RM et RSSI :

(RISK-MANAGER et RESPONSABLE SÉCURITÉ DU SYSTÈME D'INFORMATION)

Deux métiers s'unissent pour la gestion des risques liés au Système d'Information

Juin 2006

Groupe de travail collaboratif AMRAE – CLUSIF

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

30, rue Pierre Sémard, 75009 PARIS - Tél. : +33 153 25 08 80 – Fax : +33 1 53 25 08 88

clusif@clusif.asso.fr - http://www.clusif.asso.fr

ASSOCIATION POUR LE MANAGEMENT DES RISQUES ET DES ASSURANCES EN ENTREPRISE

9/ 11 Av. F. Roosevelt, 75008 PARIS - Tél +33 142 89 33 16 - Fax +33 1 42 89 33 14

amrae@amrae.fr - www.amrae.fr

TABLE DES MATIÈRES

REMERCIEMENTS

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Les deux co-animateurs du GT :

Gilbert	***BRAT***	*LA POSTE*	*AMRAE*
Annie	***DUPONT***	*JAA*	*CLUSIF*

Les animateurs des sous-groupes :

"Attentes et Apports"

Annick	***BAILLY***	*LA POSTE*	*AMRAE*
Jacques	***SIBUE***	*RENAULT*	*AMRAE*

"Cartographie"

Pascal	***RICHARD***	*SOCIÉTÉ GÉNÉRALE*	*AMRAE*
Luc	***VIGNANCOUR***	*MARSH*	*CLUSIF*

et "Glossaire"

Gérard	***MOLINES***	*MOLINES CONSULTANTS*	*CLUSIF*

Ainsi que les membres actifs qui ont participé à l'écriture de cet ouvrage

Xavier	***BERNAERT***	*LVMH*	*AMRAE*
Olivier	***MANGEOT***	*CETELEM*	*CLUSIF*
Jean-Michel	***OLOA***	*ACE*	*CLUSIF*
Morgane	***POURCHET***	*LA POSTE*	
Delphine	***PRAMOTON***	*ERNST & YOUNG AUDIT*	*CLUSIF*
Christine	***PUYHARDY***	*PW CONSULTANTS*	*AMRAE*
Patrick	***SURY***	*GIB MANAGEMENT SERVICES SA*	*CLUSIF*
Leslie	***VALVERDE***	*CCF*	*AMRAE*
Philippe	***VELARD***	*MARSH*	*CLUSIF*

1 RM – RSSI : DEUX FONCTIONS COMPLEMENTAIRES

1.1 Introduction

Il n'existe pas une définition pour chacune des *fonctions*[1] RM (**R**isk - **M**anager) et *RSSI* (**R**esponsable **S**écurité du ***S**ystème d'**I**nformation*) mais des définitions différentes selon le secteur d'activité de l'entreprise, sa culture et son organisation. De même il n'existe pas toujours d'affectation de ces fonctions dans les entreprises. Cependant ce document est focalisé sur la présence et l'interaction des deux fonctions. Les cas d'inexistence de l'une ou l'autre ne sont traités que ponctuellement, néanmoins les thèmes abordés sont exploitables.

Par ailleurs la création et l'évolution de ces fonctions s'étant réalisées historiquement indépendamment l'une de l'autre, leur complémentarité, même si elle relève du bon sens, reste le plus souvent à définir et à organiser.

En l'absence de communication suffisante, il est par exemple possible de voir souscrire (par le RSSI ou la DSI), dans le cadre d'un contrat de secours, une assurance spécifique pour les frais occasionnés par le déclenchement d'un *back up* alors que ce genre d'assurance a peut-être déjà été souscrit par l'Entreprise. L'absence d'interaction suffisante entre ces fonctions peut générer ainsi des surcoûts inutiles puisque la société assurée ne pourra être indemnisée qu'une seule fois pour un même sinistre.

Dans les faits le RM et le RSSI se rejoignent sur la gestion des *risques* liés au Système d'Information et notamment sur le respect de quatre axiomes à savoir la *disponibilité*, l'*intégrité* des *données*, leur *confidentialité* et la *traçabilité* des opérations permettant la preuve de l'échange ou du traitement de données. Si l'un de ces quatre éléments est altéré ou inadapté, il y a risque pour l'entreprise comme pour ses clients. Au même titre il y a des risques si les moyens mis en œuvre ne respectent pas les engagements pris avec les clients ou les exigences réglementaires et juridiques.

Les risques liés au Système d'Information (SI) sont parfois complexes à identifier et à gérer. Ils nécessitent d'intervenir dès la phase de développement des projets, de mettre en place des *méthodes* et de disposer d'expertises spécifiques au métier, à la réglementation, aux architectures des SI et aux technologies mises en œuvre. Pour que ces risques soient maîtrisés dans l'entreprise le RM et le RSSI doivent contribuer l'un et l'autre, à leur niveau et de manière complémentaire :

- à la définition des méthodes d'identification et d'évaluation des risques,
- aux solutions de maîtrise de risques à mettre en place (parades, moyens de contrôle, moyens de réaction et solutions de *financement des risques* résiduels).

[1] Les termes en italique sont définis dans le glossaire en fin de document.

1.2 La fonction RM

1.2.1 Rôle

D'origine anglo-saxonne, ce métier s'implante progressivement en France depuis les années 70, notamment dans les activités industrielles à hauts risques : chimie, pétrole, spatial, poudres et explosifs, etc. Selon l'AMRAE (Association pour le management des risques et des assurances de l'entreprise), environ 350 cadres l'exercent aujourd'hui à plein temps dans de grandes entreprises. Parallèlement, on assiste depuis peu au développement de consultants indépendants spécialisés dans l'audit d'assurances auprès des PME/PMI.

Généralement, le Risk Manager gère la politique et le plan d'assurance de l'entreprise. Selon les cas il éclaire la Direction Générale sur les risques majeurs encourus (risques stratégiques et opérationnels, potentiels et avérés), leur niveau de maîtrise et la façon dont sont traités les risques résiduels (solutions de financement sur fonds propres, par recours à l'assurance ou autres solutions alternatives de financement des risques).

Dans certaines entreprises, il est le moteur des dynamiques d'analyse globale des risques (l'ensemble des risques opérationnels de toutes les activités) et d'accompagnement des dispositifs de maîtrise des risques ainsi identifiés en *prévention*, détection, réaction (démarches couplées, voire confondues avec le renforcement généralisé du contrôle interne). La tendance observée est celle d'une complémentarité des rôles entre Risk – Manager et Directions Opérationnelles à qui il revient d'identifier, d'évaluer et de classer par ordre de priorité les risques sur la base d'éléments normatifs et méthodologiques (matrices de cotation, typologie, etc.) établis par le RM (en étroite collaboration avec les métiers opérationnels).

Dans le secteur bancaire par exemple, le nouvel accord dit de Bâle 2 sur la gestion des risques opérationnels offre des éléments de cadrage particulièrement pertinents.

1.2.2 Objectifs

Les principaux *objectifs* du Risk Manager sont les suivants :

Concevoir les méthodes et outils de gestion des risques

Le RM participe à la définition des méthodes et outils de *cartographie des risques*. Au-delà, il doit convaincre la Direction Générale de mettre en place un processus de gestion des risques dans l'entreprise et décliner de façon opérationnelle ce processus avec les différents acteurs Directions Opérationnelles en charge de la gestion des risques.

Élaborer et mettre en œuvre la politique et le plan d'assurance de l'entreprise En matière de traitement des risques le Risk Manager intervient sur les risques résiduels forts en intensité dont la potentialité d'apparition est faible, c'est-à-dire sur les risques majeurs pour lesquels des mesures de prévention, détection, réaction existent et/ou ont été décidées. Pour ces risques, il négocie et gère les couvertures financières et les assurances ou élabore des solutions alternatives de financement du risque. Pour ce faire, il lui faut trouver le bon équilibre entre les capacités de *rétention* de l'entreprise et les avantages procurés par le marché de l'assurance. Il sollicite dans ce contexte des courtiers et des agents généraux pour mettre au point des garanties spécifiques et trouver les meilleurs tarifs.

Conseiller les métiers sur les mesures de prévention, *protection*, détection, réaction d'un risque

Le RM intervient également en tant qu'expert pour conseiller les métiers sur les mesures de prévention, protection, détection, réaction à mettre en place avant d'élaborer des solutions de financement du risque. Il peut, par exemple, prescrire l'installation d'un système de protection pour lutter contre le piratage informatique ou encore l'ajout d'une clause sur un contrat

commercial. Il contribue ainsi à l'élaboration des moyens de prévention et de contrôle vis-à-vis des risques identifiés en étroite collaboration avec les pôles de compétence concernés.
Participer à la diffusion de la culture "risques" dans l'entreprise
Dans le cadre des actions citées précédemment, il élabore des supports de formation et participe à la diffusion de la culture « risques » dans l'entreprise.
Il participe par ailleurs aux démarches globales de sensibilisation des collaborateurs aux risques de l'entreprise et en les impliquant dans la mise en œuvre quotidienne des systèmes de prévention ainsi que dans la remontée des informations.

Communiquer sur les risques avec la Direction Générale
Les objectifs cités l'amènent à avoir une vision globale des risques de l'entreprise qui lui permet :

- D'identifier les risques majeurs.
- De faire émerger et d'évaluer les risques transverses.
- De fournir une vision de la cartographie des risques résiduels.

1.2.3 Activités

Pour réaliser ses objectifs, le Risk Manager va notamment avoir à :

Maintenir des réseaux de veille et d'alerte
Rester vigilant en mettant en place des réseaux de contacts et d'information, pour tout ce qui concerne l'apparition de nouveaux risques, et l'évolution des techniques de prévention, protection et financement.

Convaincre, fédérer le milieu professionnel
Rester en contact avec le milieu professionnel, afin de bénéficier d'un effet de groupe pour disposer d'une capacité de négociation.

Gérer les incidents et les crises
Mettre en place des systèmes de réaction souple, afin d'éviter la transformation d'incidents en crise.
Le RM doit développer des méthodologies et des outils de *gestion de crise* adaptés et élaborer et développer les outils nécessaires pour proposer des plans de continuité d'activité. Il assiste et conseille la direction générale dans la prise de décision en analysant les composantes d'une situation de crise et ses répercussions. Il assure une veille évènementielle et garantit la mise en place de bonnes pratiques en matière de gestion de crises et de continuité d'activité.

Proposer une Politique de Gestion Globale des Risques
Concilier les différents objectifs, moyens et contraintes afin de déboucher sur des politiques de gestion des risques cohérentes et efficaces.

Négocier des contrats d'assurance
Mettre à profit l'effet de masse du groupe, pour contrôler les prestations et réduire les coûts.

Développer le bon usage des techniques et méthodes
Faire des choix et fédérer les acteurs face au foisonnement des techniques et méthodes proposées. Il diffuse ainsi l'expertise groupe, par l'intermédiaire d'actions de communication et de formation.

Optimiser l'impact global du risque
Activité majeure dans la mesure où les différents coûts sont étroitement liés :

- coûts des mesures de prévention et protection,

- coûts des assurances,
- coûts des pertes résiduelles,
- coûts de gestion de ces différents postes.

Gérer les flux financiers
Arbitrer entre les différents moyens de couverture financière des risques

Diffuser la culture du risque
L'objectif est de développer une solide compréhension en matière de Gestion des Risques, à tous les niveaux.

1.2.4 Positionnement

Idéalement, le Risk Manager doit être rattaché à la Direction Générale.

Dans les faits, il est le plus fréquemment rattaché à la Direction Financière ou à la Direction Juridique.

1.2.5 Expertise et compétences

Le Risk Manager se trouve confronté à différents types de difficultés dans l'entreprise liés à l'organisation, à des *enjeux* de pouvoir ou à une culture du risque insuffisante que son expertise, sa compétence et son efficacité doivent lui permettre de surmonter. Il doit aussi faire preuve d'esprit de synthèse et de conviction pour communiquer efficacement sur les risques de l'entreprise aussi bien en Direction Générale qu'avec l'ensemble des acteurs en charge de la gestion des risques de l'entreprise. Au-delà, il doit apporter à ses interlocuteurs dans l'entreprise (Métier, RSSI, Audit, etc.) et hors de l'entreprise (Courtiers, Assureurs) une valeur ajoutée en matière de traitement des risques visant à préserver à court, moyen et long terme, les marges de rentabilité acquises par l'entreprise.

1.2.6 Tendances

À l'origine, la fonction du Risk Manager était centrée sur le financement des risques par le transfert à l'assurance. Elle s'est progressivement étendue à la *prévention des risques* (en particulier dans le domaine de la sûreté de fonctionnement et en matière de plans de continuité d'activité), et à l'évaluation des risques résiduels.

Toutes les entreprises ne disposent pas aujourd'hui d'un gestionnaire de risques.

Cette fonction existe en général dans les grands groupes, au sein desquels il est primordial d'adopter une politique globale et commune de gestion des risques pour garantir une cohérence des actions et aussi minimiser les coûts.

Les PME/PMI ont, d'une part, plus de mal à s'offrir les services d'un Risk Manager à plein temps, et d'autre part elles n'en voient pas toujours l'utilité.

Fréquemment, elles confient à l'un de leurs responsables (le plus souvent le Directeur Financier), la mission de gérer les risques de l'entreprise, c'est à dire de protéger l'ensemble du patrimoine (matériel, intellectuel et humain) ou faire appel à un consultant externe en management de risques.

Ce type de mission consisterait :

d'une part, à effectuer une prestation en amont de l'assurance, à savoir :

- étudier et analyser en profondeur l'activité de l'entreprise afin de détecter les risques névralgiques de celle-ci,

- proposer des solutions alternatives à l'assurance,
- déterminer les risques à assurer.

d'autre part, à effectuer diverses prestations d'assistance aux choix et à la gestion des contrats d'assurances :

- rédaction des cahiers des charges assurances en collaboration étroite avec l'entreprise (type de contrat),
- négociation des contrats d'assurances avec les courtiers et les assureurs en optimisant notamment les garanties, les *franchises* et les *primes*.
- gestion courante pour le compte de l'entreprise :
  - gestion des sinistres *dommages* : assurés ou non,
  - gestion des recours responsabilité civile : assurés ou non,
  - suivi des contrats.

L'absence de Risk Manager ne signifie pas que l'entreprise ne gère pas ses risques. Il existe toujours une gestion des risques même si elle est empirique, généralement réalisée par chaque direction fonctionnelle. Dans ce cas, le plus souvent, il n'existe pas de méthodes formelles et, quand elles existent, elles ne sont généralement pas harmonisées.

1.3 La fonction RSSI

1.3.1 Rôle

Selon le CIGREF : Le RSSI « assure un rôle de conseil, d'assistance, d'information, d'alerte et de préconisation. Il peut intervenir directement sur tout ou partie des systèmes informatiques et télécoms de son entité. Il effectue un travail de veille technologique et réglementaire sur son domaine et propose des évolutions qu'il juge nécessaires pour garantir la *sécurité* logique et physique du système d'information dans son ensemble. Il est l'interface reconnue des exploitants et des chefs de projets mais aussi des experts et des intervenants extérieurs pour les problématiques de sécurité de tout ou partie du SI. ».

Dans les faits son rôle va au-delà de la définition du CIGREF, les responsabilités qui lui sont confiées s'étendent plus globalement à l'identification et à la gestion des risques liés au Système d'Information (SI) dans son ensemble c'est-à-dire de tous les risques :

- *induit*s par des défauts de sécurité des moyens mis en œuvre (défauts en termes de Disponibilité, d'Intégrité, de Confidentialité, de Traçabilité des actifs et des traitements) qu'ils soient organisationnels ou techniques,
- ainsi que ceux liés aux contraintes imposées par les engagements contractuels pris avec les clients ou par les exigences réglementaires et juridiques pour l'activité.

Il assure dans ce contexte une fonction transverse de manager :

- en rassemblant de nombreux contributeurs (à la Stratégie, aux Ressources Humaines, à la Communication, au Juridique, à la Sûreté des Biens et des Personnes, au Contrôle Interne, à l'Audit, etc.)

- en dialoguant avec les Directions Métiers (MOA) et la Direction des Systèmes d'Information (MOE –Etudes et Production-) sur les objectifs de sécurité à définir, les référentiels de sécurité à appliquer, les parades à mettre en place,

- en participant la relation Fournisseur et notamment en définissant les exigences attendues en matière de sécurité.

Face à la complexité accrue des systèmes d'information et des technologies de l'information utilisées, face au développement des exigences réglementaires et face à la démultiplication des prestations d'infogérance et d'externalisation, le RSSI est obligé de considérer le système de sécurité dans sa globalité. Pour ce faire, il doit s'entourer d'experts techniques (système, réseaux, développements, juristes, etc.) afin de traiter tous les aspects inhérents à la gestion opérationnelle des risques sous sa responsabilité.

