Risk Management

Identification, Analysis and Prevention of Risks

MOTIS

ESIEE

09/04/2013

16/04/2013

Aloysius John

April 2013

Introduction

Risk Management is a

- Process for Project manager to identify factors that may more or less affect the success or the achievement of goals.
- Means for identifying facilitators and obstacles
- Means for making better decisions to enhance project or organizational performance
- Anticipate uncertainties and take decisions in time.

Risk Management

- Risk Management implies
  1. Defining what the Risk is ?
  2. Why manage Risk ?
  3. Risk Management Process ?
  4. Conditions necessary for « successful Risk Management »
  5. Taking into consideration past risk issues and how they impact the organization will certainly be an asset for relevant future Risk Management Process.

How do we understand risk?

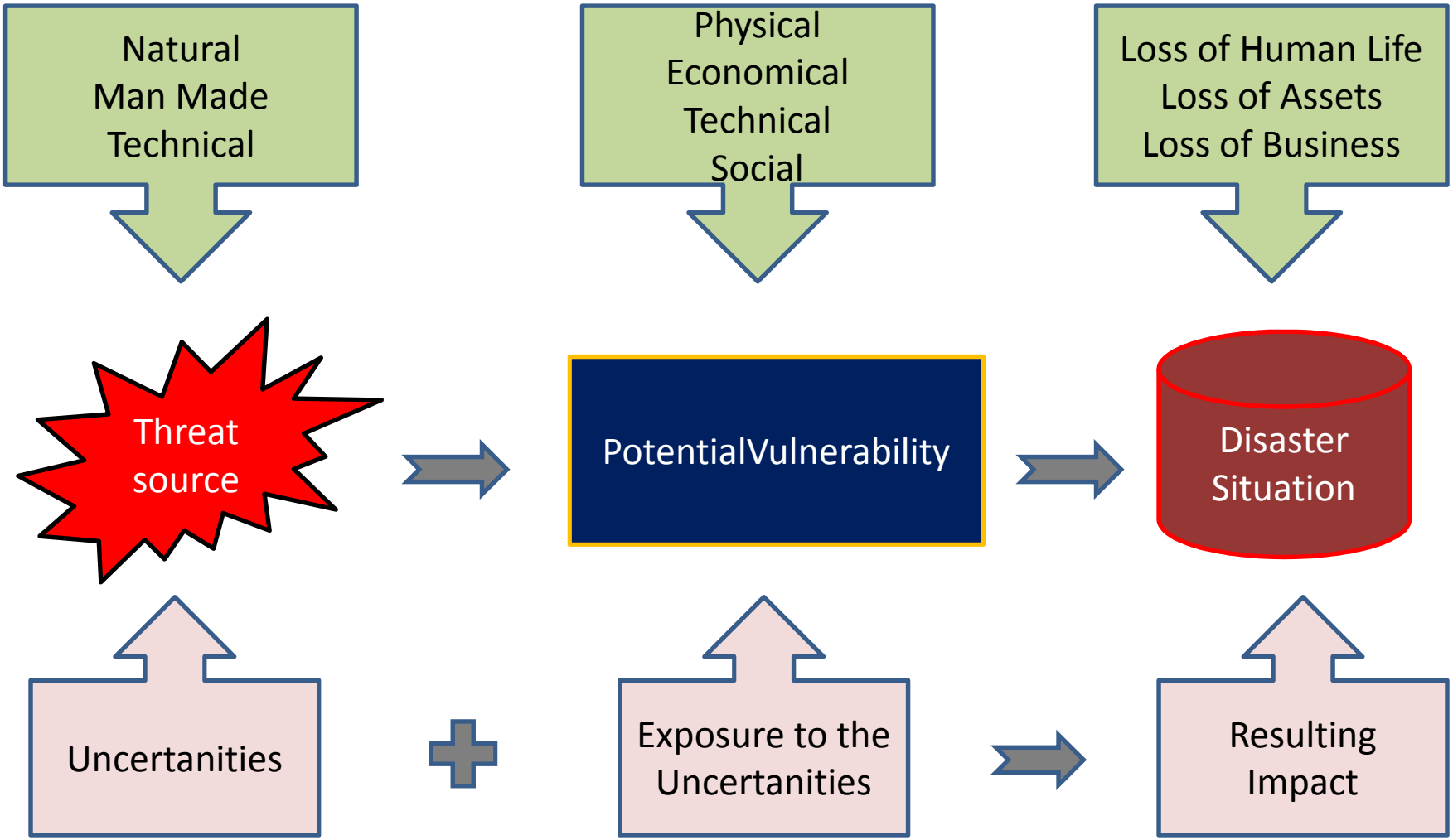
- **Risk** is understood as the effect of uncertainty on objectives which lead the project or a process to failure. They can be produced by uncertainty in finance markets, project failures (at any stage), natural causes and disasters as well as man made disasters : violence or deliberate attacks etc.
- Risks are identified as potential threats which exists in a context or a given environment. They are a combination of two components : uncertanities and the exposure to uncertainities.
    - **R = (Incertanities) (exposure to these uncertainities)**
- Uncertanity can be qualified as unknowingness. It indicates that thes uncertainities are measurable and predictable but difficult to qualify or apprehend with certitude.
- There is a possibility that Tokyo experiences a major earthquake in the years to come. But no body cas say with certainity the nature of this earthquake, how it will affect and what experience it will provoke to the inhabitants.
- Risk can be broken into threes elements : **The Event, the Impact and the consequences**
- Often there is a tendancy to assume that risks are due to ignorance. In the above example it is not a question of ignorance. It is rather a question of being aware that there is a potential known danger leading to device means to reduce the exposure to its impact.

