

**LA GESTION DES RISQUES DES SYSTEMES
D'INFORMATION DANS LES ORGANISMES PUBLICS AU MAROC :
QUELS BENEFICES A LA PERFORMANCE ?**

Par

Lahoucine IKKOU

**Chercheur à la Faculté des Sciences Juridiques, Economiques et Sociales,
Université IBEN ZOHR-AGADIR.**

&

Abdelkbir ELOUIDANI

**Professeur à la Faculté des Sciences Juridiques Economiques et Sociales,
Université IBEN ZOHR- AGADIR.**

Résumé

Les technologies de l'information croissent d'une façon très rapide ce qui rend l'environnement des systèmes d'information très complexe, très turbulent, vulnérable plus exposé aux risques, moins sécurisé. Pour cela il est indispensable d'assurer une protection des SI. La gestion des risques et l'élaboration d'une politique de sécurité des systèmes d'information sont devenues plus une nécessité qu'un choix.

L'objectif de cet article est d'expliquer comment, d'une part à travers la théorie, la gestion des risques de systèmes d'information peuvent apparaître comme l'un des déterminants de la performance au sein d'une organisation publique et d'autre part à travers une étude sur les organisations publiques au Maroc.

Pour répondre à notre question, nous avons utilisé un pôle théorique qui a constitué la source principale de notre hypothèse qui sera testée dans le but de vérifier sa validité, que nous avons privilégié hypothético- déductive.

Mots clés

Gestion des risques SI, organismes publics, performance organisationnelle.

Abstract

The information technologies are growing in a very fast manner, which makes the information systems environment very complex, very turbulent, vulnerable more exposed to risk, less secure. For this it is essential to ensure protection of the information system. Risk management and the development of a security policy of information systems have become more a necessity than a choice.

The objective of this article is to explain how, on the one hand through the theory, information systems risk management can appear as one of the determinants of performance within an organization and public on the other hand through a study on public organizations in Morocco.

To answer our question, we used a theoretical pole which was the main source of our hypothesis that will be tested in order to verify its validity; we have privileged hypothetico-déductive.

Keywords:

Risk management SI, public organizations, organizational performance.

<http://revues.imist.ma/?journal=REGS>

ISSN: 2458-6250

Introduction

Dans un environnement économique en perpétuelle transformation, en raison des grandes révolutions techniques enregistrées, le développement des échanges commerciaux, la mondialisation des marchés et l'abolition des pratiques protectionnistes, les établissements publics marocains, sont tenus à intégrer cette tendance, tout en protégeant leurs patrimoines informationnels, et en améliorant leurs potentiels compétitifs.

Aujourd'hui, les technologies de l'information et de la communication (TIC) croissent d'une façon très rapide ce qui rend l'environnement des systèmes d'information (SI) très complexe, très turbulent, vulnérable plus exposé aux risques, moins sécurisé. Pour cela il est indispensable d'assurer une protection des SI. La gestion des risques et l'élaboration d'une politique de sécurité des systèmes d'information sont devenues plus une nécessité qu'un choix.

Le Maroc s'est engagé dans le domaine de l'administration électronique. Il s'agit de mettre les technologies de l'information au service de la modernisation des services publics, d'améliorer l'efficacité de l'action des administrations de l'Etat et la qualité des relations entre celles-ci et leurs usagers. Cette dématérialisation "des services publics" ne peut s'effectuer sans une attention minimum portée sur la sécurité et particulièrement la sécurité SI.

La sécurité des SI recouvre un ensemble de méthodes, techniques et outils chargés de protéger les ressources d'un SI afin d'assurer :

- **La disponibilité des services** : les services (ordinateurs, réseaux, périphériques, applications,...) et les informations (données, fichiers,...) doivent être accessibles aux personnes autorisées quand elles en ont besoin ou la capacité à assurer la continuité de service opérationnelle des processus « métier » ;
- **La confidentialité des informations** : les informations n'appartiennent pas à tout le monde ; seuls peuvent y accéder ceux qui en ont le droit ou confidentialité : niveau de confidentialité estimé nécessaire et impact d'une divulgation éventuelle de certaines données dans le fonctionnement de chaque processus ;
- **L'intégrité des systèmes** : les services et les informations (fichiers, messages,...) ne peuvent être modifiés que par les personnes autorisées (administrateurs, propriétaires,...) ou besoins de justesse et de cohérence des données, permettant d'assurer le bon fonctionnement des processus « métier » ;

- **Traçabilité** : capacité à conserver des preuves ;
- **Conformité** : respect des lois, réglementations.

Notre problématique peut être formulée sous forme de la question suivante : **quels bénéfices de la gestion des risques SI peuvent apporter à la performance organisationnelle?**

L'objectif de notre travail est de faire sortir les bénéfices de la gestion des risques SI à la performance des organisations publiques au Maroc. D'abord, nous allons aborder le concept de la gestion des risques SI. Ensuite, nous traitons le référentiel ISO 2700x, puis nous tenterons de mettre en évidence, les liens entre la gestion des risques SI et la performance organisationnelle et enfin nous proposerons une étude empirique : cas des organisations publiques marocaines, à travers une triple analyse reposant à la fois sur une analyse descriptive, exploratoire et confirmatoire.

En somme, le besoin sécurité de l'information " **est comme l'oxygène ; quand vous l'avez, vous le prenez mais quand vous ne l'avez pas, l'obtenir devient la priorité immédiate et serrante** "

Joseph Nye, université de Harvard.

