VERS UNE AMELIORATION DE LA PERFORMANCE DES PME PAR LA REDUCTION DU RISQUE DANS UN CONTEXTE DE L'INTELLIGENCE ARTIFICIELLE

De

Driss HELMI
Chercheur en Economie et Gestion à l'Ecole Nationale Supérieure d'Arts et Métiers de Meknès, Université Moulay Ismail-Meknès.

&

Kamel KAYA
Professeur en Economie et Gestion à l'Ecole Nationale Supérieure d'Arts et Métiers de Meknès, Université Moulay Ismail- Meknès.

Résumé **:** La nature risquée de la conduite de projets est largement reconnue. En effet, aussi importants que soient les gains visés par une organisation lorsqu'elle entreprend un projet, les dépassements de budget ou de délais, l'insatisfaction des clients du projet, le manque de qualité des livrables, la perte de qualité du logiciel, la réduction de la fonctionnalité peuvent diminuer et même parfois anéantir les bénéfices escomptés. Cependant force est de constater que tout se passe comme si dans la recherche sur le processus de production de l'accident, on exclut une phase importante, celle justement de l'analyse et de l'évaluation des risques présente normalement à toutes les phases du système, depuis sa conception jusqu'à son démantèlement ou sa mise au rebut.

Comme pour le Système de Management de la Qualité défini par l'ISO 9001, le dispositif de gestion du risque opérationnel a vocation à suivre un cycle continu d'amélioration de type PDCA (*Plan, Do, Check, Act*). Il s'agit des quatre étapes de l'amélioration continue mentionnées dans la norme ISO 9001 et également s'appuie sur le processus de Management des Risques (ISO 31000).

La réduction des risques n'est que l'une des composantes de l'amélioration de la performance, qui vise également à réduire (*en moyenne et en variabilité*) les délais, les coûts et les défauts. L'objectif d'un processus de gestion des risques opérationnels est d'améliorer les processus, renégocier les assurances et sensibiliser l'entreprise aux risques opérationnels (culture risque).

Notre travail consiste à systématiser la culture de risque à travers le recours à des outils de l'Intelligence Artificielle s'appuyant sur l'utilisation des Systèmes Multi-Agents(SMA). Cela permettra sans doute à l'entreprise de :

✓ Baisser le coût lié aux pertes opérationnelles (en moyenne et surtout en variabilité) de manière à générer un accroissement durable de la rentabilité de l'établissement,

✓ Réduire la probabilité d'occurrence et la sévérité d'événements extrêmes qui pourraient amputer le résultat, voire les fonds propres.

Même si chaque entreprise a son approche personnalisée du sujet, le modèle du management du risque que nous proposons reflète l'essentiel d'un tel dispositif.

Mots clés : Management des Risques, Intelligence Artificielle, MAS, PDCA.

Abstract: Our job is to systematize risk culture through the use of tools of Artificial Intelligence based on the use of Multi-Agent Systems (MAS). This will allow the company to:

-Reduce the cost of operating losses;

-To reduce the probability of extreme events that could attribute the result or equity.

Although each company has its personalized approach to the subject, the model of risk management reflects the essence of such a device.

Keywords : Risk Management, Artificial Intelligence, MAS, PDCA.

Introduction

L'étude du risque a étendu ses ramifications dans plusieurs champs d'activités. En réalité, le risk-management a été longuement appliqué de façon accessoire et implicite dans la gestion des projets informatiques. Actuellement, de plus en plus d'organisations formalisent un tel processus, surtout pour les projets d'envergure ou stratégiques. D'ailleurs, le « PMI » (Project Management Institue) définit la gestion des risques comme l'une des neuf pratiques clé de Gestion des projets. En effet, la recherche a longtemps porté essentiellement sur des préoccupations techniques : modéliser physiquement l'accident (de l'échelle macroscopique à l'échelle microscopique) pour en connaitre les mécanismes (et ainsi les prévenir) et prévoir des distances de sécurité. Elle s'est ensuite déplacée vers les méthodes d'analyse des risques. Aujourd'hui, il est question d'analyse systémique, de responsabilité collective et d'approche sociétale. Cette approche doit s'appliquer dès la phase amont du projet (conception), et être poursuivie tout au long de son cycle de vie, en particulier à travers le « système de management de la sécurité » jusqu'au démantèlement. C'est pourquoi le management des risques d'un projet est devenu une préoccupation majeure pour les organisations. Il apparait plus que jamais que le succès d'un projet est fortement conditionné par la façon dont ses parties prenantes savent reconnaitre les risques potentiels qui le menacent, les étudier et les surmonter.