What is Risk ?

- Risk is an issue that arises when uncertainties disrupt the normal activities or process within the organization. It stems from activities, regardless of the size or the challenge.
- It is uncertainties combined with frequencies.
- Risks are factors that affect the realizations of the project. They are present in the form of factors or hazard which are uncertainties that can happen during the operations, project life or the life of the organization.
- Risks are present as possibilities, such as specific action or situation block a project or an organization from reaching its objectives.
- Any factor that can bring about told failure of the program or the paralysis of a situation is to be considered as a risk.
- Risk can be broken into threes elements : **The Event, the Impact and the consequences**

Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.

Risks



Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization

Risk

Some exmples

- The likelihood of an attack on a business center, crippling business activities due to loss of data, information and operational inability resulting in Economical loss. (September 11, 2001 WTC)
- The likelihood of a tsunami created by an earthquake that may affect the population in the coastal area affecting the normal course of life, the economical risk etc.
- There is a difference between Risk and threat. A threat , is an external factor that prevent normal functioning. Threats exist and cannot be avoided. Where as Risk is a unknown certainty and can be mitigated or its impact minimized.

Why Manage Risk ?

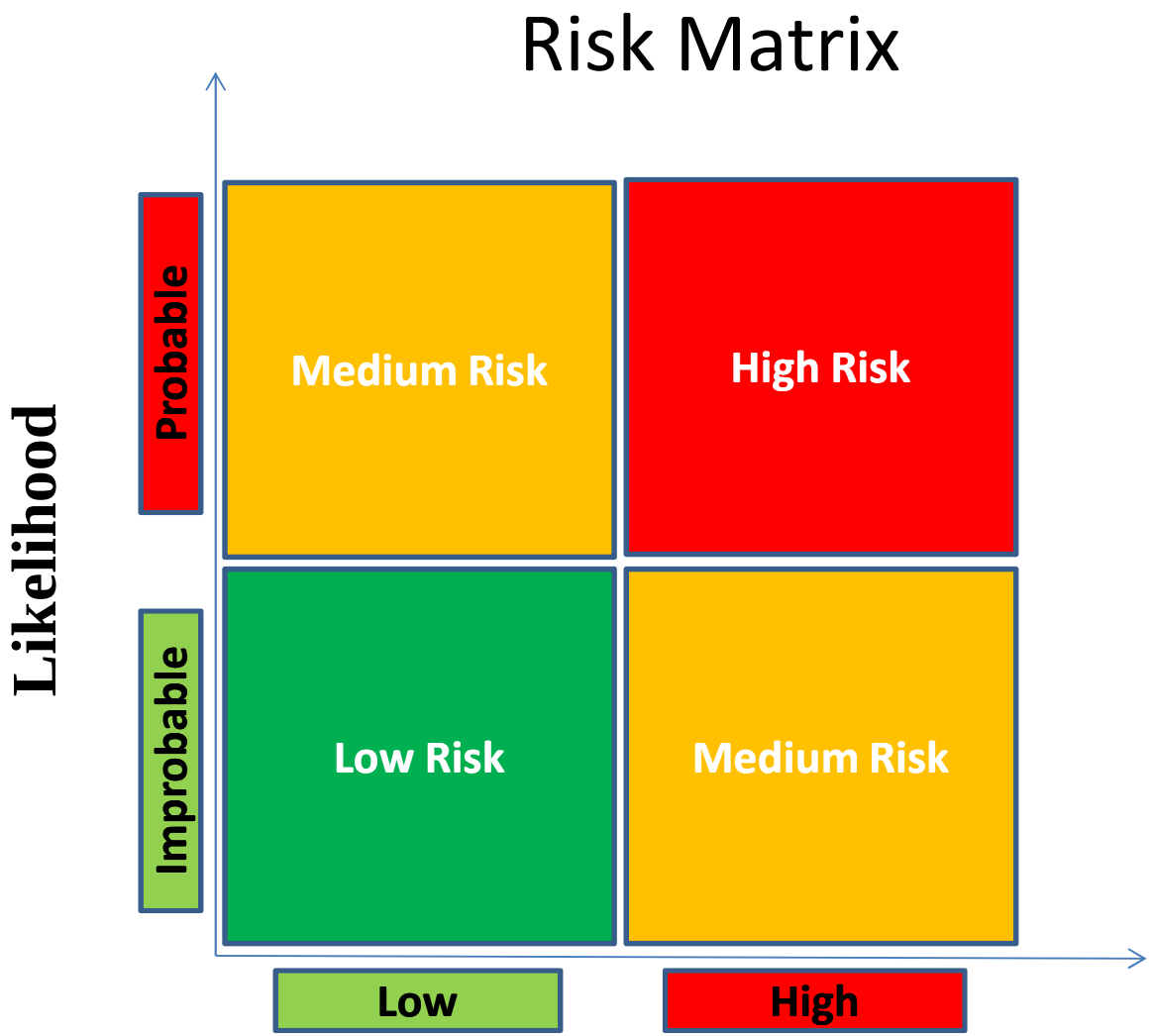
- Risk management is a means to make better decisions and dramatically improve the chances of reaching the goals and objectives.
- The probability and severity of risks helps device strategies for attaining the necessary goals to succeed a project.
- Managing Risk is part of good governance leading to anticipation of Risks factors that will affect the course of action and introducing prior action in order to mitigate or eliminate the risks. It facilitates anticipation
