



Mesurer les risques DataDrill EXPRESS

Bonnes Pratiques

Olivier Pinette – Patrick Hamon – Peter Baxter

STATUT : V1.4 – OCTOBRE 2010/10/21 - VALIDE



Avant-Propos

Ce document fait partie d'un ensemble de documents sur les « Bonnes pratiques » de développement de logiciels et systèmes aidées par les indicateurs.

1 Introduction

La compression budgétaire, la non maîtrise des technologies, la volatilité des exigences, le turnover du personnel, etc... sont autant de dangers qui guettent le projet et peuvent provoquer son échec.

Les risques sont donc inhérents à la vie des projets de développement logiciels et systèmes où ils sont incontournables. Nous avons choisi de les étudier ici et de mettre en exergue les bonnes pratiques associées à leurs mesures.

2 Définition

Un risque est une exposition à un danger, un préjudice ou tout autre événement dommageable. Les projets qui ne gèrent pas les risques ou ne les gèrent pas suffisamment bien, découvriront les problèmes au dernier moment, lorsqu'ils surviennent, ce qui est parfois trop tard et dans certains cas mortel pour le projet.

Les risques sont par définition incertains, ce qui rend leur gestion délicate. Certains projets ne retiendront que la probabilité qu'ils ne surviennent pas ou trouveront une quantité de mauvaises excuses pour ne pas gérer les risques, alors que d'autres retiendront que les risques existent et peuvent survenir. De quel côté vous placez vous ? Si il y a un danger, ne souhaiteriez vous pas le savoir le plus tôt possible, pour pouvoir prendre les bonnes décisions ? La gestion des risques consiste précisément en l'évaluation et l'anticipation des risques, ainsi qu'à la mise en place d'un système de surveillance et de collecte systématique des données pour déclencher les alertes.

Un risque est défini par la probabilité d'apparition de cet événement et par l'ampleur de ses conséquences (probabilité et impact). Un plan d'atténuation des risques s'attachera donc à maîtriser leur probabilité de survenance mais aussi à réduire leur impact si les risques s'avèrent.

3 Processus de gestion des risques

3.1 Gérer les risques

Une gestion des risques formelle implique la mise en place d'un processus logique pour le traitement des risques tout au long du cycle de vie du projet/produit.

Tout commence par une phase de lancement où il convient de se préparer à la gestion des risques. Il faut obtenir les bons sponsors, les ressources, mettre en place le processus et les outils, puis communiquer et former les parties prenantes.

Puis ensuite :

- Recenser, identifier et documenter les risques en particulier les symptômes/indices permettant de penser que le risque est avéré ou au contraire évité.

- Evaluer la probabilité et l'impact de chaque risque
- Gérer les risques
 - Développer et acter un plan d'atténuation des risques.
 - Surveiller l'apparition des symptômes et réévaluer constamment les risques
 - Gérer la transition risque -> problème

3.2 La gestion des risques suivant l'ISO

Voici le processus de gestion des risques selon les normes en vigueur.

