



**HAL**  
open science

## Modéliser les vulnérabilités

Thierry Bontems, Sabine Goulin

► **To cite this version:**

Thierry Bontems, Sabine Goulin. Modéliser les vulnérabilités. Qualita2017: 12ème Congrès International Pluridisciplinaire en Qualité, Sécurité de fonctionnement et Développement durable, INSA Bourges, Aug 2017, Bourges, France. halshs-01590749

**HAL Id: halshs-01590749**

**<https://shs.hal.science/halshs-01590749v1>**

Submitted on 20 Sep 2017

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# MODELISER LES VULNERABILITES

AVoID : Une approche hyper cubique de la vulnérabilité au profit de la prise de décision

Thierry BONTEMS

UMR PACTE

Centre National de la Recherche Scientifique - CNRS

Grenoble, France

thierry.bontems@umrpacte.fr

Sabine GOULIN

DAPEQ

Université de Lorraine

Nancy, France

sabine.goulin@univ-lorraine.fr

**Abstract—** Le management est l'art de prendre des décisions à partir d'informations insuffisantes. » Rowan Roy.

**Dans un processus d'aide à la décision, l'analyse de risque est une étape indispensable. Les méthodes d'analyses de risques sont nombreuses, mais souvent chronophage et complexe. AVoID (Analyse des Vulnérabilités pOur décIDER) propose aux décideurs une méthode simple et rapide non pas pour analyser les risques mais pour cartographier les vulnérabilités d'une décision, d'un processus, d'un écosystème à comprendre. AVoID intègre une analyse des moyens de maîtrise afin de mesurer les risques à échéances et permettre les prises de décisions.**

*Quand on lui réclamait des solutions parfaites, qui écarteraient tous les risques : « C'est l'expérience qui dégage les lois, répondait-il, la connaissance des lois ne précède jamais l'expérience. »*

*Vol de nuit<sup>1</sup>, Saint Exupéry*

## TABLE DES MATIERES

I. INTRODUCTION	1
II. UN SOCLE NORMATIF ISO	2
III. UNE APPROCHE MULTICRITÈRE, HYPER CUBIQUE	2
IV. IDENTIFICATION DES RISQUES	2
V. EVALUATION DE L'IMPACT ET DE LA PROBABILITÉ DES RISQUES BRUTS	3
VI. IDENTIFIER ET ÉVALUER LES MOYENS DE MAÎTRISES EXISTANTS	4
VII. DU RISQUE À LA VULNÉRABILITÉ	5
VIII. LISTER LES MOYENS DE MAÎTRISE À TRANSFÉRER OU À INVENTER	5
IX. ANALYSE DE LA VULNÉRABILITÉ À ÉCHÉANCES	6
X. LES LEVIERS D'INTERACTIONS	6
XI. UN OUTIL DE CARTOGRAPHIE DES RISQUES ET DES VULNÉRABILITÉS	7
XII. AU-DELÀ DE LA MÉTHODE ET DE L'OUTIL	7

## I. INTRODUCTION

Parce qu'ils sont élaborés par et pour les grandes entreprises, les outils qui pourraient soutenir l'entrepreneur [ndlr : manager] dans son processus de décision lui reste encore difficilement accessible.

À en croire certains observateurs, nous vivons désormais dans une civilisation du risque (Lagadec, 1981), dans une société du risque (Beck, 2001). Même si l'on ne partage pas pleinement cette approche du XXIème siècle, force est néanmoins d'admettre que le risque est aujourd'hui un sujet majeur du débat public, une préoccupation constante des populations, des pouvoirs publics (World Health Organization, 2002) mais également des entrepreneurs (Brockhaus, 1980).

Cette réflexion peut aussi bien s'appliquer au processus de décision de tous les managers à qui la loi impose d'intégrer ces contraintes dans leurs systèmes de management. La norme ISO 31000 le souligne d'ailleurs fort explicitement : « toutes les prises de décisions au sein de l'organisme, quelles que soient leur importance et leur portée impliquent la prise en compte explicite des risques et l'application du management des risques dans une mesure appropriée »

La méthode AVoID développée par Thierry BONTEMS (CNRS Grenoble) et Sabine GOULIN (Université de Lorraine) est issue d'une analyse des besoins du terrain pour répondre au « comment ? » réaliser une analyse de risques et de vulnérabilité. Elle s'appuie sur le processus d'analyse proposé par la norme ISO 31000.