1. La gestion des risques des systèmes d'information.

À la suite de la mondialisation de l'économie et du développement des nouvelles technologies de l'information. L'information dont l'entreprise dispose en interne de son SI, et celle qui transite via ses réseaux, avec et sans fils, est un bien souvent précieux, parfois elle est stratégique pour la bonne marche d'affaire des organisations, on aborder dans un premier lieu les définitions de la sécurité des systèmes d'information et dans deuxième lieu la notion de la gestion des risques.

1.1 Définition d'un risque

D'après le Petit Robert «Le risque est l'éventualité d'un événement ne dépendant pas exclusivement des parties et pouvant causer la perte d'un objet ou tout autre dommage ; par extension, [le risque est un] événement contre la survenance duquel on s'assure ».

Selon la directive n° 96/82 du Conseil de l'Europe¹ «Le risque est la probabilité qu'un effet spécifique se produise dans une période donnée ou dans des circonstances déterminées ».

Quant à OHSAS 180012 «[Le risque est la] combinaison de la probabilité et des conséquence (s), de la survenue d'un événement dangereux spécifié ».

1.2La gestion des risques de systèmes d'information

La sécurité d'un SI revient à essayer de se protéger contre les risques liés à l'informatique qui pouvant avoir un impact sur la sécurité de celui-ci, ou des informations qu'il traite. Cette sécurité est basée sur la gestion des risques, qui devront gérés d'une manière qui garantit la protection du patrimoine informationnelle de l'entreprise.

La gestion des risques est définie par l'ISO³ comme l'ensemble des activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. On dégage en général trois finalités à la gestion des risques pour les SI :

1. Améliorer la sécurisation des systèmes d'information.
2. Justifier le budget alloué à la sécurisation du système d'information.
3. Prouver la crédibilité du système d'information à l'aide des analyses effectuées.

La gestion des risques exige une conscience des risques de la part des cadres supérieurs, une vision claire de l'appétence de l'entreprise pour le risque, une bonne connaissance des exigences de conformité, de la transparence à propos des risques significatifs encourus par l'entreprise, et l'attribution des responsabilités en matière de gestion des risques au sein de l'entreprise⁴.

Plus généralement appliquée aux entreprises, la gestion des risques s'attache à identifier les risques qui pèsent sur les actifs (financiers ou non), les valeurs ainsi que sur le personnel de l'entreprise⁵.

Au plan opérationnel, la DSI doit être en mesure de gérer les risques IT⁶, ces risques font partie intégrante de l'activité des entreprises. Paradoxalement, on constate que ces dernières

¹Directive n° 96/82 du Conseil de l'Europe du 9 décembre 1996 concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses.

²OHSAS ou Occupational Health and Safety Assessment, certification qui précise les règles pour la gestion de la santé et la sécurité dans le monde du travail. Elle a une valeur internationale.

³ISO/IEC Guide 73:2002, Risk management – Vocabulary – Guidelines for use in standards.

⁴Dominique. M et Fabrice Garnier de Labareyre, Cobit, Pour une meilleure gouvernance des systèmes d'information, Ed Eyrolles, Paris, 2009, p.7.

⁵CIGREF, analyse et gestion des risques dans les grandes entreprises, impacts et rôle pour la DSI, 2007, p.10.

<http://revues.imist.ma/?journal=REGS>

ISSN: 2458-6250

éprouvent de réelles difficultés dans l'appréhension globale des risques des TI. N'ayant pas une politique basée sur la sécurité pour faire face aux menaces directes (virus, intrusion, etc.) et l'assurance pour couvrir un certain nombre de risques secondaires tels les catastrophes naturelles, l'arrêt de service, la perte des données, elles sont vulnérables face à ces dangers potentiels.

La sécurité des systèmes d'information se place sur un plan tactique et opérationnel alors que la gestion des risques des systèmes d'information se positionne sur un plan stratégique. La sécurité des systèmes d'information est considérée par la GTI comme une réponse à des risques spécifiques clairement identifiés. La gestion des risques dépend d'un comité appelé Team Risk Management (TRM) qui a pour rôle l'identification et l'évaluation d'un risque dans le but de déterminer la meilleure réponse possible. L'approche du TRM est basée sur quatre catégories de risques : le risque stratégique, le risque opérationnel, le risque lié aux projets, le risque de litige.

La gouvernance des systèmes d'information doit veiller à ce que la direction de la technologie d'information fonde son approche du risque sur les mêmes critères et adopte une gestion collaborative avec les directions clés de l'entreprise : audit, finance, production, ressources humaines et control de gestion, cette démarche se justifie par le fait qu'il est indispensable de connaître le niveau de tolérance et d'impact sur les technologies d'information d'une entreprise. Le risque de la technologie d'information doit être considéré comme le plus sensible, Les principaux facteurs de succès de la gestion des risques des technologies d'information sont basés sur la collaboration entre tous les membres de l'équipe, la communication et la supervision par le contrôle.

Le management du risque est basé sur la tolérance d'une organisation à être exposée à un niveau de risque susceptible d'engendrer des pertes plus ou moins importantes. L'analyse des menaces, capitale dans la gestion des risques, se fonde sur une méthodologie à trois phases ⁷:

- **Identifier le risque** : dans ce niveau on distingue quatre types des risques : le risque humain, le risque technologique, le risque d'activité, le risque naturel.
- **Évaluer le niveau de risque** : permet de définir les priorités d'actions et d'établir le niveau de risque.

⁶ Ahmed BOUNFOUR & Georges EPINETTE, valeur et performance des SI, Dunod, Paris, 2006, p.58.

