) **Human:** Threat can be from each individual or group of individuals in the form of illness, death or strikes.

b) **Operational:** Threat can be in the form of disruption to products, not being able to access or distribute the essential project equipments and so on.

c) **Reputational:** Threat can be caused by damage to reputation in the market due to loss of good business partners

d) **Procedural:** Threat can be caused due to cost over-runs, insufficient product or service quality and so on.

e) **Financial:** Threat can be caused by drop in stock market, business failure or unemployment.

Step II: Estimate Risk

After identifying the threats, the next step is to measure its impact. This can be done by estimating the probability of the event occurring and then multiplying these estimates with the cost that may incur to get the things right.

Step III: Managing Risk

Once you have identified and estimated the risk levels, the next step is to find out ways to manage them. This can be done by selecting cost effective approaches. Accepting the risk is considered to be better and cost effective approach rather than using excessive resources to eliminate it. Sometimes

accepting risks enable you to plan for an event to minimize it, rather than eliminating a risk. Elimination sometimes causes alteration in project objectives and use of extra resources to get the alteration approach and hence may not be a feasible option.

Risk can be managed in following ways:

a) By using existing assets: You can use the existing resources or can improve the existing systems or accountability to respond to any risk events. You can also bring changes in responsibilities and internal controls

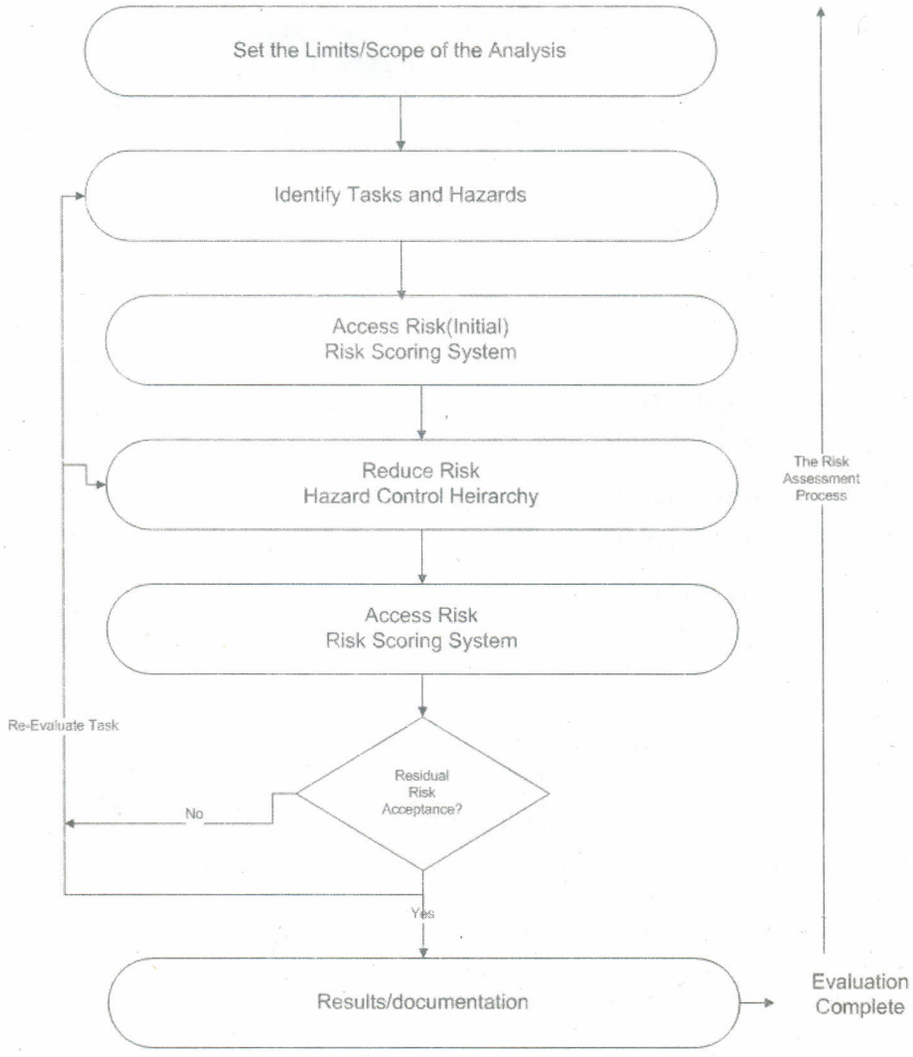
b) By Contingency planning: You must create a plan before accepting the identified risks so that you can reduce the impact of that risk. A contingency plan helps you to take quick actions in a crisis situation.

c) By investing in new resources: You can decide on to bring new resources to deal with the identified risk. If it is a high priority risk, then your organization must appoint some outsiders to deal some part of the risk management process.

Step IV: Reviews

after completing the risk analysis and risk management processes, the next and final step will be review, which must be done on regular basis. The review processes include conducting formal reviews or may involve testing systems and plans

2) A risk assessment consists of many different stages. These stages are explained in a simple step by step:



3) Benefits of Qualitative Risk Assessment

a) Financial impacts and values help to prioritize risks and the assets respectively

b) This process helps management of risks to express the results in management-specific terminology

c) The past record of data helps to gain experience and simultaneously tends to increase the accuracy

Drawback of Qualitative Risk Analysis

a) The risks that are assigned impact values are based on subjective view of people

b) Any calculations undertaken in this process are complex and time consuming

c) As results are displayed in monetary terms, the non technical people find it difficult to understand these terms.

4) Schedule Risk affects the project duration. The schedule risk estimated must be investigated to have good understanding on sources of estimates and identify the high-risk dependencies. The estimates are calculated by comparing the estimate values with the values present in the previous record and finding out any variations. This allows finding out all possible risks paths and noting the project duration risk.

The five categories that affects the project duration are:

- Project Dependencies
- Parts Delays
- Estimation errors
- Decision Delay
- Hardware Delay

Check Your Progress 2

1) Risk Identification Steps

a) Step I : Identifying Project Manager for the risk management task. The PM is the chief anchor of any project. The person must be capable of handling the entire project and must be aware of all possible risks.

b) Step II: Analyze the scope for the project which includes short term and long term tasks.

c) Step III: Examine if the project risk will bring any impact on the general business on the company or will cause loss of resources to the project.

d) Step IV: Budget can be considered as road map to identify any financial risk for the project.

e) Step V: Indentify the risk involved in the structural aspect of the project.