- Managing Risks ensures project success and achievement of goals and objectives.
- It is also a means to adopt the right strategy and the right attitude towards Risks.
- Risk management encompasses three processes: risk assessment, risk mitigation, and Follow-up

Risk Management-The Process

1. Risk Identification
2. Assess the risk – Risk Impact Analysis
3. Elaborate a Risk register
4. Device Risk mitigation plan – Actions
5. Implementation of the Risk Mitigations Plan
6. Conditions for a successful risk Management.
7. Capitalization for future use

Risk Identification

- The basic question is what could greatly go wrong in a given process or within the organization ; block the organization or the team from being able to achieve its objectives.
- What may have an impact of the ability to reach the goals ?
- Risk can be differentiated into three elements :
  1. The event
  2. Its impact
  3. The consequences
- Identification of Risks is also making reference to similar experiences in the same field and conditions



Risk Matrixes are useful if you are presenting company's risk to you Senior Management. It gives relevant data in simple terms

Consequence and likelihood tables

Severity Rating	Potential Loss	Health safety	Legal	Environmental	Public attention/ Reputation	Government Compliance
A	Establish a value	No treatment	No legal issues	Little or no physical impact	No public attention	Minor breach of regulation
B					Concerns expressed by communities	
C					Attentio from local media	
D					Attention form media or forum	
E		Major hospitalisation	Serious legal issues	Serious long term	Major repeated media attention	Major breach of regulation

Consequence Matrix
This table shows the types and scales of consequences and how severe they can be to the organisation

Risk Factors

Common convention holds that Likelihood tables rank with numerals and risk consequences with letters.