⁷ Frédéric Géorel, IT gouvernance : maîtrise d'un système d'information, Dunod, Paris, 2005.

- **Réduire le risque** : le traitement du risque est basé sur sa réduction et non sur sa suppression.

Vue l'importance de la gestion des risques à plusieurs niveaux, les praticiens ont essayé d'élaborer des normes pour réduire et bien gérer les risques.

2. La gouvernance de la sécurité : la norme 2700x

D'après Jacqueline et al⁸ le dispositif ISO 27001 permet à une entreprise d'obtenir une certification pour son système de management de sécurité des systèmes d'information.

La norme internationale ISO 27001 spécifie un Système de Gestion de la Sécurité des Systèmes d'Information (SGSSI) / Information Security Management System (ISMS). Ce SGSSI est structuré en quatre étapes récurrentes (planifier, mettre en œuvre, vérifier, améliorer), afin de respecter le principe de la roue de Deming, issue du monde de la qualité. Ce concept permet d'établir un parallèle avec les normes relatives aux systèmes de management de la qualité (ISO 9001) et de l'environnement (ISO 14001).

Pour opérer ce SGSSI, l'ISO 27001 préconise d'employer son annexe A ou l'ISO 17799 pour identifier les mesures de sécurité à mettre en œuvre au cours de l'étape de planification.

La norme ISO 27001 décrit les mesures nécessaires à la mise en place d'un SMSI. Mais si elle fixe l'objectif à atteindre, elle ne préconise pas comment, concrètement, il convient de déployer ces mesures. L'implémentation du SMSI a donc besoin d'un guide de bonnes pratiques pour les différentes actions qu'il va entreprendre.

Dans le même cadre, l'ISO 27002 répond à ce besoin par toute une série de préconisations concrètes, abordant des aspects tant technique qu'organisationnelle.

La norme ISO 27002 est constituée de 11 chapitres importants (du 5 au 15) couvrant l'essentiel des domaines relatifs à la sécurité de l'information. La liste ci-dessous présente sommairement chacun de ces chapitres⁹ :

- Politique de sécurité ;
- Organisation de la sécurité de l'information ;
- Gestion des besoins ;

⁸Jacqueline Sidi, Martine Otter et Laurent Hanaud, guide des certifications SI, comparatif, analyse et tendances ITIL, COBIT, ISO 27001, eSCM ... ,Dunod, paris 2006, p.95.

⁹Alexandre Fernandez-Toro, management de la sécurité de l'information, implémentation l'ISO 27002,2ème édition Eyrolles, 2009, p.50.

- Sécurité liée aux ressources humaines ;
- Sécurité physique et environnementale ;
- Gestion de l'exploitation et des télécommunications ;
- Contrôle d'accès ;
- Acquisition, développement et maintenance des systèmes d'information ;
- Gestion des incidents liés à la sécurité de l'information ;
- Gestion du plan de continuité de l'activité ;
- Conformité.

La norme est structurée sur trois niveaux¹⁰ :

- Les chapitres (niveau 1) ;
- Les objectifs de sécurité (niveau 2) ;
- Les mesures de sécurité (niveau 3).

Les quatre premiers chapitres de l'ISO 27002 décrivent des généralités et rappellent quelques notions de base .C'est à partir du chapitre 5 que la norme devient intéressante.

Après avoir défini la notion de la sécurité, la gestion des risques et le référentiel de bonnes pratiques ISO2700x, dans le point suivant on va mettre en évidence les bénéfices de la gestion des risques pour la performance.

3. Les bénéfices de la gestion des risques des systèmes d'information

Durant les vingt dernières années, l'intérêt pour la sécurité lors du développement et l'exploitation des SI n'a cessé de croître. Les méthodes de gestion des risques de sécurité sont des outils méthodologiques, qui aident les organisations à prendre des décisions rationnelles sur la sécurité de leur SI¹¹.

Une gouvernance centrée sur le risque permet aux dirigeants de l'entreprise d'utiliser la gestion du risque informatique comme un levier de résilience, mais aussi comme un bouclier de protection de la technologie et de l'infrastructure physique, et donc au final, comme un facteur de dynamisation de la croissance (IBM, 2008)¹².

¹⁰Alexandre Fernandez-Toro, 2009, Op. Cit.

¹¹Dominique. M et Fabrice Garnier de Labareyre , Cobit, Pour une meilleure gouvernance des systèmes d'information, Eyrolles,Paris, 2009 ,p.7.

¹²IBM, « Méthodologie de gestion du risque informatique pour les Directeurs des Systèmes d'Information : un levier exceptionnel de création de valeur et de croissance », Septembre 2008, p.14.

En outre, La politique de sécurité indique l'ensemble des mesures à prendre, des structures à définir et l'organisation à mettre en place afin (Robert Longeon et al ,1999)¹³:

- D'empêcher (au moins freiner) la détérioration, l'utilisation anormale ou la pénétration des systèmes et réseaux ;
- De détecter toute atteinte, malveillante ou non, à l'intégrité, la disponibilité et la confidentialité des informations ;
- D'intervenir afin d'en limiter les conséquences et le cas échéant, pour suivre l'auteur du délit.

Une étude récente montre que les entreprises qui font preuve de maturité et d'équilibre dans leurs gestions des risques informatiques rencontrent peu d'incidents, tout en obtenant des performances opérationnelles informatiques et métier meilleures que leurs concurrentes. Et l'équilibre est ici capital. L'étude montre qu'il est plus efficace d'associer de façon équilibrée les trois grands volets de la gestion du risque - les processus de gouvernance, l'assise informatique et la culture de prise en compte des risques - que de les adresser séparément. Les entreprises qui adoptent cette démarche font bien mieux que se prémunir contre les perturbations. Elles sont également plus performantes et démontrent une organisation plus agile, et peuvent exploiter la gestion des risques pour promouvoir de meilleures pratiques de gestion IT¹⁴.