2) Risk Identification Methods

Risk Identification Methods	Advantages	Disadvantages
Interviews	Helps to reveal sensitive matters in face to face meetings	Time consumed more
Brainstorming	Helps to share risks with others	Difficult to have get together for meetings
Consulting Experts	Provide independent view on matters	Costs more sensitive information may be disclosed
Study Project Documentations	Provides documents of the risks experienced from the past project	Risks that have already been solved may reoccur
Stakeholders Analysis	Asking the people involved, such as stakeholders, in the project and understanding their interest and potential actions	Difficult to access stakeholders and identify suitable interest groups

3) The major inputs required for qualitative risk analysis are:

   a) **Risk Register:** The outputs obtained from the risk identification process form the initial entries into the risk register.

   b) **Risk management plan:** The roles and responsibilities to perform the risk management, schedule activities, the probability and impact matrix form the main elements for qualitative risk analysis

   d) **Project Scope Statement:** It is used to evaluate the complex projects which use first of its kind or more advanced technology.

   e) **Organizational Process Assets:** Information and Studies about previous project and risk database obtained from priority sources form the assets that influence the qualitative risk analysis.

4) The tools and Techniques used in Risk response planning process:

   a) **Avoid:** This plan involves making alteration in the project management plan that eradicates the threat completely from the project. Most of the organization plan to shutdown to avoid risk.

   b) **Transfer (Deflect, Allocate):** This plan involves transferring some portion or all of the impact of a risk to the third party. This transfer does not mean that risks are avoided.

   c) **Mitigate:** Reduction in the possibility of risk events or negative impact of risks events to an acceptable level.

   d) **Accept:** If it is very difficult to eliminate the risks from the project then organization plans to accept it.

Check Your Progress 3

1) Risk breakdown structure is a hierarchical list of risks which standardizes the department's personnel resources that help in planning and controlling the project work. It also helps in identifying and managing the project risks.

2) Uses of RBS: Once an organization defines a RBS then it can be used in number of ways:

   i) **Risk Identification:** It helps in documenting the characteristics of risks. The first level of RBS uses "Sanity check" to make sure that the risks involved in all the tasks of a project are covered during the risk identification process.

   ii) **Risk Analysis (Quantitative Risk Analysis):** It helps to place the identified risks within RBS, by categorizing into various levels.

3) RBS for Software Development

Level 0	Level 1	Level 2	Level 3
PROJECT RISK	Product Engineering	Requirement	Stability
			Completeness
			Feasibility
		Design	Functionality
			Interface
			Testability
		Code and Unit Testing	Feasibility
			Testing
			Coding/Implementation
		Integration Testing	Environment
			Product
			System
		Engineering Specialties	Maintainability
			Reliability
			Security
	Work Environment	Development Process	Formality
			Process Control
			Product Control
		Development System	Capacity
			Reliability
			System Support
		Management Process	Planning
			Project Organisation
			Management Experience
		Management method	Monitoring
			Configuration Management
			Quality Assurance
		Work Environment	Cooperation
			Communication
			Morale
	Program Contraints	Resources	Staff
			Budget
			Facilities
		Contract	Type of Contract
			Restrictions
			Dependencies
		Program Interface	Customer
			Subcontractors
			Corporate Management

3.10 SUGGESTED READING

- Project Management Body of Knowledge (PMBOK Guide), 4th Edition.

UNIT 4 RISK MITIGATION

Structure

4.0 INTRODUCTION

The ultimate purpose of risk identification and analysis is to prepare for risk mitigation. Mitigation includes reduction of the likelihood that a risk event will occur and/or reduction of the effect of a risk event if it does occur. This chapter discusses the importance of risk mitigation planning and describes approaches to reducing or mitigating project risks.

The purpose of this risk mitigation plan is to outline the risks that have been identified by the team as having highest probability to impact our schedule. These risks have been categorized as High, Medium and Low.

Any risks that will affect the testing process must be listed along with the mitigation. By documenting the risks in this document, we can anticipate the occurrence of it well ahead of time and then we can proactively prevent it from occurring. Sample

risks are dependency of completion of coding, which is done by sub-contractors, capability of testing tools etc.

4.1 OBJECTIVES

After studying this unit, you should be able to:

- define risk mitigation;
- list the types of risk mitigation;
- implement strategies for risk mitigation; and
- monitor risks.

4.2 RISK MITIGATION

Risk Mitigation is nothing but ensuring the smooth functioning of day to day business and making it sure that the process is completed by sticking to quality and compliance. This naturally eliminates much of the system error and human mistakes.If at all a mistake is committed it has to be rectified before it could hurt the business.

Ideally there is an individual or group of individuals who have vast experience of the process and are well aware about the human mistakes, system error and manipulations that could hurt the process. They are also capable of identifying mistakes error and possible manipulations.

Further Risk Mitigation involes identifying the grey areas and eliminating them out of the process.This ensures that the same error dont happen in the future.

Project Manager is responsible for preparing Risk Mitigation strategy. However, he might would like to take inputs from the project team leads/members, BAs, QA, SQA and IT infrastructure support teams to come up with an effective mitigation plan.

Mitigation has to do with devising one or more approaches to control, avoid, minimize or otherwise mitigate the risk. Mitigation approaches may reduce the probability or the impact. It is more of a **proactive** initiative even before the risk becomes a problem. The objective of a mitigation should be to ensure a risk identified doesn't occur or the least reduce it's probability of occurrence.

Contingency plan on the other hand has to do with what if you are hit by the problem for the risks you could not mitigate. (This is in contrast a **reactive** mode)

Reduction of risk to an acceptable level. Risk Mitigation involves all steps and task which PM will take to reduce Risk to an acceptable level or to minimum possible

Risk Mitigation is all about forecasting the possible problems that might arise in future and finding out ways to prevent it from occuring or do alternate ways to avoid the problems from happening.

Business Continuity plan/Disaster recovery is also a part of Risk Mitigation. Let's say Al-aqueeda has planned to blast your development centre, all our clients would lose all their money. This business continuity an/Disaster recovery is a step towards taking backup of all the data in a different development centre, so that even if your office is gone, the clients don't lose out anything.

Any risks that will affect the testing process must be listed along with the mitigation. By documenting the risks in this document, we can anticipate the occurrence of it well ahead of time and then we can proactively prevent it from occurring. Sample risks are dependency of completion of coding, which is done by sub-contractors, capability of testing tools etc.

In Simple definition, Mitigation should provide a result or solution to the existing problem/risks.

Eg: Suppose Government plans to have new norms to banks, say basel 11 norms which will analyze the risk taking care during bank loans. Hence bank should think of Risk Management, Risk Measurement and Risk Mitigation.

Mitigation should provide a solution for possible credit risks, market risk at each time bank identifies a risk.

4.3 TYPES OF MITIGATION RISK

Risk Mitigation, in context of a project, can be defined as a measure or set of measures taken by a project manager to reduce or eliminate the risks associated with a project. Risks can be of various types such as technical risks, monetary risks and scheduling based risks. The project manager takes complete authority of reducing the probability of occurrence of risks while executing a project.

4.3.1 Mitigation Technical Risks

When delegating tasks to individuals, their technical competency might be overlooked. If so, then the chances of the project getting delayed and not meeting the deadline will increase. Such delays can be avoided by increasing the communication frequency between the team members and monitoring their work.