En tant que pilote de la gestion des risques liés aux SI et de façon à distinguer la MOA Sécurité de la MOE Sécurité, le RSSI se voit, de plus en plus souvent, dégagé de la mise en œuvre opérationnelle des actions de sécurité.

En revanche plus que jamais sa fonction rend indispensable son implication directe dans la définition et la gestion des actions de sécurisation des SI au travers des différentes phases du processus de gestion des risques (de l'*identification des risques* en passant par la préconisation des plans d'actions de réduction et de contrôle, jusqu'à l'évaluation de l'adéquation des contre-mesures mises en place).

1.3.2 Objectifs

Les principaux objectifs du RSSI sont les suivants :

- Prévenir les risques dès les phases de développement des projets.

  Conseiller en amont les maîtres d'ouvrage et les maîtres d'œuvre sur tous les nouveaux projets en intégrant une dimension sécurité.Identifier et évaluer les risques en production.

  En suivant une méthode d'analyse des risques et de leurs impacts, le RSSI identifie les seuils et les natures des risques inhérents à la production du système d'information.

- Proposer des plans d'actions de réduction et de contrôle des risques.

  En fonction de l'évaluation précédemment réalisée et des contraintes de l'Entreprise, le RSSI présente les moyens à mettre en œuvre pour garantir un niveau de risque acceptable et accepté par l'Entreprise.

- Obtenir les décisions vis-à-vis des plans d'actions.

- Suivre la mise en place des plans d'actions décidés.

  Le RSSI vérifie que les solutions mises en œuvre pour réduire le niveau de risque, répondent aux contraintes sécuritaires et soient conformes aux cahiers des charges.

- Vérifier la pertinence et l'adéquation *des mesures de sécurité* dans le temps et dans l'espace.

  Afin de garantir l'efficacité des mesures préventives face à une évolution fonctionnelle et/ou technique permanente du système d'information, le RSSI vérifie le niveau de sécurité : contrôle des sauvegardes, tests d'intrusion, robustesse des mots de passe…

- Rendre compte à la Direction Générale et communiquer sur la sécurité du SI avec le ou les Directeurs en charge des Systèmes d'Information.

- Sensibiliser les équipes à la sécurité du système d'information.

  Au sein de l'Entreprise, le RSSI apporte conseil et soutien auprès des différents acteurs. Il sensibilise la Direction Générale et tous les utilisateurs aux aspects sécurités de l'information : animation de réunion, formation, action de communication …

1.3.3 Activités

Pour réaliser ses objectifs, le RSSI va notamment avoir à :

- Définir et proposer la politique de sécurité du SI pour la faire approuver par la Direction Générale

  Le RSSI définit les grands principes de gestion de la sécurité du SI au sein de l'entreprise. Pour ce faire, un document de politique générale est rédigé, validé par la Direction Générale et communiquer à l'ensemble des collaborateurs via les Ressources Humaines

- Définir les référentiels sécurité de l'entreprise dont ceux relatifs aux bonnes pratiques

  Le RSSI élabore tous les documents nécessaires à la création d'un référentiel sécurité : normes et standards des matériels et logiciels utilisés, procédures organisationnelles, règles de sécurité pour les différents composants du SI…

- Définir et mettre en place des bases d'incidents.

  Pour un souci d'identification et de maîtrise des risques, le RSSI veille à la mise en œuvre de bases d'incidents et de tableaux de bords. Il peut alors évaluer les nouvelles tendances des risques (menaces) ou ceux particulièrement présents sur le SI.

- Actualiser les moyens techniques et organisationnels.

  Pour prendre en compte l'évolution des risques, (cadres juridiques, réglementation, technologies,...), le RSSI s'appuie sur les moyens à sa disposition : Cartographie, base d'incidents, systèmes d'alerte...

- S'assurer de la prise en compte des contraintes de sécurité dans les projets de développement.

- Valider les exigences de sécurité dans les Cahiers des Charges des projets sensibles.

  Pour les projets qualifiés de sensibles ou stratégiques, le RSSI s'assure que la composante sécurité est bien prise en compte par les maîtrises d'ouvrage et maîtrises d'œuvre, et qu'elle respecte les normes de sécurité en vigueur.

- Mettre en place et animer des Comités de pilotage sur la sécurité du SI.

  Le comité de pilotage sur la sécurité du SI doit présenter périodiquement à la Direction de l'Entreprise l'évaluation du niveau de sécurité atteint par le SI et définir les nouveaux objectifs et moyens pour les atteindre.

- Coordonner les projets sécurité sur le terrain

L'expertise sécuritaire du RSSI permet à ce dernier de coordonner et contrôler les actions des experts techniques en charge des mises en œuvre des solutions de sécurité.

Exemple en Annexe 5.2

1.3.4 Positionnement

Dans bien des entreprises, le RSSI est aujourd'hui rattaché au Directeur des Systèmes d'Information au mieux et plus souvent au Directeur Informatique.

Pour des entreprises de taille importante l'organisation rencontrée est généralement celle d'une cellule sécurité indépendante de la production informatique.

Dans ce type d'organisation la Direction Générale délègue à un RSSI la charge de coordonner la mise en oeuvre et le contrôle de l'application de la politique sécurité du SI à tous les échelons et domaines de l'entreprise et ce sous la responsabilité hiérarchique ou non du Directeur des Systèmes d'Information. Pour ce faire, il doit s'appuyer sur des d'experts internes ou externes.

Par ailleurs des « correspondants sécurité du système d'information » (CSSI) sont nommés dans chaque direction fonctionnelle ou filiale de l'entreprise. Ils servent de relais chargés d'appliquer la stratégie mise au point au Siège.

Selon les cas, les responsabilités de sécurité sont réparties sur plusieurs domaines : la MOA, la MOE, la production, etc.

Le RSSI préside le Comité de Coordination des CSSI qui se réunit régulièrement :

- Pour faire le point sur le niveau de sécurité du SI et le respect de la Politique de Sécurité au sein de l'entreprise.
- Coordonner les plans d'actions décidés.
- Pour proposer des orientations.

Le RSSI siège au Comité Directeur Sécurité avec les directeurs fonctionnels ou des filiales pour décider des orientations proposées.

1.3.5 Expertise et compétences

Si la maîtrise de savoir-faire technologiques est un plus, le RSSI doit posséder des savoir-faire généraux primordiaux comme la compréhension de l'environnement et du fonctionnement de l'entreprise, la connaissance des Clients de la DSI de leurs activités et de leurs besoins, et des aptitudes comportementales essentielles comme la rigueur, le sens de la méthode et de la probité ainsi que des talents de communiquant et d'organisateur pour utiliser les experts techniques au service de la sécurité du système d'information.

1.3.6 Tendances

Une fonction encore orientée sécurité des systèmes informatiques : Pour rappel (cf. Enquête du journal CSO auprès de 144 entreprises) « c'est le directeur informatique, dans plus de 66 % des cas qui prend en charge la sécurité.. ». Plus loin dans le même article « la fonction sécurité est récente : seulement 17,1 % des entreprises ont créé un poste entièrement dédié à la sécurité informatique ».

Dans les grandes entreprises un dialogue utile est nécessaire avec les services métiers, les directeurs Juridique, la Conformité et la direction de l'Audit et du contrôle interne : Ces

directions se révèlent être des alliées pour justifier les investissements en sécurité auprès des directions générales.

Dans les PME, le souci de se conformer à la réglementation et d'être « aussi bien » protégée que la concurrence : Sur ce dernier point les PME jugent que la sécurité est un facteur de compétitivité et qu'il est important pour elles d'investir pour se mettre à niveau de la concurrence.

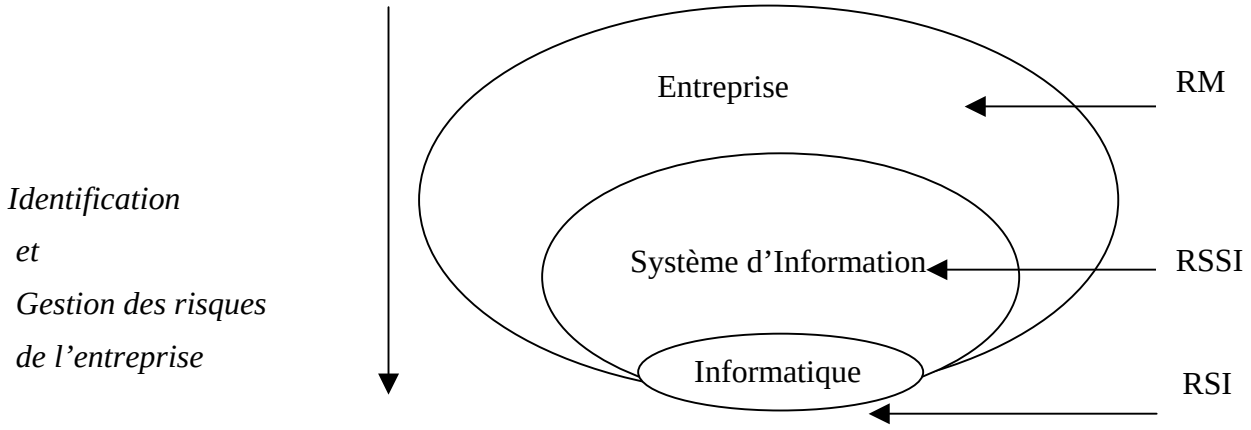
Ceci dit chaque entreprise est un cas unique qui résulte de sa culture et de son mode de management interne. De ce fait on constate aujourd'hui des écarts assez importants en terme de responsabilité et de salaire selon la taille des entreprises et le secteur d'activité.

Quoi qu'il en soit l'élément majeur est la prise en compte par les Directions Générales d'une approche globale de la gestion des risques où la fonction RSSI occupe une place importante.

1.4 Attentes et Apports

1.4.1 Complémentarités des fonctions

Périmètre :



Ce schéma illustre le périmètre des risques traités respectivement par le RM et le RSSI. Ainsi on constate que le RM a un champ d'intervention beaucoup plus large que le RSSI puisqu'il intervient sur l'ensemble des risques de l'entreprise (risques SI, risques environnementaux, risques de contrôle interne au sein des Métiers, etc.).

Points communs aux deux fonctions :

S'ils ne sont pas les seuls acteurs en charge de la gestion des risques, le RM et le RSSI sont en revanche les seuls garants de l'identification des risques liés au Système d'Information et de l'adéquation des solutions à mettre en œuvre pour :

- minimiser la *probabilité* d'occurrence du risque et son intensité du risque (prévenir) (RSSI),
- minimiser les *conséquences* du risque (détecter, réagir) (RSSI),
- financer le *risque résiduel* pour les risques forts en intensité (RM).

Le RM et le RSSI appuient leurs travaux sur une identification et une évaluation rigoureuses des risques de l'entreprise.

Le rôle du RSSI est de proposer des actions de réduction et de contrôle des risques en adéquation avec les enjeux de l'entreprise et complémentaires aux solutions de financement des risques résiduels envisageables.

En effet pour qu'elle soit efficace, la sécurité des Systèmes d'Information doit répondre de manière proportionnée à la couverture de chaque risque identifié et non accepté.

Pour apprécier l'adéquation entre le coût des mesures à mettre en œuvre et les enjeux, il a en particulier besoin d'informations sur les pertes financières encourues. Les contre-mesures décidées résultent entre autres de ce compromis.

Le RM intervient sur les risques résiduels forts en intensité dont la potentialité d'apparition est faible c'est-à-dire sur les risques majeurs pour lesquels des mesures de prévention, détection, réaction existent et/ou ont été décidées.

Il doit, sur ces bases, définir les montants à garantir et à ce titre disposer de la valorisation totale des pertes financières avec les parades existantes et après mise en place des contre-mesures décidées le cas échéant.

A ce titre, le RM et le RSSI devraient mettre en place un référentiel commun des risques ce qui est encore trop rarement le cas, chacun procédant le plus souvent selon ses propres méthodes ou critères.

Leurs travaux viennent se compléter pour maîtriser les risques non acceptés.

Le RM, qui ne dispose généralement pas d'expertise SI s'appuie sur les actions menées par le RSSI pour identifier et anticiper la maîtrise des risques (définition et mise en place de politiques de sécurité, de référentiels de sécurité, de cahier des charges spécifiques d'exigences de sécurité, etc.).

Par ailleurs le RSSI s'appuiera sur les travaux menés par le RM pour définir les priorités et le niveau des contre-mesures à mettre en place en fonction des solutions de financement des risques résiduels, envisageables.

L'absence même de ces fonctions dans certaines entreprises ou les directions différentes dont dépendent le RM et le RSSI ne permettent pas de réaliser ces travaux tant que la Direction Générale n'a pas décidé d'une approche globale de la gestion des risques incluant forcément un schéma de coordination de ces deux fonctions.

1.4.2 Attentes du RM et apports du RSSI

Un des « points durs » de la fonction RM est l'assurabilité des risques auxquels est exposée l'entreprise. D'une part tous les risques ne sont pas assurables, d'autre part compte tenu des franchises seulement une partie des risques assurables est en fait réellement assurée. Enfin l'assurabilité d'un risque n'est pas forcément identique à sa couverture réelle. Ainsi un risque peut être assuré sans être forcément totalement transféré.

Pour lever ces difficultés, le RM doit disposer des informations qui lui permettront de traiter le risque en amont et non en aval lorsqu'il s'agit de régler le préjudice.

Ces informations lui sont nécessaires pour établir un dialogue avec l'assureur à partir des référentiels de l'entreprise plutôt que des référentiels de l'assureur ou étudier des solutions de financement alternatives.

Vis-à-vis de l'assureur, il s'agit pour le RM d'établir un langage commun de façon à parvenir à la transparence recherchée pour définir des solutions d'assurance adaptées et écarter autant que faire se peut les contentieux entre l'assureur et l'assuré lors de la survenance d'un sinistre.

Ainsi pour financer un risque, l'assureur doit être en mesure :

- De comprendre le risque qu'il assure en l'absence de toutes mesures de sécurité (*impact* intrinsèque).
- D'identifier ce que l'entreprise a mis en place pour réduire l'impact et la potentialité de survenance du risque (plan d'actions de *réduction des risques* par des mesures appropriées en terme de protection, de prévention, de détection et de réaction).
- De connaître le processus de gestion des risques de l'entreprise.

Ceci dit, l'assureur ne va pas tarifer uniquement en fonction des informations qui lui seront communiquées sur le niveau de *maîtrise du risque* par l'entreprise mais aussi et surtout en fonction du marché. Autrement dit pour que le risque soit assurable, il faut non seulement en avoir évalué son impact mais aussi trouver la capacité nécessaire à son financement.

Pour le RM la difficulté rencontrée est en premier lieu de chiffrer le sinistre avéré ou potentiel. Si des bases d'incidents existent, elles restent très souvent peu voire non exploitables pour évaluer les conséquences des dysfonctionnements rencontrés. Elaborées à des fins de pilotage et de suivi de l'exploitation de l'activité notamment dans le cadre de démarches Qualité elles concentrent des informations techniques partielles quant à la description de l'incident et très rarement des informations en terme d'impact Métier (voir les études de sinistralité du CLUSIF) hormis dans le secteur bancaire.

Face à la complexité des systèmes d'information, le RM a ainsi besoin de coopérer avec le RSSI afin de connaître les méthodes de cartographie employées et pour traiter les risques résiduels sous sa responsabilité.

Sur ce premier point, les informations nécessaires au RM sont relatives :

- aux approches / méthodes employées pour identifier les risques de l'entreprise,
- aux règles / outils utilisés pour évaluer et quantifier les risques résiduels,
- au processus d'actualisation de la cartographie des risques (fréquence des analyses réalisées, processus continu d'identification des risques, etc.),
- à l'organisation mise en place pour décider et suivre les plans d'actions de réduction et de contrôle définis.

Sa participation à leur définition est indispensable pour établir une approche commune avec le RSSI en matière de gestion des risques.

Pour le traitement des risques résiduels liés au système d'information, le RM a cette fois besoin de disposer de la cartographie des risques établie par le RSSI (description des risques, de leur niveau de maîtrise) et de l'identification des moyens de prévention, détection, réaction existants et planifiés.

Les informations nécessaires au RM dans ce cadre sont les suivantes :

- description du risque,
- potentialité d'apparition / fréquence,
- intensité des risques (k€),

- criticité,
- niveau de maîtrise,
- parades mises en œuvre,
- type de risque (avéré ou potentiel),
- éléments de volumétrie caractéristiques de l'activité,
- maîtrise du risque et de son transfert.