Cette étude s'appuie sur les travaux de George Westerman et Richard Hunter, présentés dans leur ouvrage IT Risk : Turning Business Threats in to Competitive Advantage. Elle conclut que l'excellence dans un seul des trois volets de la gestion des risques informatiques ne permet d'en concrétiser que partiellement les bénéfices. L'étude montre qu'il est plus efficace d'associer de façon équilibrée ses trois grands domaines. Basée sur des entretiens téléphoniques avec 258 responsables opérationnels et directeurs informatiques, au cours des mois de juin et juillet 2008, le rapport met en évidence l'importance croissante de la gestion du risque informatique¹⁵.

¹³Robert Longeon et Jean-Luc Archimbaud ,guide de la sécurité des systèmes d'information à l'usage des directeurs, 1999, p.12.

¹⁴ IBM,« Gestion du risque informatique : la maturité et l'équilibre favorisent les performances globales », Synthèse janvier 2009, p.1.

¹⁵IBM, 2009,p.1. Op. Cit.

Dans le même sens, plus de la moitié des gestionnaires de risques interrogés indiquent que les risques informatiques sont devenus une préoccupation grandissante dans leur entreprise durant la dernière année, alors qu'ils ne sont que 8 % à déclarer l'inverse.

Selon les responsables interrogés, les principaux obstacles à une gestion efficace du risque sont une sensibilisation insuffisante ainsi que le manque de personnel formé et d'outils nécessaires pour contrer les menaces. L'association des trois grands volets de la gestion des risques permet heureusement de combler ces lacunes. Les entreprises qui ont sur équilibré leur maturité par rapport à ces trois grands domaines de la gestion du risque – au lieu de n'en développer qu'une négligeant les autres – gèrent les risques plus efficacement. Et elles affichent de meilleures performances informatiques sur plusieurs terrains¹⁶ :

- Capacité à prévenir les incidents tels que pannes et fuites d'information;
- Efficacité de l'équipe informatique ;
- Mise en adéquation des objectifs informatiques et métier ;
- Capacité d'accompagner l'évolution de l'entreprise.

Selon le Gartner¹⁷, les temps d'arrêt des systèmes informatiques peuvent coûter un million de dollars par heure aux grandes entreprises américaines. Ce chiffre peut paraître étonnant, mais si l'on tient compte de l'importance des systèmes informatiques dans les entreprises d'aujourd'hui, il n'est pas si surprenant d'apprendre qu'elles courent d'énormes risques financiers lorsque leurs systèmes informatiques ne sont plus disponibles.

Patrick Perreault a essayé de calculer le coût d'un incident à partir des éléments à considérer pour établir les pertes associées à un incident¹⁸ :

- Perte de réputation (impliquer votre équipe de marketing) ;
- Frais de campagne de marketing pour récupérer la part de marché perdu ;
- Perte de confiance de vos investisseurs (réduction de la valeur des actions) ;
- Perte de ventes (impliquer votre équipe de vente) ;
- Perte de productivité des ressources impactées par l'incident ;
- Perte d'avantages compétitifs ;

¹⁶ IBM, 2009, p.1.Op. Cit.

¹⁷ Michel Bruley, Propos Sur les SI Décisionnels, Septembre 2011, Chapitre 5 - 45/58.

¹⁸ Patrick Perreault, Le «ROI» de la Sécurité de l'information, *CISM, PCI QSA*, 15 octobre 2012, p.11.

- Frais légaux (avocats, dédommagements) (impliquer votre département légal ;
- Poursuite(s) criminelle(s) ;
- Augmentation de vos primes d'assurance ;
- Frein au développement de nouveaux projets ;
- Frais de consultation ;
- Coûts des ressources assignées à résoudre l'incident ;
- Dommage aux actifs informationnels ;

Dans le même d'ordre d'idée cadre, les entreprises dont l'approche est équilibrée ont une perception plus positive de leurs capacités de gestion des risques que celles qui ne mènent pas de front les trois types d'action. Elles sont 72 % à se déclarer efficaces dans la gestion des risques informatiques alors que ce chiffre tombe à 10 % parmi les entreprises dont l'approche est déséquilibrée. En outre, elles font état d'un meilleur taux de réussite dans la maîtrise des plus gros risques informatiques auxquels elles sont exposées¹⁹.

En revanche, le TBP permet de définir des objectifs et des indicateurs sécurité en phase avec le programme de management de la sécurité de l'information, lui-même décliné de la vision et la stratégie de l'organisation²⁰.

Dans le cadre de la relation entre la sécurité TI et la performance, la société française Hapsis²¹ a repris les concepts des BSC de Kaplan et Norton pour les décliner en une démarche de management du risques, pour conduire ce dernier à un niveau acceptable par l'organisation : c'est le tableau de bord équilibré sécurisé (TBES).

Bref, le déploiement éclairé de la stratégie et de politique de sécurité passe par la mise en place de tableaux de bord, permettant au responsable de la sécurité et au management de l'entreprise de s'assurer de la performance du système et de l'avancement des travaux qui soutiennent la vision et la stratégie de l'entreprise²².

Les résultats des efforts déployés au cours de cette section nous a permis de développer notre modèle et l'hypothèse de recherche qui sera présenté dans la section suivante.