Another alternative is to divide a complex task between team members and then delegate each part to a single individual. By reducing a complex technical task into larger simple tasks, the execution time may increase but the chances of missing the deadline for task completion can be kept up as the risk involved in the task is being diversified by the project manager among multiple individuals.

4.3.2 Mitigating Monetary Risks

A project manager is exposed to various challenges and has to make critical decisions in seeing through the project's execution with minimal risk. Cost based risk factors are difficult to estimate and intuition in making decisions which may increase the costs of deploying a task should be avoided. A safer bet used by the project managers is to use sophisticated cost estimation techniques. Some of the techniques such as Critical Path Method (CPM)/Program Evaluation and Review Technique (PERT) are used to oversee deployment of a task or set of tasks and analyzing the risks involved. Advanced techniques such as Expected Monetary Value (EMV) provide an insight on financial gain or loss if an event does or does not occur.

4.3.3 Mitigating Scheduling Risks

Executing the right task at the right time would help in lowering the risk of not meeting the project due date. Tasks can be assigned to individuals in two ways. The first one is to calculate the estimated processing time of each of the tasks and executing the tasks based on the Shortest Processing Time (SPT). The second one is to define due dates for each of the tasks and process them based on the Earliest Due Date (EDD). A project manager is the best judge here as to which method he would like to use in scheduling the tasks and delegating them to the individuals

associated with the execution of the project. An advanced method of decreasing the risks while scheduling of the work based tasks is by using the Monte Carlo Simulation method.

4.3.4 Best Practices

A project manager can mitigate risks by classifying risks based on the priority of being a threat to the project's success. The risks can be classified as being high, medium and low. Once classified, the concerned project manager will be able to devote time based on the classification and eliminate the risks in a sequential or in a random manner.

4.4 RISK MITIGATION – RISK REDUCTION

If your assessment shows that you have unacceptably high levels of risks to your business, then you need to take some action to counter them.

You could:

- reduce the probability of the risk affecting your business
- limit the impact of the risk if it does occur

In practice you will often wish to do both. However, generally you should try to reduce the probability of the risk affecting your business in the first place.

One way of doing this is risk avoidance, ie avoiding doing the things that could lead to a problem occurring, such as not entering into a line of business, a particular deal or a new IT project, because it carries a risk.

However, this might mean that you end up not doing anything new and hence not being able to benefit fully from business opportunities.

You could instead take a more positive approach by changing the way in which you carry out an activity. This is quite appropriate to IT-related risk and usually involves adopting a best practice approach to acquiring or operating IT systems.

4.5 RISK MITIGATION – IMPACT REDUCTION

There are inevitably some risks to your business that you can neither eliminate nor reduce to an acceptable level.

For these, you can only mitigate those risks by assessing what might happen as a result of the problem and reducing their impact should they occur.

In many situations, the greatest damage can occur because no one fully understands the nature of the problem and end up making it worse.

This can be avoided by common-sense procedures, which should be part of your risk mitigation approach:

- Do not take any actions that could exacerbate the problem. For example, if there is a problem with accessing files from a back-up tape using a tape drive, you should investigate whether the problem is caused by the drive, rather than just assuming there is a problem with the tape and then potentially damaging other tapes by placing them in a faulty drive.
- Implement document procedures for dealing with likely threats and train your staff in their use. For example, there are many ways that a virus can get into your system, so you should have plans for quarantining affected parts of the system so that the problem doesn't spread.

An important part of impact reduction is the early detection of problems. Where you have a risk that you can't eliminate, you should ensure that you have a fail-safe method of detecting the problem if it occurs.

Often failures are very obvious. However, occasionally, particularly in continuous or recurring processes, a failure may occur silently and its impact will grow over time. If you identify this type of risk you should build in a periodic check to detect the problem as soon as possible.

Don't forget that to reduce the cost impact of a problem should it occur, you could take out insurance. This is a form of risk transfer and is a normal part of doing business.

Sometimes you can write risk transfer clauses into the contracts for a deal such as a project. IT risk is, however, difficult or very costly to transfer effectively. See our guide on how to make the right IT choices.

4.5.1 Contingentcy Plan

A contingency plan is an impact-reduction measure. It should describe in detail what you and your staff will do if a particular problem occurs.

You may need a contingency plan when:

- you identify a risk that you think has a high chance of happening and will have a high impact
- you try to find ways of reducing the likelihood of the event, but you cannot reduce the risk to an acceptable level
- the residual risk is still so large that you need to take astructured approach to reduce its likely impact

The main considerations that you should address in a contingency plan are:

- scope – what particular risk the contingency plan is designed for
- initiation – how you will know when to put the plan into action
- actions – what sequence of actions you will take in order to control the problem and minimise its impact
- roles and responsibilities – who will do what and when

Good contingency plans are usually based on the shared experience of managers working together.

An important form of contingency plan is a business continuity plan (BCP). This is typically created to cover the most serious of problems, such as the complete loss of all your servers and network infrastructure due to a fire.

Such plans may involve planning for the rapid acquisition of temporary buildings, reciprocal arrangements with other organisations, special staffing arrangements, etc. See our guide on crisis management and business continuity planning.

BCPs should be tested if possible. A test could be a simple paper exercise where different parts of the recovery procedure are run through by the people involved. This is adequate for simple plans.

A full test of a BCP requires a full exercise. This will usually involve many people and significant cost because it will disrupt normal activities. Therefore, any exercise of this type should be carefully planned and budgeted.

4.5.2 Practical Actions for Business Managers

Risk management is relatively straightforward if you follow some basic principles. Below are some practical hints that you may find useful.

- Actively look for IT-related risks that could impact upon your business. If possible, use a small team to identify possible risks. A workshop environment will help you to think more imaginatively about risks than working alone.
- Assess IT-related risks using either a quantitative or qualitative approach. This will allow you to concentrate on those risks that are really important and not waste time on those that are not. How you actually measure the risk is less important than the activity itself, which aims to help you review risks rationally.
- Don't produce contingency plans for every risk you identify. This is a waste of time and effort. Concentrate on those problems that would have a serious impact and where you cannot reduce the probability of them happening to an acceptable level.
- You need a business continuity plan (BCP) to cover any serious IT-related risks that could jeopardise your business and which you cannot fully control. If you don't have a BCP, you should work on this first. See the page in this guide on contingency plans.
- Risk management is a continuous process. If you have not updated your risk register for a while, then there are likely to be new IT-related risks that you have not covered. Similarly, if you haven't looked at or tested your BCP for a while, it may have become out of date. Therefore, you may need to review these as soon as possible.
- Even very small businesses need to review IT-related risks. The time taken need only be small, but it gives important assurance.

Check Your Progress 1

Notes: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) What is risk mitigation? Explain with its types.

.....

.....

.....

.....

2) What is risk reduction?

.....

.....

.....

.....

3) What impact reduction?

.....

.....

.....

.....

4) Explain all the differences between risk mitigation and risk contingency?

.....

.....

.....

.....