Ces informations doivent permettre au RM de couvrir soit de façon isolée un risque soit de façon globale une famille de risques.

En conclusion :

- Ce n'est pas parce qu'un risque est quantifiable qu'il est forcément toujours assurable (l'assurance est un marché : loi de l'offre et de la demande et problème de capacités financières).
- Dans l'évaluation d'un risque certains éléments resteront toujours qualitatifs (impact en terme d'image, impact politique, etc.) et ces risques ne seront pas assurables sauf exception.

Dans ce contexte des solutions alternatives de financement des risques résiduels devront être trouvées. Ce type de solutions nécessite généralement d'avoir atteint et de justifier d'un très bon niveau de maîtrise du risque.

1.4.3 Attentes du RSSI et Apports du RM

Une des difficultés du RSSI est de proposer des actions de réduction et de contrôle des risques en adéquation avec les enjeux de l'entreprise et complémentaires aux solutions de financement des risques résiduels envisageables.

En effet pour qu'elle soit efficace, la sécurité des Systèmes d'Information doit répondre de manière proportionnée à la couverture de chaque risque identifié et non accepté.

Pour rationaliser le coût des moyens de réduction et de contrôle, le RSSI doit évaluer le niveau des pertes financières acceptables et ajuster les plans de traitement en conséquence : solutions de prévention (mesures de détection et de *dissuasion*) et de réaction (mesures de protection et palliatives).

Dans ce contexte un travail en commun avec le RM est nécessaire pour structurer la démarche de maîtrise des risques de façon à ajuster en conséquence les montants à garantir et si nécessaire concevoir des solutions alternatives de financement du risque résiduel (récupération).

Une façon d'y parvenir impose de disposer d'une cartographie des risques assurés et assurables mise à disposition par le RM.

Au-delà de cet aspect, c'est une relation permanente que le RSSI doit établir avec le RM de façon à suivre les sinistres (utilisation d'outils existants de gestion des sinistres le cas échéant).

Il s'agit pour le RSSI de :

- s'assurer que les risques à l'origine des sinistres figurent bien dans la cartographie des risques de l'entreprise,
- réactualiser les plans d'actions de réduction et de contrôle si nécessaire.

1.4.4 Exemple de coopération entre RM et RSSI dans un grand groupe industriel

Méthode d'*analyse des risques* :

Le RSSI attend du RM une stratégie.

Le RM veille à ce que la méthode retenue permette une identification la plus complète possible des risques liés aux SI de l'entreprise. Il attend du RSSI des méthodes et des outils d'évaluation adaptés aux spécificités des risques rattachés aux SI.

Analyse de risques liés au Système d'Information :

Le RSSI reporte au RM les résultats de ses évaluations concernant les risques majeurs.

Le RM consolide les risques pour chaque métier et s'assure du traitement des risques résiduels pour les risques majeurs.

Identification des plans d'action de réduction et de contrôle :

Le RSSI propose des plans d'actions de réduction et de contrôle.

Le RM intervient pour éclairer les décisions à prendre vis-à-vis des plans d'actions proposés en fonction des pertes financières estimées et du coût des solutions de financement du risque résiduel.

Organisation :

Le besoin de communication étant réciproque, le RM et le RSSI se rencontrent sur des thèmes communs ou transversaux (ex. : *risque opérationnel* lié à la logistique de l'entreprise et lié aux risques à gérer pour les SI).

L'intérêt du RM est d'exploiter la connaissance et l'expertise du RSSI en matière de Systèmes d'Information et de se tenir au courant des nouveaux projets et ou projets d'évolution sensibles.

Le RM de son coté s'avère être un allié pour le RSSI pour justifier les investissements en sécurité auprès de la Direction Générale.

Pour cela le RM peut assister le RSSI à traduire les indicateurs et tableaux de bord matérialisant le niveau de sécurité des SI en risques généraux pour l'entreprise qui seront plus simplement perçus et analysés par la Direction Générale.

À ce titre, le RM aura la responsabilité de relativiser et positionner les risques SI par rapport à l'ensemble des autres risques à gérer par l'entreprise.

2 RÉALITÉ DES RISQUES DU SI ET LEURS COUVERTURES

2.1 Identification et hiérarchisation des risques

2.1.1 Panorama du contexte réglementaire

Dans un contexte de crise sur la fiabilité des informations financières communiquées par les entreprises, les règles et les recommandations sur la gouvernance d'entreprise se multiplient. Des réglementations françaises et européennes ont répondu en écho aux lois américaines qui, à la suite des scandales du monde financier du début des années 2000, visaient à restaurer la confiance des actionnaires et du public.

Toutes ces réglementations prônent la prise en compte et la gestion de l'ensemble des risques de l'entreprise de façon organisée et formalisée.

L'objectif de ces mesures est double :

- accroître la transparence de la communication externe sur la gestion et le contrôle du risque,
- améliorer, au sein de l'entreprise, la détection précoce des risques, les mesures préventives et correctives.

En rappel, il convient de citer les principales mesures adoptées :

La Loi de Sécurité Financière (LSF) n°2003-706 du 1er août 2003 impose de nouvelles exigences, d'influence anglo-saxonne, en matière de transparence.

Elle importe le concept de « Gouvernement d'entreprise », défini comme la mise en place de dispositifs permettant la défense des intérêts des actionnaires et de l'ensemble des parties prenantes et formalise le contrôle interne dans l'ensemble des sociétés anonymes, cotées ou non, faisant appel public à l'épargne, quel que soit le secteur d'activité.

Ainsi, ces sociétés doivent, entre autres (art. 117 de la loi codifiée à l'article 225-37 al. 6 du code de commerce), rendre compte, dans un rapport joint au rapport annuel, des conditions de préparation et d'organisation des travaux du conseil, des procédures de contrôle interne adoptées et, le cas échéant, pour les SA à conseil d'administration, des éventuelles limitations aux pouvoirs du directeur général apportées par le conseil. Les associations professionnelles (**Association Française des Entreprises Privées AFEP, MEDEF**) ont rédigé des trames de référence pour l'aide à la rédaction de ces rapports.

La LSF répond, par effet de contagion, au **Sarbanes Oxley Act (SOA)** américain du 30 juillet 2002 sur les aspects financiers du contrôle interne (section 404), qui s'applique à toutes les sociétés cotées sur les marchés américains.

L'évaluation des risques est une étape indispensable au contrôle interne.

Dans son rapport 2004, **l'Autorité des Marchés Financiers (AMF)** insiste sur la nécessité d'identifier les risques au travers d'une cartographie précise et dynamique (c'est-à-dire hiérarchisée), qui constitue « la première étape d'un rapport interne digne de ce nom », en vue d'établir l'adéquation des procédures de gestion de risque correspondant à chaque catégorie.

A la différence de la France, les États-Unis, se sont dotés d'un référentiel de gestion de risque et de contrôle interne, élaboré par un organisme privé « **Committee of Sponsoring Organizations of the Treadway Commission » ou COSO (COSO I** sur le contrôle interne

et COSO II plus largement sur la gestion des risques). Dès 2006, les sociétés cotées à New York devront communiquer sur l'efficacité de leur contrôle interne en matière d'information comptable et financière.

Par ailleurs les établissements financiers, sont également soumis à **la réglementation internationale Bâle II**, publiée en 2004, **et à la future transposition de la Directive européenne (CRD)** sur l'adéquation des fonds propres.

Cette réglementation décompose les risques des établissements en 5 catégories :

- le risque de marché,
- le risque de crédit,
- le risque opérationnel (dont certaines catégories, par leur nature, sont communes avec de nombreux autres secteurs d'activités),
- le risque de réputation,
- le risque stratégique.

et requiert une allocation de fonds propres formelle face aux trois premiers risques (crédit, marché et opérationnel), identifiés et estimés selon des méthodes définies.

De leur côté, les établissements de crédit français, en quelque sorte précurseur, sont soumis depuis 1997 au **Règlement CRBF 97-02 du 21 février 1997** relatif au contrôle interne des établissements de crédit, modifié à plusieurs reprises et en dernière date par l'arrêté du 31/03/2005, sur le contrôle interne permanent et la fonction conformité. Ils doivent, à ce titre, en vertu des art. 42 et 43, élaborer un rapport sur les conditions dans lesquelles le contrôle interne est assuré, ainsi que sur la mesure et la surveillance des risques.

Enfin, les compagnies d'assurance, déjà soumises à la loi LSF et à d'autres réglementations spécifiques, appliqueront dès 2008-2009, dans le cadre du projet de **Directive Solvabilité II (« Solvency 2 »)** des procédures similaires à celles de Bâle II.

De ces différentes réglementations et recommandations, il ressort que la gestion des risques et le contrôle interne sont, au sein des entreprises, à l'origine de démarches formalisées d'identification :

- des activités et fonctions dans l'entreprise (ligne métier ou filière),
- de l'articulation par fonctions et par processus de chaque entité organisationnelle,
- des risques attachés aux processus,
- des procédures adéquates évitant ou limitant l'exposition au risque.

Contrôle :

- Efficacité des opérations.
- Fiabilité des états financiers.
- Respect des lois et des règlements.

Gestion du risque :

- Identification des événements pouvant affecter l'entreprise en fonction des objectifs.
- Analyse qualitative et quantitative du risque (fréquence – intensité).
- Suivi des plans d'action.
- Evolution des procédures.

Cette définition d'un cadre d'analyse des risques pour l'auto évaluation des entreprises pousse les entreprises non soumises aux différentes réglementations ci-dessus à mener un projet similaire. L'exercice de « cartographie » des risques, permet de formaliser la maîtrise par l'entreprise de ses risques.

En ce qui concerne, plus particulièrement, les risques relatifs aux systèmes d'information, les instances professionnelles (le CLUSIF, l'AMRAE, l'APSAD (Assemblée Plénière des Société d'Assurances Dommages)) ont développé depuis plusieurs décennies des méthodes d'évaluation des risques (MARION / MEHARI, etc.) qui reposent sur l'analyse de scénario de type : « conséquences-*causes*- origines », et qui ont pour but de permettre une planification des besoins et des actions de sécurité.

2.1.2 Définitions des risques

Le risque se définit généralement par la possibilité qu'un événement, une action ou une inaction affecte la capacité de l'organisation à atteindre ses objectifs.

2.1.2.1 Risque d'entreprise

Sa définition est plus ou moins extensive : il s'agit du risque, lié aux décisions que prend ou ne prend pas une entreprise, dans le but d'engendrer un profit ou un avantage. Il s'apparente au risque stratégique. Il est traditionnellement jugé non assurable.

2.1.2.2 Risque d'image et de réputation

Il s'agit du risque de voir les consommateurs, les partenaires et/ou les marchés financiers se détourner de l'entreprise qui n'a pas répondu aux attentes en matière de performance ou d'éthique.

Non inclus dans le risque opérationnel au sens de Bâle II, ce type de risque, susceptible de générer de lourdes pertes, est à prendre en compte dans une politique générale de gestion de risque.

2.1.2.3 Risque opérationnel

Dans la terminologie Bâle II, le risque opérationnel est défini comme le risque de pertes résultant de carence ou défaut (inadaptation ou défaillance) attribuables à des procédures, personnels, systèmes internes ou d'événements extérieurs. Il inclut les risques liés à la sécurité des systèmes d'information, les risques juridiques et réglementaires et les risques environnementaux. C'est dans cette catégorie de risque que se trouvent les risques aujourd'hui assurables.

La répartition ci-dessus reprend l'idée d'une distinction entre les risques pris par l'entreprise dans le but de réaliser un profit et les risques subis, à la suite desquels elle ne peut qu'enregistrer une perte. Le risque d'image ou de réputation est à la frontière de ces deux notions, l'entreprise pouvant en effet prendre une décision sans en avoir décelé les effets négatifs potentiels qu'elle ne peut tolérer.

2.2 Les risques opérationnels du système d'information

2.2.1 Les critères d'analyse de risque

Lorsque l'on évoque les risques susceptibles d'engendrer la défaillance ou la destruction de l'un des éléments constitutifs d'un système d'information, on établit un classement en deux familles :

- Les risques physiques

- Les risques logiques

Les risques physiques

- Ils sont appelés risques matériels. Il s'agit des *atteinte*s physiques dont peut être victime un système d'information. En général, il s'agit d'événements tels que :
- incendie; explosion; fumées,
- dommage électrique ; foudre,
- tempêtes ; dégâts des eaux ; événements naturels,
- bris de machine ; vol,

qu'ils soient d'origines accidentelles ou malveillantes.

Les conséquences de ces événements sont aisément identifiables, elles endommagent ou détériorent les *ressources* matérielles. Cependant, bien qu'évidentes aux yeux de tous, ces atteintes ne représentent qu'un faible pourcentage des sinistres informatiques.

Les risques logiques : les familles « Accident Erreur Malveillance »…

Avec le développement de l'informatique distribuée, l'interconnexion des réseaux et l'intégration des systèmes d'information au milieu des années 90, il s'est opéré une migration de la valeur du matériel vers la valeur des données et des applications. Dans cette dynamique, la démarche de détermination des risques a fait appel à l'expérience du passé. Comment évaluer et analyser la valeur de ce qui n'est pas physique, de « l'immatériel » ?

C'est ainsi que sont apparues les notions d'Accident, d'Erreur et de Malveillance, directement issue des méthodes d'évaluation et d'analyse de risques :

- **L'Accident** : il s'agit là d'un évènement perturbant les données ou les flux de données en l'absence de dommages aux équipements.
- **L'Erreur** : que ce soit une erreur de conception, de programmation, de paramétrage ou de manipulation ***de données ou de leurs supports***, l'erreur désigne les préjudices consécutifs à une intervention humaine dans le processus de traitement automatisé des données.
- **La Malveillance** : qu'elle soit d'origine interne ou externe, la malveillance est constituée par l'usage non autorisé du système d'information, avec des intentions préjudiciables. Le *virus* informatique est l'un des actes de malveillance les plus médiatisés.

Cette approche des risques immatériels constitue une première étape mais va montrer ses limites face aux enjeux de flux auxquels seront très rapidement confrontés les acteurs de la dématérialisation (hébergeurs, etc.).

Avec le temps, la manière d'appréhender les risques immatériels s'est transformée. La donnée a changé de statut pour devenir de l'information. Sa volumétrie, c'est à dire l'espace qu'elle occupe sur les supports physiques, a, en outre, connu une croissance exponentielle. Aujourd'hui, quelle que soit la nature de l'information (structurée ou pas) elle devient disponible par un simple clic !

C'est ce que les Anglo-saxons appellent ILM « Information Lifecycle Management ». Plus clairement, la valeur de l'information n'est plus statique mais fluctue au gré de sa nécessité, son environnement, des opportunités et de bien d'autres facteurs.

…pour, finalement, définir les impacts de Disponibilité, d'Intégrité, de Confidentialité et de Preuve

Voix - données - images sur les mêmes réseaux, la frontière entre les télécommunications et l'informatique s'est estompée. À l'instar des évolutions technologiques, l'environnement des risques s'est lui aussi transformé. La *menace* s'est accrue sur l'intégrité de l'information ainsi que sur sa circulation.

Face au nouvel environnement engendré par le statut et le flux de l'information, la nouvelle vision des risques immatériels est fondée sur une identification des menaces et des *vulnérabilités* faisant référence aux notions de disponibilité, d'intégrité de l'information, de confidentialité et de preuve de cette même information :

- **La disponibilité** : représente l'aptitude d'un système d'information à remplir une fonction dans des conditions prédéfinies de délai et de performance. C'est la possibilité de pouvoir obtenir l'information recherchée au moment où elle est nécessaire.

- **L'intégrité** : est une notion apparaissant lors d'une modification, par une action volontaire et légitime, du système d'information et de l'information traitée. Lorsque l'information est échangée, l'intégrité s'étend à l'*authentification* du message, c'est-à-dire la garantie de son origine et de sa destination. C'est le fait que l'information obtenue soit correcte.

- **La confidentialité** : est constituée par le caractère réservé d'une information, dont l'accès est limité aux seules personnes admises à la connaître pour une raison de fonctionnement.

- **La preuve** : sont les éléments permettant d'auditer la chaîne de parcours entre l'émetteur et le destinataire de l'information.

Nous définirons, pour chacun des risques, répartis en dix familles, son type d'impact et sa conséquence finale pour l'entreprise.

En complément nous décrirons le système d'information comme étant la combinaison de ressources matérielles, d'applications standards ou métiers qui, à leur tour, génèrent des données. L'objectif de cette association de moyens étant le traitement de l'information.

Impact sur le système d'information : effet direct ou immédiat produit par un événement sur l'information.