¹⁹ IBM, janvier 2009, p.1.Op.Cit.

²⁰ Matthieu Bennasar, Alain Champenois, Patrick Arnoud, Thierry Rivat, *manager la sécurité du SI, planifier, déployer, contrôler, améliorer*, Dunod, Paris, 2007, p .118 .

²¹ Se reporter aux livres blancs de Hapsis (gestion des risques et tableaux de bord et le TBES au centre de la stratégie sécurité).

²² Matthieu Bennasar, Alain Champenois, Patrick Arnoud, Thierry Rivat, « manager la sécurité du SI, planifier, déployer, contrôler, améliorer », Edition DUNOD, paris, 2007, p .118 .

4. Construction de l'hypothèse de recherche et du modèle conceptuel

Dans un premier temps, nous allons présenter l'hypothèse de recherche en se basant sur les soubassements théoriques et les études des spécialistes. Ensuite, nous proposerons notre modèle de recherche.

4.1 Hypothèse de recherche

Depuis plus de dix ans, pour mesurer l'impact de gestions des risques liés aux systèmes de l'information sur la performance des organisations est un travail complexe et coûteux.

D'après plusieurs études ont été réalisées pour clarifier la relation positive entre la bonne gestion risques SI et la performance organisationnelle. Dans le but d'évaluer cette relation nous retenons l'hypothèse de la recherche suivante : **le niveau atteint en matière de performance organisationnelle est lié à la bonne gestion risques SI.**

Etant donné que le domaine de la gestion des risques, auquel nous nous intéressons, est assez connu, on va opter pour la méthode déductive.

En effet, il existe des études qui a constitué la source principale de notre hypothèse qui sera testée dans le but de vérifier leur validité, que nous avons privilégié hypothético-déductive.

Dans notre cas, on peut représenter nos variables de la recherche comme le suivant :

- La variable explicative (Indépendante): la gestion des risques SI ;
- La variable à expliquer (Dépendante) : la performance organisationnelle.

4.2 Modèle de recherche

La construction de notre modèle de recherche relève d'un état de l'art centré sur les travaux de la gestion des risques des systèmes d'information.

En effet, pour établir les relations entre nos variables, nous avons dressé un modèle conceptuel. Ce modèle présente un variable dépendant (la performance organisationnelle) et un variable indépendant (la gestion des risques SI), le point suivant traitera l'analyse empirique de notre étude.

5. Etude empiriques

L'enquête de notre recherche s'est déroulée entre début février 2014 et fin avril 2014 et a porté sur 140 organisations publiques avec un taux de réponse qui se situe à 42%. Ce taux est important pour ce type de questionnaire non obligatoire et relativement long. Pour faire notre étude nous avons utilisé un questionnaire.

Nous allons aborder d'abord l'analyse descriptive, puis l'analyse exploratoire (ACP et ACM) et enfin l'analyse confirmatoire.

5.1 Etude descriptive des données

Pour la plupart des organisations (93,1%) sont exposés aux risques liés au SI dans leurs organisations, ce qui est évident dans un environnement turbulent et vulnérable.

En ce qui concerne l'existence d'un responsable sécurité, on voit que la situation actuelle des organisations enquêtées vis à vis aux risques, les responsables sont conscients de ce problème qui touche la majorité des organisations, du ce fait un taux de 61,7% des organisations ont un responsable sécurité SI.

Du fait de l'omniprésence de l'informatique dans toutes des activités des organisations, il va sans dire que les risques auxquels s'expose une organisation découle de ceux liés à l'informatique et à l'infrastructure physique associée. Les hauts dirigeants des entreprises sont de plus en plus conscients de la nécessité d'une meilleure gestion du risque informatique. Selon l'étude « IT Governance Global Status Report-2008 » menée par l'ITGI (IT Governance Institute), 62% des PDG et des DSI interrogés ont pris, en 2007, des mesures destinées à améliorer la gestion des risques, contre 45% en 2005 et 18% en 2003²³.

Pour l'utilisation des méthodes de risque, on constate que d'après les résultats de l'enquête, seulement 35,6% des organisations utilisent des méthodes de gestion de risques. Pour le moment, 41,4% des organisations ont une norme de sécurité de SI.

Selon l'enquête, on constate que 46,6% des organisations interrogées confirment avoir une politique de sécurité de SI « PSSI ».

²³ IT Governance Institute, IT Governance Global Status, report 2008. www.itgi.org. La synthèse « IT Governance Global Status Report – 2008 » est basée sur une enquête internationale menée auprès de DSI et de PDG par Price water house Coopers pour l'IT Governance Institute (www.itgi.org).

En outre, 62,1% des organisations enquêtées ont une charte d'informatique, alors que 37,9 % de ces organisations n'ont pas cette charte. En plus un taux de 69% de ces organisations ont une charte formalisée contre 31% non formalisé.

Dans le même contexte, un taux de 82,8% des organisations sont partagés des risques SI avec la direction générale.

Nous constatons que 50% des organisations appliquent la loi 0908. De même seul 50,8% des organisations utilisent la politique de sécurité qui est aligné avec le processus métier pour positionner leur organisation par rapport à la sécurité. Alors, 29,5% utilisent la sécurité qui prend en compte les aspects humains et 21,3% utilisent la sécurité qui est aligné sur les standards d'organisation ISO2700X, ITIL, COBIT, etc.

Selon les résultats de l'enquête, la totalité des organisations 100% jugent que la gestion des risques améliore la performance organisationnelle. Le point suivant sera consacré à l'analyse exploratoire des données.