Nous traitons trois points essentiels. De prime abord, nous présentons les effets escomptés du management des risques. Dans un deuxième point, nous dressons les principales étapes du management des risques pour tout projet. Enfin, une application sur la fonction maintenance

1. Finalité du management des risques

Si l'on se réfère à la stricte définition du Mangement des Risques, les principaux résultats attendus sont :

- Obtenir une réelle capacité à anticiper les difficultés potentielles :
  - Mieux gérer les incertitudes liées à l'environnement ;
  - S'adapter au SI et à ses modifications.
- Une compréhension commune du périmètre et une stratégie bien définie de gestion des risques ;
- Des actions préventives et protectrices, priorisées, planifiées et mises en œuvre :
  - Mettre en œuvre une organisation adaptée ;
  - Fournir une souplesse de mise en œuvre ;
  - Vérifier la faisabilité.
- Un réel partage de la connaissance, et par l'entremise, une mesure régulière du niveau d'exposition aux risques :
  - Rendre, analyser, remonter les informations ;
  - Renforcer le pilotage par une meilleure visibilité.

Les enjeux sont d'éviter la mise en place d'une solution hâtive à un problème brutalement survenu et de concourir efficacement à l'optimisation des coûts, des délais et de la qualité, grâce à une démarche fondée sur l'anticipation.

2. Management de risques des projets

La méthode la plus couramment utilisée repose sur quatre processus bien définis : identification des risques, évaluation, élaboration de la réponse aux risques, maîtrise des risques. Il faudra y ajouter un processus transversal, la communication.

✓ Identifier les risques

La première étape consiste donc à identifier les risques auxquels le système d'information de l'entreprise peut être soumis. Il convient pour cela de procéder à un audit de sécurité définie et d'actualiser ou de produire une cartographie des vulnérabilités.

Soit le recours à des méthodes reconnues et disponibles sur le marché pour notamment la partie organisationnelle.

A ce niveau, nous pouvons citer quelques méthodes formelles, à savoir :

- La méthode FEROS (Fiche d'Expression Rationnelle des Objectifs de Sécurité des SI), développée par la DCSSI (Direction Centrale de la Sécurité des S.I).

Ses principaux objectifs sont :

Une fois les risques énoncés, il est souhaitable de déterminer des objectifs de sécurité. Ces objectifs sont l'expression de l'intention de contrer des risques identifiés et/ou de satisfaire à des politiques de sécurité organisationnelle. Un objectif peut porter sur le système cible, sur son environnement de développement ou sur son environnement opérationnel. Ces objectifs pourront ensuite être déclinés en fonctions de sécurité, implémentables sur le système d'information.

- La méthode MEHARI (Méthode Harmonisée d'Analyse de Risques) développée par le CLUSIF (Club de la Sécurité des S.I Français). Elle est dérivée de deux autres méthodes d'analyse des risques :
  - MARION (Méthode d'Analyse de Risques Informatiques Optimisée par Niveau) et MELISA (Méthode d'Evaluation de la Vulnérabilité Résiduelle des S.I).

Elle se présente comme une véritable boîte à outils de la sécurité des S.I, permettant d'appréhender le risque de différentes façons au sein d'une organisation, et composée de plusieurs modules. En outre, MEHARI expose une grande diversité dans l'utilisation de ses modules (cf Figure 5).

- Quant à la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), son principal objectif est la formalisation d'objectifs de sécurité adaptés aux besoins du système audité (et son périmètre) (6).
- Enfin, la méthode OCTAVE (OperatioallyCriticalThreat, Asset, and Vulnerability Evaluation), publiée par le SEI de la Carnegie Mellon University, reconnue dans le domaine de la sécurité des SI (Fédération des Computer Emergence).