4.6 RISK CONTROL

The collapse of Barings, Britain's oldest merchant bank and the billion-dollar losses suffered by Sumitomo Corporation catapulted the need for sound risk control into corporate consciousness. But even before these spectacular losses, risk control had occupied the minds of those whose business it is to know – the regulators and the senior managers of the world's leading financial institutions. They knew that sound internal risk control is essential to the prudent operation of a financial institution and to promoting stability of the financial system as a whole.

Risk control has a wider ambit than risk management. The latter is often defined as hedging or neutralising the financial risks that result from one or a series of transactions. For the purposes of this discussion, risk control is the entire process of policies, procedures and systems an institution needs to manage prudently all the risks resulting from its financial transactions and to ensure that they are within the bank's risk appetite. To avoid conflicts of interests, risk control should be separated from and sufficiently independent of the business units, which execute the firm's financial transactions, (the latter are often responsible for hedging the risks which result from their trades.) In some organisations, risk control work is carried out by independent risk management units rather than specially-named risk control sections, but the difference here is a question of semantics rather than job function.

Numerous reports have come out in the last four years with recommendations on best practices in risk control and risk management. Two stand head and shoulders above the rest. They are the G-30 report released in July 1993, entitled "Derivatives: Practices and Principles" (a private sector initiative) and "Risk Management Guidelines for Derivatives", written jointly by the Basle Committee on Banking Supervision and the International Organisation of Securities Commissions (IOSCO) which came out a year later. These two reports together have shaped today's best practices in risk control.

Both reports are rooted in simple common sense. They emphasise the importance of determining at the highest level the policy and scope of a firm's involvement in and the use of financial instruments; oversight by boards of directors and senior managers; a risk management process that involves continuous measuring, monitoring and controlling of all risks (especially market and credit); accurate and reliable management information with comprehensive limits; frequent management reporting; sound control and operational systems; and thorough audit and control procedures. They also stress the importance of the human factor in risk management – professionals involved must have the necessary skills and experience and the firm should not deal in any instrument until senior managers are fully satisfied that all relevant personnel understand and can manage the risks involved. The specific way an institution applies these recommendations depends on the complexity and nature of its financial holdings and activities.

The G-30 report caters for both dealers (financial institutions) and end-users (corporates). The guidelines are embodied in 20 recommendations which firms can use to set up and evaluate their risk management and control practices. The guidelines are divided into five main areas;

- general policies for senior management
- valuation and market risk management
- credit risk measurement and management
- systems, operations and controls
- recommendations for legislators, regulators and supervisors.

The full text of the report is available from the G-30.

The Basle Committee/IOSCO paper is directed towards banking organisations and supervisors – to provide both a framework to follow and against which they can reassess their own risk management procedures. These guidelines are more detailed than those of the G-30 and include sound risk management practices for each major risk identified – credit, market, liquidity, operations and legal. And while the G-30 report called for independent credit and market risk management functions, the Basle Committee/IOSCO goes one step further by suggesting that the entire process of measuring, monitoring and controlling risk consistent with the firm's established policies, should be independent. This independence should be reflected in the senior hierarchy of the institution as well as the firm's exposure-reporting system. The 1994 document has become the definitive word on best practices in risk control for derivatives.

Resulting from the Basle Committee's increasing focus on sound internal controls is "Framework for the Evaluation of Internal Control Systems"(1998). This final report released in October 1998 follows an earlier draft issued in January of the same year. The Committee notes, "An analysis of the problems related to the losses [incurred by several banking organisations] indicates that they could probably have been avoided had the banks maintained effective internal control systems. Such systems would have prevented or enabled earlier detection of the problems that led to the losses, thereby limiting damage to the banking organisation." The Committee noted that the control breakdowns typically seen in recent problem bank situations could be grouped into five broad categories:

- Lack of adequate management oversight and accountability and failure to develop a strong control culture within the bank.
- Inadequate assessment of the risk of certain banking activities, whether on- or off-balance sheet.
- The absence or failure of key control activities, such as segregation of duties, approvals, verifications, reconciliations and reviews of operating performance.
- Inadequate communication of information between levels of management within the bank, especially in the upward communication of problems.
- Inadequate or ineffective audit programs and other monitoring services.

It is thus not surprising that the 13 principles issued by the Basle Committee cover management oversight and the control culture; risk assessment; control activities; information and communication; monitoring; and evaluation of internal control systems by supervisory authorities. Unlike previous guidance, the latest principles on internal control are not area-specific. Instead, the Committee wants supervisors to use them when evaluating internal controls for all the on- and off-balance sheet activities of a bank.

The guidelines stress the importance and role of senior management in establishing a robust internal control system. Principle 2 states that senior management must not only set out and monitor the adequacy and effectiveness of the internal control system; they should also develop processes that identify, measure, monitor and control risks incurred by the bank; maintain an organisational structure that clearly assigns responsibility, authority and reporting relationships and ensure that these delegated responsibilities are effectively carried out.

Principle 3 deals only with establishing a strong control culture which reflects the importance the Basle Committee now places on the subject because it sees the former as an essential element of an effective system of internal control. The Committee believes that it is the responsibility of the board of directors and senior management to push home the importance of internal controls through their actions and words. This includes the ethical values management displays in their business dealings, both inside and outside the organisation. For example, senior management may weaken the control culture by promoting and rewarding managers who are successful in generating profits but fail to implement internal control policies or address problems identified by internal audit. Such actions send a message to others in the organisation that internal control is considered secondary to other goals in the organisations and thus diminish the commitment to and quality of the control culture.

The Joint Forum on Financial Conglomerates addresses the lack of management oversight in its consultative documents on how financial conglomerates should be supervised. One of the constituent reports, Fit and Proper Principles (1999), sets out the criteria which supervisors can use to assess whether managers and directors are competent to fulfil their responsibilities. These include fitness, propriety or other qualification tests being applied at the authorisation stage and thereafter, on the occurrence of specified events. These tests will not only apply to managers and directors but to shareholders whose holdings are above specified thresholds and/or who exert a material influence on regulated entities within the financial conglomerate.

The importance of these issues was again reiterated in a paper on corporate governance by the Basle Committee. "Enhancing Corporate Governance in Banking Organisations" (1999) lists six key practices for banks and the Committee hopes the paper will help supervisory authorities worldwide to promote sound corporate governance principles. One proposed practice stands out because it reflects the growing concern among regulators over compensation programmes in banks. Practice 6 states that the board of directors and senior management should ensure their compensation approaches are consistent with the bank's ethical values, objectives, strategy and control environment. Failure to link incentive compensations to the business strategy can encourage managers to book business based upon volume and/or short-term profitability to the bank with little regard to short or long-term risk consequences. This can be seen particularly with traders and loan officers, but can also adversely affect the performance of other support staff.