5.2 Analyse exploratoire des données

Dans le cadre de notre recherche, nous traiterons l'analyse exploratoire en deux phases : d'une part une analyse en composantes principales sans rotation et avec rotation et d'autre part une analyse en composantes multiples.

5.2.1 Analyse composantes principales (ACP)

- **ACP avec pour variables actives les Items de la quatrième variable latente « Gestion Risque SI »**

Nous pouvons remarquer d'après les résultats présentés ci-dessous ; le premier axe explique 35,74% de la variance totale et est fortement lié aux variables relatives aux normes de sécurité SI (Item), aux moyens utilisés pour assurer la continuité(Item), avec une politique de sécurité formalisée(Item), grâce aux démarches mises en œuvre telle que la loi 0908(Item) et le positionnement de l'organisation par rapport à la sécurité(Item). Le deuxième axe explique 13,21% de la variance totale.

Tableau 1 : Variance Totale Expliquée

Composante	Valeur propre initiale	Extraction Sommes des carrés des facteurs retenus
------------	------------------------	---

	Total	% de la variance	Cumulés %	Total	% de la variance	Cumulés %
1	3,574	35,743	35,743	3,574	35,743	35,743
2	1,322	13,218	48,961	1,322	13,218	48,961
3	1,180	11,796	60,757	1,180	11,796	60,757
4	1,070	10,698	71,455	1,070	10,698	71,455
5	,894	8,943	80,399			
6	,538	5,380	85,779			
7	,489	4,892	90,671			
8	,445	4,447	95,118			
9	,276	2,758	97,876			
10	,212	2,124	100,000			
Méthode d'extraction : Analyse en composante principale						

Tableau 2 : Matrice des composantes

	Composante			
	1	2	3	4
34	,186	-,775	,390	,186
35	,692	,212	-,456	-,289
36	,671	,044	-,317	,013
38	,715	-,369	-,130	,165
40	,701	-,259	-,330	,294
42	,803	,074	,233	-,200
43	,694	,144	,148	,132
44	,561	,063	,638	-,184
46	,409	,521	,323	-,013
49	,013	,413	,077	,864

Les Items 34 ; 43 ; 44 ; 46 et 49 ne présentent pas un fort degré de cohérence avec les autres items (sur l'axe1) et par conséquent, ils seront éliminés pour améliorer les résultats de l'analyse.

Par contre, les items 35 et 36 seront gardés à cause de leur importance pour la suite de l'analyse.

- ***ACP avec pour variables actives les Items de la quatrième variable latente « Gestion Risque SI » (Après Itération)***

Nous pouvons remarquer dans le tableau ci-dessous que le premier axe explique 58,77% de la variance totale.

Tableau3: Variance totale expliquée

Composante	Valeurs propres initiales			Extraction Sums of Squared Loadings		
	Total	% de la variance	Cumulés %	Total	% de la variance	Cumulés %
1	2,939	58,777	58,777	2,939	58,777	58,777
2	,783	15,654	74,431			
3	,497	9,934	84,365			
4	,400	8,008	92,373			
5	,381	7,627	100,000			
Méthode d'extraction: Analyse en composante principale						

Test de Validité :

Le test de signification de Bartlett est inférieur à 0.05 ce qui nous permet de rejeter l'hypothèse nulle selon laquelle nos données proviendraient d'une population où la matrice de corrélation serait une matrice d'identité.

L'indice KMO est égale à 0.7 ce qui valide notre Analyse factorielle.

Tableau4: Indice KMO et Test de Bartlett

Mesure de précision de l'échantillonnage de Kaiser-Meyer-Olkin		,768
Test de sphéricité de Bartlett	Khi-deux approximé	73,495
	Ddl	21
	Signification de Bartlett	,000

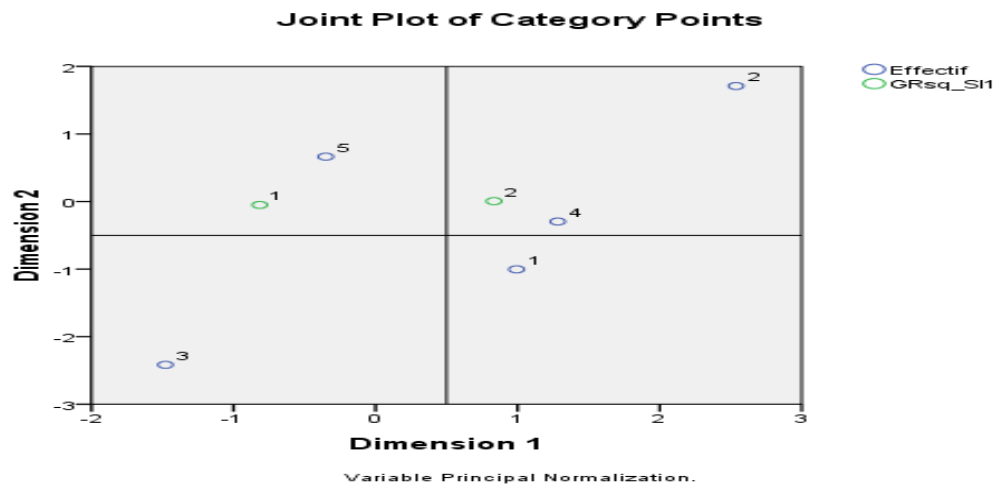
Tableau5: Fiabilité Statistique

Cronbach's Alpha	N of Items
,799	7

Alpha de Cronbach est égal à 0,7 ; le test statistique est fiable.