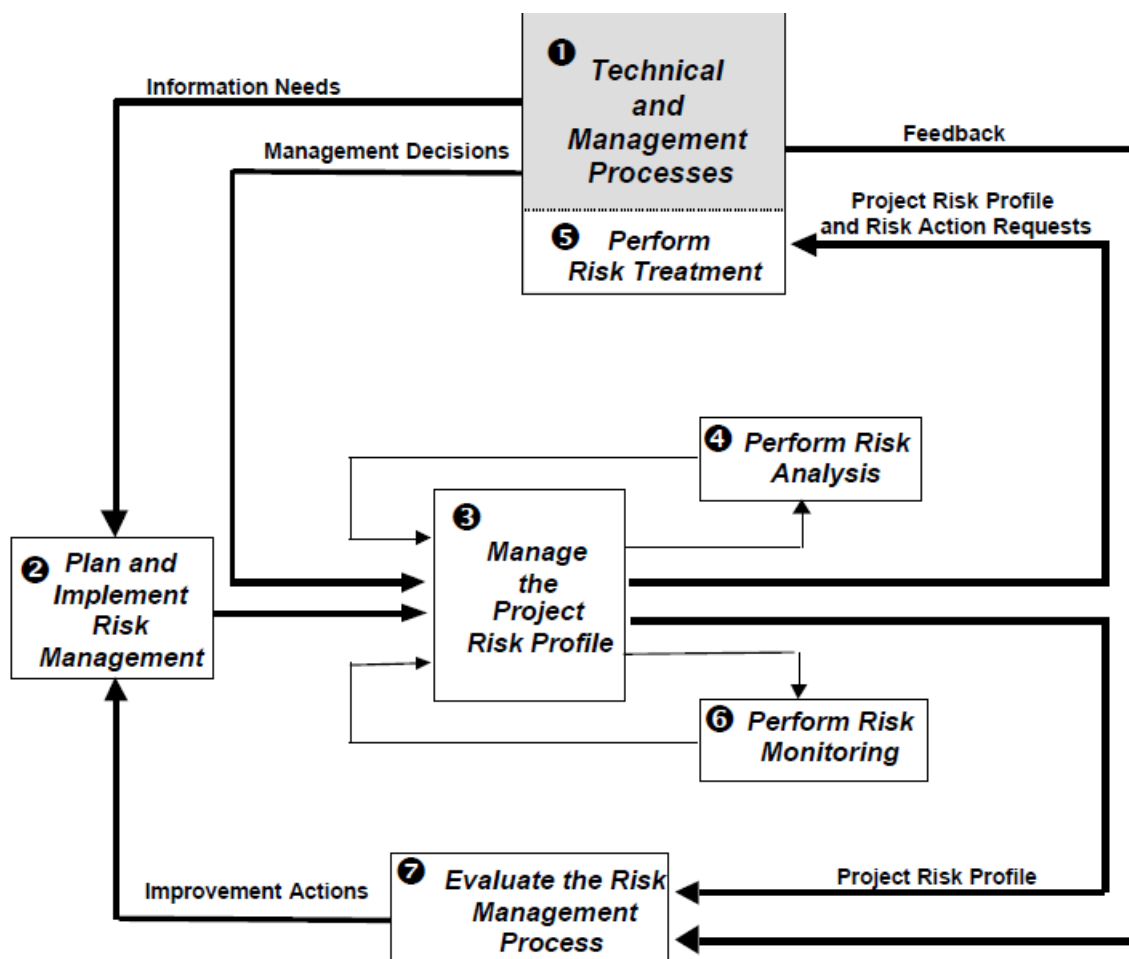


Figure 1 : IEEE - Software Risk Management Process Model (std 1540-2001)

Ce standard est aligné sur ISO/IEC "Software Engineering: System and Software engineering - Life Cycle Processes, Risk Management" (Std 16085:2006). En voici quelques détails:

1. « Technical and Management Processes », qui est l'influence et les liens des autres processus sur la gestion des risques. Ils définissent les exigences de la gestion des risques (besoins d'information, types de risques à considérer, politique de gestion des risques, seuils d'acceptabilité). En outre, ils dictent les décisions face aux risques, et induisent les recommandations d'amélioration du processus.

2. « Plan and Implement Risk Management », met en place la politique et le processus de gestion des risques (inclus les activités, les parties prenantes, les responsabilités, les outils).
3. « Manage the Project Risk Profile » crée le référentiel (vue historisée) des risques projet et de leurs traitements. Cela inclus également la définition type des risques à traiter, des objectifs, des parties prenantes, des seuils d'acceptabilité du projet, et la communication des informations aux parties prenantes.
4. « Perform Risk Analysis » liste les risques projet, estime leurs probabilités et impacts, les ordonne en terme de priorité, propose les traitements applicables. Il inclut aussi la mise en place des indicateurs de suivi de l'efficacité des actions de traitement des risques.
5. « Perform Risk Traitment » Pour chaque risque sélectionné, le traitement du risque en fonction de ce qui à été défini en 4.
6. « Perform Risk Monitoring » permet la revue et mise à jour individuelle de chaque risque, de son état, de l'efficacité des actions associées. Identifie également les éventuels nouveaux risques.
7. « Evaluate the Risk Management Process » assure la capitalisation de l'information. Identifie les améliorations potentielles du processus, les propose au management, les met en place.

Nous pouvons ajouter que cette norme est dans la droite ligne de l'ISO/IEC 15939 :2007 « Systems and software engineering -- Measurement process ».

3.3 La gestion des risques suivant le CMMI

Voici maintenant ce que nous dit le CMMI sur la gestion des risques.

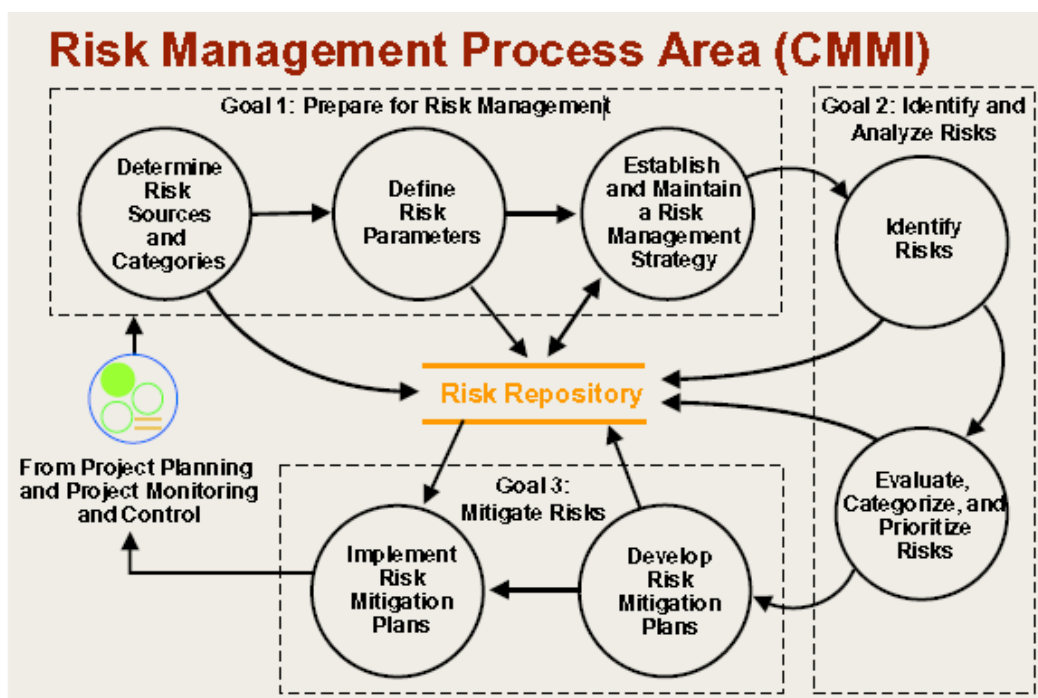


Figure 2 : CMMI – Risk Management Process Area (RSKM)



CMMI sépare la gestion des risques en 3 parties, correspondant aux 3 objectifs du domaine de processus RSKM:

1. La définition de la stratégie de gestion des risques.
2. L'identification et l'analyse des risques.
3. La gestion des risques identifiés.