IOSCO has also published a paper which addresses risk controls from a supervisory perspective. Risk Management and Control Guidance for Securities Firms and their Supervisors (1998) states that supervisors must make an effort to understand the control environment of each firm and ensure that these controls are adequate. They must therefore be proactive, rather than reactive, in devising high quality control standards. Some suggestions IOSCO puts forward are capital tiering, regulations requiring the establishment of specified risk management and controls at securities firms and working with industry associations to promulgate the establishment of management controls.

The IOSCO paper sets outs 12 basic elements of a risk management and control system. Supervisors should use these elements as benchmarks to measure the

adequacy of firms' control systems. The 12 elements are grouped under five categories: the control environment, nature and scope of controls, implementation, verification and reporting.

Despite the BIS and IOSCO guidelines on risk control discussed above, recent developments in the financial markets show that there are still serious deficiencies in banks and securities houses' risk management practices. The granting of extensive credit facilities to Long-Term Capital Management which allowed it to build up a market exposure of over $200 billion on a capital base of about $4 billion and its subsequent near-collapse prompted the Basle Committee to analyse the relationships between banks and highly leveraged institutions (HLIs). "Banks' Interactions with Highly Leveraged Institutions" (1999) and "Sound Practices for Banks' Interactions with Highly Leveraged Institutions" (1999) highlight several deficiencies in some banks' risk control practices with respect to HLIs.

Banks did not appear to possess effective policies and guidelines for managing exposures to HLIs in a manner consistent with their overall credit standards, possibly because the activities of HLIs are so opaque and their trading strategies always changing. The Committee also singled out strong competitive pressures as one reason why some banks compromised important elements of the risk management process to agree to generous credit conditions. Also banks did not generally conduct stress tests on their exposures to HLIs nor did they update frequently the information they received from HLIs..

The Committee recommends that before establishing a credit relationship with a HLI, a bank should ensure that all relevant information be disclosed on a timely and ongoing basis. This should include the HLI's liquidity profile, changes in the general direction of trading strategies, significant changes to leverage and profit and loss developments. The same report also suggests that banks improve the way they set credit limits for HLIs. These limits should recognise and reflect the risks associated with the near-term liquidation of derivatives positions if the counterparty defaults.

The Basle Committee's thoughts are echoed in "Report of the President's Working Group on Financial Markets on Hedge Funds, Leverage and the Lessons of Long-Term Capital Management."(1999). The main lesson to be learnt from the LTCM episode is how to constrain excessive leverage, not just by hedge funds but all participants in the financial system. The report notes, "Our market-based economy relies primarily on market discipline to constrain leverage. In the case of LTCM, market discipline seems to have largely broken down. The breakdown in market discipline was made possible by risk management weaknesses at LTCM as well as at the large banks and securities firms that were LTCM counterparties." US banking regulators have notified banks that their examiners will be looking at the following points:

- Senior management and boards of directors must understand the strengths and weaknesses of their risk measurement systems, including model risk, liquidity risk and the risk of breakdown of historical correlations among different instruments and markets.
- Senior management and boards of directors must have a realistic assessment of their tolerance for losses in adverse markets
- The interconnection of material risks, including market, credit and liquidity risks needs to be integrated into credit and risk management decisions.

The Basle Committee has also released guidelines specifically for interest rate risk management. "Principles for the Management of Interest Rate Risk" contains 11 principles which banking supervisory authorities must apply when assessing banks' management of interest rate risk. The specific manner in which a bank

applies these elements depends upon the complexity and nature of its holdings and exposure to interest rate risk.

The Basle Committee believes that interest rate risk should be monitored on a consolidated basis, to include interest rate exposures in subsidiaries. At the same time, however, institutions should fully recognise any legal distinctions and possible obstacles to cash flow movements among affiliates and adjust their risk management process accordingly. While consolidation may provide a comprehensive measure of interest rate risk, it may also underestimate risk when positions in one affiliate are used to offset positions in another affiliate. This is because a conventional accounting consolidation may allow theoretical offsets between such positions from which a bank may not in practice be able to benefit because of legal or operational constraints. The 1997 report is more specific than the 1994 one and suggests ways of measuring interest rate risk, because prudent interest-rate risk control is conditional on a robust measurement system. The Committee believes that an interest rate risk measurement system must be able to assess the effects of rate changes on both the bank's accrual or reported earnings and the economic value of the bank's assets, liabilities and off-balance sheet positions.

The Bank of England's report into the collapse of Barings brings to life the recommendations of both the G-30 and BIS/IOSCO reports. Sections 10 and 11 of the "Report of the Board of Banking Supervision inquiry into the Circumstances of the collapse of Barings (1995)" illustrate vividly the logic of every risk control practice promulgated by the above-mentioned reports. By doing so, the Barings report answers all doubts about the validity of risk control recommendations made by the Basle Committee, the International Organisation of Securities Commissions and the Futures and Industry Association, to name a few. The report also drives home the point that the essence of risk control is plain common sense and not technological and mathematical wizardry. It seems almost pedantic that the first two lessons for management singled out by the Inquiry are: (a) management teams have the duty to understand fully the businesses they manage (b) responsibility for each business activity has to be clearly established and communicated – two principles that apply to all businesses not just financial institutions.

The G-30 cites the failure of Barings and trading losses at Morgan Grenfell and Sumitomo Corporation as proof for the need of a new supervisory approach to global institutions. It believes that the largest proportion of serious financial problems at financial firms arise from problems which the organisations ought to be able to control themselves. It also thinks it is unreasonable to expect supervisors alone to keep global institutions from mishaps. Its report on international systemic risk, Global Institutions, National Supervision and Systemic Risk(1997) thus argues that major financial institutions should take a leading role in developing a global framework for comprehensive and effective management controls, in cooperation with supervisors.

Such a framework must take into account market volatility and the differences in institutional complexity and geography. "Yet," the report acknowledges, "the greatest challenge to address is... excessively risky behaviour. Since no code of ethics is likely to eliminate that tendency, an institution's control system must at least aim to check the excesses of human nature by establishing an internal vigilance system that will provide early warning of such behaviour. Controls must withstand both external shocks and internal breakdowns."

An effective internal control system requires a major commitment to:

- Hire, support and retain employees throughout the management system with appropriate training and background in trading, modelling, information technology and other required skills.

- Invest in global risk-monitoring systems, encompassing both sophisticated risk models and sufficient computer and communications capacity to handle high-volume, high speed transactions in all their financial and legal complexity.
- Establish a management structure with appropriate checks and balances, between front and back office, for example and with more direct responsibility to the respective audit committees.
- Adopt a more sophisticated approach to credit risk, operational risks and management of collateral and related disciplines.

This list drives home the point that comprehensive and effective controls are not solely a matter of skills and technologies, but of organizational culture as well.