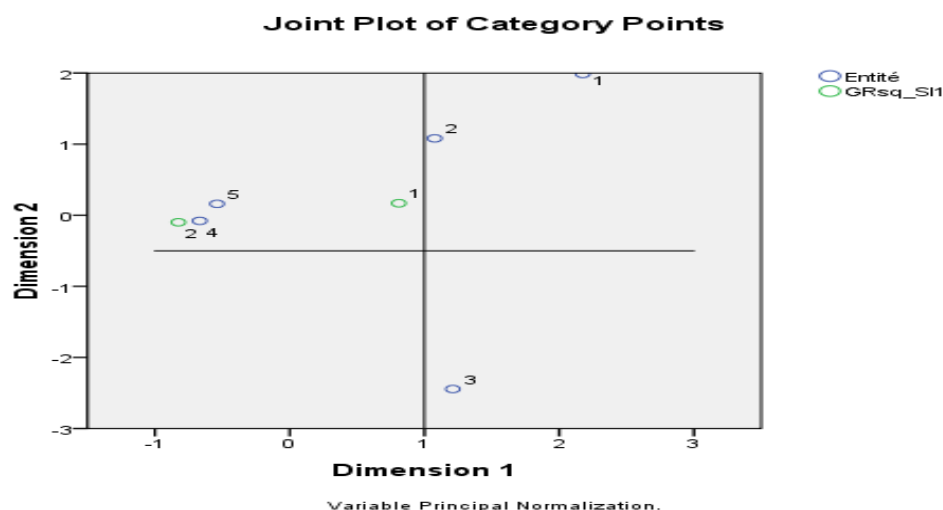
5.2.2 Analyse en correspondance multiple (ACM)

Figure 1: Gestion de risque du système d'information et Effectif



Le diagramme ci-dessus donne le résultat de l'analyse en correspondance multiple entre les variables latentes Gestion de risque du système d'information et la variable nominale Effectif. Nous pouvons remarquer ici que l'intersection des deux axes regroupe dans le même segment les organisations ayant un niveau élevé de Gestion de risque et les Entreprises ayant une grande taille (proximité entre les points 2 et 4). On peut ainsi dire que la majorité des organisations ayant un niveau de Gestion de risque élevée sont les organisations ayant une grande taille.

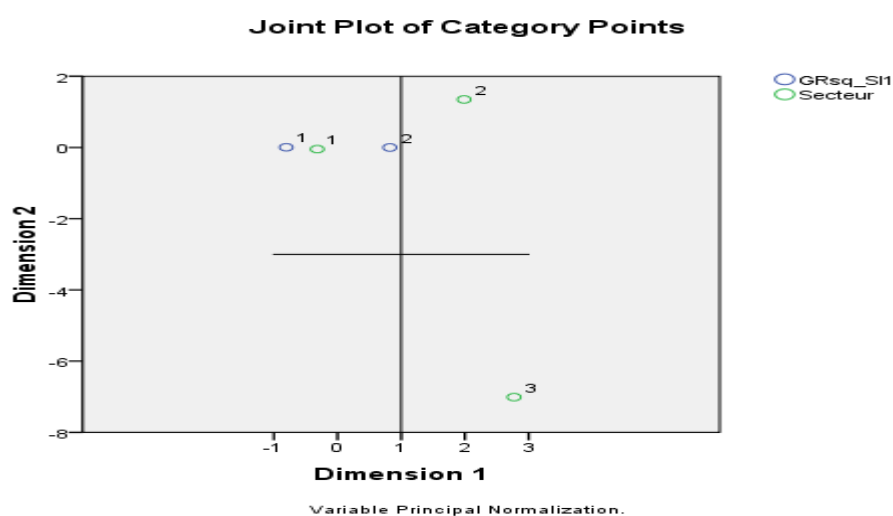
Figure 2 : Gestion de risque du système d'information et Entité



Le diagramme ci-dessus donne le résultat de l'analyse en correspondance multiple entre les variables latentes gestion de risque du système d'information et la variable nominale entité.

Nous pouvons remarquer ici que l'intersection des deux axes regroupe dans le même segment les organisations ayant un niveau élevé de gestion de Risque et les organisations s'ayant comme entité « service informatique » (proximité entre les points 2 et 5). On peut ainsi dire que la majorité des organisations ayant un niveau de Gestion de risque élevée sont les organisations ayant comme entité « un service informatique ».

Figure 3 : Gestion de risque du système d'information et Secteur



Le diagramme ci-dessus donne le résultat de l'analyse en correspondance multiple entre les variables latentes gestion de risque du système d'information et la variable nominale Secteur.

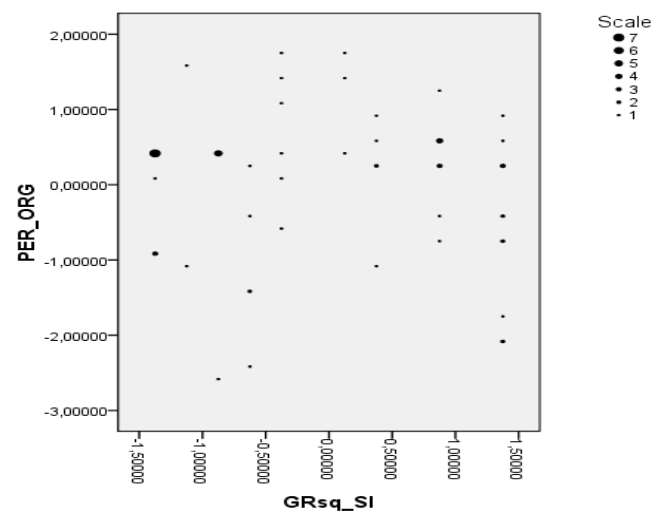
Nous pouvons remarquer ici que l'intersection des deux axes regroupe dans le même segment les organisations ayant un niveau élevé de Gestion de Risque et les organisations exerçant dans le secteur public (proximité entre les points 2 et 2). On peut ainsi dire que la majorité des organisations ayant un niveau de gestion de risque élevée sont les organisations exerçant dans le secteur public.