SG1 – Se préparer pour la gestion des risques

- Déterminer les sources et les catégories de risques
- Définir les paramètres utilisés pour analyser et catégoriser les risques, ainsi que les paramètres pour contrôler la charge de gestion des risques
- Etablir et maintenir la stratégie qui sera utilisée pour la gestion des risques

SG2 – Les risques sont identifiés et analysés pour déterminer leur importance relative

- Identifier et documenter les risques
- Evaluer et catégoriser chaque risque identifié en utilisant les catégories et les paramètres des risques établis et déterminer leur priorité relative

SG3 – Les risques sont gérés et atténués, lorsque nécessaires, afin de diminuer les impacts qui peuvent nuire à l'atteinte des objectifs

- Développer un plan d'atténuation du risque pour les risques les plus importants du projet tel que défini dans la stratégie de gestion des risques.
- Surveiller périodiquement le statut de chaque risque et mettre en œuvre, selon les besoins, le plan d'atténuation du risque.

Au centre, nous trouvons le référentiel des risques incluant :

Une partie documentaire :

- La liste des sources possibles de risque
- Les catégories de risque
- Les critères d'évaluation, de catégorisation et de priorisation des risques
- La stratégie de gestion des risques du projet

La liste des risques proprement dite avec :

- Le contexte, les conditions et conséquences de chaque risque
- Une priorité attribuée à chaque risque
- Les différentes options de traitement et d'atténuation de chaque risque
- Les actions en cas de survenance du risque
- Les responsabilités



4 Evaluation des risques

4.1 Evaluation de la probabilité et de l'impact des risques

Après avoir répertorié les risques, il convient de les évaluer et de les prioriser. Pour cela, nous utilisons généralement les 2 critères suivants :

- Probabilité d'apparition
- Impact du risque, c'est-à-dire l'importance des conséquences sur le projet/produit (en terme de coûts, délais et éventuellement qualité).

Remarque : La garantie de l'efficacité de l'évaluation des risques passe par son indépendance de toute pression politique.

Les risques majeurs (et donc inacceptables), sont alors identifiables comme étant ceux qui cumulent à la fois un fort taux de probabilité de survenance et un impact élevé.

Les risques peu critiques (et donc acceptables), sont a contrario les risques à faible impact et/ou à faible probabilité.

Entre les deux, il y a les risques que nous appellerons critiques

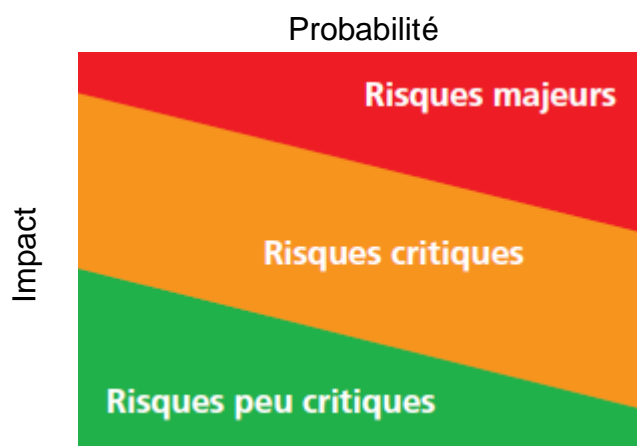


Figure 3 : matrice des risques

Exemple :

ITEM	R25
Facteur de risque	Il peut s'avérer nécessaire d'écrire un pilote d'imprimante spécifique.
Etendu	500 Points de fonctions
Probabilité	20 %
Impact coût	150 000 €
Impact délai	+ 5 mois
Symptômes	Echec des tests d'impression utilisant le driver standard.

L'impact pondéré (Impact * probabilité) est alors : 30 K€ et 1 mois



4.2 Relation entre les risques

Les risques sont liés entre eux. Un ensemble de risques liés peut avoir un impact d'autant plus important sur une mission donnée. Nous entendons par mission la finalité d'une activité ou d'un processus. La non exécution de certaines missions peut avoir des conséquences fortes sur le projet et l'organisation.