La notion d'impact est classée en quatre familles :

- **D** la disponibilité de l'information.

- **I** son intégrité.

- **C** sa confidentialité.

- **P** sa preuve ou traçabilité.

Conséquence pour l'entreprise: suite logique provoquée par un *fait générateur*

Les conséquences pour l'entreprise sont de quatre ordres :

- **FIN** Financières : perte de valeur ou de biens, dépenses supplémentaires.
- **IMA** Atteinte à l'image de l'entreprise.
- **HUM** Risque humain : risque vital ou désorganisation.
- **JUR** Juridique : responsabilité civile ou pénale vis-à-vis d'Autrui, des Cocontractants, des Autorités, des Clients.

2.2.2 Les familles de risque

Par souci de simplicité nous n'introduirons, à ce stade, que deux concepts principaux : l'impact sur le système, et la conséquence finale pour l'entreprise.

Les risques identifiés sont regroupés suivant les dix familles énoncées ci-dessous.

L'annexe **5.4** reprend le détail de ces risques et associe l'impact et les conséquences sur l'entreprise pour chacun d'entre eux.

- Risques environnementaux (Ensemble des risques provenant de l'extérieur des systèmes d'information et ayant une origine indépendante de la volonté humaine).
- Risques sociaux / Guerres (Ensemble des risques provenant de l'extérieur des systèmes d'information et ayant une origine humaine ou sociale, mais généralement non ciblée contre le système en question).
- Risques physiques des locaux (Ensemble des risques créés par les infrastructures externes aux systèmes d'information).
- Risques sur les matériels informatiques.
- Risques sur les logiciels.
- Risques de piratage, hacking informatique.
- Risques liés aux ressources humaines.
- Risques liés aux projets de développement.
- Risques générés par les partenaires de l'entreprise.
- Autres risques réglementaires et juridiques.

2.2.3 Maîtrise du risque

Une fois identifiés et évalués l'impact et les conséquences du risque, les responsables SI disposent de moyens pour le prévenir et en limiter les effets.

Par exemple :

- Mise en place et diffusion d'une politique de sécurité du SI
- Trace et *auditabilité* des systèmes (contrôle d'accès physique, applications, etc.).
- Indépendance du service d'audit au sein de l'entreprise.

- Application d'une méthodologie de conduite de projet.
- Cartographie des processus et documentation des procédures et applications.
- Existence de procédures de reprise d'activités (PRA / PCA).
- *Sauvegarde, restauration* et archivage des données (site et *plan de secours*).
- Recours à l'assurance.

2.3 Cartographie de l'assurabilité des risques

L'assurance joue un rôle majeur dans l'économie : celui de garantir les biens et les personnes. Ce rôle contribue au développement économique en favorisant la *prise de risque* des entreprises par la diminution des conséquences préjudiciables issues des sinistres potentiels.

L'assurance est un transfert de risque de l'assuré vers l'assureur, celui-ci acceptant donc de porter les risques engendrés par l'activité de l'assuré dans les limites du contrat d'assurance.

2.3.1 Principe de l'assurance

2.3.1.1 Principes généraux

En général, chez les assureurs, le mot « risque » revêt deux sens : le bien assuré et l'événement assuré. Pour être éligible à une couverture d'assurance, un risque doit pouvoir répondre à trois critères:

Aléatoire : c'est le fait que la probabilité de survenance d'un sinistre ne soit pas certaine. Autrement dit, que l'*évènement* qui déclenche la garantie tienne du hasard.

Quantifiable : le risque doit pouvoir être quantifié et estimé en terme de coût. L'objectif étant de permettre à l'assureur de connaître et de délimiter ses engagements afin de pouvoir les tenir.

Mutualisable : pour pouvoir équilibrer ses engagements, l'assureur doit mutualiser ou diversifier ses risques. Cela implique que les risques soient homogènes et indépendants : dans un portefeuille structuré, regroupant un grand nombre de risques indépendants, les assurés non-sinistrés financent, par *compensation*, les assurés sinistrés.

Pourquoi un grand nombre de risques ? Parce que le mécanisme d'équilibre est fondé sur la loi des grands nombres.

Selon cette loi, plus le nombre d'expériences aléatoires effectuées est élevé, plus les résultats se rapprochent de la probabilité théorique de survenance d'un événement.

Cette probabilité de survenance du risque s'appelle la fréquence et est connue par les statistiques de sinistralité.

Autrement dit, l'assureur fait face à une sinistralité individuelle aléatoire, compensée par une sinistralité globale certaine de la somme des risques indépendants.

2.3.1.2 Mécanismes de l'assurance

L'assurance consiste à tarifer aujourd'hui (encaissement d'une prime) un service qui aura demain un coût aléatoire (indemnisation d'un sinistre) : c'est l'inversion du cycle de production. C'est à dire que l'assureur perçoit un montant de prime sur le coût d'un risque qu'il ne connaît qu'à la fin de l'exercice.

Légalement, pour faire face à ses engagements et éviter le risque de ruine, les fonds reçus par les assureurs sous forme de primes doivent être placés en « sûreté », sous la forme de provisions techniques. Ces provisions techniques représentent des créances des assurés sur les assureurs.

Quelques mécanismes de base sont détaillés en annexe à ce document.

2.3.1.3 Couverture des risques liés aux systèmes d'information

Les difficultés d'une couverture adaptée demeurent. Rares sont les assureurs qui continuent à commercialiser des garanties immatérielles destinées aux systèmes d'information. De plus, certains segmentent leurs cibles et se cantonnent aux institutions financières. Dans tous les cas, les garanties de dommages proposées le sont sous forme de ressources financières.

Concrètement, c'est une démarche qui découle d'une approche « *premier risque* » représentée par un capital, un montant limité par sinistre et par an. L'assuré pourra, selon la typologie du dommage, solliciter son capital selon ses besoins.

Le montage habituel de la couverture des risques se compose de deux volets :

- La désignation des biens assurés.
- L'énumération des dépenses garanties.

En général, les biens assurés sont les équipements informatiques et les données. Leur couverture consiste à indemniser les coûts de remplacement, de reconstitution ou de réparation.

Pour les dépenses ou pertes garanties on retrouve les principales lignes suivantes :

- Les frais supplémentaires d'exploitation.
- Les pertes d'exploitation.
- Les honoraires d'experts.
- Les dépenses de relations publiques.

La vocation de ce type de couverture est de prendre en compte des pertes importantes (ou sévères) et non de pallier aux problèmes de fréquence. Les conditions de franchise proportionnelles au sinistre avec un montant minimum illustrent bien cette volonté. L'assureur ne peut en effet, pour un coût économiquement raisonnable, couvrir à la fois les sinistres de fréquence et les sinistres d'intensité.

Énumérons en détail les garanties :

La reconstitution de données : c'est le préalable des formules de garanties actuelles. Ce sont les frais exposés pour reconstituer les données endommagées. Ce sont notamment les coûts nécessaires pour :

- se procurer à nouveau les programmes standards perdus ou rendus illisibles par la machine,
- ressaisir manuellement ou par tout autre moyen plus adapté des données à partir des documents ou des programmes d'origine,
- rechercher et rassembler les éléments d'information disponibles à partir des sauvegardes ou de tout autre support informatique ou non y compris la documentation d'origine,
- déterminer les causes, le mécanisme et l'étendue d'une infection informatique et pour décontaminer les données,
- déterminer la cause, le mécanisme et l'étendue de la panne ou du dérangement à l'origine du dommage,
- décontaminer, nettoyer et restaurer les supports de données,
- se procurer à nouveau les supports interchangeables perdus ou rendus illisibles par la machine,
- les frais d'acquisition des licences de remplacement pour les programmes dont le système de protection d'accès a été endommagé ou détruit,
- les frais généraux associés aux coûts de reconstitution des informations perdues.

Lorsque les données endommagées ont été achetées, l'indemnisation est limitée à la valeur d'achat initiale.

Point important, il doit exister des éléments permettant la reconstitution des informations. Sinon, le mécanisme de garantie ne peut s'exercer. En définitive, ce ne sont pas les frais de recherche et de développement qui seront couverts chez un éditeur de logiciel, mais les frais de transfert de l'original vers un support numérique.

Les frais supplémentaires d'exploitation : ce sont les frais engagés par l'assuré en vue d'éviter ou de limiter durant la période d'indemnisation, la perte de marge brute due à la réduction du chiffre d'affaires imputable au sinistre. Ils sont constitués par les dépenses suivantes :

- l'utilisation d'équipements et de matériels extérieurs loués ou pris en leasing,
- la mise en œuvre d'autres méthodes de travail ou d'autres modes de production,
- le recours à la sous-traitance ou à un prestataire de service extérieur,
- les frais de main-d'œuvre liés au recours à du personnel supplémentaire,
- tous les frais liés à la mise en exploitation de locaux.

Les pertes d'exploitation : cette garantie couvre la dégradation ou la perte de marge brute résultant de la baisse du chiffre d'affaires causée par l'interruption ou la réduction de l'activité de l'entreprise.

La marge brute annuelle se définit généralement comme la somme des charges fixes et du résultat d'exploitation.

L'objectif de l'assurance des pertes d'exploitation est de replacer dès que possible l'entreprise assurée dans la situation financière qui aurait été la sienne si le sinistre n'avait pas eu lieu. La durée de cette couverture s'étale sur une période d'indemnisation précise.

Les honoraires d'experts : ce sont les dépenses engagées par l'assuré pour faire évaluer par ses propres experts les préjudices subis.

Les dépenses de relations publiques : ce sont les dépenses engagées par l'assuré pour rétablir sa réputation ou son image dès lors qu'elles ont été directement affectées par la cause du dommage.

L'activité du SI peut engendrer la mise en cause de diverses responsabilités de l'entreprise.

Responsabilité Civile Professionnelle et Responsabilité Civile Produit livré : elle est engagée par toute faute ou erreur qui cause une perte financière à un Tiers ayant une relation contractuelle avec l'Assuré.

Responsabilité Civile Exploitation : elle est engagée lorsque les moyens d'exploitation - humains ou matériels - causent un dommage à autrui, personne physique ou morale.

Les dommages peuvent être :

- Corporels : atteinte à l'intégrité physique d'une personne.
- Matériels : atteinte à une chose, un animal.
- Immatériels : perte financière consécutive à un dommage corporel ou matériel.

Responsabilité Civile des Mandataires sociaux : elle est engagée par toute faute dans l'exécution du mandat social ; la mise en cause est souvent le fait des actionnaires.

2.3.1.4 L'assurabilité

L'assurabilité des risques énoncés dans le paragraphe 2.2. sera déterminée selon trois critères :

- *non éligible à l'assurance,*
- *éligible partiellement à l'assurance (exclusions, limitations, hors incidence d'une franchise),*
- *éligible à l'assurance.*

Par ailleurs nous rappelons la *classification* utilisée pour les conséquences pour l'entreprise.

Les conséquences pour l'entreprise sont de quatre ordres :

- Financières (FIN) : perte de valeur ou de biens, dépenses supplémentaires.
- Atteinte à l'image de l'entreprise (IMA).
- Risque humain (HUM) : risque vital ou désorganisation.

- Juridique (JUR) : responsabilité civile ou pénale vis-à-vis d'Autrui, des Cocontractants, des Autorités, des Clients.

Le lecteur est invité à se reporter à l'annexe **5.4** pour identifier la couverture d'assurance proposée en fonction de la nature du risque et des conséquences pour l'entreprise.

Globalement, l'assurabilité des risques est traduite dans le tableau ci-dessous. Les % énoncés sont calculés sur la somme des risques identifiés en fonction de leur assurabilité. Par exemple, 14,5% des risques financiers sont éligibles à l'assurance.

Note d'éligibilité	Financier	Image	Humain	Juridique
0 : non éligible	48%	68%	55%	13%
1 : éligibilité partielle	37,5%	32%	45%	87%
2 : éligible	14,5%	0%	0%	0%
Total	100%	100%	100%	100%

Plusieurs constats s'imposent :

Conformément aux critères théoriques d'éligibilité à l'assurance précisés au 2.1.1, ce sont les conséquences financières et juridiques de la matérialisation des risques qui peuvent le plus aisément trouver une couverture par l'assurance

Au-delà des impacts, l'assurance privilégiera, dans sa prise de risque, une certaine typologie de faits générateurs du risque : les actes malhonnêtes d'un employé, par exemple, ou, parmi les faits générateurs purement externes, la malveillance (bien que très évolutive) et le dommage physique

Le marché de l'assurance n'est, en revanche, pas en mesure d'apporter une solution satisfaisante aux problématiques humaines et d'image issue de l'occurrence d'un risque informatique. Ses réponses sont également extrêmement limitées sur les problématiques :

- de choix technologiques,
- d'organisation interne de la ligne métier « systèmes d'information »,
- inhérentes aux développements, aux projets,
- de sous-traitance.

L'entreprise devra tenir compte de ces contraintes dans l'élaboration de sa politique de *transfert du risque.*

2.3.1.5 Le dialogue avec l'assureur

Les déclarations de l'entreprise vers l'assureur pour permettre la *couverture du risque* vont reposer sur plusieurs types d'approches.

Le risque physique

L'assureur va demander en premier lieu une déclaration du montant total des capitaux à assurer sans nécessité de communiquer un inventaire détaillé. En complément l'assureur souhaitera connaître aussi la ventilation des capitaux entre le matériel fixe et le matériel portable. Pour parfaire son approche il peut aussi lui être communiqué l'accumulation de

valeur sur le site le plus important. De même toutes les mesures de sécurité au niveau du risque physique mises en place pourront lui être communiquées (protection contre l'incendie, le vol, les dégâts des eaux, etc.).

Le risque logique

Pour ce domaine de risque, il faut sortir de la notion de « déclaration de risque ». L'assureur basera plus son approche sur une perception de la sensibilité de l'entreprise au risque. L'un des objectifs principaux que va avoir l'assureur est d'approcher au mieux les impacts d'un sinistre informatique sur l'entreprise. En effet dans le domaine des risques logiques, l'assureur ne peut pas déterminer un « standard » de protection que devraient atteindre toutes les entreprises. L'utilisation ou l'implication des systèmes d'information au sein d'une entreprise sont systématiquement différents d'une entreprise à une autre, il est donc extrêmement difficile, voire impossible de déterminer un seuil d'assurabilité basé sur un niveau « standard » de protection.

Nous devons donc admettre qu'une entreprise peut être assurable quel que soit le niveau de ses protections dans la mesure où l'entreprise est capable de démontrer qu'elle est consciente de ses risques et qu'elle a mis en œuvre les moyens nécessaires pour la gestion de ses risques. L'entreprise va donc faire appel à l'assurance pour la part de risque qu'elle ne peut pas supprimer et pour laquelle les conséquences financières sont insupportables.

C'est dans cet état d'esprit que se situe l'assurance des risques logiques. L'Assureur, lors de sa collecte d'information va essayer de comprendre/estimer cette part de risque qu'il peut être amené à financer. Pour ce faire, il va essayer de :

- Comprendre le risque par la connaissance de l'organisation du système d'information
- Estimer l'impact d'un sinistre sur l'activité économique de l'entreprise par l'analyse de la ventilation du chiffre d'affaire en fonction des métiers ou des applications
- Vérifier l'adéquation de la politique sécurité de l'entreprise avec l'exposition aux risques.

Nous voyons donc que lors de l'analyse de l'assurabilité d'un risque, l'assureur va avoir plusieurs interlocuteurs :

Le Responsable Sécurité des Systèmes d'Information pour comprendre comment est organisé ce système et quelle est la politique sécurité qui est appliquée,

Le Risk Manager pour évaluer quelles seraient les conséquences d'un sinistre au niveau du fonctionnement de l'entreprise

Les critères qui seront analysés par l'assureur reposent sur :

- Organisation générale du système d'information.
- Matériel.
- Système d'exploitation.
- Réseaux.
- Administration.
- Comment ce SI contrôle l'activité économique de l'entreprise ?