The higher the number and the letter, the higher the Risk

Likelihood Rating	Probability	Description	Example
1	<5%	Very Rare	Little evidence it has occu-red, but theoritcially possible
2	5-8%	Rare	It has occured elsewhere
3	8-10%	Unlikely	Known to have occured before
4	11-20%	Possible	Occurs occasionally
5	21-40%	Likely	Occurs periodically
6	41-80%	Almost certain	Occurs frequently
7	>80%	**Imminent**	Event occurs on a regular basis

Likelihood Matrix
Helps to forecast or describe the potential likelihood or probability of a risk event occuring

Risk Identification -2

- Discuss with the team members to reflect on the event.
- Analyze the reports {Finance, narratives etc.}
- Analyze each event, its impact and the consequences
- What is the impact that can occur and what are the chances that it occurs.
- What are the consequences ?

It is important to focus on major issues and avoid minor issues which are threats

The outcome of these analysis will give the Risk Profile.

Risk Assessment

- When assessing a risk we do not focus only on the weakness, but anticipate future problems. They are long sighted and not immediate situation analysis.
- It is the act of determining the probability that a risk will occur and the impact, the event would have. It is rather a cause and effect analysis. In other words the cause is the event that might occur and the effect is the impact.
  - Tsunami that may occur and it may wash away the houses ;
  - Loss of data in an enterprise due to man made or natural disasters.
- Assessment of Risk takes into consideration two important factors : One is the probability of the risk occurring (likelihood) and the second is its impact (consequence)on the project or the process (Nil-Low-Medium-High). Even though it is significantly subjective, it must be quantified as far as possible.

Risk Assessment

- The Risk assessment once it has been appropriately apprehended, will have a certain rating or quantification in terms of finance or even quality.
- Ex. Introduction of an agricultural program in the post communist context in Mongolia. The program was introduced without apprehending the entrepreneurial capacity of the beneficiaries and also their capacity to handle the program in autonomy (because used to government aid and government implementing it). There is lack of ownership, and the project is initiated without keeping these issues in mind.
- The Probability that the project does not attain its goals is quite high and can be rated at : 7
- The impact of this failure is that the project will not be sustainable and can be rated as : E
- The Risk in the case of this project : 7 X E = 7E Very High Risk and this can be further qualified as :
- There will be **scope impact**, because the project will not be completed as envisioned.
- There will be **cost impact** because loss of financial inputs
- **Schedule impact** because, even if the project is to be completed, it will not happen in time. **Schedule, Cost and Scope are risk categories in a project**

Risk Categories

Cost :

The impact estimated in amount has direct influence on the project { Idling, abandonment of equipments, loss of business activities, this can affect the critical path of the program}

Scope

Whenever there is a probability of not completing the work as originally planned, then there is a scope impact. This can be due to poor planning, reduction in Human Resources, overestimated objectives etc. This also affects the critical path of the program.