OCTAVE est une méthode d'évaluation des vulnérabilités et des menaces sur les actifs opérationnels. Une fois ces derniers identifiés, la méthode permet de mesurer les menaces et les vulnérabilités pesant sur eux.

En résumé, ces méthodes sus-décrites remplissent efficacement leur rôle dans la conduite d'une démarche de Risk-management. En outre, malgré des différences de terminologie, le but demeure identique en termes de couverture du processus de gestion des risques.

Aujourd'hui, le recours à la norme ISO 17799 (8) étant la plus utilisée quant à la définition des exigences de sécurité de haut niveau (appelées « objectifs ») puis de bas niveau (appelées « exigences »).

✓ Evaluer les risques

A ce niveau, il convient d'évaluer le niveau des pertes supportables par l'entreprise, puis évaluer le risque lui-même ; mais aussi évaluer la probabilité de l'occurrence des risques et leur impact sur le projet : le fait de quantifier et qualifier chaque risque permettra de les prioriser.

Une fois cette première évaluation réalisée, les risques peuvent être rangés dans une matrice en fonction de sa provenance (Interne ou Externe) et de la volonté de nuire ou non qui est à son origine. Généralement, les risques élevés se retrouvent toujours dans la même position.

	Acte non volontaire		Acte volontaire	
	Utilisateur non privilégié	Utilisateur privilégié	Utilisateur non privilégié	Utilisateur privilégié
Externe	Risque faible	Risque faible à moyen	Risque faible à moyen	Risque élevé
Interne	Risque faible à moyen	Risque moyen	Risque élevé	Risque très élevé

Source : Computer Associates

✓ Elaborer la réponse à ces risques

Une fois ce premier travail essentiel réalisé, il convient d'élaborer la réponse à apporter à ces risques. En prenant en compte le coût des contre-mesures nécessaires, et le niveau de performance que s'est fixée l'entreprise, l'objectif est de réduire le risque à un niveau acceptable.

Les diverses actions possibles sont :

- Eviter le risque ;
- Déplacer le risque ;
- Réduire les vulnérabilités ;
- Réduire l'impact ;
- Eliminer ou réduire la menace.

Le risque 0 n'existant pas, il faut définir ce niveau de risque acceptable avant de décider quelle action prendre, pour quel risque.

L'audit de sécurité réalisé lors de la première étape a représenté un compte-rendu détaillé préconisant les moyens à mettre en œuvre pour chaque vulnérabilité identifiée. Le rôle du management des risques est ici de décider si la vulnérabilité doit être réparée ou tolérée en connaissance de cause. Les différents plans d'action sont alors élaborés. Et s'il y a lieu, la politique globale de sécurité peut être retouchée.

✓ Maîtriser les risques

Maîtriser les risques, c'est mettre en œuvre et tenir à jour les plans relatifs aux risques. Pour ce faire l'entreprise doit se doter d'un instrument clé du pilotage et du suivi de la sécurité : les tableaux de bord. Ces outils de reporting sont jugés prioritaires par les responsables de la sécurité.

De différents types (opérationnels, stratégiques, internes et externes), le tableau de bord n'est pas toujours géré par le service de Risk Management, certains indicateurs sont suivis la production et l'exploitation voire le responsable de la sécurité. S'ils sont d'une extrême importance, il reste difficile à définir, à mettre en place et à entretenir des indicateurs pertinents ; car un réel décalage existe entre les outils de mesure disponibles sur le marché de ce que les responsables sécurité souhaitent mesurer :

- Des indicateurs sur un risque donné et sur les actions en cours (criticité évaluée ou réévaluée, actions réalisées,…) ;
- Des indicateurs sur l'efficacité du dispositif de gestion des risques (délai pour mettre sous contrôle un risque, régularité de la revue des risques…) ;
- Des indicateurs sur le niveau global de maîtrise perçu (somme des criticités, évolution dans le temps…).

Bien souvent il devient nécessaire de combiner plusieurs sources, plusieurs méthodes et plusieurs outils pour arriver à un résultat parlant. Les indicateurs internes doivent être complétés par des indicateurs externes sur l'image, la visibilité et la notoriété de l'entreprise.

