

# Gestion de Risques et d'opportunités-2

## Identification, Analyse et Prévention des Risques

*Séminaire IPMA*

*ESIEE*

*25/09/2015*

Aloysius John  
September 2015

# Objectifs et perspective

- Identifier, Comprendre et analyser les risques dans le cadre du montage et de la gestion des projets. Proposer une démarche méthodologique
- Gérer les risques plutôt que de les subir
- Mesurer, calculer et établir la gravité de risques.
- Etablir un plan d'action pour les prévenir ou atténuer leur impact sur le projet.

# Introduction

## Gestion de Risques

- C'est identifier et analyser des risques plutôt que les subir.
- Processus pour les managers du projet pour identifier les facteurs qui affecteront les projets et l'aboutissement des objectifs.
- Moyens d'identifier les facilitateurs et les obstacles dans la gestion de projet
- Moyen d'anticiper et de prendre des bonnes décisions à temps et ainsi permettre une meilleure performance du projet.

# Comment comprendre le risque?

- **Risque peut être défini comme** l'influence des incertitude ou aléas dans un cycle de projet et qui influence son succès ou échec. Les risques peuvent être diverses natures : naturels, fait par l'hommes, financiers, environnementaux
- Les Risques peuvent être compris comme des menaces potentielles qui existe dans un contexte ou dans un environnement donné, dans lequel évolue un projet. C'est une combinaison de deux éléments : Les aléas et l'exposé aux aléas.

$$\text{Risques (R)} = (\text{Aléas}) (\text{exposé à ces aléas})$$

- Aléas sont les imprévisibilités qui peuvent être mesuré ou prévenu mais leur impact est difficile à prédire. Ex. Un séisme ; un attentat .
- Risque peut être divisés en trois entités : L'événement, l'impact et son conséquence
- Dans la gestion d'un projet, il faut être conscient de la présence des risques. Il n'est plus possible de dire que « nous n'avons savons pas » ou « si on avait su ! », « on a été pris par surpris ».

# Risques est

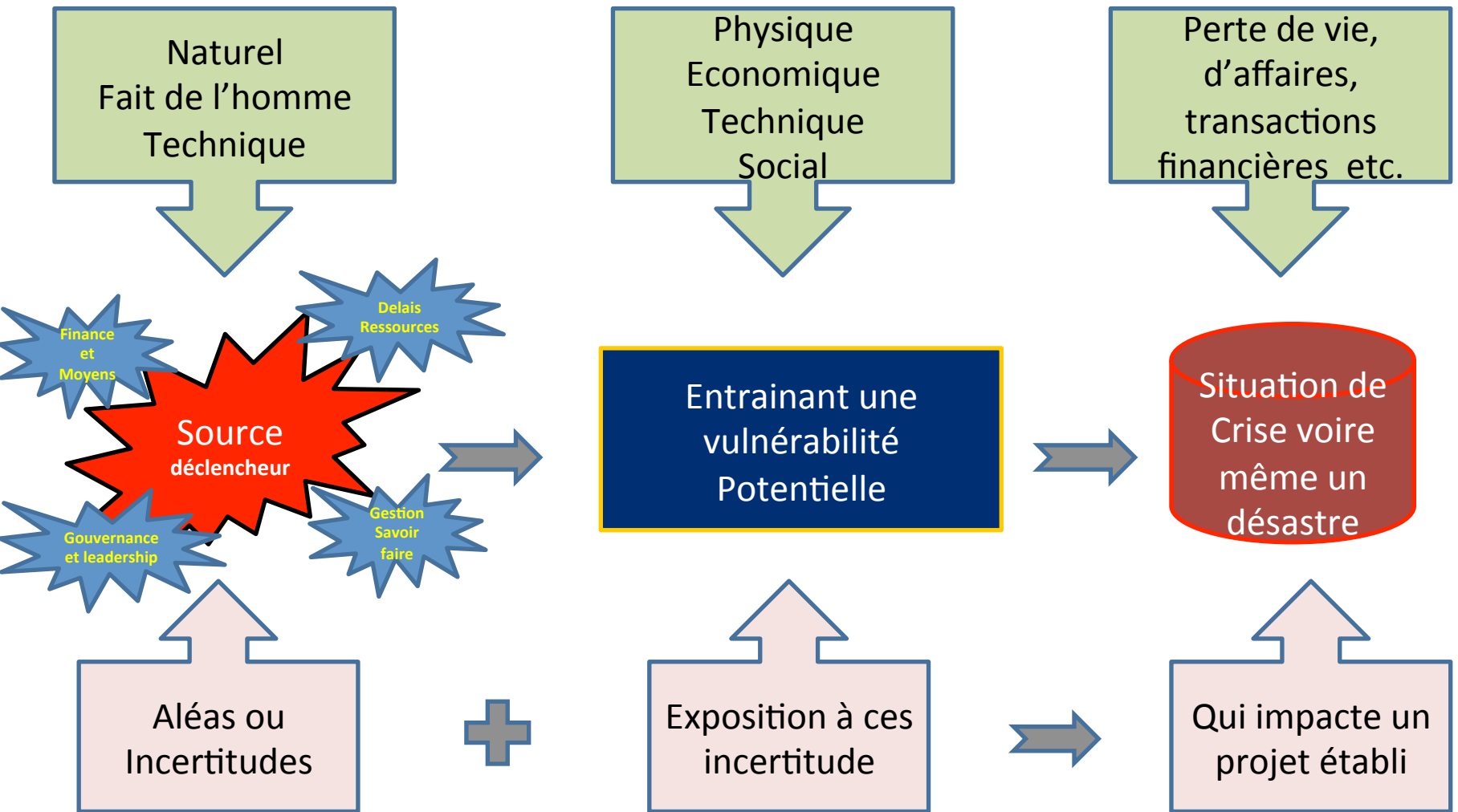
- Tout factor qui peut entrainer l'échec total ou partiel d'un projet est un risque.