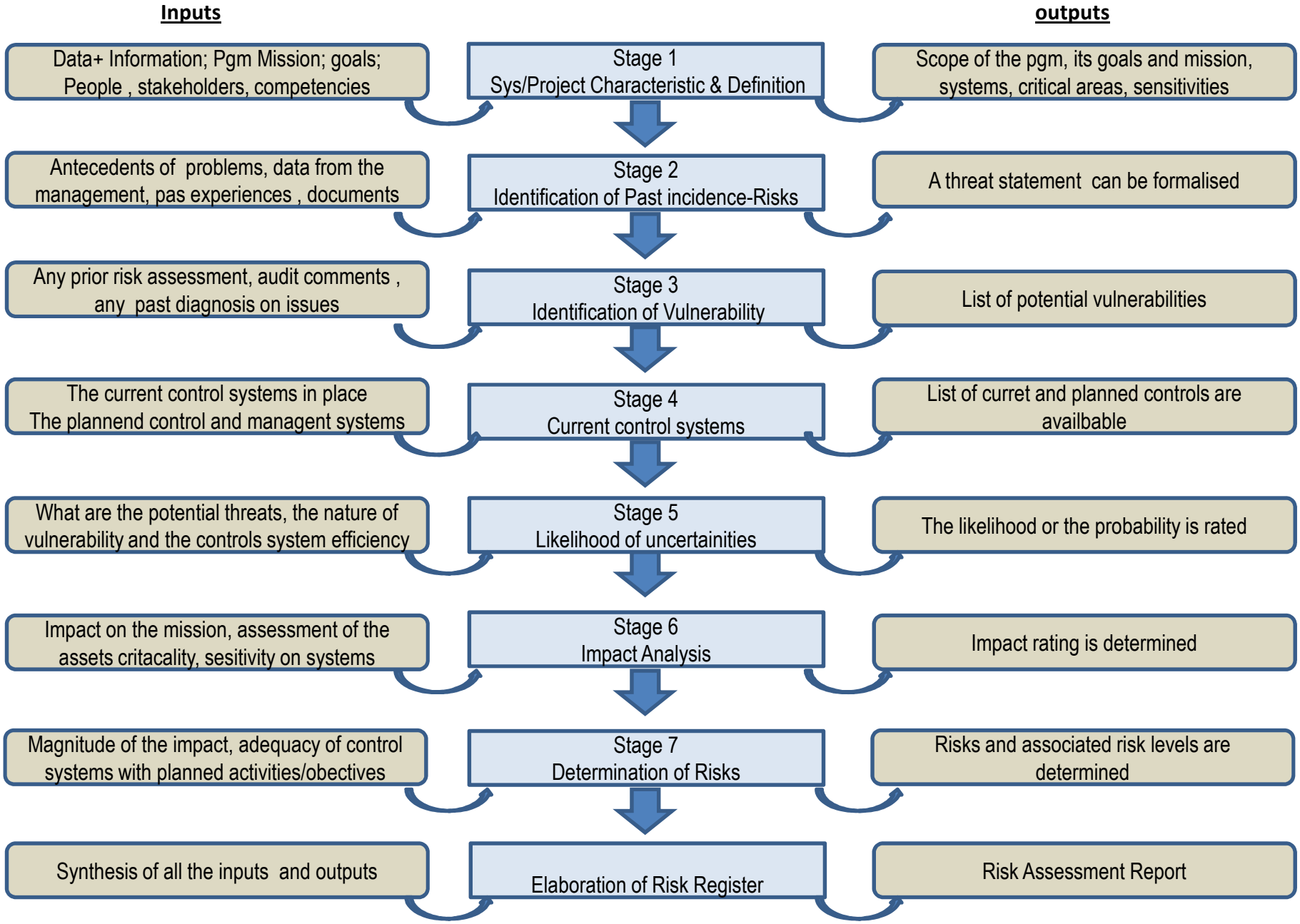
Schedule

This category is inter related to the scope and cost. The schedule delays results in cost increases, reduction of scope or quality. But this will depend on the nature of the impact and the attitude of the stakeholder

Quality

Often cost cuts or reduction in price contribute to the reduction in quality. The reduction in quality leads to lack of satisfaction by the stakeholders with the risk of the project being abandoned.

Risk Assessment Activities



Risk Assessment Activities

Step -1 Definition of the program or system	
Input	Output
Define the scope of the program. The resources and information that constitute the program or the system. What are the technical, operational and management control systems introduced ? How are they executed and who are the people responsible ? Methods for data collection : Questionnaire, On-site Interviews Document Review,	The program is clearly defined with the different parameters , with the relevant data necessary to, understand how it will be executed; capture the potential threats and risk that may be encountered.