Les objectifs de la méthode AVoID sont multiples. Le premier est de proposer aux décideurs (on entendra par décideur, toute personne physique ou morale habilitée par ses fonctions ou sa position à décider, à orienter ou bien à faire prévaloir une décision) une méthode rapide, fiable pour lister, visualiser, hiérarchiser et analyser les vulnérabilités d'un système. Le second objectif est d'avoir une vision qui ne se focalise pas sur le risque mais qui s'intéresse avant tout à la vulnérabilité, c'est-à-dire plus au moyen de maîtriser le risque qu'au constat du

<sup>1</sup> éd. Gallimard (ISBN 2-07-036004-0), p. 105 -

risque en lui-même. Enfin le troisième objectif de la méthode est d'utiliser un certain nombre de leviers pour observer les systèmes sous d'autres angles de vue afin de prioriser, hiérarchiser et décider des actions à mener pour minimiser la prise de risque et réduire les vulnérabilités d'un système.

## II. UN SOCLE NORMATIF ISO

La méthode AVoID s'appuie sur la norme ISO 31000v2009 - management des risques, cette norme décrit le processus de management par les risques. (Figure 1 : Processus de management du risque - Iso 31000).

La méthodologie itérative proposée par les normes qualités permet de rentrer dans la démarche par n'importe quel endroit et notamment par la phase d'identification des risques. Nous verrons ultérieurement en quoi il est intéressant de ne pas entrer par l'établissement du contexte et pourquoi nous préconisons une approche accès sur l'identification des risques et des moyens de maîtrise associés

Le questionnaire lié à l'identification des risques, des moyens de maîtrise et de leur efficacité sera également construit sur ce même processus itératif

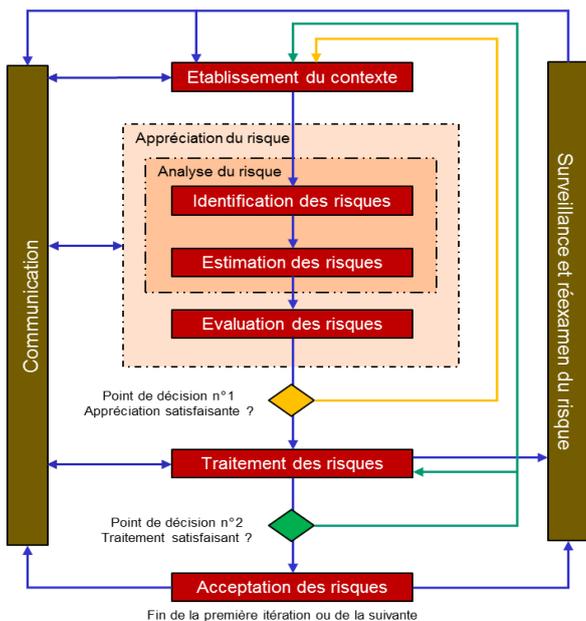


Figure 1 : Processus de management du risque - Iso 31000

## III. UNE APPROCHE MULTICRITERE, HYPER CUBIQUE

Le concept de la méthode AVoID est de travailler avant tout à partir de la notion de vulnérabilité. L'établissement du niveau de vulnérabilité est issue d'une analyse tridimensionnelle. Dans un premier temps, le principe est d'établir une liste des risques. Cette identification que nous proposons par approche

participative (Leguenic, 2001) permet d'identifier un certain nombre de risques.

Une fois l'identification de ces risques réalisés, nous allons construire une première matrice Impact/Probabilité. Cette matrice nous permet d'établir une première carte du niveau de risques perçus. Cette première matrice est indispensable pour conduire l'analyse mais en aucun cas suffisante.

Prendre des risques n'est pas contre-indiqué, ce qui est critique c'est de ne pas maîtriser les risques que l'on prend, c'est

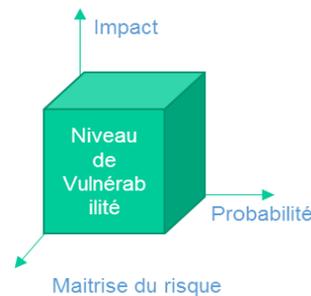


Figure 2 : Cube de vulnérabilité

pourquoi dans ce système il convient d'analyser pour les risques identifiés quel est le niveau de maîtrise que l'on a. On obtient ainsi un « cube de vulnérabilité (Figure 2 : Cube de vulnérabilité) en croisant les trois dimensions Impact / Probabilité / Maîtrise des risques.

Il y a maintenant plusieurs façons de regarder ce cube de vulnérabilités. Soit de façon neutre, « quelles sont mes vulnérabilités à l'instant t », soit de façon plus éclairée, c'est la seconde étape de la méthode, on peut ainsi, jouer sur la temporalité de mise en place des moyens de maîtrise, ou introduire d'autres critères d'observation, le coût, le délai de mise en œuvre du moyen de maîtrise, le niveau d'influence du porteur de projet, l'impact d'un acteur, etc...