***Risque est la probabilité d'une facteur externe qui a la possibilité de remettre en cause la bonne marche de l'organisation ou un projet.***

# Gestion de Risque

- La gestion de Risque implique :
  1. Nommer le risque ! l'identifier.
  2. Gérer les Risques en les priorisant.
  3. La gestion des risques - Le Processus
  4. Conditions nécessaires pour une bonne gestion de risques.
  5. Prendre en considération les expériences passées pour mieux faire –La capitalisation de l'expérience
  6. Suivi Evaluation des risques

# Risques



***Le Risque est un produit de la probabilité que la source déclencheur exerce une vulnérabilité potentielle ayant pour résultat l'impact sur le projet ou l'organisation parfois entraînant une situation de crise.***

# Risques

## Quelques exemples

- La possibilité d'un attentat
- La possibilité d'un tsunami
- Un projet que l'on pense être bien développé et qui ne marche pas.
- Rappelons qu'il y a une différence entre Risque et menace.
- La Menace est un facteur externe qui peut agir sur un projet et il se transforme en risque. Par exemple : un projet soutenu par une collectivité locale et qui, à un moment donné, refuse les crédits. C'est une menace qui vient d'un facteur externe (politique) mais le risque étant le manque de crédit.
- Le risque donc est l'arrêt de financement qui est prévisible et par rapport auquel il faut se préparer par des solutions alternatives pour atténuer son impact.



# Pour quoi gérer le risque?

- La gestion de risqué est un moyen de prendre les meilleures décisions et se donner les moyens d'agir à temps.
- L'analyse de risque permet d'adopter la bonne stratégie pour réduire leur impacte. C'est important pour atteindre les objectifs du projet.
- La gestion de risque fait partie de la bonne gouvernance elle permet l'anticipation
- La gestion de risque permet le succès du projet et la l'aboutissement des objectifs.
- Permet d'adopte la bonne stratégie et la bonne attitude envers les situation de risques.
- La gestion de Risque comportent trois processus: Gestion de risques, réduction de risque et le suivi.

# La Gestion des Risques -Le Processus

1. Identification des Risques
2. Diagnostic des risques – Analyse de l’impact
3. Elaboration d’un Cahier de Risques
4. Maitriser les Risques Plan de réduction de Risques– Actions à entreprendre
5. Mise en œuvre du plan de réduction de risques.
6. Conditions pour une bonne gestion de risques.
7. Capitalisation pour les références futures