Step -2 Identification of threats	
Input	Output
A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. A vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised Threat-Source Identification : Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability. Common threat sources are Natural, Man made or environmental. In assessing threat-sources, it is important to consider all potential threat-sources that could cause harm to the program or the system	A list of potential threats Causes or motivations of threats are available.

Risk Assessment Activities

Step -3 Vulnearbility Identification	
Input	Output
The analysis of the threat to a program or a system must include an analysis of the vulnerabilities associated with the environment. The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources. It should be noted that the types of vulnerabilities that will exist, and the methodology needed to determine whether the vulnerabilities are present, will usually vary depending on the nature of program or the system **Vulnerability Sources :** Environment analysis , previous experiences in similar conditions, experiences in the same field with similar vulnerabilities. **Analysis of the risks** • **Management** : Assignment of responsibilities, separation of duties , line management etc. • **Operational**: definition of operation methodology, clear orientations, objectives are clearly set • **Technical.** :Clear mechanisms for project or system management ;	A list of potential vulnerabilities are available .

Step -4 Analysis of the control systems	
Input	Output
The goal of this step is to analyze the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability. To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the implementation of current or planned controls must be considered. For example, a vulnerability (e.g., system or procedural weakness) is not likely to be exercised or the likelihood is low if there is a low level of threat-source interest or capability or if there are security controls that can eliminate, or reduce the magnitude of the impact.	List of current and planned controls. • Preventive controls • Detective controls warn of violations of security policy and include such controls as audit trails.

Risk Assessment Activities

Step -5 Determination of likelihood of Uncertainties	
Input	Output
To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered: • Threat-source motivation and capability • Nature of the vulnerability • Existence and effectiveness of current controls. **High** : The threat-source is sufficiently capable., Controls to prevent the vulnerability from being exercised are ineffective. **Medium :** The threat-source is capable, but controls are in place that may impede successful exercise of the vulnerability **Low :** The threat-source lacks capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised	Likelihood rating is in place

Step -6 Impact Analysis	
Input	Output
The next major step in measuring level of risk is to determine the adverse impact resulting from a threat exercise of a vulnerability. **BIA** or **Project Impact Analysis** **Impact is :** **High : V**ulnerability (1) may result in the highly, costly loss of major tangible assets or resources; (2) may significantly harm or impede an organization's mission, reputation, or interest; or (3) may result in death or serious injury. **Medium: V**ulnerability (1) may result in the costly loss of tangible assets or resources; (2) may harm, or impede an organization's mission, reputation, or interest; or (3) may result in serious injury. **Low: V**ulnerability (1) may result in the tangible assets or resources; (2) may noticeably harm, or impede an organization's mission, reputation, or interest.	Impact rating is available

Risk Assessment Activities

Step -7 Determination of Risks

Input	Output
The purpose of this step is to assess the level of risk to the project or system. The determination of risk for a particular threat/vulnerability pair can be expressed as follows : • The likelihood of a given threat-source's attempting to exercise a given vulnerability • The magnitude of the impact should a threat-source successfully exercise the vulnerability • The adequacy of planned or existing security controls for reducing or eliminating risk. The final determination of mission risk is derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact. The combination of the matrixs in Slide 12 will give relevant information on the potential risks and the interpretation will show how it will affect the organisation or the system or the project. . The determination of these risk levels or ratings may be subjective. The rationale for this justification can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level. For example, 7E will be a high risk for the programme or the action or the organisation 1A will be very low risk.	

	Risk scale et Action
High	Need for urgent and appropriate action to be undertaken to correct ive measures. Need for quick action plan
Medium	Need for appropriate action and an action plan to be introduced as soon as possible
Low	Reflection on need for action. Accept Risk but vigilance
VeryLow	No or insignificant risk

Risk Register

Priority	Issue	Description	Probability of impact	schedule	scope	quality	cost	Activity undertaken

Risk Assessment Report

EXECUTIVE SUMMARY

I. Introduction

• Purpose; Scope of this risk assessment (Describe the system components, elements, users, field site locations (if any) details about the system to be considered in the assessment.)