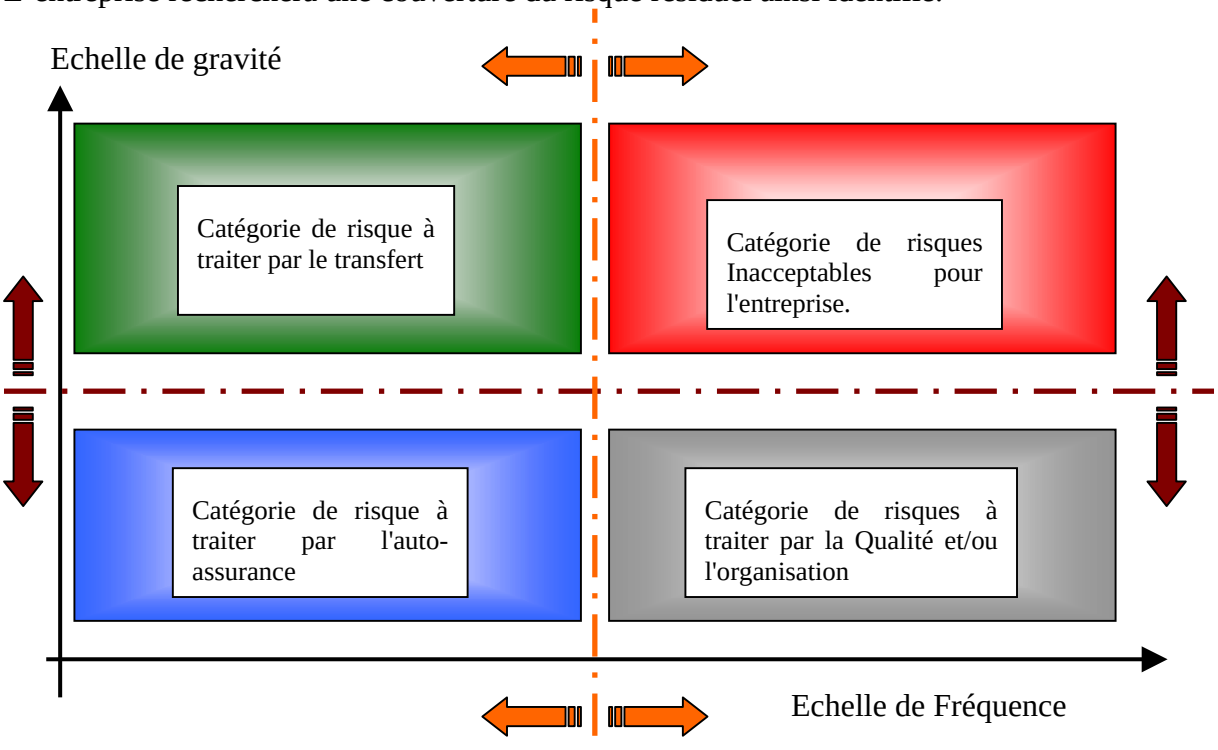
- Profil de l’entreprise.
- Nombre d’utilisateurs.
- Infogérance, hébergement.
- Estimation des impacts suite à arrêt des systèmes.
- La politique sécurité de l’entreprise, notamment sur les points suivants :
  - Protection physique.
  - Sauvegarde.
  - Organisation de la Sécurité informatique.
  - Mesures anti-intrusion.
  - Politique d’habilitation.
  - Protection contre les malwares (antivirus, chevaux de Troie, etc.).
  - Plan de reprise d’activité.

2.4 Politique de transfert du risque

Après avoir déterminé les risques résiduels auxquels est exposée l'entreprise, c’est-à-dire identifié et estimé les risques, défini et mis en place les processus visant à contenir :

- l’exposition au risque et/ou,
- la sévérité de la perte en cas de réalisation du risque.

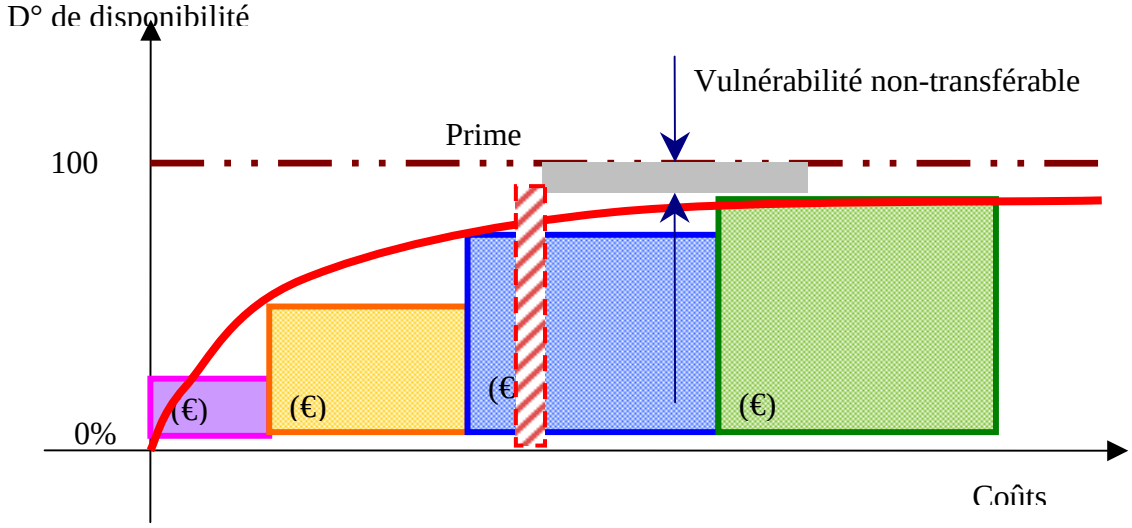
L’entreprise recherchera une couverture du risque résiduel ainsi identifié.



L'emplacement des deux curseurs sera déterminé par l'entreprise en fonction de ses propres contraintes.

2.4.1 Intérêt du transfert à l'assurance

De l'analyse ci-dessus il ressortira souvent le traitement ci-dessous :



L'amélioration du niveau de protection d'une entreprise va passer par des investissements financiers. On constate généralement que la « rentabilité » (dans le sens progression du niveau de protection par rapport au montant de l'investissement) d'un investissement sécurité va décroître avec le montant investit. Il va donc apparaître un moment ou ce montant nécessaire pour continuer l'amélioration du niveau de protection devient trop élevé et non rentable. C'est à ce niveau que le transfert du risque (transfert uniquement financier) devient une solution adéquate, dans le schéma ci-dessus, il est matérialisé par la prime d'assurance.

Les investissements dans la partie gauche du graphique sont plus économiques que l'assurance et nécessaires pour acheter une couverture d'assurance étendue en termes de périls couverts et de montant de garantie.

Dans la partie droite du graphique, l'investissement n'est plus nécessaire. L'assureur, satisfait du niveau de prévention/protection mis en place, accepte de prendre en charge le risque.

Après avoir décelé, analysé, évalué et traité ses risques, l'entreprise va décider de son niveau de rétention. Pour lui permettre de conserver une trésorerie adéquate au lendemain d'un sinistre important, toute organisation doit disposer d'une couverture spécifique prévoyant un financement pour ce genre de situations:

- Soit en interne (rétention).
- Soit en externe (transfert vers l'assurance).

La mise en place d'une couverture pour les systèmes d'information doit permettre de compenser les pertes et, même, d'en limiter les conséquences dommageables en fournissant la trésorerie nécessaire à un redémarrage rapide après la survenance du sinistre. Cette couverture est une contribution à la solidité financière de l'entreprise par un financement des risques qui n'ont pas pu être réduits par les moyens et procédures de gestion des risques.

Entre autres avantages, cette couverture appropriée permet de substituer un coût connu : la prime périodique d'assurance, à des coûts très incertains : un ou plusieurs sinistres dont la gravité serait imprévisible.

L'assurance peut être considérée comme une protection partielle complémentaire sinon totale, voire une alternative à la mise en place d'une solution interne. Cette option n'écarte cependant pas des exigences plus ou moins lourdes de la part de l'assureur pour mettre en place ou maintenir les garanties d'assurance requises.

2.4.2 Limites du transfert à l'assurance

Le recours à l'assurance a toutefois ses limites : conditions de prix, d'étendue de garantie et de capacité offerte. Certains risques ne peuvent être placés en totalité, les conditions de franchises et de prix pouvant être dissuasives et incitant l'assuré à revoir sa politique assurance : acheter une couverture moins large en ciblant les risques, ou rechercher des solutions alternatives (auto – assurance, constitution d'une *captive* ou appel au marché financier, etc.)

2.4.3 Prise en compte du transfert à l'assurance

Au regard des tiers (actionnaires, agences de notation, fournisseurs et partenaires, etc.), la politique de transfert du risque par l'assurance est de plus en plus considérée comme un élément constitutif de la gestion du risque par l'entreprise.

Pour les sociétés cotées, les dispositions de la **loi relative aux nouvelles régulations économiques (NRE)** n°2001-420 du 15 mai 2001, et leur déclinaison par l'AMF dans ses recommandations requièrent la rédaction d'un chapitre « assurance/couverture des risques » au sein du document annuel de référence. Ceci afin d'identifier les *facteurs de risques* de l'entreprise et de présenter la politique de couverture assurance de l'émetteur.

Dans le même esprit, suivant les conclusions de Bâle II, les superviseurs bancaires déterminent dans quelles conditions le transfert au marché de l'assurance permet de diminuer l'allocation de fonds propres correspondant à un type de risque opérationnel. La prise en compte du transfert au marché de l'assurance sur cet aspect est en tout état de cause fortement limitée, elle sera :

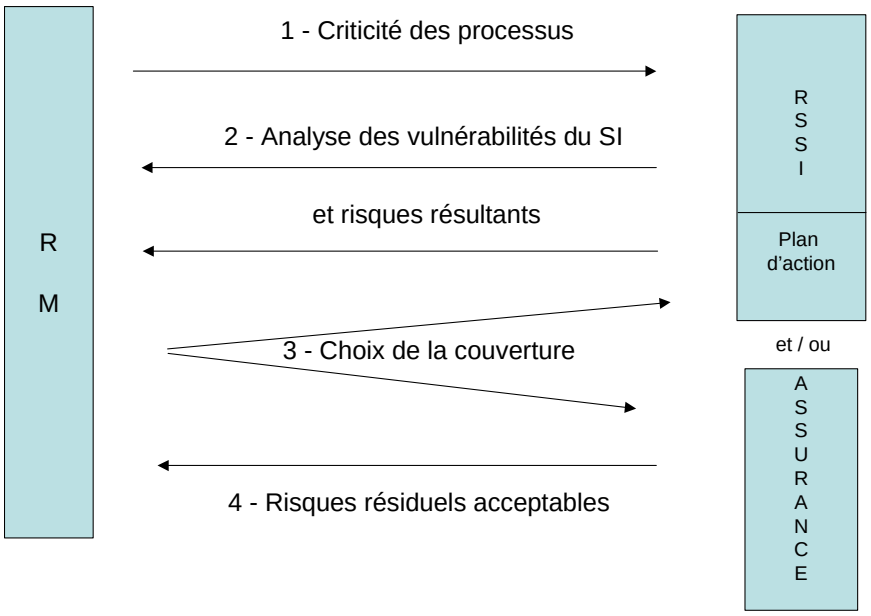
- plafonnée à 20 % du capital alloué au risque avant assurance,
- réservée aux seuls établissements ayant opté pour la méthode avancée du calcul du capital alloué,
- soumise à des conditions très strictes d'éligibilité des contrats d'assurance.

3 COMMUNICATION ENTRE LES DEUX FONCTIONS

Force est de constater qu'entre le RM qui évolue dans la sphère financière de l'entreprise et le RSSI qui étudie principalement les dysfonctionnements du système informatique, la communication est quasi inexistante au sein de certaines entreprises. Le vocabulaire, propre au métier de chacun, n'est pas non plus en concordance. Lorsque le RM parle de probabilité de survenance (au sens espérance mathématique du terme), le RSSI parle plutôt de potentialité de survenance (au sens possibilité du terme). Il apparaît donc une réelle nécessité d'établir entre les deux fonctions une terminologie commune et des indicateurs qui apportent à l'un comme à l'autre une même compréhension du risque opérationnel lié au système d'information de l'entreprise.

3.1 Méthodes de communication

Quels que soient les outils ou les méthodes employés, le RM et le RSSI procéderont au niveau de leur communication, à des allers et retours qui pourraient se synthétiser de la manière suivante :



1. Le RM indique au RSSI qu'un processus particulier, dépendant du SI, est critique pour l'entreprise.
2. Le RSSI va alors déterminer les vulnérabilités du SI liés à ce processus ainsi que les risques en résultant.
3. Conjointement, le RM et le RSSI prendront les décisions nécessaires sur la méthode à employer pour traiter ce risque, méthode qui peut, ou non, être liée au SI

La mise à jour périodique de ces informations par un dialogue fréquent et constructif entre le RM et le RSSI (ou inversement) est nécessaire pour maintenir l'adéquation du processus de gestion de risques avec les attentes de l'entreprise.

3.1.1 Les indicateurs du RM vers le RSSI

Le RSSI, pour rendre son plan d'action efficace, attend du RM la mise en perspective des risques potentiels de l'entreprise.

Pour ce faire, le RM :

Identifie, évalue et hiérarchise les risques majeurs en élaborant les cartographies des risques aux niveaux des Métiers, des Directions, des Sites, des risques Pays, etc.

Assure le déploiement des plans d'actions de prévention grâce à un pilotage au niveau d'un Comité des Risques

Promeut des outils de gestion des risques au sein des différentes instances de l'entreprise en fonction des cartographies réalisées et veille à leur cohérence

Le RM pourra donc transmettre au RSSI la criticité des processus de l'entreprise en ce qui concerne la Disponibilité, l'Intégrité, la Confidentialité des informations traitées par le SI et même la nécessité de Preuve pour certaines informations.

Cette criticité peut être mesurée sur une échelle de 0 à 4 pour chacun des critères de sécurité, comme par exemple :

0 : sans aucune criticité

1 : criticité faible

2 : criticité moyenne

3 : criticité forte

4 : criticité extrêmement forte pour l'entreprise.

Cette criticité est liée à l'impact intrinsèque que pourrait avoir un sinistre sur une ressource ou un processus de l'entreprise en l'absence de toute mesure de sécurité.

3.1.2 Les indicateurs du RSSI vers le RM

Le RSSI apportera au RM une certaine garantie des mesures de sécurité mises en place, notamment en matière d'efficacité et de robustesse face au sinistre redouté.

Le RSSI :

- Identifie pour le domaine informatique, les risques à gérer en matière de Disponibilité, Intégrité et Confidentialité, et de Preuve le cas échéant.
- Veille à faire réduire les vulnérabilités et adapte au mieux la mise en œuvre des mesures de sécurité qu'il juge nécessaires pour protéger la ressource ou le processus en fonction des risques majeurs.
- Contrôle la mise en œuvre du plan d'action et vérifie l'efficacité, la robustesse et la pertinence des mesures existantes pour protéger cette dite ressource ou ce dit processus. Cette vérification se fera à une fréquence à déterminer selon les besoins.
- Indique au RM le risque résultant issu de la mise en œuvre de son plan d'action. Ce risque résultant sera :

  Soit totalement couvert par les moyens techniques et organisationnels mis en place,

  Soit, en raison du manque d'efficacité ou de robustesse des mesures mises en place, il ne sera que partiellement couvert,

Soit, en raison de l'impossibilité proprement dite de protéger cette ressource ou ce processus par les moyens techniques ou organisationnels disponibles, ce risque ne sera pas couvert du tout.

3.1.3 Choix de la couverture

Le RM analysera avec le RSSI l'état des risques résultants. Il devra donc décider si les risques résultants sont acceptables ou non en fonction de sa politique de gestion des risques. Si ces risques résultants sont encore inacceptables, il fera appel aux mesures de transfert vers l'assurance afin d'adapter le risque résiduel à un niveau acceptable pour l'entreprise. Dans le cas où le risque résiduel reste inacceptable, il lui faudra procéder à des provisions internes pour couvrir ce risque.

La LSF oblige les sociétés cotées à communiquer sur les risques et en particulier sur le risque financier et le risque opérationnel. Cette charge est en général dévolue au RM lorsqu'il existe dans l'entreprise. Il est donc important que le RM ait toutes les informations nécessaires en sa possession.

Cette communication est importante pour l'image de l'entreprise et pour l'estimation réalisée par les analystes financiers et les agences de notations.

3.2 Les outils disponibles

Les outils de communication entre le RM et le RSSI seront issus des méthodes d'analyse des risques utilisés par chacun d'eux. Ils devront néanmoins les adapter pour une compréhension commune des termes utilisés.

3.3 Les outils du RM

Le RM s'appuie sur la méthodologie et les indicateurs qu'il a mis en place dans son entreprise. Ces outils sont différents selon les entreprises.

Les outils traditionnels sont :

- la cartographie des risques et les cotations (gravité, occurrence, criticité, etc.),
- les plans d'action et leur suivi (avec les indicateurs de suivi déterminés par chaque entreprise).

Pour les standards, il existe :

- Pour les banques : Bâle II.
- Pour les sociétés cotées : loi sur la Nouvelle Régulation Economique, etc.
- Les normes définies par COSO II.