"Framework for Voluntary Oversight" (1995), written by the Derivatives Policy Group, also contains a section on best practices for risk control. The group believes that the design and implementation of an effective system of control should reflect the circumstances of the firm. However, all risk control systems must have a high-level authorizing body that draws up the guidelines for the firm. These guidelines must address, among other things:

i) the scope of authorized activity or any non-quantitative limitation on the scope of authorized activities;

ii) quantitative guidelines for managing the firm's overall or constituent risk exposures;

iii) the significant structural elements of the firm's Risk Monitoring and Risk Management systems and processes;

iv) The scope and frequency of reporting by management on risk exposures; and the mechanisms for reviewing these guidelines. The members of this authorizing body should be selected by the firm's board of directors (or its equivalent) based on, among other things, the composition and expertise of the board, the customary allocation of equivalent responsibilities within senior management of the firm and the nature, scope and complexity of the firm's trading activities.

Some risk control documents worth reading are more targetted. The main thrust of a 1995 report by the technical committee of IOSCO was to examine the implications for securities regulators of value-at-risk models. But The Implications for Securities Regulators of the Increased Use of Value At Risk Models by Securities Firms also contains a set of best practices for financial institutions to implement when using models. These best practices include recommendations on data integrity and reconciliation, the assumptions and parameters of the model and its operating environment, independent reviews of pricing algorithms, regular backtesting and understanding how the model influences the firm's decision making process.

Motivated by concern over the large exposures generated in currency settlements, the Bank for International Settlements commissioned a report on how to reduce settlement risk. A report prepared by the Committee on Payment and Settlement Systems released in 1997 calls upon individual banks and industry groups to devise mechanisms for addressing settlement risk. Appendix 2 in the report, titled "Settlement Risk in Foreign Exchange Transactions" contains a summary of best practices for controlling settlement risk. The 16 recommendations, drawn up by The New York Foreign Exchange Committee, range from basics such as understanding the settlement process and exposure to setting prudent settlement exposure limits, which must be adhered to. These exposures should be updated on-line and aggregated globally across all dealing centers. Banks are also encouraged to review correspondent bank relationships to ensure that the services

they receive give them maximum control over their nostrum accounts. Reconciliation of all transactions should be completed as early as possible and senior management should establish procedures to evaluate non-receipts of payments and to alert all concerned parties to potential problematic situations.

Another report prepared by the same committee examined clearing arrangements for exchange-traded derivatives in G-10 countries. Clearing Arrangements for Exchange-Traded Derivatives (1997) discusses the sources and types of risks to clearing houses and the risk control techniques they can employ to safeguard themselves against such risks. The two main risks discussed are: (1) defaults by clearing members and (2) failure of settlement banks. The most basic way of protecting against both risks is to deal only with creditworthy counterparties. This is easier said than done! Most clearing houses demand that their counterparties and members meet minimum financial requirements, including minimum capital requirements. But information on compliance with regulatory capital requirements is available only at discrete intervals. Given the considerable leverage and liquidity of derivatives, the risk profiles of clearing house members can change dramatically between reporting periods. Clearing houses are thus asked to conduct surveillance on members' positions on an on-going basis.

Other risk control safeguards include: (i) margin requirements that collateralize potential future credit exposures and either collateralize current credit exposures or limit the build-up of such exposures by periodically settling gains and losses; (ii) procedures that authorize prompt resolution of a clearing member's default through close-out of its proprietary positions and transfer (to a non-defaulting clearing member) or close-out of its clients' positions; and (iii) maintaining supplemental clearing house resources (capital, asset pools, credit lines, guarantees or the authority to make assessments on non-defaulting members) to cover losses that may exceed the value of the defaulting member's margin collateral and to provide liquidity during the time it takes to realize the value of that margin collateral.

Some clearing houses mitigate their risks of settlement bank failures by structuring agreements that minimize the clearing house's potential losses and liquidity pressures if a failure occurs. Under such agreements, transfers between clearing members and the clearing house on the books of each settlement bank are effected simultaneously and are final. Also, transfers of funds between settlement banks are effected as soon as possible. Together, these steps can reduce substantially the amount and duration of a clearing house's exposures to any one settlement bank.

Check Your Progress 2

Notes: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) What is the difference between risk and ambiguity?

.....

.....

.....

.....

2) What is a compound risk?

.....

.....

.....

.....

3) What is risk mitigation strategy?

.....

.....

.....

.....

4) What are the four risk strategies for controlling risk?

.....

.....

.....

.....

4.7 RISK MITIGATION PLAN

The risk mitigation plan is also called a risk response plan. The plan tells how specific risks will be dealt with and the action or steps that are required to carry them out. The risk mitigation plan is often used in the project management software as a series of tasks in addition to those that were already on the original activity list. As risks are about to happen, the plan identifies what actions should occur and who is responsible for carrying out those actions.

Risk management planning needs to be an ongoing effort that cannot stop after a qualitative risk assessment or a Monte Carlo simulation or the setting of contingency levels. Risk management includes front-end planning of how major risks will be mitigated, and managed once identified. Therefore, risk mitigation strategies and specific action plans should be incorporated in the project execution plan or risk analyses are just so much wallpaper. Risk mitigation plans should

- Characterize the root causes of risks that have been identified and quantified in earlier phases of the risk management process.
- Evaluate risk interactions and common causes.
- Identify alternative mitigation strategies, methods and tools for each major risk.
- Assess and prioritize mitigation alternatives.
- Select and commit the resources required for specific risk mitigation alternatives.

Although risk mitigation plans may be developed in detail and executed by contractors, the owner's program and project management should develop standards for a consistent risk mitigation planning process. Owners should have independent, unbiased outside experts' review the project's risk mitigation plans before final approval. This should be done prior to completing the project design or allocating funds for construction. Risk mitigation planning should continue beyond the end of the project by capturing data and lessons learned that can benefit future projects.

Get a clear perception of risk mitigation strategies & its concept; as we furnish descriptions of the procedures performed to come up with a risk mitigation plan. Appreciate the use of said plan for monitoring risks in project management, since it serves as a checklist of all threats & action plans.

4.7.1 Strategies for Reducing the Adverse Impacts of Anticipated Risks

Risk mitigation strategies are action plans you conceptualize after making a thorough evaluation of the possible threats, hazards or detriments that can affect a project, a business operation or any form of venture. The purpose of such strategies is to lessen or reduce, if not totally eliminate the adverse impacts of the known or perceived risks inherent in a particular undertaking, even before any damage or disaster takes place.

Best practices require that the known and perceived risks be analyzed according to the degree and likelihood of the adverse results that are anticipated to take place. Thereafter, all such risks analyzed shall be documented according to their levels of priority in a form known as the risk mitigation plan. After which, the development and integration of the corresponding risk mitigation strategies follows and shall be referenced against the previously prepared risk management plan.

Take note however, not to confuse risk management plan with the risk mitigation plan. The former is the framework for the entire risk management aspect of the project while the latter pertains to the entire risks and response actions plan

4.7.2 What Comprises a Risk Mitigation Plan?

A risk mitigation plan shall serve as the checklist of the anticipated risks, listed in accordance with the degree of their probability, as High, Medium or Low. Some project managers, however, deem it more appropriate to categorize the risks as most Likely, Likely or Unlikely.