L'historique est un élément déterminant pour la pertinence d'un tableau de bord. Si au cours du temps, les courbes baissent, les risques sont maîtrisés. Si les courbes stagnent ou montent, il est nécessaire de renforcer les dispositions prises.

Mais attention, ces tableaux de bord ne doivent pas priver l'entreprise d'une réflexion sur la méthodologie et l'analyse des résultats.

✓ **Communiquer :**

Le processus de communication doit inclure, transversalement à ces activités, cette information sur les risques et leur management. Pour ce faire, il faut prendre en compte la communication sur les risques dans la structuration de la communication sur la politique de sécurité mise en place et veiller à définir spécifiquement la communication à réaliser en cas de concrétisation de risques considérés comme majeurs (communication dite « de crise »). Il importe particulièrement de veiller à la crédibilité d'ensemble de cette communication, et définir par exemple les acteurs habilités à communiquer.

Par ailleurs, les besoins prioritaires de sécurisation sont définis à partir des temps de remise en route après sinistre des applications et des écarts par rapport aux temps clients « supportables ».

Tout cela aboutit à une remise à jour avec les « clients » de la liste des applications à sécuriser en priorité, une première liste d'actions (prévention, protection ou assurance) concrètes et pas nécessairement très coûteuses. En effet, le niveau de protection doit correspondre au « juste nécessaire » défini par adéquation entre le coût et le niveau de sécurité souhaité.

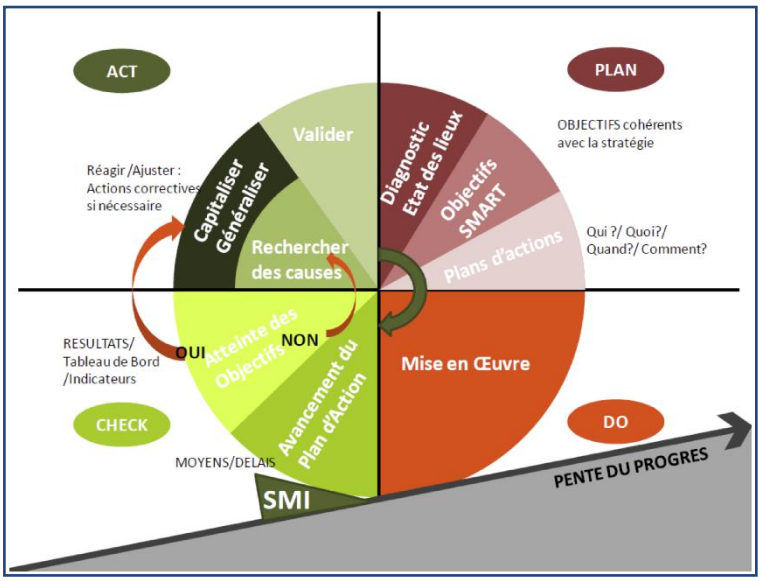
3. Management des risques de la Fonction Maintenance

L'architecture élaborée emprunte la démarche qualité qui correspond à une dynamique de changement. Elle est basée sur le cycle de W. Shewhart : Plan-Do-Check-Act (PDCA) qui devient avec W. E. Deming un véritable outil de management pour toute l'entreprise.

Le cycle PDCA comporte 4 étapes à savoir : stabiliser le processus, appliquer le standard débugué, respecter vigoureusement le standard et améliorer le standard. C'est amélioration à travers le temps qui conduit sans cesse à la performance.

Cette démarche préconise que les entreprises doivent étudier et comprendre avec toujours plus de précision leurs processus de production ou de prestations de services. Si l'entreprise veut diviser son système en différents blocs à des fins d'analyse, elle se doit d'étudier aussi "clients internes" qui mettent en œuvre les processus demandés.

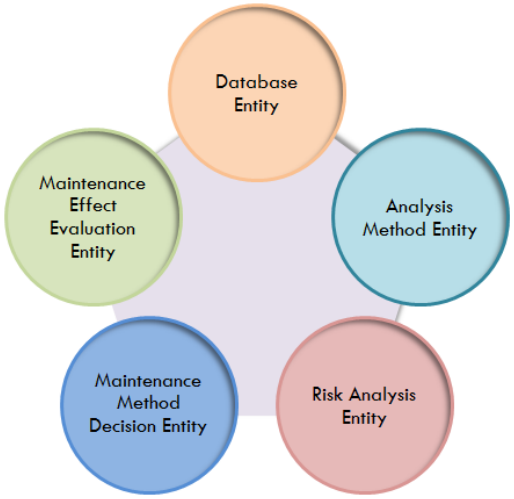
L'analyse quantitative des processus est également très importante. Les entreprises doivent les examiner soigneusement avant et après les changements, en répétant chaque fois l'approche du cycle PDCA.