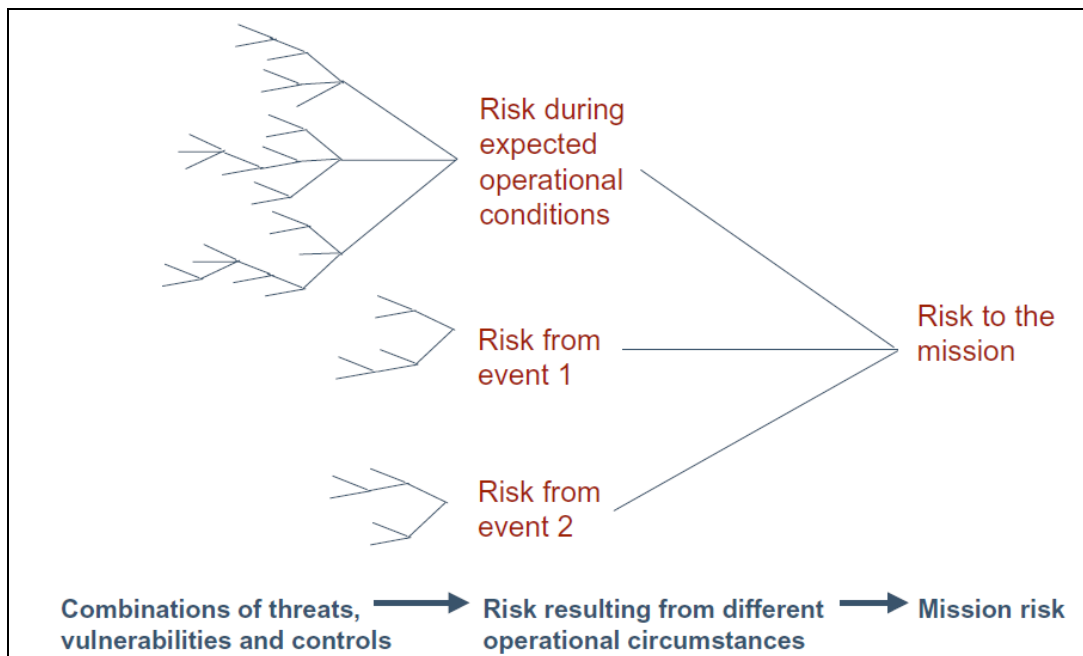


Figure 4 : D'après SEI-“Advanced Risk Analysis for High-Performing Organizations” par Christopher Alberts et Audrey Dorofee - 2006

(<http://www.sei.cmu.edu/library/assets/advancedrisk.pdf>)

Ainsi, nous ne pouvons que recommander d'avoir une vue globale de l'impact des risques, ce qui permet :

- De mieux évaluer l'impact et/ou la probabilité des risques
- De mieux calculer l'exposition réelle aux risques
- De mieux anticiper les événements imprévus
- De mettre en évidence les possibilités d'atténuation des risques par modification des processus

4.3 L'impact des risques

Nous pouvons également montrer que l'impact d'un risque sera aussi dépendant de la façon dont l'organisation s'est préparée à le recevoir.

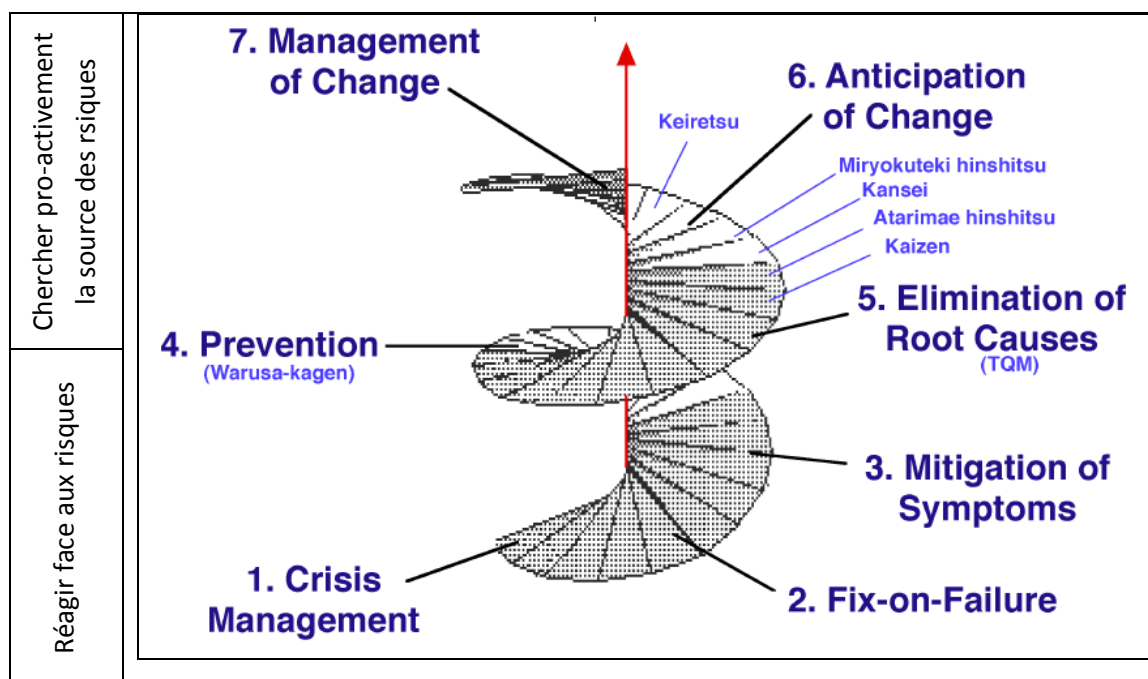


Figure 5 : D'après "Going Up the Down Escalator" par Robert Charette, ITABHI Corporation 1993

<http://www.itmpi.org/assets/base/images/itmpi/privaterooms/robertcharette/UpTheDownEscalator.pdf>

La meilleure lecture de cette figure/escalier consiste à commencer par son centre, la marche 4. C'est une marche de transition entre **réagir** face aux risques lorsqu'ils arrivent et **pro-agir** sur la source des risques pour éviter qu'ils n'arrivent. A ce niveau, nous nous efforçons de prévenir les risques et traduisons cela principalement en termes d'ordonnancement d'actions à mener. Mais face aux impondérables, quoi faire ?