The set of mitigation strategies shall likewise be listed in the plan, properly labeled as such and categorized under each risk. This document shall now serve as the project manager's checklist for project monitoring.

4.7.3 How is Risk Mitigation Strategies Implemented?

Inasmuch as the main objective of risk mitigation strategies is to curtail the effects of possible threats or hazards, these strategies shall be taken into consideration during the project planning stage. While in the process of developing each phase, procedure or methodology, the project management team or the principal players of a transaction or venture shall also establish the critical points where the possible risks may take place.

Each critical point identified shall have a set of mitigation strategies incorporated in its procedural guidelines. In actual practice, these procedures may be referred to as code of practices. In financial institutions, where numerous risks against lost of assets, particularly cash, are perceived, these set of mitigation strategies are simply referred to as the internal control policies.

In another aspect of risk management, a separate set of mitigating actions shall be incorporated to address the threats or hazards that were previously evaluated as having the highest levels of adverse impact in the event of its happening. The risk mitigation strategies are contained in a crisis management plan and shall form part of the initial emergency measures to take, in order to contain and prevent the worsening of the damages caused by an accident or catastrophe.

4.7.4 How is Risks Monitored and Mitigated in Project Management?

As project plans get underway, effective project management becomes more critical and will require rigid monitoring of all executions by way of an efficient and constant communication with the team members. The project manager tracks the

progress of assigned tasks and inquires from team members of any issues that may affect the successful completion of the project's objectives.

Poor management can result to runaway executions that tend to lack cohesion, which can create more complexities and risks of not meeting the timelines and the budget. It could further result to intellectual drain for the entire team and depletion of financial resources. Hence, the importance of consistently checking the present status of the project against scope, limitations, methodologies, exclusions, mitigation plans and budget, to ensure that there is diligent compliance and that all risks anticipated are being mitigated at their critical stages.

The project manager should also take note of new risks that may surface, for which immediate plans and additional risk mitigation strategies will be developed, documented and integrated.

Check Your Progress 3

Notes: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) What comprises a risk mitigation plan?

.....

.....

.....

.....

2) How is risk mitigation strategies implemented?

.....

.....

.....

.....

3) How is Risk mitigated & monitored in project management?

.....

.....

.....

.....

4.8 RISK MITIGATION, MONITORING AND MANAGEMENT

This section in detail describes Risk Mitigation, Monitoring and Management for each of the possible risks. It will talk about ways to avoid, monitor and to have ways to manage the risks.

4.8.1 Risk Mitigation for Risk

In this section several different software development risks will be identified, a plan will be created to avoid these risks. We will think of the risks possible and of the way to keep the software development process from encountering these risks.

It is important to have mitigation plan to avoid risks once and for all. Goal is to attack the risk even before it comes into existence. The plan will help in identifying the possible risks and to monitor them.

4.8.2 Product Size

In this risk concern is of under or overestimation (mainly underestimation) of the number of Function Points. If we estimate too few LOC (line of code) necessary for the project we may get wrong cost figures which can prove fatal to the software development plan. To avoid this from happening we will use conservative figures to reduce the probability of the risk. This means we will overestimate the LOC a little. If we end up finishing the project earlier than that will not create any troubles. If the software cost estimations are passed with higher than actual cost required delivering the product, the software development team can get credited for finishing the product sooner. Also for any reason the delivery dates get pushed back development team can still deliver the product on the time. In normal circumstances companies are not picky about the product size, so increasing the number will not cause any troubles in getting approval for the project.

4.8.3 Business Impact

In this risk category we are concerned about the quality of the final product. As mitigation step we will spend more time with the users to understand their needs. This way we can gather all the information necessary for the project to be successful. We will try to understand business environment and can try to provide the user with help in defining software requirements. More the time team spends with the customer better the understating the team will have regarding the software. This will help in coming up with just right product at right price for the customer. Team has to make sure that the palm size PC integration and the cost of the palm size PC is justified, meaning that it really improves inspection process.

4.8.4 Customer (User) Risks

If the users of the product fail to participate during the different phases of the software development we fail to recognize problems with the software. To avoid this in the mitigation phase we will try to meet the customer frequently and present software in phases so that customer and we can have better understanding the software being developed. More the time team spends with the customer better the understating the team will have regarding the software. This will help in coming up with just right product at right price for the customer. If customer fails to mention some special operations that have to perform with totally separate checklist and have to be stored separately, software development team does not know anything about it thus leaving big problem in the software.

4.8.5 Process Risks

We want quality of the product to be as high as possible. To achieve this we will set up guidelines to be followed for each of the team members during all the phases of the software development cycle. The standard will be set and defined for all of the software development. This will help the team in delivering the high quality product thus increasing our reputation in the market. This will help bring in more clients in the future. It will also save customer from getting low quality product. For example, palm size PC checklists are easy to get used too. If inspector cannot get used to the forms in the PC they may go back to using pen and paper which is not good for the reputation of the team.

4.8.6 Technology Risks

To avoid risk of using technology that may become obsolete in few years after the product have been developed. We will do excessive research on what technology

to use for software development and will use the latest technology (programming languages etc.) to avoid this risk. Software development team has to make sure that the equipment requested (i.e. Palm-size PC) are current and will not be obsolete in near future.

4.8.7 Development Risks

If the necessary tools are not provided to all of the team members, their work will lack quantity and quality. As mitigation phase we will make sure that the budget includes cost for latest technology and tools needed to achieve the desired product. For example if the government refused to deliver the Palm-size PC to the DEQ the PC integration part will be useless until the units are actually bought.

4.8.8 Employee Risks (Team Members)

This risk concerns the knowledge and of the employees and their willingness to help make the project succeed. As mitigation step of this risk we will make sure that someone in all of the project development phases knows exactly what to do and the tools to use to achieve the goals. If the employees that have little knowledge in the main software implementation language fail to learn it, it may cause big problems when coding part begins.

Check Your Progress 4

Notes: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) What is Process Risk?

.....

.....

.....

.....

.....

2) What is Technology Risk?

.....

.....

.....

.....

.....

3) What is Development Risk?

.....

.....

.....

.....

.....

4) What is Employee Risk?

.....

.....

.....

.....

4.9 LET US SUM UP

This unit covers risk mitigation. Risk Mitigation is all about forecasting the possible problems that might arise in future and finding out ways to prevent it from occurring or do alternate ways to avoid the problems from happening. It also covers the list and explanation of the types of risk mitigation and also discussed different strategies for risk mitigation and to monitor the risks.

4.10 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) Risk Mitigation is nothing but ensuring the smooth functioning of day to day business and making it sure that the process is completed by sticking to quality and compliance.This naturally eliminates much of the system error and human mistakes.If at all a mistake is committed it has to be rectified before it could hurt the business.Ideally there is an individual or group of individuals who have vast experience of the process and are well aware about the human mistakes, system error and manipulations that could hurt the process. They are also capable of identifying mistakes error and possible manipulations. Further Risk Mitigation involes identifying the grey areas and eliminating them out of the process.This ensures that the same error dont happen in the future.