Approche dynamique de l'amélioration du processus

Nous mettons l'accent sur l'amélioration continue de la qualité de la fonction maintenance mais non pas de la qualité du produit ou service comme chez son inventeur. Une maintenance qui vise la disponibilité, la fiabilité, la maintenabilité et la sécurité des outils de production tout en évitant au maximum les Muda des ressources dédiées à cette structure.

Notre architecture comporte plusieurs étapes, chacune d'elles est assurée par une entité et/ou agent. Les flux d'informations dispensées par chaque entité et/ou agent sont diffusées systématiquement à travers l'architecture proposée vers l'ensemble des phases. Ce qui permettra une mise à jour en temps réel de tous les indicateurs relatifs à l'efficacité de la maintenance (XP X60 020). C'est un gage d'une actualisation permanente de la Base de Données et l'assurance de support de décision idoine.



Architecture de la Maintenance industrielle

✓ **Data base Entity: Documentation & BDD**

Dans notre cas, l'entité "Data base" incarne le système documentaire qui capitalise les informations et les décisions. Elle est à la fois la dernière et la première de la roue PDCA. Elle est la dernière en réceptionnant les nouveaux indicateurs suite à l'expérience établie, et elle sera

la première à se servir de ces nouvelles informations et de les considérer comme le nouvel état lieu à conserver voire à améliorer.

Cette entité enregistre, directement ou indirectement, par l'entremise des supports informatiques existants (transfert des pannes relatives aux différentes structures du parc via intranet par exemple) la totalité des arrêts programmés ou non des lignes de production du parc industriel apparues tout au long d'une période donnée tout en précisant leurs causes, leurs durées et les actions réalisées. Cette entité informatique, considérée comme une base de données brutes qui regroupe toutes les informations dont ont besoin les autres agents (normes fournisseurs, fiche technique des équipements, indicateurs…). En outre, elle évalue la maintenabilité, la disponibilité, la fiabilité et la sécurité des outils de production tout en fournissant des indicateurs techniques tels que l'indicateur quantité d'interventions, l'indicateur de fiabilisation (Mean Time Between Failure), l'indicateur de compétence (Mean Time To Repair), l'indicateur d'indisponibilité (MTBF/MTBF+MTTR), l'indicateur de coûts et maintenance par équipement et l'indicateur d'incidence de la maintenance.

✓ **Analysis Method Entity**

Elle a pour objet de déterminer dans une démarche d'analyse de systèmes qui s'appuie sur un raisonnement inductif (causes- conséquences) pour l'étude organisée des causes, des effets de défaillances et de leur criticité. Elle identifiera les fonctions, les contraintes d'utilisation et d'environnement, les paramètres critiques à mettre sous contrôle et sur lesquelles les analyses telles que l'A.F, FMECA, L'AVA et le management des risques. De ce fait, elle est composée de deux agents et une entité qui interagissent entre eux par coordination à savoir :

- Agent diagramme causes-effets

Ce diagramme est une méthode graphique visant à analyser à fond une situation particulière (l'effet) pour en faire ressortir toutes les causes potentiellement reliables au problème à l'étude. Cette arborescence permet :

- De structurer un message,
- De visualiser une situation en vue de faire apparaitre les points clés,
- D'identifier toutes les causes possibles de l'effet d'un problème,
- De choisir les causes à traiter en priorité.

Les causes sont regroupées classiquement par famille, autour des 5 M :

- Matières, Matériels, Main d'œuvre, Méthodes de travail, Milieu. Parfois des 8 M en rajoutant : Management-Money-Market.