5.3 Analyse confirmatoire

Nous pouvons remarquer dans le graphique ci-dessous que les nuages de points relatifs aux variables performance organisationnelle et la gestion des risques du système d'information évoluent de façon décroissante de la droite vers la gauche, ce qui signifie l'existence d'une relation positive entre ces 2 variables. Autrement dit une évolution de la gestion des risques

du système d'information n'entraîne pas forcément une évolution de la performance organisationnelle.

Figure 4 : L'analyse ANOVA



L'analyse ANOVA relative à ces deux variables ci-dessous nous permet de remarquer que cet impact n'est pas significatif ((Sig.<0.05).

Tableau6: ANOVA

GRsq_SI					
	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	31,676	32	,990	,978	,528
Within Groups	27,324	27	1,012		
Total	59,000	59			

En somme, nous pouvons dire que l'hypothèse selon laquelle le degré de gestion des risques du système informatique a un impact positif sur la performance organisationnelle est vérifiée. Néanmoins, cet impact n'est pas statistiquement très significatif (c'est-à-dire qu'une évolution du niveau de gestion de risque du système informatique n'entraîne pas à elle seule une augmentation de la performance organisationnelle).

Conclusion

La gestion des risques SI, avant qu'elle soit une question technique, elle est une question de comportement et de culture. La communication et la compréhension de la politique de sécurité est une condition nécessaire pour réussir sa mise en place.

Dans ce travail de recherche, nous avons cherché, mieux expliquer la manière dont la gestion des risques SI pourraient contribuer à la performance au sein des organisations publiques au Maroc.

La question de la sécurité SI reste toujours central dans les recherches relatives à la gestion des risques SI, nous a conduits également à mener, au préalable, une analyse descriptive puis une analyse exploratoire visant à accroître la validité de nos résultats.

D'après les résultats issus de l'analyse descriptive, on peut constater le rôle l'importance de la gestion des risques SI comme l'un des préoccupations pour les responsables SI et également le rôle de la gestion des risques SI dans la performance des organisations. En effet, l'analyse exploratoire confirme cette relation significative entre la gestion des risques SI et la performance des organisations.

Au niveau de l'analyse descriptive, selon les résultats de l'enquête, la totalité des organisations 100% jugent que la gestion des risques améliore la performance organisationnelle

Au niveau de l'analyse confirmatoire, on présente dans le tableau suivant les résultats synthétiques de notre travail de recherche :

Hypothèse	Tests et outils statistiques utilisés	observations
La Gestion des Risques du Système d'information a un impact positif sur la performance Organisationnelle	Nuages de points : existence d'une relation linéaire positive Test ANOVA : non significatif	Validée

Bibliographie

- Ahmed BOUNFOUR & Georges EPINETTE, valeur et performance des SI, Dunod, Paris, 2006.
- Alexandre Fernandez-Toro, management de la sécurité de l'information, implémentation l'ISO 27002, 2ème édition Eyrolles, 2009.
- CIGREF, analyse et gestion des risques dans les grandes entreprises, impacts et rôle pour la DSI, 2007.
- Dominique. M et Fabrice Garnier de Labareyre, Cobit, Pour une meilleure gouvernance des systèmes d'information, Eyrolles, Paris, 2009.
- Directive n° 96/82 du Conseil de l'Europe du 9 décembre 1996 concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses.
- Frédéric Géorel, IT gouvernance : maîtrise d'un système d'information, Dunod, Paris, 2005.
- Jacqueline Sidi, Martine Otter et Laurent Hanaud, guide des certifications SI, comparatif, analyse et tendances ITIL, COBIT, ISO 27001, eSCM ... ,Dunod, paris 2006.
- Michel Bruley, Propos Sur les SI Décisionnels, Septembre 2011, Chapitre 5 - 45/58.
- Matthieu Bennasar, Alain Champenois, Patrick Arnoud, Thierry Rivat, manager la sécurité du SI, planifier, déployer, contrôler, améliorer, Edition DUNOD, Paris, 2007.
- OHSAS ou Occupational Health and Safety Assessment, certification qui précise les règles pour la gestion de la santé et la sécurité dans le monde du travail. Elle a une valeur internationale.
- Patrick Perreault, Le «ROI» de la Sécurité de l'information, CISM, PCI QSA ,15 octobre 2012.
- ISO/IEC Guide 73:2002, Risk management – Vocabulary – Guidelines for use in standards.
- IBM, « Méthodologie de gestion du risque informatique pour les Directeurs des Systèmes d'Information : un levier exceptionnel de création de valeur et de croissance », Septembre 2008.
- IT Governance Institute, IT Governance Global Status, report 2008. www.itgi.org.

- Robert Longeon et Jean-Luc Archimbaud, guide de la sécurité des systèmes d'information à l'usage des directeurs, 1999.
- Synthèse, «IT Governance Global Status Report – 2008» est basée sur une enquête internationale menée auprès de DSI et de PDG par Price water house Coopers pour l'IT Governance Institute (www.itgi.org).
- Synthèse, « Gestion du risque informatique : la maturité et l'équilibre favorisent les performances globales », janvier 2009.