L'observation de ce cube de vulnérabilité se fait maintenant au travers d'un, de deux, de n critères, qui sont autant de prismes différents pour observer nos vulnérabilités (Figure 3 : Des leviers pour analyser les risques)

L'analyse de chaque levier aura pour effet de mettre en lumière de manière différente les alternatives qui s'offrent aux décideurs.

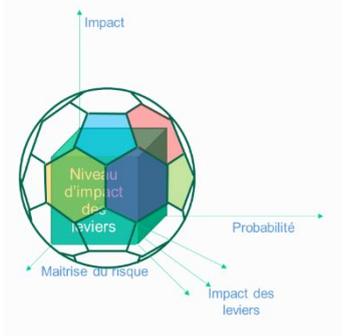


Figure 3 : Des leviers pour analyser les risques

## IV. IDENTIFICATION DES RISQUES

La première étape de la méthode AVoID consiste à identifier les risques pour lesquels nous souhaitons avoir une visibilité. L'objectif de la méthode n'est pas d'être exhaustif dans l'identification des risques mais plutôt d'identifier de manière très rapide une majorité de risques ou de dysfonctionnements perçus. C'est la composition du groupe de personnes interviewées qui augmentera la pertinence du résultat final ainsi que le coté itératif de la méthode.

## A. Composition du groupe de personnes interviewées.

A minima ce groupe peut se composer de vous-même. La méthode est ainsi faite que vous seul devant un micro système que vous maîtrisez complètement pourrez faire une analyse extrêmement rapide des vulnérabilités auxquels ce microsystème est soumis. Néanmoins, il n'est pas recommandé d'agir ainsi, la vision de l'autre permet une prise de recul qu'il n'est jamais simple de mettre en œuvre seul.

Dans l'idéal, le groupe de personnes interviewé se composera au minimum, de vous en tant que garant de la méthodologie et animateur de la démarche, d'un expert du système étudié et d'un opérateur de ce système. Plus se groupe s'étoffera, plus l'analyse sera fine et moins "l'effet risques perçus" se fera sentir.

Avant de s'intéresser à la collecte à proprement parler des risques, nous souhaitons revenir sur la définition même du risque au sens de l'ISO 31000, "le risque [est] l'effet de l'incertitude sur la réalisation d'un objectif". Cette définition peut être interprétée, ainsi nous pouvons voir le risque comme un évènement potentiel faisant passer d'un état prévu (objectif) à un état atteint (résultat), la gravité de la variation entre l'objectif et le résultat étant la conséquence du risque. Or si on se réfère à cette interprétation, et que nous définissons le dysfonctionnement comme un évènement potentiel faisant passer d'un état prévu à un état atteint alors *tous les dysfonctionnements sont des risques*. Cette prise de conscience au niveau d'une organisation simplifie grandement la tâche de l'analyse de risques, en effet, si les participants ne sont pas vraiment sensibilisés à la notion de risques, tous le sont à la notion de dysfonctionnement.

## B. La « collecte des risques bruts »

Afin de percevoir toute la richesse du groupe de travail, nous proposons pour capter les risques bruts d'un système de travailler par<sup>2</sup> entretien participatif ou par focus group et d'utiliser l'ensemble des méthodologies de recueil d'information qui paraissent adaptées à ces situations.

Nous pouvons proposer de travailler par analyse systémique, en analysant non seulement les dysfonctionnements perçus au niveau des Inputs et des Outputs mais également en réalisant une analyse organisationnelle, humaine et technologique de notre système.

L'analyse Ishikawa combinée aux 7M (Milieu, Matériel, Méthode, Matière première, Main d'œuvre, Moyens financiers et Management) offre une approche plus précise de l'analyse d'un système et permet à défaut d'être exhaustif, tout du moins

<sup>2</sup> Guide de la recherche-action, la planification et l'évaluation participative – SAS2 Dialogue, Ottawa – Mars 2013 – J. Chevalier, D. Buckles, M. Bourassa

de ne pas oublier de branche majeure dans l'énumération des risques.

Autres méthode que nous utilisons régulièrement dans nos analyses, la méthode dite « Post-it »<sup>3</sup>. Cette méthode a pour avantage d'anonymiser à la source le recueil de données et de permettre à tout individu de donner sa vision des situations.

Toutes ces méthodes sont misent en œuvre et exploitées lors d'entretiens participatifs ou de focus group.

Les résultats de ces entretiens peuvent être visualisé sous formes de cartes heuristiques (Figure 4 : Carte heuristique des



Figure 4 : Carte heuristique des risques liés à un projet

risques liés à un projet), ce format ayant pour avantage de porter un regard non seulement sur l'énumération des risques mais aussi leur classification ainsi que les liens qui existent entre les uns et les autres.

Une fois cette première étape de recueil d'information effectué, nous pouvons constituer une liste de risque brut établie, en commentant chaque risque. Cette étape de commentaire est importante lorsque l'on veut revenir sur les analyses à posteriori.