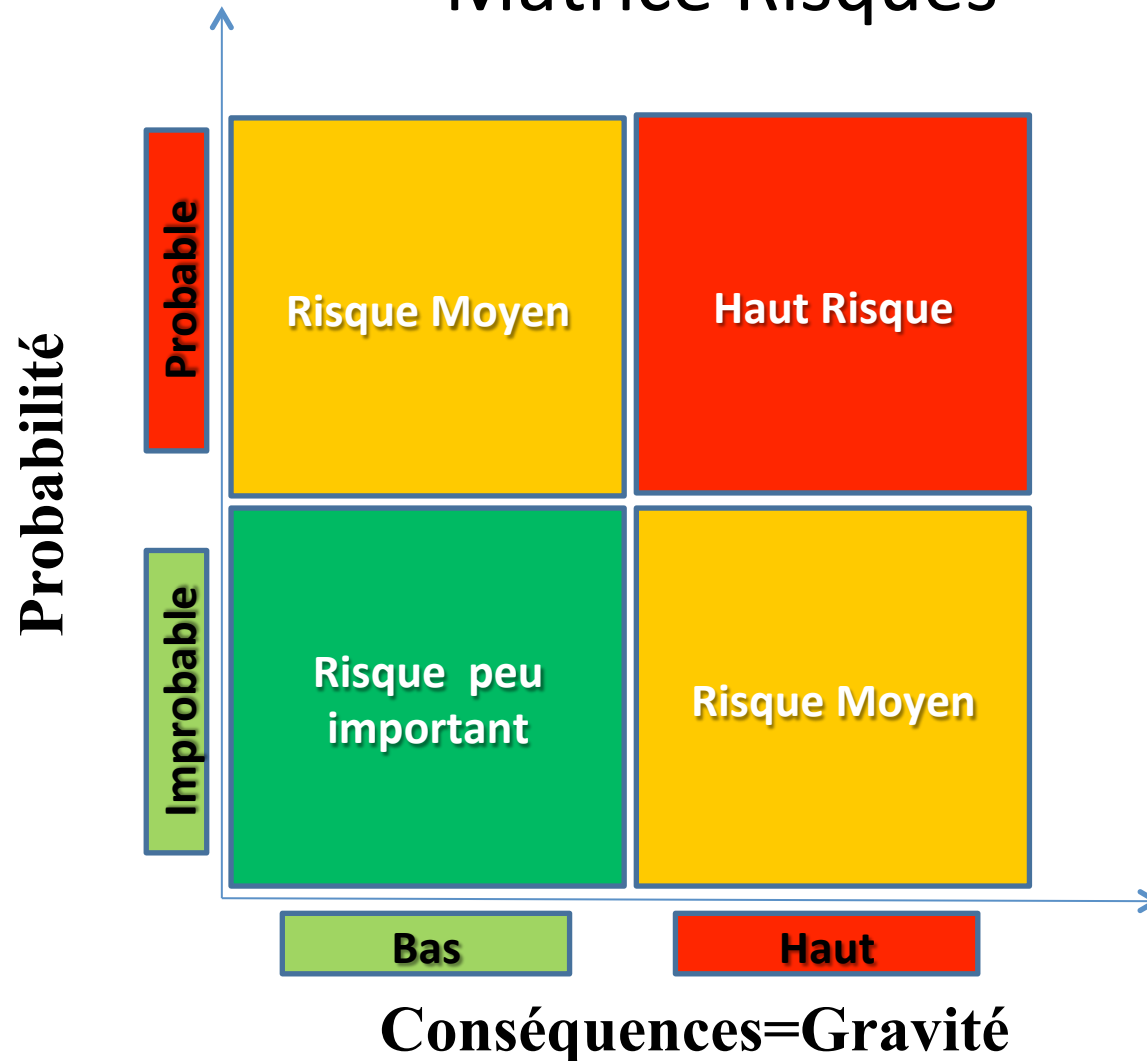
# Risque Identification

- La question de base ou la question principale à poser est : ce qui peut dériver dans un processus donné ou dans un projet, impactant sur l'atteinte des objectifs..
- Quels sont les facteurs qui peuvent avoir un impact sur la capacité du projet ou de l'organisation à atteindre ses objectifs. ?
- Quels sont les sources de menace ?

# Identification du Risque

- Le Risque comporte trois éléments :
  1. L'Événement
  2. Son impact
  3. Ses Conséquences
- L'Identification des Risques renvoi également aux expériences similaires dans les mêmes domaines et dans le même contexte.
- En terme de **méthodologie**, l'identification des risques pourrait se faire par des discussions en groupe, l'arbre à problèmes, les expériences capitalisées, etc

# Matrice Risques



**Un matrice de Risque est utile dans une analyse qualitative pour présenter les risques de projet à son supérieur ou au Conseil d'Administration. C'est un moyen pour présenter faits complexes simplement.**

# Matrices de Probabilité et Conséquences

Echelle de Gravité	Perte Potentielle	Sécurité sanitaire	Problèmes légaux	Environnemental	Attention de média/ Réputation	Gouvernement Respect des normes humanitaires
5	Chiffrer Peu importante	Pas de problème	Aucun problèmes	Pas de problèmes	Très bonne couverture médiatique	Bonne réaction de l'Etat
4						
3						
2						
1	Très importante	Hospitalisation	Problèmes importants	Important problèmes environnemental	Pas de couverture médiatique	Non respect de régulation

Matrice de Conséquence  
Cette grille met en évidence les types et gravité des conséquences

## Risk Factors

Les facteurs de Risques sont identifiés à partir du croisement des probabilités et les conséquences. Plus les chiffres son grands, les risques sont qualifiés comme étant graves.

Likelihood Rating	Probability	Description	Example
1	<10%	Very Rare - Rare	Il y a peu d'évidence dans le passé, mais théoriquement c'est possible
2	11-16%	Unlikely - Possible	Il y eu des problèmes. Pourrait arriver des fois
3	16-24%	Possible	Cela arrive de temps en temps
4	24-48%	Likely	Occurrence est fréquente.
5	48-100%	Très certainement	Imminent

Matrice de probabilité  
Permet de prédire ou décrire la probabilité d'un aléa et le gradué qualitativement à partir des expériences de passé.