3.4 Les outils du RSSI

Le RSSI s'appuie sur des standards du marché pour appliquer les bonnes pratiques internationales :

Les approches de bonne gouvernance (comme Cobit), d'exploitation (comme ITIL) pour gérer la politique de sécurité du SI tant en interne qu'avec les partenaires,

L'utilisation du standard de sécurité informatique (comme l'ISO 27001) pour faire évoluer la politique de sécurité en place qui implique de définir et déployer un système de gestion de sécurité de l'information (ISMS) et d'intégrer la gestion de risque.

Mais les points de contrôle proposés par ces standards sont à analyser systématiquement puisqu'ils ne s'appliquent pas tous à l'entreprise ou sont, pour certains insuffisants, en raison des risques spécifiques encourus. Il est donc important que l'entreprise vérifie de quelle manière elle sélectionne et met en place ses mécanismes de sécurité par rapport à la norme et à son contexte. Elle pourra ainsi entamer une démarche de certification ISO 27000 si elle le souhaite ou si elle lui est imposée dans le cadre de son activité ou des relations avec ses partenaires.

Cette analyse des risques du SI peut être réalisée, par exemple, avec la méthode MEHARI du CLUSIF. Elle apportera, outre une vision globale de la vulnérabilité du SI des indicateurs fort précieux au RM et/ou à la Direction Générale de l'entreprise.

4 CONCLUSION

Le RM est concerné par une partie des risques gérés par le RSSI, ceux qui ont un impact sur le fonctionnement général de l'entreprise. Il traite des risques **de l'entreprise** par l'analyse des impacts sur les divers secteurs qui la composent :

- Production.
- Finance.
- Ressources humaines.
- Engagement à l'égard des tiers.

Il manque au RM la sensibilité des SI à des risques généralement peu pris en compte tels que les intrusions, le piratage... Le système d'information est souvent perçu comme un ensemble d'outils pour l'entreprise plutôt que comme un processus intégré dans l'entreprise.

Le RM attend du RSSI principalement les résultats de la cartographie des risques (description, fréquence, intensité, criticité...) lui permettant d'intégrer les risques du SI dans la gestion des risques de l'entreprise.

Le RSSI s'intéresse à la totalité des risques des **systèmes d'information** ; il traite ces risques par l'analyse des impacts sur son domaine :

- Disponibilité.
- Intégrité.
- Confidentialité.
- Traçabilité.

Il manque au RSSI les conséquences de ces impacts sur le fonctionnement de l'entreprise.

Le RSSI attend du RM les informations lui permettant d'intégrer la stratégie de gestion des risques de l'entreprise dans son domaine d'action.

Cette prise en compte des attentes réciproques initie un processus de communication interactif. De ce schéma vertueux, le RSSI retirera un support supplémentaire pour la gestion des risques liés au SI et une reconnaissance accrue de son domaine d'intervention. Le RM en retirera une connaissance plus complète des risques de ce domaine spécifique qui déboucheront sur une meilleure gestion des risques de l'entreprise.

5 ANNEXE

5.1 Le RM

Qualités requises :

Le Risk Manager doit être à l'écoute et réactif vis-à-vis de ce qui se passe en interne dans l'entreprise (métiers, environnement, projets d'évolution…) et à l'extérieur. Il doit être aussi capable d'argumenter et de convaincre car il n'a, à lui seul, pas de réel pouvoir de décision.

Une de ses qualités est le contact humain, notamment la capacité à dialoguer et à travailler avec tous les niveaux hiérarchiques dans l'entreprise : directeurs, opérationnels, membres du conseil d'administration, direction générale, experts fonctionnels et techniques sans oublier les tiers externes comme les juristes, les investisseurs et les partenaires commerciaux.

Le Risk Manager va ainsi devoir se constituer un réseau de contacts à tous les niveaux et dans tous les métiers de l'entreprise.

Pour ce faire il devra faire preuve de bon sens, disposer d'une fibre relationnelle particulière, et montrer de la rigueur et de l'ouverture d'esprit.

Pour amener les acteurs en charge des risques à s'approprier les outils et méthodes définis en matière de gestion des risques dans l'entreprise il doit également posséder les capacités nécessaires pour animer et former des équipes.

Son expertise l'amène aussi à jouer un rôle de conseil important pour assister les métiers sur les moyens de prévention à mettre en place.

Dans ce domaine une bonne connaissance de la finance et de la comptabilité contribue à mieux appréhender et par conséquent maîtriser les pertes financières encourues.

Formation :

La formation initiale peut être soit technique (école d'ingénieurs), soit commerciale (école de commerce ou troisième cycle spécialisé), soit juridique (DESS en droit des assurances).

Les formations aux pratiques de Risk Management les plus reconnues en Grande-Bretagne sont les diplômes délivrés par l'« Institute of Risk Management ». Toutefois, il existe de plus en plus de filières menant à cette profession : citons la licence de gestion des risques de la Glasgow Caledonian University ou la maîtrise d'assurance et gestion des risques de la City University à Londres. Quant à la London School of Economics, elle possède un centre dédié à l'analyse des risques et de la législation.

En France, les écoles qui préparent au métier sont l'ESMA Marne-La-Vallée, l'IMR Bordeaux, le CARM – Institute, l'ECEMA, l'ISEA Il y a aussi de plus en plus de formations dans les universités.

Les Risk Managers les mieux armés sont ceux qui possèdent à la fois une formation théorique à la gestion des risques et une excellente connaissance de leur secteur d'activité. Enfin, la maîtrise de l'anglais constitue un plus car la fonction a souvent une dimension internationale.

Profil :

Il est difficile de conférer au Risk Manager un profil type. L'approche « maîtrise des risques » reste très différente selon la taille de l'entreprise et sa capacité à se doter de structures dédiées, selon sa culture, et aussi selon son activité.

Selon le type d'organisation de l'entreprise le champ d'action et le périmètre de responsabilité du Risk Manager sont plus ou moins étendus. Dans certains cas, il peut être sollicité au-delà de son champ d'expertise, dans d'autres cas, il a plus un rôle de gestionnaire et est moins impliqué dans le traitement des risques. Les entreprises les plus importantes organisent la fonction de telle sorte que le Risk Manager joue un rôle de coordinateur vis-à-vis des acteurs en charge de la gestion des risques et apporte son savoir-faire en support aux métiers.

Parcours :

Le métier est encore trop récent pour parler de parcours professionnel. On peut néanmoins estimer que le Risk Manager n'a que l'embarras du choix pour s'orienter, s'il le souhaite, vers le consulting, l'expertise technique au sein d'une société d'assurances ou encore la reprise d'une agence ou d'un cabinet de courtage.

5.2 Le RSSI

Qualités requises :

- Connaître et comprendre les activités, les processus, et l'organisation de l'entreprise.
- Avoir une expertise dans au moins un des domaines suivants :

  le métier,

  les technologies liées à la sécurité des SI,

  le domaine réglementaire,

  au plan juridique,

  en matière d'architecture des systèmes d'information dans l'activité considérée.
- Savoir diriger des projets transverses regroupant MOA et MOE.
- Savoir communiquer pour sensibiliser les différents acteurs.
- Avoir une vision claire des aspects stratégiques pour l'entreprise.
- Savoir convaincre la Direction des enjeux et de l'importance de décider de plans d'actions.
- Etre patient car l'identification et la gestion des risques est un travail de longue haleine.

Profil :

La sécurité n'est pas quelque chose que les entreprises viennent de découvrir avec les récentes attaques. Dans bien des entreprises elle est intégrée depuis plus de dix ans si ce n'est comme une mission au moins comme une dimension à prendre en compte notamment concernant la sureté des personnes, la sécurité physique et logique des moyens informatiques et aussi de façon à répondre aux objectifs qualité / performance définis par le métier.

Dans ce contexte les RSSI sont souvent d'anciens responsables de la sécurité physique ou des informaticiens. Pour les informaticiens il s'agit d´anciens chefs de projet, généralement des ingénieurs qui possèdent en moyenne plus de 10 à 15 ans d'expérience. Quelques uns sont issus du monde de l'audit, très peu sont issus du métier.

La réussite de la mission de RSSI passe par la connaissance du métier et du SI très souvent acquise sur le terrain dans des postes d'experts techniques ou métiers.

Il n'existe pas aujourd'hui de diplôme spécifique pour cette fonction. En revanche il existe depuis quelques années un DESS sur la Sécurité du Système d'Information à l'Université de Technologies de Troyes.

Des certifications françaises et internationales se mettent en place.

5.3 *Activités d'un RSSI : exemple*

Copyright CIGREF

1) Rôle organisationnel Mise en place de structures de relais chargées d'appliquer la stratégie de l'entreprise Création et animation d'un réseau interne de correspondants de sécurité et de compétences Intermédiaire et/ou coordonnateur entre les différents intervenants en cas de problèmes (hiérarchie, sites extérieurs concernés, police…) Transversalité par rapport aux Métiers de l'Entreprise Chef d'orchestre des experts techniques	2) Définition de la politique de sécurité Définition des objectifs et des besoins Définition et mise en place des procédures Définition de l'organisation et de la politique de sécurité
3) Analyse de risques Méthode d'évaluation des risques Analyse des risques et des menaces et évaluation des conséquences Remontée de l'ensemble des éléments qui permettent de prendre les décisions Etude des *vraisemblances* et des conséquences d'un sinistre tant au niveau technique que fonctionnel Étude des moyens d'assurer la sécurité et le respect de leur application Établissement du plan de prévention et plans de continuité	4) Sensibilisation et formation aux enjeux de la sécurité Sensibilisation de la direction générale Formation des directions opérationnelles et métiers Participation à la réalisation de la charte de sécurité Animation des réunions de sensibilisation à la sécurité Conseil et assistance auprès des équipes Assure la promotion de la sécurité auprès de tous les utilisateurs
5) Étude des moyens et préconisations Gestion et évaluation des actifs Validation technique des outils de sécurité Définition des normes et des standards de sécurité Participation à l'élaboration des règles de sécurité au niveau global de l'entreprise ou du groupe	6) Reporting à la DG Assurance que les plans de sécurité ont été faits suivant les plans préétablis Garantie que les équipes ont pris toutes les mesures permettant de gérer la sécurité S'assure du « test » des vulnérabilités de l'entreprise Contrôle régulier du niveau de sécurité du SI par l'évaluation des risques résiduels Elaborer des tableaux de bord de la sinistralité (construction d'indicateurs efficaces)
7) Veille technologique et prospective	8) Conseil et préconisations auprès des directions de l'entreprise :

Suivi des évolutions réglementaires et techniques de son domaine Veille sur les évolutions nécessaires pour garantir la sécurité logique et physique du SI dans son ensemble	Proposer des stratégies annuelles et à moyen terme, Définir des orientations, Elaborer et mettre en œuvre une politique de sécurité, Proposer des évolutions nécessaires pour garantir la sécurité logique et physique du SI, Définir la politique de sécurité de l'entreprise, Veiller à influencer les choix d'architectures et de technologies du SI par l'analyse des services et réponses de sécurité dans le cadre de projet, de changement majeur du SI, d'infrastructures globales…

5.4 Familles de risque et leur assurabilité

(1) : **D**isponibilité, **I**ntégrité, **C**onfidentialité, **P**reuve ou traçabilité.

(2) : **FIN**ancier, **IMA**ge, **HUM**ain, **JUR**idique.

(3) : **0** (Non éligible à l'assurance), **1** (éligible partiellement à l'assurance), **2** (éligible à l'assurance).

Famille de risques	Liste des risques	Impact SI (1)				Conséquences Entreprise (2)				Assurabilité (3)			
		D	I	C	P	FIN	IMA	HUM	JUR	FIN	IMA	HUM	JUR
Risques environnementaux	Evènements naturels	☒	☐	☐	☐	☒	☒	☒	☒	2	1	1	1
	Infections sanitaires	☒	☐	☐	☐	☒	☒	☒	☒	1	0	1	1
	Indisponibilité des fluides (eau, électricité...)	☒	☐	☐	☐	☒	☒	☒	☒	1	0	1	1
Risques sociaux / Guerres	Terrorisme / Guerre / Guerre Civile	☒	☐	☐	☐	☒	☒	☒	☒	1	0	1	0
	Emeute, grève, manifestation	☒	☐	☐	☐	☒	☒	☒	☒	1	0	0	1
Risques physiques des locaux	Risque d'infrastructure	☒	☐	☐	☐	☒	☒	☒	☒	1	0	0	1
	Les équipements informatiques et télécoms	☒	☐	☒	☐	☒	☒	☐	☒	1	0	-	1
	Les bureaux utilisateurs	☒	☐	☐	☐	☒	☒	☐	☐	1	0	-	-
Risques sur les matériels informatiques	Infrastructures réseaux, télécoms et serveurs	☒	☐	☐	☐	☒	☒	☐	☒	1	0	-	1
	Téléphonie	☒	☐	☐	☐	☒	☒	☐	☒	1	0	-	1
	Vol ou destruction de matériel	☒	☒	☒	☒	☒	☒	☐	☒	2	0	-	1
	Technologies utilisées	☒	☐	☐	☐	☒	☒	☐	☒	0	0	-	1
	Dimensionnement des équipements	☒	☐	☐	☐	☒	☒	☐	☒	0	0	-	1
	Maintenance	☒	☐	☐	☐	☒	☒	☐	☒	0	0	-	1
	Equipements de secours	☒	☐	☐	☐	☒	☒	☐	☒	1	1	-	1
Risques sur les logiciels	Systèmes non conformes aux spécifications	☒	☒	☒	☒	☒	☒	☐	☒	0	0	-	1
	Maintenance insuffisante	☒	☐	☐	☐	☒	☒	☐	☐	1	1	-	-
	Technologies utilisées	☒	☐	☐	☐	☒	☒	☐	☒	0	0	-	1
	Perte de données	☒	☒	☒	☒	☒	☒	☐	☒	0	0	-	1
	Bogue logiciel	☒	☒	☒	☒	☒	☒	☐	☒	0	0	-	1
	Propriété intellectuelle	☐	☐	☐	☐	☒	☒	☐	☒	1	1	-	1

Famille de risques	Liste des risques	Impact SI (1)				Conséquences Entreprise (2)				Assurabilité (3)			
		D	I	C	P	FIN	IMA	HUM	JUR	FIN	IMA	HUM	JUR
Risques de piratage, hacking , informatique	Virus et infections informatiques	☒	☒	☒	☒	☒	☒	☐	☒	2	1	-	1
	Spoofing	☐	☐	☒	☒	☒	☒	☐	☒	2	1	-	1
	Phishing	☐	☐	☒	☒	☒	☒	☐	☒	2	1	-	1
	Intrusion malveillante sur le système informatique	☒	☒	☒	☒	☒	☒	☐	☒	2	1	-	1
	Attaques par déni de service	☒	☐	☐	☐	☒	☒	☐	☒	1	1	-	1
	Pratiques d'ingénierie sociale	☐	☐	☒	☒	☒	☒	☐	☒	0	0	-	1
	Fraude, détournement de fonds (interne ou externe)	☐	☒	☒	☒	☒	☒	☐	☒	2	1	-	1
	Racket, chantage	☒	☒	☒	☐	☒	☒	☐	☒	1	1	-	1
	Interception d'un échange de données sensibles avec un tiers	☐	☒	☒	☒	☒	☒	☐	☒	1	1	-	1
	Mauvaise gestion des habilitations et droits d'accès	☐	☒	☒	☒	☒	☒	☐	☒	1	1	-	1
Risques liés aux ressources humaines	Indisponibilité d'un homme clé, d'une équipe	☒	☐	☐	☐	☒	☒	☐	☒	1	0	-	1
	Démission ou départ d'un homme clé	☒	☒	☒	☐	☒	☒	☐	☒	0	0	-	1
	Surcharge de travail d'un collaborateur ou d'une équipe	☒	☐	☐	☐	☒	☒	☒	☒	0	0	0	1
	Erreur d'utilisation d'un système ou de procédures	☒	☒	☒	☐	☒	☒	☐	☒	1	1	-	1
Risques liés aux projets de développement	Déploiement	☒	☐	☐	☐	☒	☒	☐	☒	0	0	-	1
	Technologies utilisées	☒	☐	☐	☐	☒	☒	☐	☒	0	0	-	1
	Ressources humaines	☒	☐	☐	☐	☒	☒	☒	☒	0	0	0	1
	Rôles et responsabilités définis	☒	☐	☐	☐	☒	☒	☐	☒	0	0	-	1
	Erreur de conception	☒	☐	☐	☐	☒	☒	☐	☒	0	0	-	1
	Délai de mise en œuvre	☒	☐	☐	☐	☒	☒	☐	☒	0	0	-	1
	Intégration de la sécurité dans les projets	☒	☒	☒	☒	☒	☒	☐	☒	0	0	-	0
	Indépendance des environnements informatiques	☒	☒	☒	☐	☒	☐	☐	☒	0	-	-	1
Risques générés par les partenaires de l'entreprise	Externalisation	☒	☒	☒	☒	☒	☒	☒	☒	0	0	0	0
	Défaillance d'un fournisseur	☒	☐	☐	☐	☒	☐	☐	☒	0	-	-	1
Autres risques réglementaires et juridiques	Contrats avec les prestataires ou sous-traitants	☐	☐	☐	☐	☒	☐	☐	☒	0	-	-	0
	Nouvelles réglementations	☒	☐	☐	☐	☒	☒	☐	☒	0	0	-	0
	Evolution des structures juridiques	☒	☐	☐	☐	☒	☐	☐	☒	0	-	-	0