## V. EVALUATION DE L'IMPACT ET DE LA PROBABILITE DES RISQUES BRUTS

Attention, l'objectif de la méthode n'est pas d'être exhaustif dans l'identification des risques mais plutôt d'identifier de manière très rapide une majorité de risques ou de dysfonctionnements perçus.

### A. La notion d'impact

La méthode AVoID définit une échelle d'impact unique pour tout type de risque. Cette échelle a cinq niveaux

**Très significatif:** désastre susceptible de provoquer l'effondrement du système observé

**Significatif:** évènement critique supportable si géré correctement

<sup>3</sup> Pierre Mongin, Mieux s'organiser, la stratégie du Post-it et du Kanban personnel, Inter éditions, 2013

**Modéré** : l'objectif est majoritairement atteint mais dans des conditions insatisfaisante

**Mineur** : le risque avéré complique l'atteinte de l'objectif sans le dégrader

**Non significatif** : événement dont l'impact peut être absorbé par l'activité normale

Une des grandes difficultés dans les méthodes d'analyses de risques existantes (AMDEC ; MEHARE ...) est de définir en amont de tous travaux une échelle d'impact par domaine. Or l'individu sait de lui-même quand il est expert d'un domaine déterminer si un impact est significatif ou mineur. Prenons un exemple très simple : vous jouez au poker, vous avez un risque de perdre cinq mille euros. Vous savez si pour vous le risque est mineur ou significatif. Sur les systèmes que nous avons pu observer, ce même phénomène se reproduit sur le domaine d'expertise de la personne interrogée. Si lors des travaux de groupes, plusieurs personnes ont des avis divergents sur le niveau d'impact à donner à un risque identifié alors nous prenons l'impact le plus fort.

### B. La notion de probabilité

De même que pour les impacts, nous avons établi une échelle de fréquence sur cinq niveaux décrivant la probabilité d'apparition du risque évalué

**Quasiment certain** : événement attendu dans la plupart des cas (>90%)

**Probable** : événement probable dans la plupart des cas (50-90%)

**Possible** : événement devant se produire à un moment donné (30-50%)

**Peu probable** : événement risquant de se produire à un moment donné (10-30%)

**Rare** : événement risquant de se produire uniquement dans des cas exceptionnels (<10%)

Cette échelle est à moduler en fonction du contexte, mais comme pour l'impact, l'individu et le groupe ont une bonne perception de la probabilité d'un dysfonctionnement.

Cette analyse permet de fabriquer une première matrice d'analyse de risque brut perçus (Figure 5 : Matrice des risques bruts perçus) qui croise l'impact et la probabilité pour chaque risque.

Cette première matrice est à interpréter comme étant la photographie à l'instant t des risques bruts du système observé. Ces risques étant évalués en cinq niveaux correspondant à la surface, de très élevé (rouge foncé à très faible en vert foncé) voir figure 4

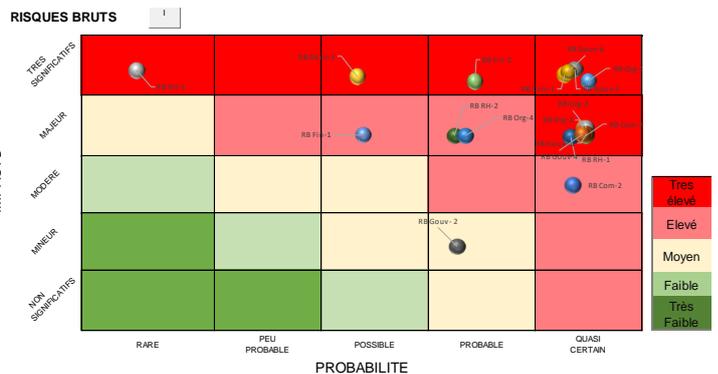


Figure 5 : Matrice des risques bruts perçus

## VI. IDENTIFIER ET EVALUER LES MOYENS DE MAITRISE EXISTANTS

Prendre des risques est une activité inhérente à chaque être humain et à chaque organisation. Toute décision est une prise de risque<sup>4</sup>. L'organisation pour faire face à cette prise de risque a probablement mis en place un certain nombre de moyen de maîtrise.

Nous arrivons à ce moment de la méthode à la nécessité d'analyser risque par risque les moyens de maîtrise en place dans l'organisation. Nous pouvons utiliser pour se faire les mêmes méthodes que vu précédemment §III.B

Plus simplement et par expérience, nous constatons à ce stade du travail, que les membres des groupes non plus de difficultés dans les prises de paroles et ainsi la conduite de l'analyse passe très souvent par une discussion collective libre et constructive si les étapes précédentes ont été menées avec les méthodes participatives.