# Matrice de Risques

Probabilité	Très Probable	5	5 R	10 MR	15 HR	20 HR	25 HR
		4	4 LR	8 MR	12 MR	16 HR	20 HR
		3	3 LR	6 R	9 MR	12 MR	15 HR
	Peu Probable	2	2 NR	4 LR	6 R	8 MR	10 MR
		1	1 NR	2 NR	3 LR	4 LR	5 R
			1	2	3	4	5
HR:Haut Risque; MR:Moyen Risque; R=Risque certain; LR= Bas Risque, NR=Risque nul							

Peu Grave

Très Grave

Gravité

AJ-Avril 2013/ESIEE

# Identification des Risques-2

- Discuter avec l'équipe et réfléchir sur les aléas ou évènements probables.
- Analyser les rapports {Finance, narratives etc.}
- Analyser chaque évènement, son impact sur le projet et les conséquences.
- Quels sont les impacts les plus probables et quelle est la probabilité que cela arrive.
- Quelles sont les conséquences ?

Il faut éviter de se perdre dans les détails et center sur les problèmes qui risquent d'affecter les objectifs critiques du projet

Les résultats de cette analyse permettront de d'identifier le profil du risque.



# Diagnostic des Risques

- Quand on engage un diagnostic de risque, il faut aller au-delà des problèmes et faiblesses perceptibles et aussi anticiper les problèmes futurs. Cela veut dire que l'on doit avoir une perspective à long terme et non pas l'analyse de la situation immédiate seulement.
- C'est plutôt une question de déterminer la probabilité qu'un risque soit présent et l'impact que l'évènement aura sur le projet. C'est une question de comprendre l'évènement qui peut arriver comme une cause et l'effet quand l'évènement quise produit est l'impact. C'est donc une analyse de cause à effet.
  - Ex. Un cyclone pourrait se produire et il peut détruire les maison. Mais quand précisément, comment et avec quelles force est difficile à prédire.
- Comme on a vu dans le matrice de risque, le diagnostic des risques prends en considération deux facteurs clefs: la probabilité de risque et le deuxième est la conséquence ou son impact sur le projet..

# Diagnostique des Risques

- Une fois le diagnostic est fait, il y aura un résultat sous forme de de chiffre comme dans la matrice de risqué. Ces résultats pourront être par la suite appliqué par rapport à des éléments divers dans le projet (finance, Ressources Humaines, délais etc.).
- Ex. En Mongolie un projet agricole a été introduit dans le contexte post communiste. Aucune précaution a été prise par rapport à la capacité entrepreneuriale de la population, leur capacité à prendre en main le projet ( car il ont été trop habitué à recevoir de l'état). Il y a manque de appropriation du projet. Le projet a été initiés sans tenir compte de toutes ces question.
- La Probabilité que le projet atteint pas les objectifs est très importante et on peut le définir comme étant 5
- L'impact sur le projet sera important , car le projet ne sera pas soutenable ou durable. On peut dire que conséquence sera importante et on peut dire c'est 5
- Le Risque dans le cas de ce projet est :  $5 \times 5 = 25$  (Haut Risque). Ce résultat pourra être plus qualifié de la manière suivante :
- Il y aura un « **Impacte sur envergure** », car le projet ne pourra pas être complété comme prévu. (**scope impact**)
- Il y aura un « **Impact financier** » car le projet ne pourra devenir autosuffisant.
- « **Impacte sur le delivvable** » **Schedule impact** car le delais ne sera pas respecté. Envergure, finance, et delivvable sont les catégories de risques.

# Catégories de Risque

## Coût ou finance :

L'impact estimé financièrement aura un impact direct sur le projet : temps d'inactivité, abandon des équipements, perte de rendement, perte de commerce etc. ces éléments pourraient affecter le chemin critique d'un projet.

## Envergure (étendu)

Quand il y a une probabilité de ne pas pouvoir terminer le travail comme planifié au départ. Les raisons ou les causes sont multiples : Mauvais planning, réduction dans les ressources humaines, les objectifs surestimés etc. Ces éléments impactent également le chemin critique d'un projet.

## Délais (Schedule)

Cette catégorie est liée à l'envergure et le coût. Les délais ont pour conséquences l'augmentation des coûts, réduction dans l'envergure, enfin dans la qualité même du projet. Cela dépendra de la nature de l'impact et l'attitude des parties prenantes.