Réagir – la partie basse de l'escalier

Par définition les risques ne sont pas connus avec certitude et peuvent donc tout à fait ne pas survenir. Parfois il est décidé de n'agir que sur les conséquences, voir de ne pas agir du tout, tant qu'ils ne sont pas avérés.... Nous sommes là dans la partie basse de l'escalier dédié à la « réaction » qui consiste en 3 stratégies : Réduire le risque à l'apparition des symptômes, traiter le problème lorsqu'il survient, gérer la crise.

Réduire le risque aux symptômes (3) consiste généralement, dès l'apparition des premiers symptômes, à augmenter une ressource ou le temps passé pour couvrir la conséquence du risque. Cette stratégie n'est efficace que si le planning et/ou le budget du projet ont de la marge. Traiter le problème lorsqu'il survient (2) impose que les problèmes n'arrivent que lorsque nous avons prévu qu'ils arrivent. Par exemple, la détection des défauts peut être prévue pour arriver à la fin des tests unitaires, puis des tests d'intégration. Mais que ce passe-t-il si les défauts apparaissent très tard, voir chez le client ? Nous nous retrouvons alors sur la dernière marche à devoir gérer la crise (1).



Pro-agir – la partie haute de l’escalier :

A l’opposé de la partie basse de l’escalier où nous nous attachions à réagir aux risques survenus sur les produits et services livrés, nous nous attachons ici à éliminer les causes racines des risques (5) en examinant et améliorant les processus. Cela implique obligatoirement que les processus soient définis, répétables et mesurables. C’est de cette manière que les processus deviendront stables et prédictibles. Cela implique donc de placer davantage de ressources pour gérer les risques là où les processus ne sont pas encore matures. La progression normale est alors de faire cela à chaque fois qu’un processus est créé ou révisé, où l’on anticipe les changements provoqués et les risques potentiels (6). La marche ultime étant de rentrer dans cette logique naturellement, celle où la gestion du changement est toujours considérée (7). C’est une sorte d’asymptote enviable, mais aussi dangereuse, car difficile à gérer et pouvant produire des réactions contre-productives.

Il a été pendant longtemps considéré que la meilleure solution/compromis (effort/efficacité) pour la gestion des risques était la marche 3. Mais c’était oublier que nous ne pouvons pas prédire le futur. Alors la dimension prévention (4) est apparue comme plus avantageuse. De plus, la prévention est une approche généralement réduite dans le temps, et très dépendante de la période où elle est menée. D’où l’idée que corriger le problème avant qu’il n’arrive pourrait être bénéfique. Cela permettait aussi de transformer les risques en avantage. Nous avons alors franchi le niveau 4 pour atteindre le 5, puis le 6 où le traitement du risque commence à devenir naturel et mature.

4.4 Positiver la notion de risque

Par nature, la notion de risque a généralement une consonance négative, car met en exergue les possibilités d’échec du projet. Dit comme cela, nous ne voyons que la partie « négative » du risque. Mais ce n’est jamais très facile et très motivant de gérer des actions permettant de « potentiellement » ne pas perdre d’argent. Alors que diriez-vous d’étendre et de transformer cette notion négative du risque, pour la rendre plus attractive, lui donner un aspect positif. Plutôt que de risques, si nous parlions d’opportunités. Nous pourrions alors considérer les opportunités comme un moyen de gagner plus d’argent... c’est tout de même plus motivant que ne pas perdre d’argent. Ainsi certaines organisations préfèrent parler de gestion des risques et opportunités

5 Evaluer la gestion du risque

5.1 Difficultés d’évaluer le processus de gestion des risques

Nous venons d’expliquer, pourquoi suivre le nombre de risques ne pouvait pas être suffisant pour déterminer l’efficacité des activités de gestion des risques. De plus nous sommes (tous) généralement optimistes et avons tendance à sous-estimer les risques. Par exemple, il n’est pas rare qu’un projet démarre avec une liste de 100 risques identifiés, après 6 mois 20 restent à traiter, mais parmi ces 20, seulement 10 étaient dans la liste initiale.



La solution consiste donc à donner une bonne visibilité du processus de gestion des risques et à identifier le vrai besoin d'information associé. C'est-à-dire à définir ce que nous avons besoin (dans notre contexte) de savoir ou d'apprendre pour contrôler la gestion des risques, leurs traitements et leurs prévisions.

Pour cela, le matériel fourni par la norme ISO 15939 (ISO/IEC 15939 :2007 Systems and software engineering -- Measurement process), mais aussi PSM (Practical Software as System Measurement - <http://www.psmc.com/>) peut être utilisé pour définir formellement ce besoin d'information.