5.5 Familles de risque et MEHARI v3

Les numéros indiqués dans la colonne scénarii de MEHARI v3 correspondent à la numérotation des scénarii des la base de connaissance de la méthode MEHARI

Famille de risques	Liste des risques	Scénarii MEHARI v3
Risques environnementaux	Evènements naturels	02.10 - 2.30
	Infections sanitaires	1.70
	Indisponibilité des fluides (eau, électricité...)	1.23a/b/c/d/e
Risques sociaux / Guerres	Terrorisme / Guerre / Guerre Civile	02.40
	Emeute, grève, manifestation	01.50 - 01.60
Risques physiques des locaux	Risque d'infrastructure	01.71a - 01.71b - 2.20
	Les équipements informatiques et télécoms	01.20
	Les bureaux utilisateurs	01.71c
Risques sur les matériels informatiques	Infrastructures réseaux, télécoms et serveurs	01.20
	Téléphonie	
	Vol ou destruction de matériel	10.50 - 2.40 - 4.40 - 7.40 - 9.20
	Technologies utilisées	
	Dimensionnement des équipements	
	Maintenance	01.40 - 03.20
	Equipements de secours	3.31a/b - 4.20
Risques sur les logiciels	Systèmes non conformes aux spécifications	5.10 - 5.20 - 5.30
	Maintenance insuffisante	1.42
	Technologies utilisées	
	Perte de données	4.10 - 4.40 - 10.30 - 10.40 - 11.10 - 11.20
	Bogue logiciel	01.30
	Propriété intellectuelle	09.40 - 12.21

Famille de risques	Liste des risques	Scénarii MEHARI
Risques de piratage informatique, hacking ,	Virus et infections informatiques	04.50 - 10.10 - 10.20 - 5.10
	Spoofing	7.61 - 8.25
	Phishing	07.63
	Intrusion malveillante sur le système informatique	07.10 - 07.20 - 07.30 - 08.10
	Attaques par déni de service	3.40
	Pratiques d'ingénierie sociale	7.51 - 7.61
	Fraude, détournement de fonds (interne ou externe)	07.50
	Racket, chantage	
	Interception d'un échange de données sensibles avec un tiers	08.20 - 09.10 - 09.30 - 7.62
	Mauvaise gestion des habilitations et droits d'accès	8.31b - 8.32a/b
Risques liés aux ressources humaines	Indisponibilité d'un homme clé, d'une équipe	01.10
	Démission ou départ d'un homme clé	01.10
	Surcharge de travail d'un collaborateur ou d'une équipe	
	Erreur d'utilisation d'un système ou de procédures	04.30 - 06.10 - 06.20
Risques liés aux projets de développement	Déploiement	
	Technologies utilisées	
	Ressources humaines	
	Rôles et responsabilités définis	
	Erreur de conception	3.10
	Délai de mise en œuvre	
	Intégration de la sécurité dans les projets	
	Indépendance des environnements informatiques	
Risques générés par les partenaires de l'entreprise	Externalisation	
	Défaillance de fournisseur d'un fournisseur	01.42
Autres risques réglementaires et juridiques	Contrats avec les prestataires ou sous-traitants	
	Nouvelles réglementations	
	Evolution des structures juridiques	12.10 - 12.20

5.6 Critères analysés par l'assureur et leur points de contrôle possibles

Contact		Critères analysés par l'assureur	Invariants de MEHARI	Items ISO 17799 : 2000
DSI	Organisation générale du système d'information			
		Matériel		
		Système d'exploitation		
		Réseaux		
		Administration		
DF	Comment ce S.I. contrôle l'activité» économique de l'entreprise			
		Profil de l'entreprise		
		Nombre d'utilisateurs		
		Infogérance, hébergement		
		Estimation des impacts suite à arrêt des systèmes		
RSSI	La politique sécurité de l'entreprise			
		Protection physique	B1 - B2	7.1
		Sauvegarde	F2	8.6
		Organisation de la Sécurité informatique	A1	4.1
		Mesures anti-intrusion	C2	9.4
		Contrôle d'accès logique interne	D1	9.5
		Protection antivirus	Sous services : 08D07 - 11D06	8.3
		Plan de reprise d'activité	F1	11.1

5.7 Les mécanismes de l'assurance

La tarification

La prime couvre les charges suivantes :

- le coût du risque, soit la fréquence multipliée par le coût moyen (les sinistres),
- une réserve de sécurité (dotation de la provision de sinistres),
- les chargements (frais d'acquisition et frais de gestion),
- la rémunération de l 'intermédiaire (commission),
- les taxes réservées à l'état.

Le principe indemnitaire

Le contrat d'assurance est soumis au principe indemnitaire énoncé par l'article L 121-1 du Code des Assurances dont le premier alinéa stipule que « l'assurance relative aux biens est un contrat d'indemnité : l'indemnité due par l'assureur à l'assuré ne peut dépasser le montant de la valeur de la chose assurée au moment du sinistre ».

Très important, « L'assurance ne peut être une cause de bénéfice pour l'assuré; elle ne lui garantit que la réparation de ses pertes réelles ou de celles dont il est responsable ».

Dans les faits, un dommage n'est indemnisable que pour autant qu'il existe des éléments de preuve précis sur le mécanisme du sinistre démontrant qu'il résulte bien d'une cause garantie. La charge de cette preuve incombe à l'assuré.

Les exclusions

Une police d'assurance comporte toujours des exclusions, certaines légales (fait intentionnel de l'assuré), d'autres contractuelles et peuvent concerner tant les biens assurés que les événements.

Si l'assureur entend invoquer une exclusion pour refuser son intervention, la charge de la preuve lui appartient, il devra démontrer que le sinistre entre dans le champ d'application de l'exclusion.

Les exclusions peuvent être directes ou indirectes selon la forme de rédaction de la police :

Dans les polices "Tous risques sauf", tout ce qui n'est pas expressément exclu est garanti, alors que dans les polices "périls dénommés" tout ce qui n'est pas expressément garanti est exclu."

Rapport Sinistre/Prime (%)

Afin de maintenir les principes de fonctionnement, la somme des sinistres payés par les Assureurs ne doit pas excéder la somme des primes encaissées, majorées des profits financiers. Le rapport des sinistres payés sur les primes encaissées représente donc le rapport S/P.

Les franchises

c'est la somme qui, dans le règlement d'un sinistre, reste à la charge de l'assuré. L'assuré dont le contrat comporte une franchise s'engage à conserver à sa charge une partie des dommages.

Les différentes sortes de franchise

la franchise simple ou relative : l'assureur prend en charge l'intégralité des dommages dès l'instant qu'ils excèdent le montant de la franchise ;

la franchise absolue (cas le plus fréquent) : elle est toujours déduite de l'indemnité, quelle que soit l'importance des dommages ;

la franchise proportionnelle : elle est exprimée en pourcentage (précisé dans le contrat) du montant du sinistre.

Cette somme détermine le montant de rétention de l'assuré et indique le seuil d'intervention de l'assureur.

Limites contractuelles de garantie

L'indemnité d'assurance correspond à la somme que l'assureur verse après un sinistre. De façon quasi-systématique, ce montant est limité à une certaine somme en fonction des garanties et fixée contractuellement par le contrat. Elle est stipulée par sinistre, par événement et/ou par année d'assurance.

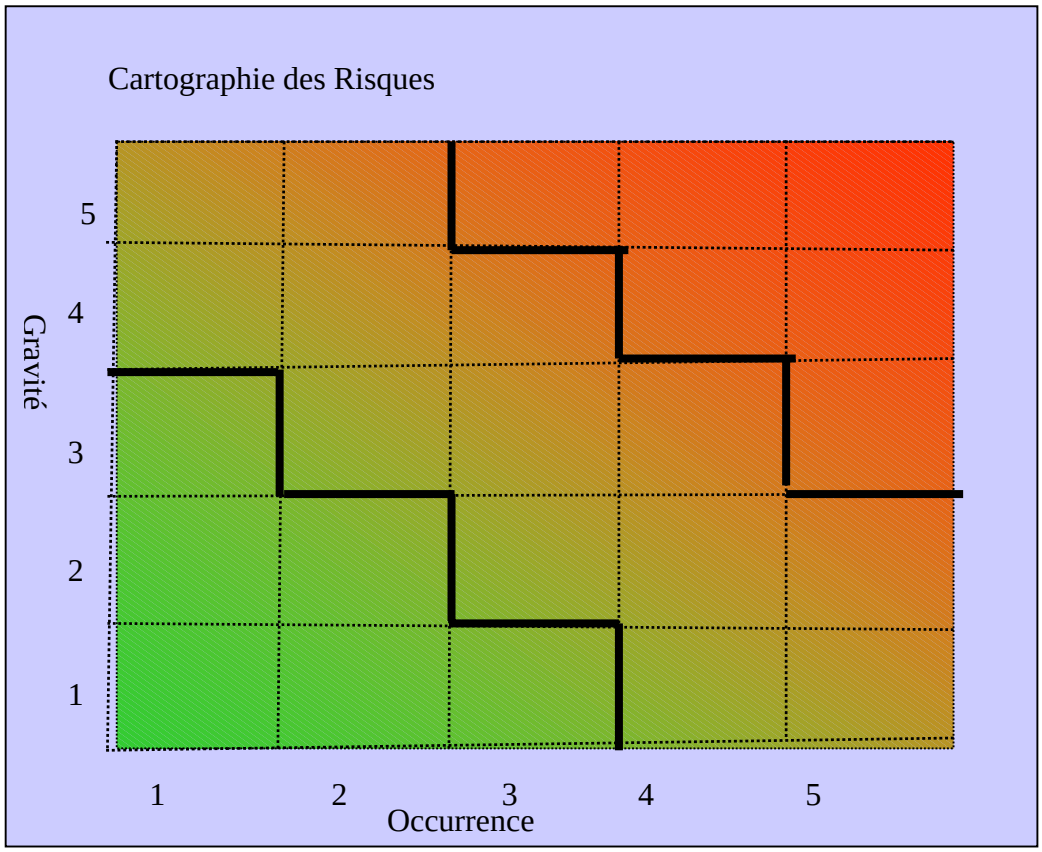
Premiers risques

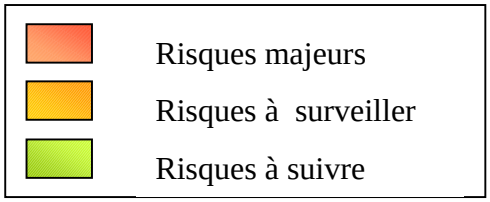
c'est une couverture d'assurance d'une valeur beaucoup moindre que la valeur du bien assuré. Le dommage est indemnisé jusqu'à concurrence de la somme assurée qui a été fixée sans que l'on puisse mettre en avant une sous-assurance. La somme d'assurance convenue est toujours inférieure à la valeur intégrale. On retrouve cette démarche quand l'assuré ne prévoit pas de perte totale due au risque considéré ou que le marché de l'assurance ne fournit pas les capacités suffisantes.

5.8 Exemples d'indicateurs du RM

Les indicateurs issus de la cartographie, de la revue effectuée régulièrement mettent en évidence l'évolution des risques et l'efficacité des plans d'action retenus.

Les indicateurs doivent être définis par les propriétaires des processus Métier.



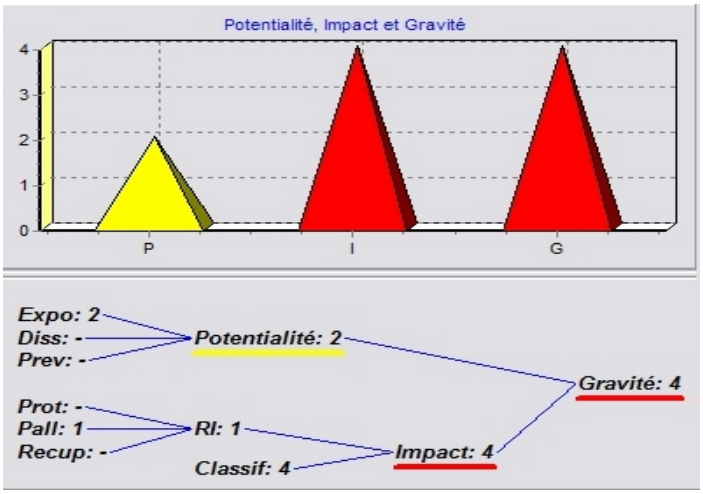


Détermination du modèle graphique : le pilote du projet détermine le critère d'évaluation correspondant à l'axe des abscisses et celui correspondant à l'axe des ordonnées. Si un troisième critère d'évaluation a été retenu , il faut déterminer le moyen de le faire apparaître sur le graphique : points de couleurs différentes, de tailles différentes, visage plus ou moins souriant, etc.

Plusieurs modèles graphiques sont possibles. Quel que soit le graphique, le visuel est identique. Ce sont les axes qui sont modifiés.

5.9 Exemples d'indicateurs du RSSI

Ces indicateurs, sont, par exemple, pour une ressource donnée et scénario de sinistre défini, extraits du logiciel RISICARE supportant le Plan Opérationnel de Sécurité de MEHARI :



Cet exemple montre que d'après les conventions de la méthode MEHARI :

- les mesures qui doivent réduire la potentialité de survenance sont de niveau moyen (niveau 2 sur une échelle de 0 à 4),
- les mesures de réduction d'impact (RI) sont peu efficace et de niveau 1 (niveau 1 sur une échelle de 1 à 4).

La ressource atteinte par le scénario étudié étant classifiée à 4 donc très critique (niveau 4 sur une échelle de 1 à 4)

Le scénario étudié a donc une gravité de 4 c'est-à-dire qu'il met en péril le devenir même de l'entreprise

5.10 Exemples d'indicateurs communs

La communication sous forme d'allers – retours (le RM vers le RSSI puis le RSSI vers le RM) nécessite une compréhension commune des risques du SI de l'entreprise.

Exemple d'indicateurs communs issus de la méthode MEHARI :

I = 4	G = 3	G = 3	G = 4	G = 4
I = 3	G = 2	G = 3	G = 3	G = 4
I = 2	G = 1	G = 2	G = 3	G = 3
I = 1	G = 1	G = 1	G = 1	G = 3
	P = 1	P = 2	P = 3	P = 4

Tableau dans lequel l'impact et la potentialité spécifient la gravité du sinistre redouté :

I est le niveau d'impact d'un sinistre sur une ressource ou un processus avec :

I = 1 : Impact **insignifiant** au niveau de l'entreprise

I = 2 : Impact **significatif** causant du tort à l'entreprise

I = 3 : Impact **très grave** sans menacer la vie de l'entreprise

I = 4 : Impact **extrêmement grave** menaçant l'entreprise

P est la potentialité de survenance du sinistre avec :

P = 0 : **Non envisageable** ou non envisagé

P = 1 : Très **improbable**, ne surviendra probablement jamais

P = 2 : **Possible**, bien qu'improbable

P = 3 : **Probable**, devrait arriver un jour

P = 4 : **Très probable**, surviendra sûrement à court terme

G la gravité résultante du sinistre pour l'entreprise

Niveau 4 : Vital

A ce niveau le dysfonctionnement redouté est extrêmement grave et met en danger l'existence même ou la survie de l'entité ou de l'une de ses activités majeures.

Niveau 3 : Très Grave

Il s'agit là des dysfonctionnements très graves au niveau de l'entité, sans que son avenir soit compromis.

Niveau 2 : Important

Il s'agit là de dysfonctionnements ayant un impact notable au niveau des opérations de l'entité, de ses résultats ou de son image, mais restant globalement supportables.

Niveau 1 : Non significatif

A ce niveau les dommages encourus n'ont pratiquement pas d'impact sur les résultats de l'entité

ni sur son image, même si certaines personnes sont fortement impliquées dans le rétablissement de la situation d'origine.