II. Risk Assessment Approach (Briefly describe the approach used to conduct the risk assessment) such as—

• The participants (e.g., risk assessment team members) , The technique used to gather information (e.g., the use of tools, questionnaires)

• The development and description of risk scale : 1A -> Low risk and 7E High risk

III. System Characterization

Characterize the project or organization context, system, goals , operating system, data, and users.

- diagram or system input and output flowchart to delineate the scope of this risk assessment effort.

IV. Threat Statement

Compile and list the potential threat-sources and associated threat actions applicable to the system assessed.

V. Risk Assessment Results

- List the observations (vulnerability/threat pairs). Each observation must include a brief description of observation
- • A discussion of the threat-source and vulnerability pair
- • Identification of existing controls
- • Likelihood discussion and evaluation (e.g., High, Medium, or Low likelihood)
- • Impact analysis discussion and evaluation (e.g., High, Medium, or Low impact)
- • Risk rating based on the risk-level matrix (e.g., High, Medium, or Low risk level)
- • Recommended controls or alternative options for reducing the risk.

VI. Summary

- Highlight the most significant observations. Summarize the observations, the associated risk levels, the recommendations, and any comments in a table format to facilitate the implementation of recommended controls during the risk mitigation process.

Risk Mitigation

- Risk mitigation, the second process of risk management, involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process.
- Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior management and functional and business managers to use the ***least-cost approach and implement the most appropriate controls to decrease mission risk to an acceptable*** level, with ***minimal adverse impact on the organization's resources and mission and the program.***
- Risk mitigation is a systematic methodology used by senior management to reduce mission risk. Risk mitigation can be achieved through any of the following risk mitigation options:

• **Risk Assumption.**

To accept the potential risk and continue operating the program or system or to implement controls to lower the risk to an acceptable level

• **Risk Avoidance.**

To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the program or close down when risks are identified.

• **Risk Limitation.**

To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls)

• **Risk Planning.**

To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls

• **Research and Acknowledgment.**

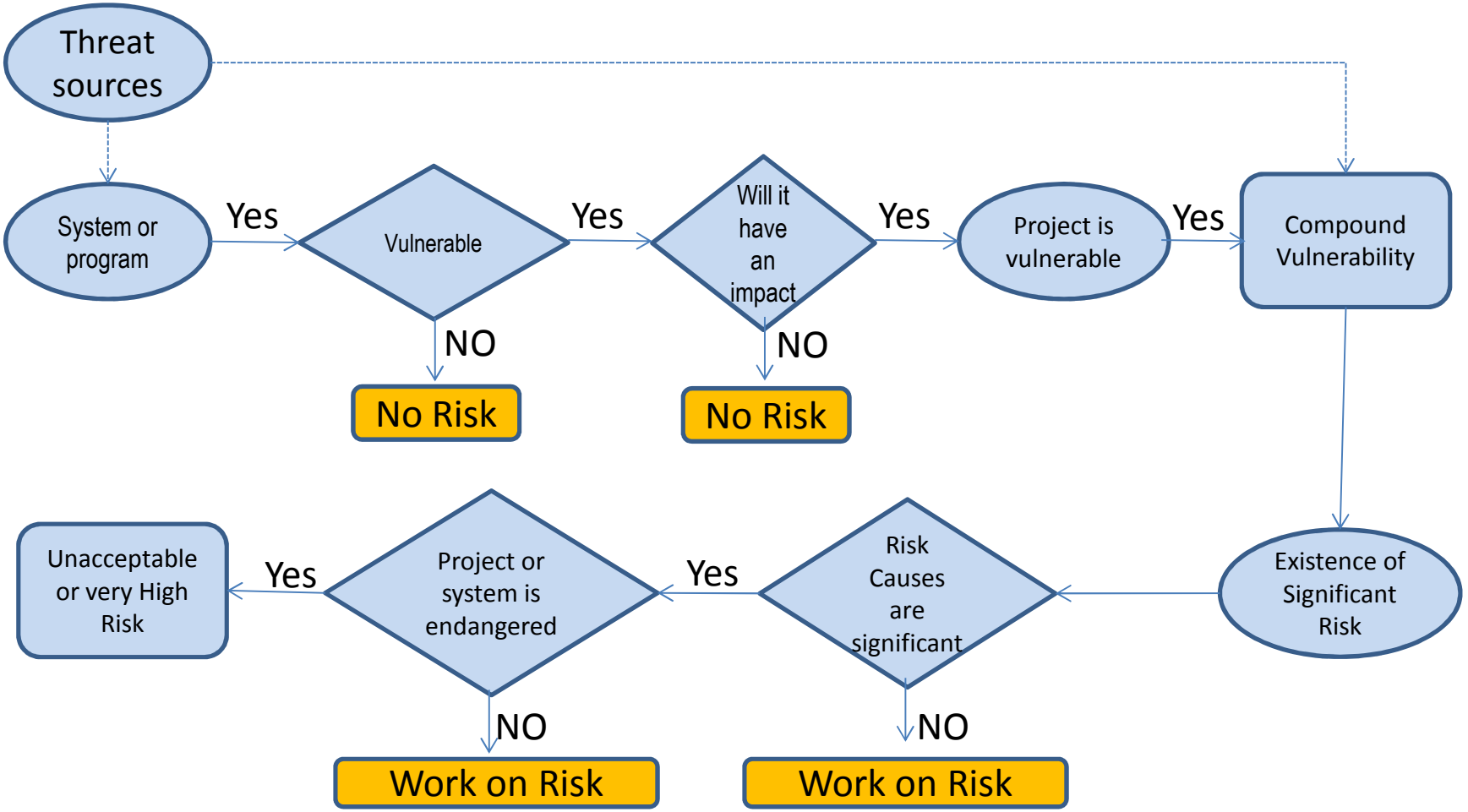
To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability

• **Risk Transference.**

To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

The **goals and mission** of an organization should be considered in selecting any of these risk mitigation options. It may not be practical **to address all identified ris**ks, so **priority should be given** to the threat and vulnerability pairs that have the potential to **cause significant mission impact or harm**

Mitigation strategy



Conditions for a successful Risk Management

- 1. A successful risk management program will rely on (1) senior management's commitment.
- 2. the full support and participation of the technical and operational team
- 3. the competence of the risk assessment team, which must have the expertise to apply the risk assessment methodology to a specific program or organization or system, identify mission risks, and provide early safeguards that meet the needs of the organization
- 4. The awareness and cooperation of members of the concerned team , who must follow procedures and comply with the implemented controls to safeguard the mission of the organization
- 5. An ongoing evaluation and assessment of the program and mission related risks.
- 6. Risk Assessment is an essential element in the Disaster Recovery Plan

Annexe – Information collection

Information-Gathering Techniques

- Any, or a combination, of the following techniques can be used in gathering information relevant to the program or the system :

Questionnaire.

- To collect relevant information, risk assessment personnel can develop a questionnaire concerning the management and operational controls planned. This questionnaire should be distributed to the applicable technical and nontechnical management personnel who are designing or involved in the program. The questionnaire could also be used during on-site visits and interviews.

On-site Interviews. Interviews with IT system support and management personnel

- can enable risk assessment personnel or those involved in the program to collect useful information about the operations (e.g., how the program is operated and managed). On-site visits also allow risk assessment personnel or program staff to observe and gather information about the physical, environmental, and operational progress of the program. Interview questions asked during interviews with program staff will help to have a better understanding of the operational characteristics of the project and the organization.
- **Document Review. Policy documents (e.g., legislative documentation, directives),**
- Documentation on the progam, the complexities related to the program and documents related previous audit report, risk assessment report, financial results, narrative reports c*an provide good information about the risk factors*. An organization's mission impact analysis provides information regarding the uncertainties and sensitivity. around a project.

Use of Mapping Tool.

- Proactive technical methods can be used to collect system information efficiently. For example, a program activity mapping will give a good understanding of the areas of risk and failures that are probable.