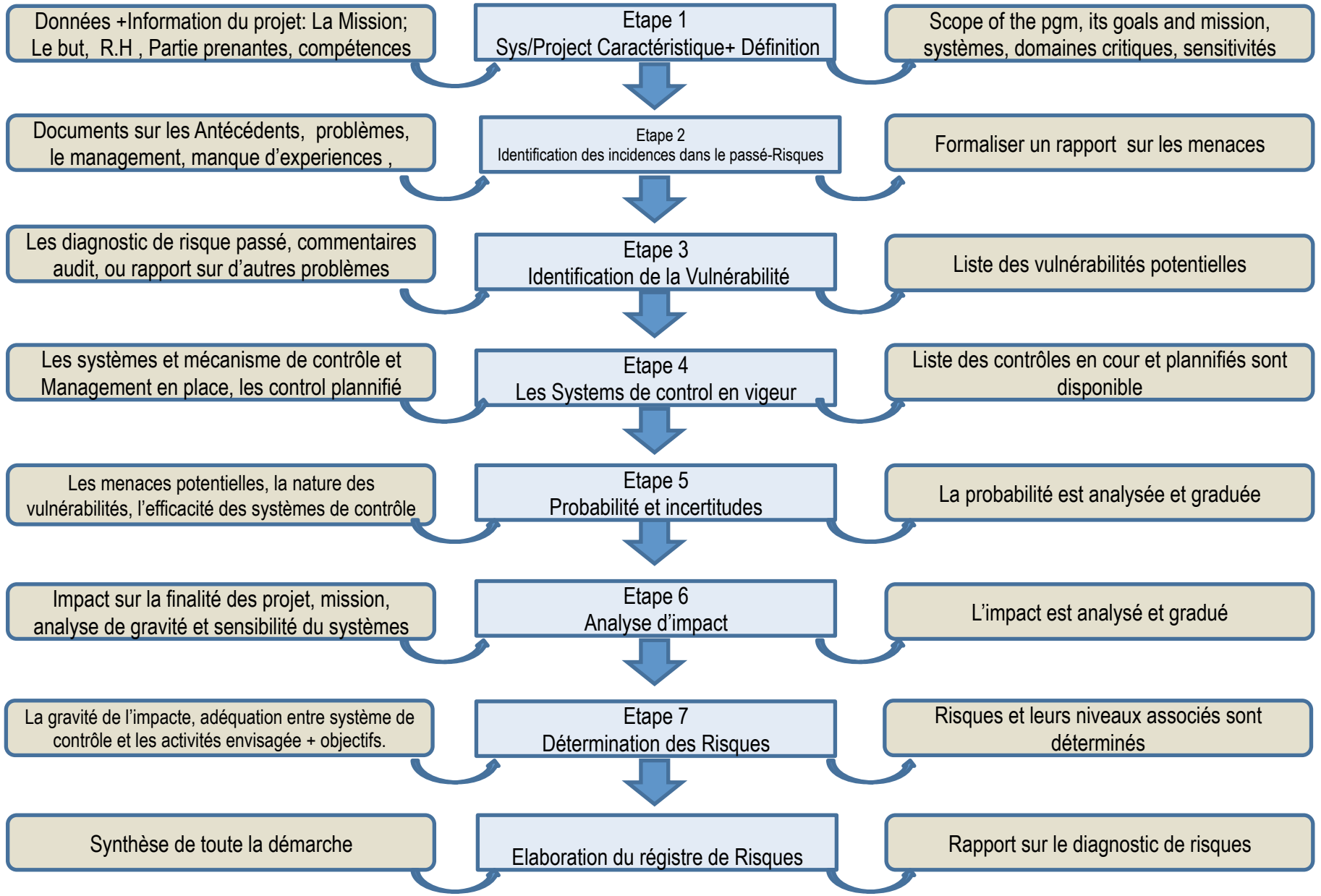
## Qualité

Souvent la réduction des coûts ou réduction de prix contribue à la réduction de qualité. La réduction de qualité entraîne la insatisfaction des parties prenantes avec le risque que le Project n'obtienne pas l'adhésion ou bien soit abandonné.

# Les activités du diagnostic

## Domaine d'investigation

## Résultat de l'analyse



# Activités du diagnostic de Risques

## Etape -1 Definition du programme ou système

<u>Domaine d'investigation</u>	<u>Résultat de l'analyse</u>
<p>Définir la portée du programme. Les ressources et les renseignements qui constituent le programme ou le système. Quels sont les problèmes techniques, opérationnels et systèmes de contrôle de gestion introduites ? Comment sont-elles exécutées et qui sont les personnes responsables ?</p> <p>Les méthodes de collecte des données : Questionnaire, sur place, des entrevues</p> <p>Examen des documents,</p>	<p>Le programme est clairement défini avec les différents paramètres , avec les données pertinentes nécessaires pour comprendre comment il sera exécuté; capturer les menaces potentielles et les risques qui pourraient être rencontrés.</p>

## Etape -2 Identification des Menaces

<u>Domaine d'investigation</u>	<u>Résultat de l'analyse</u>
<p>Une menace est une source potentielle de nuisance qui crée la vulnérabilité dans un projet. Une vulnérabilité est une faiblesse qui peut être déclenchée accidentellement ou délibérément. Une source de menace ne présente pas un risque lorsque le projet or l'organisation n'est pas vulnérable.</p> <p>Identification des sources de menace : soit (1) il est crée intentionnellement pour aggraver une situation de vulnérabilité, ou (2) une situation inattendu, défaillance méthodologique, qui pourrait rendre un projet vulnérable.. Les sources de menace sont naturelles, d'origine humaine ou environnementale.</p> <p>Dans l'évaluation de la menace et ses sources, il est important de tenir compte de toutes les sources à la menace potentielle que pourrait contribuer à la défaillance du programme ou le système</p>	<p>Une liste de menaces potentielles</p> <p>Les causes ou les facteur déclenchant des menaces sont disponibles.</p>