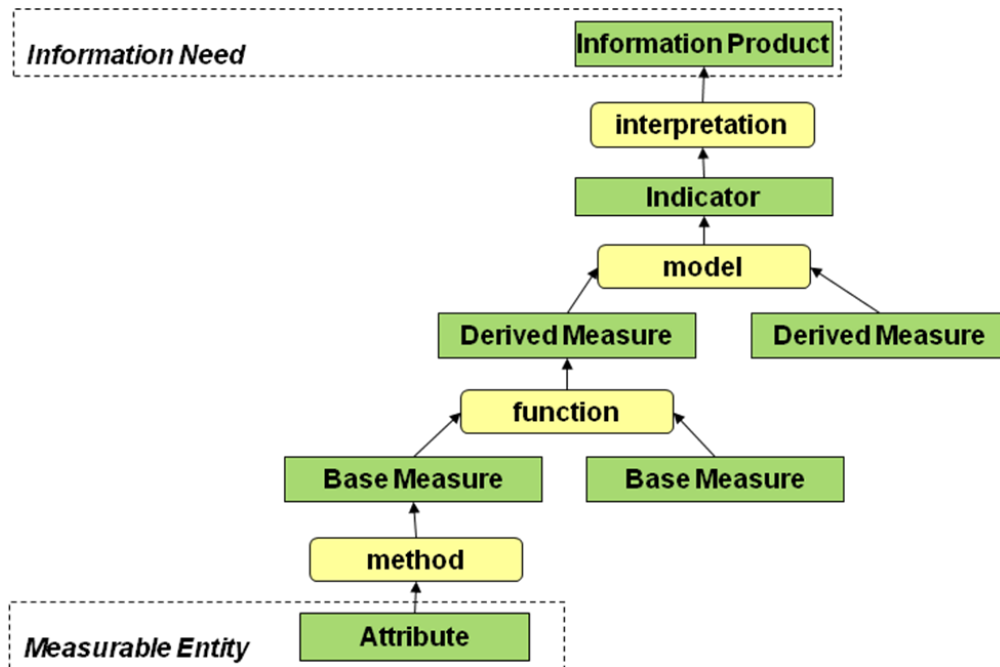


Figure 6 : Modèle d'information de ISO 15939

Utilisons ce formalisme pour définir les 4 besoins d'information suivant :

- Quelle est l'efficacité du processus de gestion des risques ?
- Quels est la tendance et le coût actuels des risques ?
- Quel est le coût prévu des actions d'atténuation des risques?
- Quelle est l'économie réalisée grâce à la gestion des risques ?



Quelle est l'efficacité du processus de gestion des risques ?

Puis-je avoir confiance dans mon processus de gestion des risques ? L'approche est assez semblable à celle utilisée pour les défauts :

Produit d'information	Précision de la planification de la gestion des risques
Interprétation	< 20% -> ok Entre 20 et 50% -> surveiller et analyser les risques > 50 % -> replanifier/ rebudgéter les risques
Indicateur	% risques non planifiés (%Rnp)
Modèle	%Rnp = 100 * Rnp/Rt
Mesure dérivé	Risques non planifiés (Rnp)
Fonction	Rnp = Rt – Rp
Mesure de base	Rt = Total Risques : nb actuel de risques identifiés sur le projet Rp = Risques initiaux : nb risques identifiés/prévus au démarrage

Quels est la tendance et le coût actuels des risques ?

Produit d'information	Etat courant de l'atténuation des risques
Interprétation	Pc entre 0.9 et 1.05 -> OK Pc entre 0.75 et 0.9 ou entre 1.05 et 1.15 -> à surveiller Pc < 0.75 ou > 1.15 -> replanifier/ rebudgéter les risques
Indicateur	Ta =Tendance d'accroissement des risques Pc= Indice de performance des coûts des risques
Modèle	Ta = Ro / Rf Pc = Cr / Ce
Mesure dérivé	Ro = Cumul des risques ouverts Rf = Cumul des risques fermés Ce = Cumul des coûts estimés Cf = Cumul des coûts réels
Fonction	Ro = nb risques ouverts Rf = nb risques fermés Ce = Somme des coûts prévus Cr = Somme des coûts réels engagés
Mesure de base	Chaque risques avec : <ul style="list-style-type: none"> - état (ouvert=non traité ou en atténuation, fermé=maitrisé) - coût estimé/prévu de l'atténuation - coût réel de l'atténuation

Quel est le coût prévu des actions d'atténuation des risques?

Produit d'information	Prévision du coût d'atténuation des risques
Interprétation	Autour de 10% du budget -> ok Entre 10 et 30% du budget -> à surveiller Supérieure à 30% du budget -> à rebudgéter
Indicateur	Estimation du coût d'atténuation des risques en % / budget
Modèle	$100 * Br / [E + E * \%Rnp]$
Mesure dérivé	Br = Budget Restant= Restant du budget d'atténuation des risques E = Estimation Coût restant = estimation du coût pondéré d'atténuation des risques non maîtrisés actuellement. %Rnp = % risques non planifiés comme calculé dans le premier indicateur
Fonction	Br = Budget Restant = Budget – cout réel E = Estimation Coût restant = Somme (Proba * Impact) pour chaque risque restant
Mesure de base	Budget total : Budget total de l'atténuation des risques Coût réel = coût de l'atténuation jusqu'à aujourd'hui Probabilité et impact (coût) de chaque risque restant (non maîtrisé)

Quelle est l'économie réalisée grâce à la gestion des risques ?