Cette phase de recueil des moyens de maîtrise existants permet de lister l'ensemble des moyens de maîtrise présents sur le système et de fait plus qu'une simple identification, cette liste

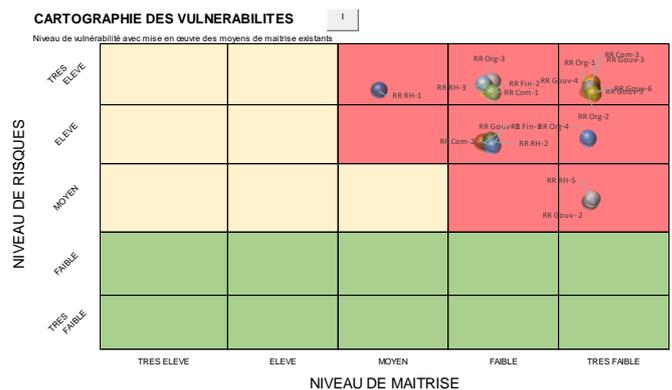


Figure 6 : Matrice (carte) de vulnérabilité

permettra par la suite de déterminer les actions à mener pour conforter ou améliorer le système actuel. Les moyens de

<sup>4</sup> Alain Fernandez [www.piloter.org](http://www.piloter.org), piloter la performance

maîtrise sont alors évalués en termes d'impact et de probabilités comme décrit au paragraphe IV. Ce recueil d'informations

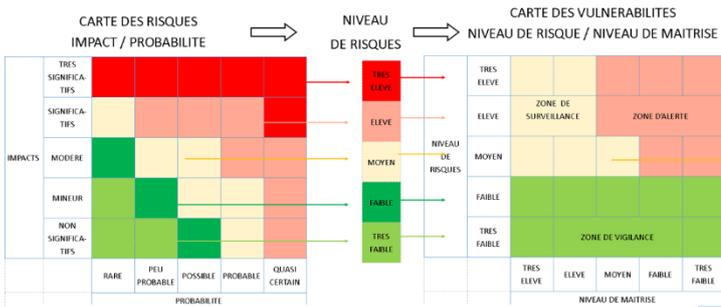


Figure 8 : du risque à la vulnérabilité

permet de décrire une matrice des risques résiduels, photographie du système à l'instant t intégrant les moyens de maîtrise en place dans l'organisation.

### VII. DU RISQUE A LA VULNERABILITE

C'est la combinaison de ce niveau de risque résiduel (surface de la matrice de risque échéance – Figure 6 : Matrice (carte) de vulnérabilité) avec le niveau de maîtrise de risque qui permet de déterminer la vulnérabilité du système (Figure 7 : Matrice des risques résiduels) Pierre Mongin, Mieux s'organiser, la stratégie du Post-it et du Kanban personnel, Inter éditions, 2013)

Cette matrice (carte) de vulnérabilité permet de positionner et d'observer non plus les risques résiduels mais bien les vulnérabilités du système, c'est-à-dire les risques et les dysfonctionnements pour lesquels l'organisation n'a pas encore les moyens de maîtriser le risque.

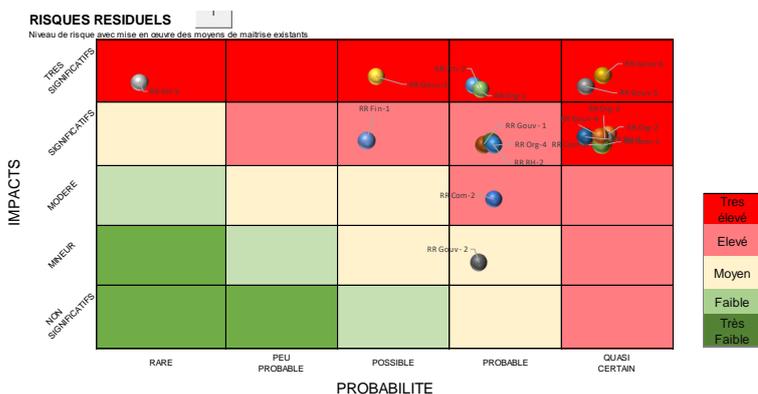


Figure 7 : Matrice des risques résiduels

Cette carte de vulnérabilité se découpe en trois zones (Figure 8 : du risque à la vulnérabilité). En rouge, la zone d'alerte, tout risque situé dans cette zone de responsabilité doit obligatoirement être traité sous peine de mettre en péril le système observé.

En jaune, la zone de surveillance, où il conviendra de valider la solidité de la pérennisation des moyens de maîtrise mis en œuvre dans le cas d'une solution de maîtrise apportée à un risque.

En vert, une zone de vigilance, où l'on vérifiera lors des itérations prochaines du processus que les risques situés dans cette zone ne croissent pas en termes de niveau de risques.