# Activités du diagnostic de Risques

## Etape -3 Identification de la Vulnérabilité

<u>Domaine d'investigation</u>	<u>Résultat de l'analyse</u>
<p>L'analyse de la menace à un program or système doit aussi inclure une analyse de la vulnérabilité associé avec son environnement. L'objectif de cette étape est de développer une liste vulnérabilité dans le systèmes (les défaillance, faiblesses ) qui pourraient être exposé par des sources de menaces potentielles.</p> <p>Précisons que les types de vulnérabilité qui existent, et la méthodologie nécessaire pour détecter les vulnérabilités varie selon nature du programme ou le système.</p> <p><b>Sources de Vulnérabilité :</b> Analyse Environnementale , Expériences dans le passés dans des conditions similaire, expériences dans le même domaine avec les vulnérabilités similaires.</p> <p><b>Analyse des Risques</b></p> <ul style="list-style-type: none"> <li>• <b>Management :</b> Répartition de responsabilités, séparation of devoir , Gestion des ressources humaines etc.</li> <li>• <b>Opérationnel:</b> définition de la méthodologie opérationnelle, Orientation claires Clarté des o bjectifs</li> <li>• <b>Technique. :</b> Mechanisms claire pour la gestion des projet ou système</li> </ul>	<p>Une liste de vulnérabilités potentielles sont disponible.</p>

## Etape -4 Analyse du système de contrôle

<u>Domaine d'investigation</u>	<u>Résultat de l'analyse</u>
<p>Le but de cet étape est l'analyse des contrôles mis en place ou son planifié pour être mis en place, dans le cadre du projet ou par l'organisation, pour minimiser ou eliminer la probabilité à ce qu'une menace rends le système vulnérable..</p> <p>Pour bien appréhender la vulnérabilité sur un système ou un élément dans un projet, il est nécessaire de analyser le système de contrôle en place dans les zones de menace pour le projet. Par exemple, la vulnérabilité (système ou procédure) sera moindre si le source de menaces qui pèse sur le systèmes sont mises sous contrôle. Car cela permettra de réduire l'impact sur le système en prenant les mesure préventive..</p>	<p>Une Liste système de contrôle existant et planifié.</p> <ul style="list-style-type: none"> <li>• Contrôles Préventifs</li> <li>• Système d'alerte qui permet de prendre en main les problèms à partir de suivi des audits ou d'autres contrôles interne ou externe.</li> </ul>

# Activités du diagnostic de Risques

## Etape -5 Détermination de la probabilité des incertitudes

<u>Domaine d'investigation</u>	<u>Résultat de l'analyse</u>
<p>Pour avoir une idée de la probabilité qu'une source de menace pourrait exercer sur le projet pour le rendre potentiellement vulnérable, les facteurs suivant doivent être pris en considération :</p> <ul style="list-style-type: none"> <li>• La source de menace et sa capacité à nuire le projet</li> <li>• Nature de la vulnérabilité</li> <li>• L'existence et l'efficacité des systèmes de contrôles existents.</li> </ul> <p><b>Haute Vulnérabilité</b> : La source de menace est suffisamment capable de nuire, les systèmes de contrôles en place sont inefficaces..</p> <p><b>Moyenne Vulnérabilité</b> : La source de menace pourrait affecter, mais les systèmes de contrôles existents peuvent agir et prévenir la vulnérabilité</p> <p><b>Basse Vulnérabilité</b> : Les sources de menaces ne sont pas nuisibles, les systèmes de contrôle en place protègent le projet et il est peu vulnérable.</p>	<p>Une grille incertitude est en place.</p>

## Etape -6 Analyse d'Impact

<u>Domaine d'investigation</u>	<u>Résultat de l'analyse</u>
<p>L'Etape suivante dans la mesure du niveau de risque est de déterminer l'impact des menaces venant des sources diverses qui produiront la vulnérabilité..</p> <p>Chaque élément du projet est analysé en faisant une analyse d'impact sur le projet ou sur les activités.</p> <p><b>Impact is :</b></p> <p><b>Important : Haute Vulnérabilité</b> (1) ayant pour conséquence coût important, perte de ressources ou de moyens (2) Peut nuire significativement le projet ou la mission de l'organisation, la réputation ou les intérêts ou (3) des conséquences graves pour le projet ou l'organisation.</p> <p><b>Moyenne: Vulnérabilité</b> (1) Pourrait avoir une perte de ressources, (2) Pourrait affecter le projet.</p> <p><b>Low: Vulnérabilité</b> (1) N'impactera pas trop les ressources ou les moyens, mais elle est présente. (2) Pas d'incidences grave, mais il faut garder la vigilance.</p>	<p>Une analyse d'impact est disponible</p>

# Activités du diagnostic de Risques

## Etape -7 Détermination de Risques

### Domaine d'investigation

Cette étape nous permet de mesurer les niveaux de risques dans le projet ou les système ou dans l'organisation. Le risque pour un particulier Menace-Vulnérabilité est déterminé comme suit :

- La probabilité d'une source de menace qui produit la vulnérabilité
- La gravité de l'impact
- La pertinence des contrôles existant ou planifié pour réduire ou éliminer l' impact de ces risques.