   Project Manager is responsible for preparing Risk Mitigation strategy. However, he might would like to take inputs from the project team leads/members, BAs, QA, SQA and IT infrastructure support teams to come up with an effective mitigation plan.

2) In practice you will often wish to do both. However, generally you should try to reduce the probability of the risk affecting your business in the first place.One way of doing this is risk avoidance, ie avoiding doing the things that could lead to a problem occurring, such as not entering into a line of business, a particular deal or a new IT project, because it carries a risk.However, this might mean that you end up not doing anything new and hence not being able to benefit fully from business opportunities.You could instead take a more positive approach by changing the way in which you carry out an activity. This is quite appropriate to IT-related risk and usually involves adopting a best practice approach to acquiring or operating IT systems.

3) There are inevitably some risks to your business that you can neither eliminate nor reduce to an acceptable level. For these, you can only mitigate those risks by assessing what might happen as a result of the problem and reducing their impact should they occur.In many situations, the greatest damage can occur because no one fully understands the nature of the problem and end up making it worse.

4) A contingency plan is an impact-reduction measure. It should describe in detail what you and your staff will do if a particular problem occurs.

Check Your Progress 2

1) Risk can be managed by working on certain mitigation and contingency strategies. Ambiguity cannot be 'managed'. Complex projects will naturally introduce areas of ambiguity. Each ambiguity is a potential source of conflict, rework and failure. When ambiguity arises; check the project plan to understand whether it can be resolved during the natural execution of the project. Start by reviewing project scope. Is this as unambiguous as possible? Is everyone clear on what is in scope and what is out of scope?

   Ambiguity may be a potential risk e.g. if the requirements are ambiguous at a particular stage in the project it can be a potential risk.

   Both risk and ambiguity can also turn into something positive. Risk may be positive if it leads to an opportunity. Also, it is possible that ambiguity over something may lead to research and innovation.

2) Unfortunately, many project managers misunderstand what compound risks really are. Some think that a compound risk is one big risk (like a flood) with sub-risks falling under it (offices closed, data center flooded, hardware damaged, etc.). Others believe that it's a collection of related risks.

   Here's the real definition of what a compound risk is, it's a risk that will result in creating other risks. A flood risk can be considered a compound risk, but the way it is explained above is wrong, because the other risks are not sub-risks, they're just risks that were ensued by the flood risk.

   Let me give you another example, suppose near the middle of your IT project, the most important and knowledgeable resource decided to quite (that's a resource risk), what happened is that you were forced to hire another person, who may or may not be as skilled as your previous employee (Lack of experience risk) and who may ask for more (Cost risk). Not only that, other employees may sympathize with the employee who quit and may decide to do the same (lack of resource risk) and the whole project will be delayed. You see, when that key resource quit, he created a myriad of other risks that may result in getting your project killed or at best, increasing its costs and the schedule. Hence "key resource leaving" is a compound risk.

3) It is a strategy devised to minimize, to the lowest level possible, any risks to an enterprise while still managing to maintain the optimum output and delivery of labor, goods, services, etc.

4) Four Risk Strategies:

   a) Controlling risk

   b) Avoiding risk -(Changing the source that is subjecting the program to risk such as reducing the scope of the performance objectives)

   c) Assuming risk

   d) Transferring risk

Check Your Progress 3

1) A risk mitigation plan shall serve as the checklist of the anticipated risks, listed in accordance with the degree of their probability, as High, Medium or Low. Some project managers, however, deem it more appropriate to categorize the risks as most Likely, Likely or Unlikely.

   The set of mitigation strategies shall likewise be listed in the plan, properly labeled as such and categorized under each risk. This document shall now serve as the project manager's checklist for project monitoring.

2) While in the process of developing each phase, procedure or methodology, the project management team or the principal players of a transaction or venture shall also establish the critical points where the possible risks may take place.

   Each critical point identified shall have a set of mitigation strategies incorporated in its procedural guidelines. In actual practice, these procedures may be referred to as code of practices. In financial institutions, where numerous risks against lost of assets, particularly cash, are perceived, these set of mitigation strategies are simply referred to as the internal control policies.

   In another aspect of risk management, a separate set of mitigating actions shall be incorporated to address the threats or hazards that were previously evaluated as having the highest levels of adverse impact in the event of its happening. The risk mitigation strategies are contained in a crisis management plan and shall form part of the initial emergency measures to take, in order to contain and prevent the worsening of the damages caused by an accident or catastrophe.

3) As project plans get underway, effective project management becomes more critical and will require rigid monitoring of all executions by way of an efficient and constant communication with the team members. The project manager tracks the progress of assigned tasks and inquires from team members of any issues that may affect the successful completion of the project's objectives.

   Poor management can result to runaway executions that tend to lack cohesion, which can create more complexities and risks of not meeting the timelines and the budget. It could further result to intellectual drain for the entire team and depletion of financial resources. Hence, the importance of consistently checking the present status of the project against scope, limitations, methodologies, exclusions, mitigation plans and budget, to ensure that there is diligent compliance and that all risks anticipated are being mitigated at their critical stages.

   The project manager should also take note of new risks that may surface, for which immediate plans and additional risk mitigation strategies will be developed, documented and integrated.

Check Your Progress 4

1) We want quality of the product to be as high as possible. To achieve this we will set up guidelines to be followed for each of the team members during all the phases of the software development cycle. The standard will be set and defined for all of the software development. This will help the team in delivering the high quality product thus increasing our reputation in the market. This will help bring in more clients in the future. It will also save customer from getting low quality product. For example, palm size PC checklists are easy to get used too. If inspector cannot get used to the forms in the PC they may go back to using pen and paper which is not good for the reputation of the team.

2) To avoid risk of using technology that may become obsolete in few years after the product have been developed. We will do excessive research on what technology to use for software development and will use the latest technology (programming languages etc.) to avoid this risk. Software development team has to make sure that the equipment requested (i.e. Palm-size PC) are current and will not be obsolete in near future.

3) If the necessary tools are not provided to all of the team members, their work will lack quantity and quality. As mitigation phase we will make sure that the budget includes cost for latest technology and tools needed to achieve the

desired product. For example if the government refused to deliver the Palm-size PC to the DEQ the PC integration part will be useless until the units are actually bought.

4) This risk concerns the knowledge and of the employees and their willingness to help make the project succeed. As mitigation step of this risk we will make sure that someone in all of the project development phases knows exactly what to do and the tools to use to achieve the goals. If the employees that have little knowledge in the main software implementation language fail to learn it, it may cause big problems when coding part begins.

4.11 SUGGESTED READING

- Project Management Body of Knowledge (PMBOK Guide), 4th Edition.

MPDD-IGNOU/P.O.1T/**November, 2011**

ISBN-978-81-266-5713-1