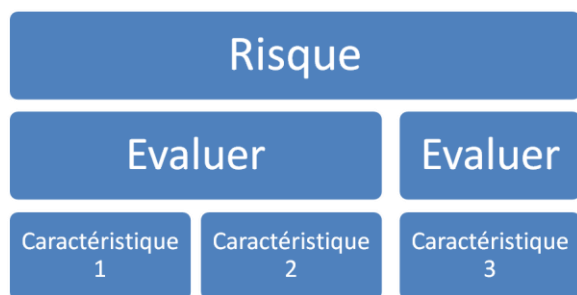
Produit d'information	Retour sur investissent
Interprétation	Acceptable si ≥ 0.90 Inacceptable si < 0.90
Indicateur	Retour sur investissent
Modèle	ROI= Gain/Dépense
Mesure dérivé	-
Fonction	-
Mesure de base	Dépense = Somme des ressources utilisées à la gestion des risques Gain = Somme des coûts évités par l'atténuation des risques



5.2 Difficulté d'identifier les indicateurs

Le programme de gestion des risques n'est pas toujours intégré et/ou pris en compte par le processus de mesure et analyse. Il est nécessaire d'examiner et d'évaluer chaque risque individuellement et manuellement, cela peut être long et coûteux

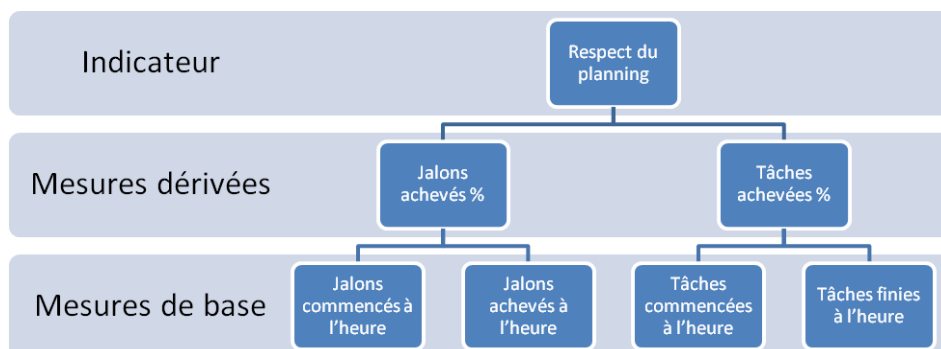
Il est généralement facile d'utiliser le système de mesure de l'organisation pour gérer les risques. Souvent les caractéristiques nécessaires à l'évaluation des risques sont déjà plus ou moins prises en compte.



- **Evaluer** un risque (pour l'atténuer) consiste à analyser l'état courant du projet son apparition.
- Analyser implique de déterminer dans quelle mesure les conditions indiquant le risque, qu'on appelle **caractéristiques**, se sont manifestées
- Un risque peut avoir un **ensemble de caractéristiques**.

Les mesures (mesures de base, mesures dérivées et indicateurs) déjà gérées par le processus de Mesure se chevauchent avec les caractéristiques des risques.

Ainsi le processus de mesure ne donne pas directement l'évaluation ni le statut global du risque, mais fournit les données/caractéristiques permettant de l'établir.