- Agent Failure Mode, Effects and Criticity Analysis

Cet agent identifie et examine méthodiquement les défaillances potentielles des systèmes – analyse des modes de défaillances-, leurs causes et leurs incidences sur le fonctionnement de l'ensemble et leurs effets. Il est à signaler qu'il convient au préalable que l'entité EMECA mène une analyse fonctionnelle de l'outil de production. Il s'agit d'identifier clairement les éléments à étudier, leur environnement et leurs fonctions. C'est une phase indispensable pour structurer et conduire l'étape ultérieure d'analyse des défaillances. Chacune d'elles, est caractérisée par :

- Severity of the potential effect ;
- Occurrence of the potential cause ;
- Detection (efficiency of the monitoring system) ;
- Recovery (time, cost) to come back to a normal situation.

Nous déduisons alors le Risk Priority Number (RPN) qui est le produit de S*O*D ou S*O*D*R. Le RPN sera utilisé, dans la méthode pour définir les priorités parmi les actions à réaliser et à suivre. Il convient de souligner que le FMECA demeure une démarche préalable :

- Au design of experiment (DOE) pour limiter le nombre de « marginalité » d'un processus,
- A l'élaboration des plans de contrôle,
- A l'anticipation des problèmes liés à toute modification des processus (accroissement de la production, introduction d'un nouvel équipement, processus…).

Par ailleurs, dans le cadre de la maintenance, le FMECA moyen est un parfait outil pour collecter et axiomatiser toutes les informations sur les défaillances observées, notamment en l'absence de données historiques. L'expérience de chacun pourra ainsi mieux être capitalisée et transmise. C'est également un outil efficace de communication entre les divers entités/agents concernés par les équipements : méthodes et opérateurs de maintenance, travaux neufs, méthodes et opérateurs de production, etc.

✓ RiskAnalysisEntity

Le risque repose non seulement pas sur un acteur de la chaîne mais issu d'une série d'erreurs qui s'accumulent. Rien ne sert de viser le zéro défaut sur une des phases s'il existe des défaillances importantes aux autres niveaux. Toute gestion des risques opérationnelle associe la déclaration des événements non souhaités, des recueils périodiques des ENS, l'analyse des causes, l'identification et l'analyse des processus à risque, l'estimation de la criticité des risques principaux.

L'agent doit disposer d'un cadre méthodologique pour une réalisation d'une estimation du risque en amont d'une prise de décision (FD X50-252). De même, la norme ISO 31000 (principes et lignes directrices pour la mise en place d'un processus de management des risques) vise à harmoniser le processus de management du risque et les définitions qui lui sont rattachées, donner des conseils sur la mise en œuvre et la maintenance du système de management et sensibiliser les entités/agents au management des risques.

✓ Maintenance Method Decision Entity

Au regard des résultats dégagés par les autres entités et/ou agents en termes de documentation, méthodes, évaluations, l'agent est en mesure de préconiser la maintenance adéquate qui respecte le cahier des normes et exigences fournisseurs, l'état technique du matériel (obsolescence, usure) et les contraintes de la production. Il a pour objectif de déterminer la politique de maintenance (corrective, préventive- prédictive), la gestion des stocks des pièces de rechange, les procédures à mettre en œuvre, la formation des salariés et les études de faisabilité financières de mise à niveau et de remplacement des équipements.

Pour lui permettre ce rôle, l'entité est dotée de différents types de maintenance et de leurs conditions d'utilisation en se référant à la norme (NFX 60-010).

✓ Maintenance Effect Evaluation Entity

Le retour d'expérience (REX) est essentiel pour l'efficacité, l'efficience, la pertinence et l'effectivité. La modélisation de la fonction maintenance est justifiée si et seulement si les indicateurs techniques de retour se sont améliorés. Il devient utile et exploitable à condition qu'il permette d'éviter au maximum le Muda des ressources. En effet, les pannes sont des creux de production l'occasion de générer des dépenses improductives. L'agent a pour rôle d'élaborer les nouveaux indicateurs de la performance. Il dresse un état des indicateurs techniques de performance des équipements : Maintenabilité, fiabilité, disponibilité et sécurité.