Le matrice de risque dans le diapo N° XX donnera une idée claire de qualification des risques.

Ces graduations des risques sont peut être subjectives, mais elles sont indispensable et donnent une valeur de référence à partir des données identifiées dans le projet.

Dans le projet, chaque élément du projet doit être analyse pour bien saisir tous les aspects à l'intérieur du projet qui peuvent affecter le chemin critique d'un projet.

### Résultat de l'analyse

	<b>Risk scale et Action</b>
High	Importance d'une action urgente pour prendre des mesures nécessaires pour gérer
Medium	Besoin d'action appropriée et un plan d'action doit être introduit assez vite.
Low	Accepter le risque mais réfléchir pour les actions à mettre en oeuvre
Unlikely - Possible	Il y eu des problèmes. Cela Pourrait arriver des fois
VeryLow	Pas de risque significatif



# Registre de Risques

Priorité	Le problème ou menace identifié	Description	Probabilité de l'impacte	Délais	Etendu (scope)	qualité	coût	Activité entreprise

# Rapport de bilan de risque

## Résumé

### I. Introduction

- La raison d'être; Etendu du diagnostic des risques (Décrire le système ,des composants, des éléments, des utilisateurs, l'emplacement des sites de terrain -le cas échéant, des détails sur le système à prendre en considération dans l'évaluation.)

### II. Risk Assessment Approach

- Les participants (par exemple, Les membres de l'équipes d'évaluateur), La technique utilisée pour recueillir des informations (par exemple, l'utilisation d'outils, questionnaires)
- Explication sur la grille des risques :

### III. Présentation du système ou de projet

Expliquer le contexte du projet ou de l'organisation, le système de gestion, les objectifs, les données disponibles sur le fonctionnement ainsi que l'utilisateur.

- Il faut un bon schéma directeur pour bien délimiter le travail de diagnostic de risques.

### IV. Threat Statement

Mettre ensemble la liste des sources de menaces potentielles et les menaces associées qui pourraient influencer le système ou projet étudié.

### V. Résultats de diagnostic de Risques

- Dressez la liste des observations (paires vulnérabilité / menace). Chaque observation doit inclure une brève description de l'observation :
  - Une discussion de la menace et de la vulnérabilité
  - Identification des contrôles existants
  - la discussion et à l'évaluation de la Probabilité (par exemple, élevé, moyen ou faible probabilité)
  - la discussion et à l'évaluation de l'analyse de l'impact (par exemple, élevé, moyen ou faible incidence)
  - Évaluation des risques basée sur la matrice de niveau de risque (par exemple, élevé, moyen ou faible niveau de risque)
  - contrôles recommandés ou des options alternatives pour réduire le risque.
- **VI. Résumé :** Mettre en évidence les observations les plus importantes. Résumer les observations, les niveaux de risque associés, des recommandations et des commentaires dans un format de tableau pour faciliter la mise en œuvre de contrôles recommandés pendant le processus de réduction des risques.

# Risk Mitigation

- Atténuation des risques, le deuxième processus de gestion des risques, implique la hiérarchisation, l'évaluation et la mise en œuvre des contrôles de réduction des risques appropriées recommandées par les procès d'évaluation des risques.
- Parce que l'élimination de tout risque est généralement difficile ou presque impossible, il est de la responsabilité de la haute direction et les gestionnaires fonctionnels et d'affaires d'utiliser l'approche la moins coûteuse et mettre en œuvre les contrôles les plus appropriées pour réduire le risque de projet à un niveau acceptable, avec un minimum impact négatif sur les ressources et la mission de l'organisation et le programme.
- La réduction des risques est une méthode systématique utilisée par la haute direction pour réduire le risque de mission. La réduction des risques peut être atteinte par l'une des options d'atténuation de risque suivants :

- **Acceptation du Risque.**

Accepter le risque potentiel et continuer le déroulement du programme ou du système ou de mettre en œuvre des contrôles pour réduire le risque à un niveau acceptable

- **Eviter les Risques.**

Eviter le risque en éliminant la cause de risque et / ou la conséquence (par exemple, renoncer à certaines fonctions du programme ou fermer lorsque les risques sont identifiés).