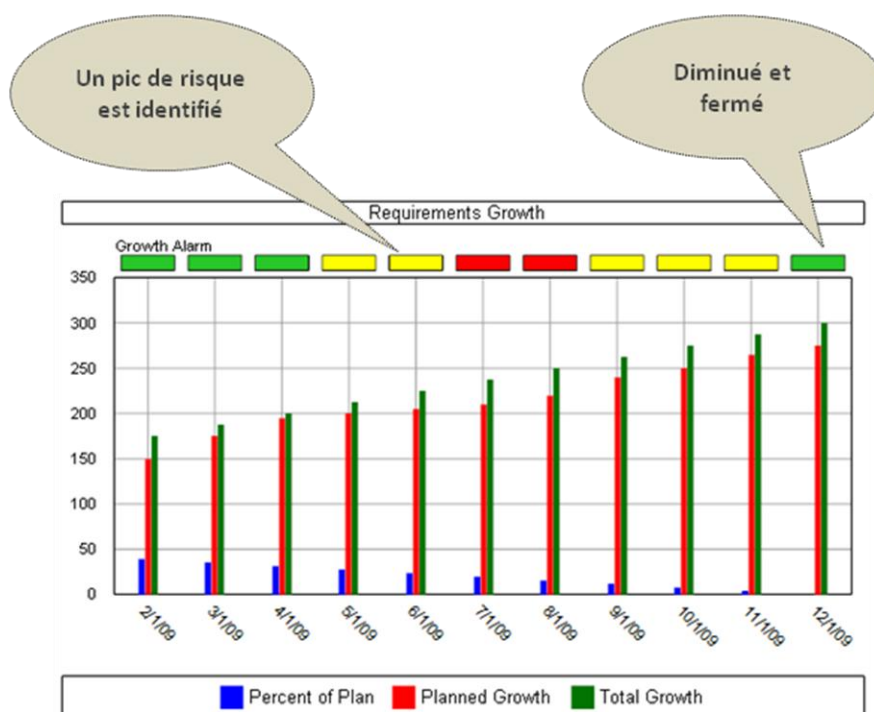




5.3 Difficulté de quantifier l'atténuation

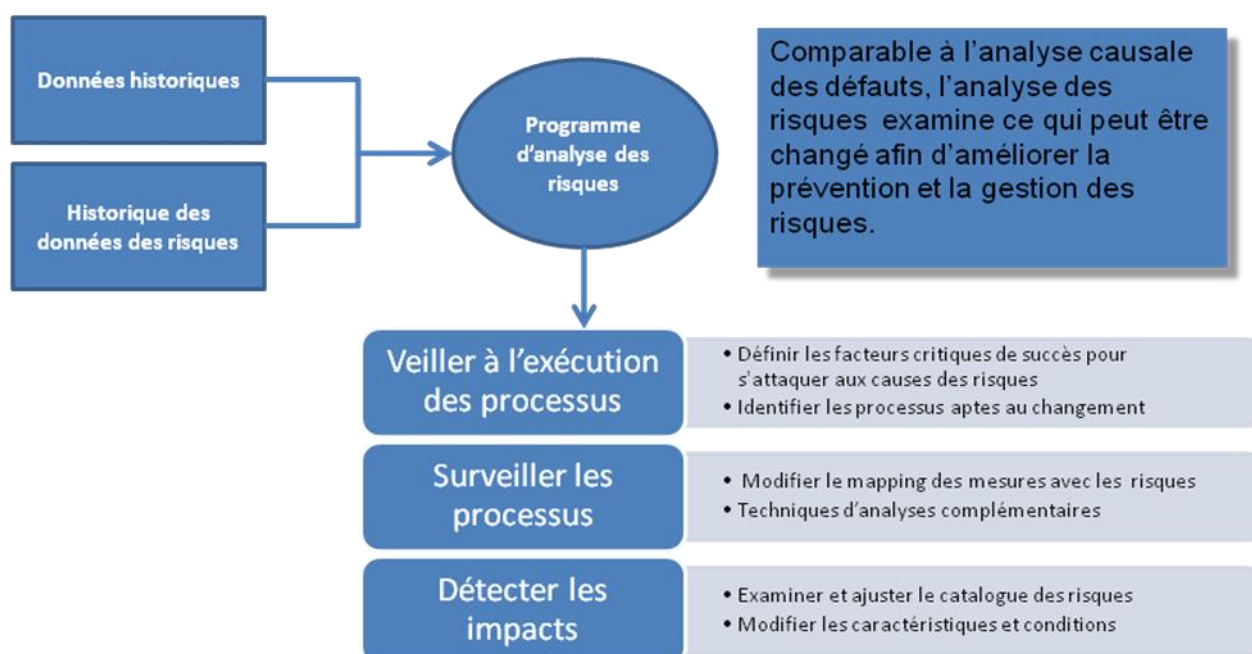
Quand un risque est avéré (c'est-à-dire lorsqu'il est devenu un problème), des actions pour l'atténuer sont mises en place afin de contrôler et/ou limiter son impact. Si les actions d'atténuation entreprises ne sont pas suivies quantitativement, les managers n'ont aucun moyen de suivre l'évolution du risque et ainsi évaluer l'efficacité des décisions d'atténuation. Sans mesure quantitative il est impossible de déterminer si l'atténuation a effectivement contenu ou limité l'impact du problème ou si elle a permis d'identifier une bonne pratique d'atténuation qu'il sera intéressant d'incorporer aux prochains plans de gestion des risques.

Exemple:



5.4 Difficulté à capitaliser sur les problèmes des projets

Lorsqu'un risque s'avère, il devient un problème pour le projet, qui doit le prendre en compte jusqu'à fermeture. Durant la vie du projet, les managers gèrent les risques et les problèmes à l'intérieur de leur sphère de responsabilité et de leur budget. A la fin de chaque projet, l'organisation a donc une liste de risques, de problèmes et d'actions sur lesquels elle peut capitaliser. Mais beaucoup d'organisations n'utilisent pas ces données en les réinjectant dans le processus de gestion des risques. Parfois parce que le processus ne le prévoit pas, mais aussi souvent parce que les données ne sont pas accessibles.



6 Conclusions

L'objectif de la gestion des risques n'est pas d'éliminer les risques, mais bien de maximiser les opportunités et minimiser les mauvais effets des risques avérés. Nous avons montré que cette gestion repose en grande partie sur les capacités du processus de mesure et analyse de l'organisation.

L'intégration des pratiques de gestion des risques dans le processus de développement est indispensable pour obtenir une bonne efficacité de la gestion des risques.

7 Spirula en bref

Depuis près de 10 ans, Spirula propose des solutions pour mieux estimer et piloter les projets de développement de logiciels et systèmes.

Leader sur son marché, l'offre Spirula – expertise, outils, formation – permet de mieux Comprendre le passé, Piloter le présent et Prévoir l'avenir des projets d'ingénierie logicielle et systèmes.

Nous aidons nos clients à définir les processus de développement les plus efficaces, implémenter des tableaux de bords pour le suivi des projets et augmenter la fiabilité des estimations des coûts, effort et délais des projets.

Nos consultants sont experts dans le pilotage de projet et les estimations et conduisent l'implémentation des bonnes pratiques, comme le CMMI, dont Spirula est un des co-auteurs.

Parmi nos clients, nous comptons des PME/PMI ayant une forte activité de développement de logiciels et de systèmes ainsi que des grands comptes internationaux tel qu'Alstom, BAe, Continental, Philips, Renault, Thales, ...