Conclusion

Tout au long de cette communication, nous avons tenté de montrer que la notion de risque, qui demeure intangible, reste difficile à appréhender. En outre, au regard de tous les facteurs de risque et variables associées auxquels sont soumis les SI, l'amélioration du niveau de sécurité de l'organisation doit faire l'objet d'une politique globale d'entreprise, managée au niveau du

comité de direction. Autrement dit, elle doit prendre en compte à la fois les processus, les « ressources humaines », les applications et les aspects métier. Un point important à souligner est que la sécurité ne doit pas être interprétée comme une contrainte, mais comme un ensemble de règles librement consenties. Et cette politique doit être connue de tous les acteurs (direction, utilisateurs, administrateurs,…). La politique de sécurité doit contenir une sensibilisation aux risques encourus. Il faut donc au préalable se mettre d'accord au sein de l'organisation sur ce que doit être une politique de sécurité car chaque acteur a une vision différente : donner un cadre de référence en fixant les règles et les usages en matière de sécurité relativement aux SI.

Toute organisation a le devoir de s'interroger sur le comportement à adopter face aux importants chamboulements de son environnement. La gestion de la sécurité en contexte projet des SI doit être considérée au même titre que la gestion des risques financiers ou business.

Aujourd'hui, le TOP Management est conscient que la sécurité de leurs SI peut contribuer directement à la création de valeur. En effet, le coût est souvent un frein à la mise en place d'une politique de sécurité, mais ces coûts supplémentaires induits seront bien maîtrisés si la politique de sécurité est bien définie avant de démarrer la mise en œuvre technique. En réalité, l'absence de sécurité peut s'avérer onéreuse si l'on considère les conséquences des incidents qui frapperaient l'organisation.

Une politique de sécurité bien réfléchie, doit trouver un compromis entre le coût et l'objectif à atteindre, sachant que le coût le plus important est celui des « ressources humaines », tant la surveillance doit être effectuée de façon régulière. Le Risk-management tel que nous l'avons précédemment souligné doit être à l'origine de cette politique de sécurité pour définir ce que l'on doit protéger par rapport à quels risques, identifier les vulnérabilités (faille ou brèche) et permettre de définir les axes de la politique sécurité à retenir qui se matérialisent par des normes formant les référentiels bases des audits futurs.

REFERENCES

[1] Kilian C, *The World of W. Edwards Deming, Second Edition*, vol. TN: SPC Press, Knoxville, 1992.

[2] G. Theodoropoulos, R. Minson, R. Ewald, and M. Lees, *Multi-Agent Systems: Simulation and Applications*: CRC Press, 2009.

[3] FERRAND N, "*De l'apport potentiel de la sociologie pour l'ingénierie des systèmes sociaux artificiels*," *journées de RocheBrune " Du collectif au social "*, 1996.

[4] Müller J.P, "*Des systèmes autonomes aux systèmes multi-agents : interactions, émergence et systèmes complexes*," *Rapport présenté pour l'obtention de l'HDR,* p. 58 2002.

[5] Shewhart W.A, "*Les fondements de la maitrise de la qualité* " *Econimica*, 1989.

[6] X. X60-020, " *Maintenance. Indicateurs de maintenance.*," ed, 08/1995.

[7] F. X. 50-252, "*Une démarche pour estimer ses risques*," ed, 01/2007.

[8] Mazouni M.H, "*Pour une Meilleure Approche du Management des Risques : De la Modélisation Ontologique du Processus Accidentel au Système Interactif d'Aide à la Décision*," Doctorat, Institut National Polytechnique de Lorraine, 2008.

[9] NFX 60- 010, "*Vocabulaire de maintenance et de gestion des biens durables*," ed. Paris: Afnor Gestion, 1984 p. 8.

[10] HELMI D., KAMEL KAYA S. A., RADOUANI M., EL FAHIME B., "*Specificities of Information Systems Organizations LEAN in mastering QCDM Tetrahedral*". Research

Journal of Science and IT Management – The International Journal's, ISSN: 2251-1563. Volume 3, Issue no 10. Pages 10 à 19, August 2014.

[11]HELMI D., RADOUANI M., EL FAHIME B., KAMEL KAYA S. A., "*Maintenance model based on multi agent system improving the performance to a total quality management*". International Journal of Management & Information Technology. ISSN: 2278-5612. Volume 9, Issue no 2. Pages 1593 à 1599, April 2014.