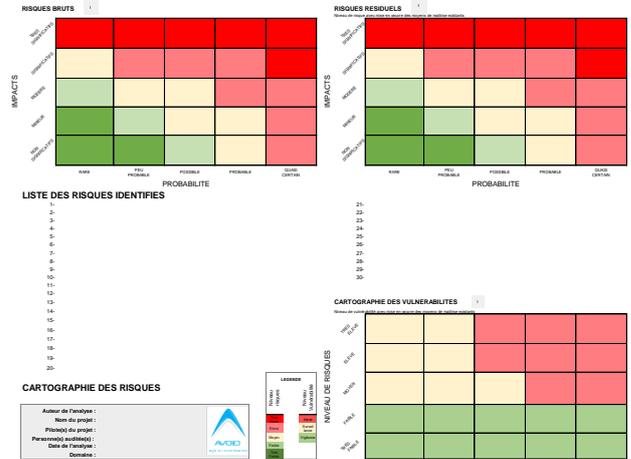


Figure 9 : Cartographie des risques et des vulnérabilités produites par l'outil AVoID

Arrivé à cette étape de la méthode, nous avons une cartographie actuelle des risques et des vulnérabilités auxquels est soumis notre système, nous pouvons effectuer un premier diagnostic et proposer un certain nombre de préconisation (Figure 9 : Cartographie des risques et des vulnérabilités produites par l'outil AVoID)

Nous pouvons nous arrêter à ce niveau si l'objectif est de faire un diagnostic d'un système à un instant t. Néanmoins, tout l'intérêt d'AVoID réside dans son utilisation en aide à la décision et donc en mode prédictif.

### VIII. LISTER LES MOYENS DE MAITRISE A TRANSFERER OU A INVENTER

Nous préconisons de réfléchir ensuite aux moyens de maîtrise à transférer, c'est-à-dire déjà en place dans d'autres systèmes attendant au système étudié ou complètement à inventer. Cette liste permet de mettre au jour un plan d'action connu des parties prenantes du système étudié mais souvent pas identifié en tant que tel. Cet effet d'amélioration confère à AVoID un principe de mise en lumière de signaux faibles connu de certains acteurs du système mais qui pour des raisons très diverses ne sont jamais ressorti dans les diagnostics précédents.

De la même manière que précédemment pour les risques bruts et les risques résiduels, nous pouvons cartographier les risques résiduels à échéance, c'est-à-dire une fois que tous les moyens

de protection (minimisation de l'impact) et de prévention (minimisation de la probabilité) auront été déployés. En évaluant l'impact et la probabilité du risque résiduel à échéance et en évaluant le niveau de maîtrise espéré sur ce risque, nous créons deux matrices supplémentaires : une matrice

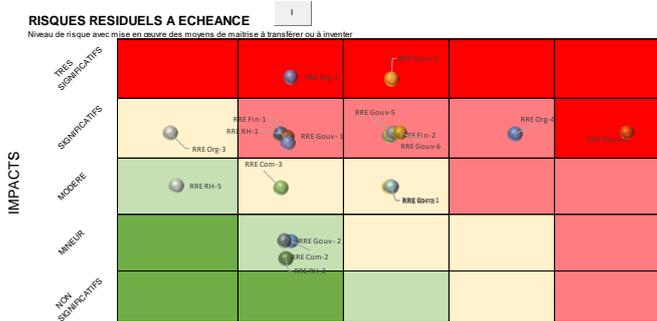


Figure 10 : Carte de Risques Résiduels à Echéances

de risque résiduel à échéance (Figure 10 : Carte de Risques Résiduels à Echéances) et une matrice de vulnérabilité à échéance (Figure 11 : Matrice de vulnérabilités à Echéance).

### IX. ANALYSE DE LA VULNERABILITE A ECHEANCES

Nous attirons votre attention en particulier sur cette dernière carte, qui est souvent le point de départ de l'analyse de

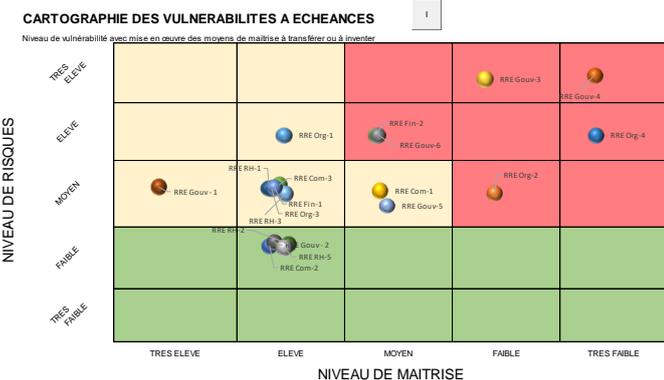


Figure 11 : Matrice de vulnérabilités à Echéance

vulnérabilité produite grâce à cette méthodologie.