- **Limiter les Risques.**

Limiter le risque par la mise en œuvre des systèmes de contrôles qui minimisent l'impact négatif d'une menace est d'exercer une vulnérabilité (par exemple, l'utilisation de soutien, de prévention, de contrôles de détection)

- **Planifier les Risques Planning.**

Gérer le risque en élaborant un plan privilégié de réduction des risques qui, met en œuvre et maintient des contrôles•

- **Reconnaissance et Recherche.**

Diminuer les risques privilégié en reconnaissant qu'il y a une certaine vulnérabilité et des défauts et rechercher les moyens de contrôles pour corriger les vulnérabilités.

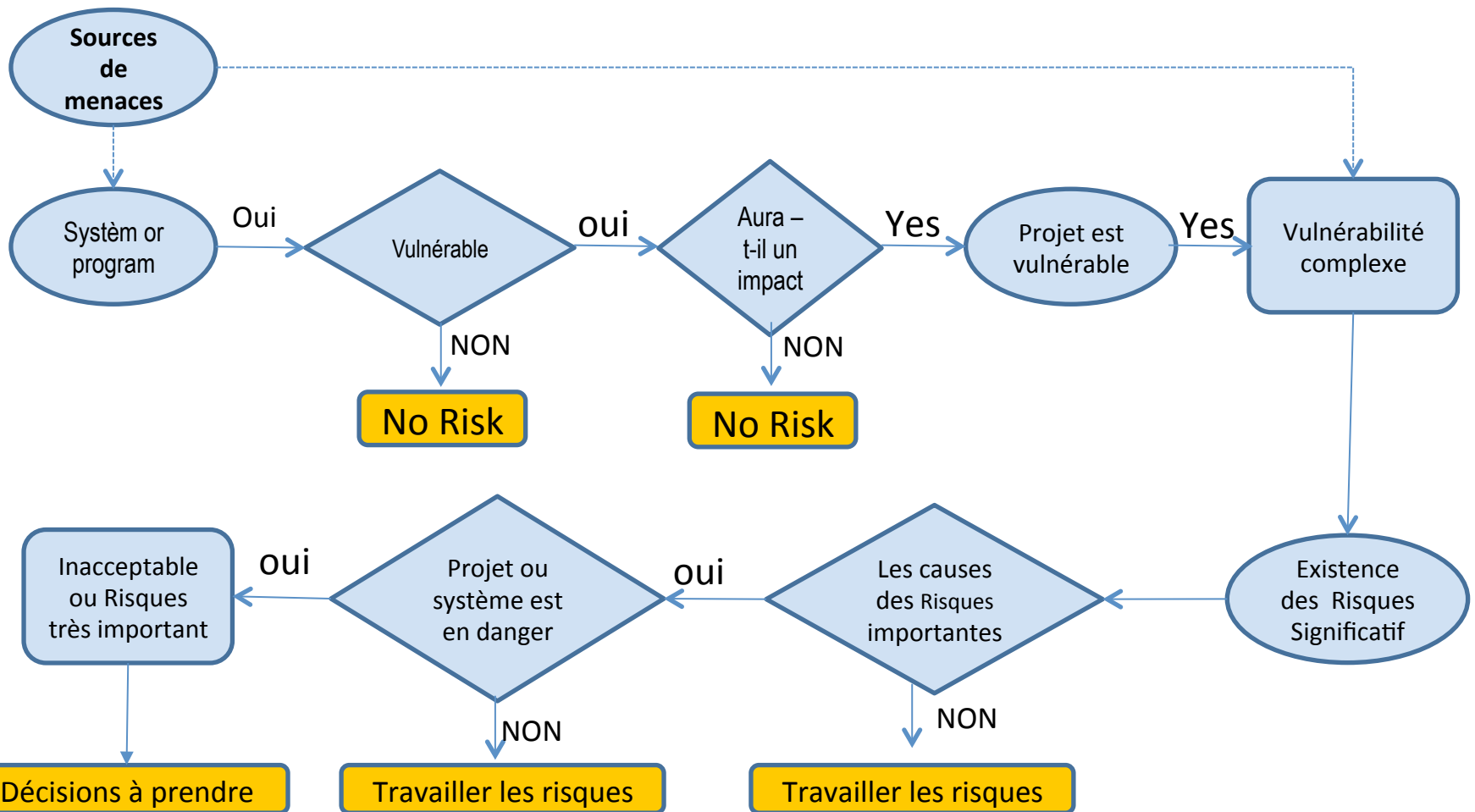
- **Transférer les Risques.**

Transférer les risques en ayant recours à d'autres options pour compenser la perte, telle que les assurances, etc..

Les objectifs et la mission d'une organisation doivent être considérés dans le choix de ces options de réduction des risques. Il peut ne pas être pratique pour traiter tous les risques identifiés, donc la priorité devrait être donnée à la menace et de la

vulnérabilité qui ont le potentiel d'avoir un impact significatif

# Gestion et réduction des risques



# 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 program, the complexities related to the program and documents related previous audit report, risk assessment report, financial results, narrative reports *can 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.