Les risques situés en zone d'alerte (en rouge sur la Figure 11 : Matrice de vulnérabilités à Echéance) sont des risques de niveaux élevés ou très élevés qui n'ont pas trouvé de moyens de maîtrise suffisamment établis pour être complètement contrôlés. Il nécessite donc une prise de décision politique par le décideur qui pilote le système observé. Cette décision passe forcément par l'acceptation et le maintien du risque, le transfert de ce risque à un tiers ou le refus du risque (ISO 31000).

Les risques situés en zone de surveillance (en jaune Figure 11 : Matrice de vulnérabilités à Echéance) sont à consolider en termes de niveau de maîtrise. Il convient de garantir à tout prix le niveau de maîtrise annoncé, pour les risques récurrents en mettant en place une procédure qualité par exemple, pour les risques non récurrents en validant préalablement le niveau de maîtrise.

A cette étape du déroulement de la méthode, nous avons à notre disposition outre la cartographie des risques bruts, résiduels et résiduels à échéance, la cartographie des vulnérabilités actuelles et à échéances, ainsi que la listes des moyens de maîtrise en place et la liste des moyens de maîtrise potentiels.

### X. LES LEVIERS D'INTERACTIONS

Afin d'accompagner la prise de décision, il nous a paru essentiel d'observer notre cube de vulnérabilité (Figure 2 : Cube de vulnérabilité) sous des angles différents. Cette approche hyper cubique au sens modèle de traitement de données multidimensionnel<sup>5</sup> permet une approche décisionnelle différente suivant les axes observés. Dans l'absolu nous pouvons observer le système suivant une infinité de paramètres. Objectivement dans toutes les expériences que nous avons réalisées nous n'avons jamais dépassé des modèles de quatre ou cinq dimensions. La richesse contenue dans ces cinq dimensions permet déjà une aide à la décision conséquente.

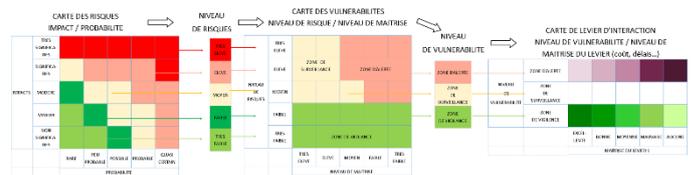


Figure 12 : De la cartographie des risques à la cartographie des leviers

Sur le même principe que précédemment, nous partons de la matrice de vulnérabilité à échéances que nous croisons avec le niveau de maîtrise du levier (Figure 12 : De la cartographie des risques à la cartographie des leviers).

Cette approche nous permet de créer pour chaque levier préalablement défini par l'utilisateur d'AVoID (ex : coût, délai, impact du changement, difficultés de mise en œuvre, impact

<sup>5</sup> Huret Augustin, Huet Jean-Michel, « L'intelligence artificielle au service du marketing », L'Expansion Management Review, 3/2012 (N° 146), p. 18-26.

d'un syndicat, géopolitique...) une nouvelle matrice (Figure 14 : Cartographie des risques et des vulnérabilités AVoID)

C'est la lecture de ces différentes matrices qui positionne AVoID comme un outil d'aide à la décision puissant, efficace, et rapide.

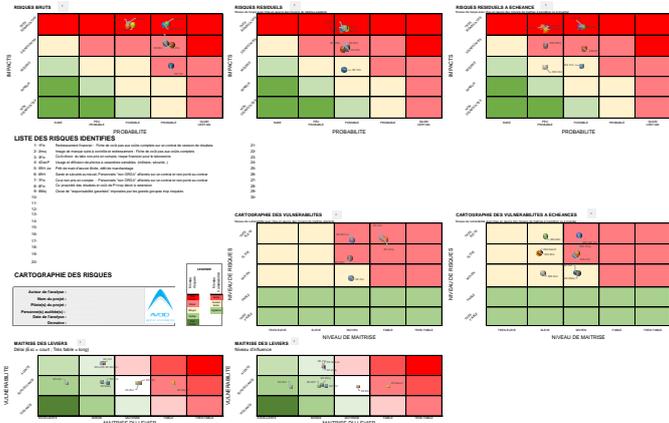


Figure 14 : Cartographie des risques et des vulnérabilités AVoID

XI. UN OUTIL DE CARTOGRAPHIE DES RISQUES ET DES VULNERABILITES

AVoID est non seulement une méthode mais c'est également un outil de saisie et de cartographie associé à la méthodologie qui permet de produire en grande série et rapidement les tableaux de moyens de maîtrise existants, à venir, ainsi que les cartographies précédemment cité dans cet article.

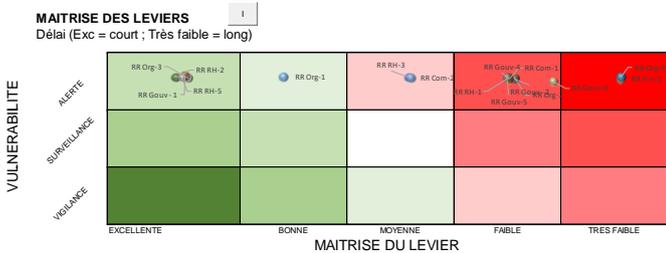


Figure 15 : Matrice de maîtrise du levier

La feuille de saisie (Figure 13 : feuille de saisie AVoID) permet de reprendre et de saisir directement pendant les entretiens la totalité des éléments que nous avons explicité dans le déroulé de la méthodologie pendant que se construit automatiquement la feuille de cartographie des risques et des vulnérabilités identifiés sur la Figure 15 : Matrice de maîtrise du levier

Cet outil permet un détachement complet de la forme pour pouvoir travailler le fond avec les acteurs du système observé.

| Id | Titre     | Description                | Impact       | Probabilité        | Impact       |
|----|-----------|----------------------------|--------------|--------------------|--------------|--------------------|--------------|--------------------|--------------|--------------------|--------------|--------------------|--------------|--------------------|--------------|--------------------|--------------|
| 1  | RR Org-1  | Risque de perte de données | Impact élevé | Probabilité élevée | Impact élevé |
| 2  | RR RH-2   | Risque de perte de données | Impact élevé | Probabilité élevée | Impact élevé |
| 3  | RR RH-3   | Risque de perte de données | Impact élevé | Probabilité élevée | Impact élevé |
| 4  | RR Com-1  | Risque de perte de données | Impact élevé | Probabilité élevée | Impact élevé |
| 5  | RR Gov-1  | Risque de perte de données | Impact élevé | Probabilité élevée | Impact élevé |
| 6  | RR Gov-2  | Risque de perte de données | Impact élevé | Probabilité élevée | Impact élevé |
| 7  | RR Gov-3  | Risque de perte de données | Impact élevé | Probabilité élevée | Impact élevé |
| 8  | RR Gov-4  | Risque de perte de données | Impact élevé | Probabilité élevée | Impact élevé |
| 9  | RR Gov-5  | Risque de perte de données | Impact élevé | Probabilité élevée | Impact élevé |
| 10 | RR Gov-6  | Risque de perte de données | Impact élevé | Probabilité élevée | Impact élevé |
| 11 | RR Gov-7  | Risque de perte de données | Impact élevé | Probabilité élevée | Impact élevé |
| 12 | RR Gov-8  | Risque de perte de données | Impact élevé | Probabilité élevée | Impact élevé |
| 13 | RR Gov-9  | Risque de perte de données | Impact élevé | Probabilité élevée | Impact élevé |
| 14 | RR Gov-10 | Risque de perte de données | Impact élevé | Probabilité élevée | Impact élevé |

Figure 13 : feuille de saisie AVoID

XII. AU-DELA DE LA METHODE ET DE L'OUTIL

La méthode AVoID ne fournit pas une boule de cristal mais un véritable outil d'aide dans la prise de décision par la vulnérabilité.

L'approche démontre que les interactions et les combinaisons entre les risques, les vulnérabilités, les leviers d'interactions maintenant et à échéances expliquent deux à trois fois mieux la réalité des phénomènes et des comportements que les méthodes d'analyse de risques classiques.

L'efficacité de la mise en œuvre pour l'observation des systèmes observés en fait un outil indispensable dans la trousse à outil du manager actuel.

TABLE DES ILLUSTRATIONS

Figure 1 : Processus de management du risque - Iso 31000 ..... 2

Figure 2 : Cube de vulnérabilité..... 2

Figure 3 : Des leviers pour analyser les risques ..... 2

Figure 4 : Carte heuristique des risques liés à un projet ..... 3

Figure 5 : Matrice des risques bruts perçus..... 4

Figure 6 : Matrice (carte) de vulnérabilité ..... 4

Figure 7 : Matrice des risques résiduels..... 5

Figure 8 : du risque à la vulnérabilité ..... 5

Figure 9 : Cartographie des risques et des vulnérabilités produites par l'outil AVoID ..... 5

Figure 10 : Carte de Risques Résiduels à Echéances ..... 6

Figure 11 : Matrice de vulnérabilités à Echéance..... 6

Figure 12 : De la cartographie des risques à la cartographie des leviers ..... 6

Figure 13 : Cartographie des risques et des vulnérabilités AVoID..... 7

Figure 14 : Matrice de maîtrise du levier ..... 7

Figure 15 : Feuille de saisie AVoID..... 7