Autre exemple d'indicateurs concernant le risque résiduel :

RM	RSSI		RM	
Impact sur la ressource	Potentialité de survenance	Mesures de réduction d'impact	Risque résiduel	Assurance
Fort	Forte	Fortes, efficaces, robustes	Faible	Non
Fort	Faible	Aucune possible	Fort	Oui, partiellement

Les niveaux fort à faible pourront s'exprimer selon une grille prédéfinie en termes

quantitatif (par exemple : financier, perte d'efficacité, montant de pénalités ou d'amendes),

qualitatif (par exemple : image de marque, troubles sociaux ou politiques, retard de livraison, risque de santé publique, etc.)

Le transfert à l'assurance se fera dans ce cas, en tenant compte de la politique de transfert du risque adaptée à chaque entreprise (voir tableau page 26) d'une part, et des familles de risques et leur assurabilité d'autre part (voir annexe page 35).

5.11 Glossaire

Préambule :

Ce référentiel terminologique a pour objectif de faire mieux comprendre les termes utilisés dans le cadre du management des risques en entreprises. Il se décompose en trois parties :

- **Le vocabulaire utilisé par les Risk-Managers (en noir)**
- **Le vocabulaire utilisé par les RSSI (en bleu)**
- **Le vocabulaire utilisé par les Assureurs (en rouge)**

ACCEPTATION DU RISQUE (Risk Acceptance)

Décision d'accepter un risque.

Note 1 :

Le verbe "accepter" a été choisi pour exprimer l'idée selon laquelle l'acceptation est prise dans le sens fondamental que donne le dictionnaire.

Note 2 :

L'acceptation du risque dépend des critères de risque.

Source ISO/IEC Guide 73:2002

ACCIDENTS (Accident)

Toute atteinte dont l'origine est en général liée à des éléments naturels, ou à certaines causes de nature **involontaire**. Les conséquences dues aux accidents sont tangibles et se manifestent surtout sur l'environnement physique.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

Evénement soudain et imprévu.

ACTUAIRE (Actuary)

Spécialiste qui applique, en assurances et en réassurance Vie et non-Vie(Dommages), la théorie des probabilités à l'évaluation des risques et au calcul des primes, des provisions techniques et des provisions mathématiques.

Source Fonction : Risk Manager aux Editions DUNOD

AGRESSION – ATTAQUE (Aggression – Attack)

Concrétisation d'une menace qui provoquera une atteinte sur l'environnement physique, logique ou organisationnel de la donnée et/ou de l'information. Les mesures de sécurité retenues pour lutter contre l'agression seront la dissuasion et, à un niveau plus fort, la protection dont le premier objectif sera de détecter l'agression, de tenter de la neutraliser ou à défaut d'en atténuer les effets.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

ALEA (Contengency – Fortuitous Event)

Phénomène ou événement dont la réalisation n'est connue qu'en termes de probabilités.

ANALYSE DU RISQUE (Risk Analysis)

Utilisation systématique d'informations pour identifier les sources et pour estimer le risque.

Note 1: L'analyse du risque fournit une base à l'évaluation du risque, au traitement du risque et à l'acceptation du risque.

Note 2 : Les informations peuvent inclure des données historiques, une analyse théorique, des opinions justifiées, et des préoccupations des parties prenantes.

Source ISO/IEC Guide 73:2002

APPLICATION STRATÉGIQUE (Strategic Application)

Application ou information qui en cas de destruction, de perte d'intégrité, de vol ou de copie, **peut entraîner des risques majeurs**.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

APPRECIATION DU RISQUE (Risk Assessment)

Ensemble du processus d'analyse du risque et d'évaluation du risque.

Source ISO/IEC Guide 73:2002

APPROCHE ANALOGIQUE (Analogical Approach)

Approche pragmatique s'appuyant sur des scénarios qui se sont déjà produits et qui servent d'exemples à des fins de sensibilisation ou d'appréciation d'enjeux.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

APPROCHE ANALYTIQUE (Analytical Approach)

Approche s'appliquant aux actions ponctuelles, c'est-à-dire à celles qui correspondent à des incidents imprévus ou à une volonté impérative de traiter un point particulier ressenti comme dangereux. Les actions menées dans cette approche agissent sur des problèmes isolés où les efforts sont concentrés sur des éléments bien précis. Elle considère plus la nature des interactions avec les autres systèmes que les effets de ces interactions. Elle valide des faits en effectuant la preuve expérimentale dans les cadres d'une théorie. L'approche est efficace lorsque les interactions sont linaires et faibles. L'ensemble des actions est programmé dans le détail mais le but est mal défini.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

APPROCHE SYSTÉMIQUE (Systemic Approach)

Approche permettant d'aborder un problème avec une vision globale. Elle est utilisée en particulier pour faire face aux complications caractérisant les systèmes. Elle fait prendre conscience de nouvelles propriétés que ne possèdent pas individuellement les éléments du système. L'approche systémique se concentre sur les interactions entre les éléments, dont elle considère les effets. Elle valide les faits par comparaison du fonctionnement d'un modèle avec la réalité. L'approche systémique conduit à une action par objectif où le but est bien défini mais où les détails sont flous. Elle permet de s'élever pour mieux voir, pour mieux comprendre, pour mieux situer et relier, et surtout pour mieux agir.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

ASSURE (policy holder)

Bénéficiaire de l'assurance

ATTAQUE LOGIQUE (Logical Attack)

Utilisation **non autorisée des ressources du système** d'information, conduisant à un préjudice au moins qualitatif pour la victime, cela se traduisant essentiellement par une **perte d'intégrité** et/ou de **disponibilité**, entraînant le plus souvent un profit indirect pour le criminel et/ou commanditaire éventuel. Il s'agira de sabotage immatériel, d'infection informatique, de programme « simple », de bombe logique, de cheval de Troie, de sabotage « manuel », de programme autoreproducteur, de ver ou de virus.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

ATTEINTE (Attack)

Effet ou dégradation résultant de l'agression. Elle sera traduite en termes :

- ***d'impacts tangibles*** qui pourront être une altération physique (supports, machines...), un

dysfonctionnement logique (programmes...), une désorganisation du système (procédures...) ;

- ***d'impacts logiques*** (non disponibilité de l'information, altération de l'intégrité de l'information, violation de la confidentialité de l'information),

- ***d'impacts stratégiques*** qui sont sur le plan financier liés aux :

- frais supplémentaires d'hébergement, de transport, de télécommunications, d'intervention d'experts, d'achat/location de matériel et progiciels, de personnels, et de sous-traitance.

- aux pertes :

- d'exploitation (pertes de marge, de trésorerie, de clientèle),

- de fonds ou de biens,

- des enjeux majeurs, comme le dépôt de bilan.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

ATTENUATION DES RISQUES (Risk Mitigation, Risk Reduction)

Limitation de toute conséquence négative d'un événement particulier.

Source ISO/IEC Guide 73:2002

Moyens de réduction des risques avant leur occurrence, de confinement des risques pendant l'événement et de restauration ou remplacement après la survenance.

Source Fonction : Risk Manager aux Editions DUNOD

AUDIT (Audit)

Vérification de la conformité d'un dispositif par rapport à un référentiel de normes préalablement fixé.

Source Fonction : Risk Manager aux Editions DUNOD

AUDITABILITÉ (Auditability)

Propriété pour un système de permettre l'**identification des actions des utilisateurs**, par exemple, en cas de fraude, de tentatives d'accès non autorisés ou en cas d'incidents.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

AUTHENTIFICATION (Authentication)

Procédure conventionnelle permettant de s'assurer de la qualité de son correspondant (J.O. du 30/12/1984).

BACKUP (Backup)

Actions de remise en état du soutien informatique apporté aux fonctionnalités de l'entreprise.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

BASE INCIDENTS (Incidents and Claims Database)

Outil permettant de constituer un historique de données, d'identifier les mécanismes de prévention, et à terme, de prioriser les plans d'action et de préciser les coûts d'opportunité engendrés par certains choix budgétaires.

Ensemble organisé des données nécessaires à la connaissance et à la gestion des événements de risques.

Source Fonction : Risk Manager aux Editions DUNOD

BIEN – ACTIF (Asset)

Tout élément représentant de la valeur pour l'organisme.

Source ISO/IEC 13335-1:2004

BOGUE (Bug)

Erreur de programmation qui n'a pas été localisée pendant la phase de bêta-test ou de recette provisoire et qui est encore présente dans un produit commercialisé ou une application.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

(2) Défaut de conception ou de réalisation se manifestant par des anomalies de fonctionnement (J.O. 19/02/1984).

BOMBE LOGIQUE (Logical Bomb)

Programme informatique illicite dont l'objectif est d'attaquer un système d'information et qui se **déclenche en fonction d'événements particuliers**, par exemple, pour effacer des données.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

BRIS DE MACHINE (Computer Breakdown)

Assurance des risques de destruction ou bris accidentel des machines servant à la production de l'entreprise.

CAPACITE (Capacity)

Montant maximal d'assurance ou de réassurance disponible pour couvrir des risques au niveau d'une entreprise ou d'un marché en général. Pour un assureur, la capacité est généralement fonction des capitaux propres, du chiffre d'affaires et des moyens complémentaires obtenus par la réassurance.

Source Fonction : Risk Manager aux Editions DUNOD

CAPITAL ASSURE (Sum Insured)

Somme déclarée au contrat d'assurance pouvant servir d'assiette de prime ou de limite maximum d'indemnité.

CAPTIVE (Captive Insurance - Reinsurance Company)

Société d'assurance ou de réassurance créée par un groupe industriel ou commercial pour couvrir les risques du groupe.

CARENCE DE FOURNISSEURS (Suppliers and Subcontractors Extension)

Sinistre

CARTOGRAPHIE DES RISQUES (Risk Mapping)

Processus d'identification, de quantification et de hiérarchisation des risques permettant d'établir un état des lieux à un instant T des différents risques avérés ou potentiels que pourrait supporter ou supporte l'entreprise ou le groupe.

CATASTROPHES NATURELLES (Natural Events)

Ce sont les événements naturels tels que les cyclones, inondations, secousses sismiques…

Tout événement qui constitue par son importance et son étendue un risque catastrophique. Elles sont imprévisibles.

Pour que le contrat fonctionne et que la garantie soit accordée il faut que l'état de catastrophe naturel soit constaté par un arrêté ministériel et publié au journal officiel.

Source Fonction : Risk Manager aux Editions DUNOD

CAUSE (Cause)

L'événement, l'état, le contexte, l'entité, l'action... qui sont l'**origine** et qui produisent "l'**effet**" dont on subira les "**conséquences**".

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

CELLULE DE CRISE (Cell of Crisis)

Dispositif en principe ponctuel, activé en cas de crise déclarée (risque matérialisé et non maîtrisé) pour prendre l'ensemble des décisions relatives à la gestion de la crise.

CLASSIFICATION (Classification)

Opération permettant d'évaluer conventionnellement la valeur d'un objet ou d'une ressource du système d'information en fonction de plusieurs composantes (Disponibilité, Intégrité, Confidentialité, Preuve et contrôle).

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

CODE DES ASSURANCES (Insurance Regulation)

C'est l'ensemble des lois et des règlements qui doivent être respectés par les assureurs et qui régissent les relations assurés/assureurs.

Source Fonction : Risk Manager aux Editions DUNOD

COMITÉ DE DÉCISION (Decision Committee)

Groupe de personnes dont la principale fonction est délibérative. Il est composé de membres qui occupent des postes à haut niveau de responsabilité : la Direction Générale sera représentée par un "financier" ou par un spécialiste du contrôle de gestion budgétaire ayant le pouvoir d'affecter des budgets, le responsable des services centraux de sécurité, l'informatique, qui est représentée par son Directeur, assisté par les responsables des études et de l'exploitation / système. Les fonctions de secrétaire et d'animateur seront assurées par le RSSI.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

COMITÉ DE SÉCURITÉ OPÉRATIONNELLE (Committee of Operational Safety)

C'est un groupe de travail composé de spécialistes opérationnels. Il traitera l'ensemble des problèmes de sécurité selon les urgences préconisées par le schéma directeur préalable ou simplement en fonction de l'intuition.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

COMMUNICATION RELATIVE AU RISQUE (Risk Communication)

Echange ou partage d'informations concernant le risque entre le décideur et d'autres parties prenantes.

Note :

Les informations peuvent concerner l'existence, la nature, la forme, la probabilité, la gravité, l'acceptabilité, le traitement, ou d'autres aspects du risque.

Source ISO/IEC Guide 73:2002

COMPENSATION (Compensation)

C'est la mesure de sécurité qui aura un effet indirect sur les conséquences des atteintes mêmes, et surtout pour celles où il n'est prévu aucune action, mais simplement un report sur l'assurance en cas de "sinistres" ou de "pertes". Elle atténuera les conséquences de l'atteinte (pertes financières résiduelles) non prises en compte par les autres mesures. Elle intègrera également les récupérations financières d'ordre juridique.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

CONFIDENTIALITÉ (Confidentiality)

Caractéristique d'une donnée ou d'une information, qui, selon son degré, permet d'accorder, ou non, son accès en lecture à des individus, en fonction de leur habilitation à prendre connaissance de son contenu.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

CONSEQUENCE (Consequence – Effect)

Résultat d'un événement.

Note1 :

Il peut y avoir plus d'une conséquence d'événement.

Note 2 :

Les conséquences peuvent englober des aspects positifs et des aspects négatifs. Cependant, les conséquences sont toujours négatives pour les aspects liés à la sécurité.

Note 3:

Les conséquences peuvent être exprimées de façon qualitative ou quantitative.

Source ISO/IEC Guide 73:2002

Répercussion de l'effet, au second degré, sur d'autres plans, qui pourront être successivement de niveaux : physiques (destruction matérielle), logiques (atteinte organisationnelle), puis conceptuels (atteinte stratégique, pertes financières ou réalisation d'enjeux).

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

COUVERTURE DU RISQUE (Risk Coverage)

Niveau de maîtrise du risque à un instant T.

CRITERES DE RISQUE (Risk Criteria)

Termes de référence permettant d'apprécier l'importance des risques.

Note :

Les critères de risque peuvent comprendre les coûts et les avantages, les exigences d'ordre légal et réglementaire, les aspects sociaux économiques et environnementaux, les préoccupations des parties prenantes, les priorités et d'autres éléments pour l'appréciation.

Source ISO/IEC Guide 73:2002

CRITICITE (Criticality)

(Ou gravité des risques)

Ensemble des conséquences (financières, humaines, …) d'un risque.

CUMUL (Aggregate)

Ensemble des risques pouvant être touchés par un même événement dommageable ou ensemble des participations souscrites sur un même risque.

Source Fonction : Risk Manager aux Editions DUNOD

DISPONIBILITÉ (Availability)

Caractérise une donnée ou une information attendue, qui, prise dans un contexte de résultat, lui donne les

facultés d'être obtenue en temps voulu. On peut par extension y associer la notion de PÉRENNITÉ, c'est-à-dire la notion de conservation dans le temps qui contribue à cette disponibilité.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

DISSUASION (Dissuasion)

Mesure de sécurité qui limitera la concrétisation de la menace en agression et aura un effet atténuateur sur des agressions en cours de réalisation. Elle correspond à la mise en œuvre de moyens appropriés, en vue de décourager un éventuel "agresseur", de tenter contre "l'entreprise" un acte d'agression via ses systèmes d'information. Les actions qui la composent tendront à lui prouver que la valeur de l'enjeu qu'il convoite est inférieure à celle des dommages que le système menacé peut lui infliger.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

DIVULGATION D'INFORMATIONS (Information Disclosure)

Utilisation **non autorisée des ressources** du système d'information, entraînant la divulgation à des tiers d'informations confidentielles.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

DOMMAGE CORPOREL (Damage)

Atteinte à l'intégrité physique des personnes.

DOMMAGES IMMATERIELS (Consequential Loss)

Tout préjudice résultant de la privation de jouissance d'un droit, de l'interruption d'un service rendu par une personne ou par un bien meuble ou immeuble ou de la perte de bénéfice qu'entraîne directement ou indirectement la survenance de dommages corporels ou matériels.

DOMMAGES MATERIELS (Material Damage)

Toute atteinte à la structure ou à la substance d'une chose ou d'un animal.

DONNÉE (Data)

(1) C'est une représentation conventionnelle d'un fait, d'un objet, d'un état.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

(2) Représentation d'une information sous une forme conventionnelle destinée à faciliter son traitement (en anglais : data) (J.O. 17/1/1982). Au niveau conceptuel, cette information est représentée par des entités, propriétés, relations.

EFFECTIF (Effective)

Ce qui est en général concret, réel et qui a eu lieu (dans les causes qui sont à l'origine de cette atteinte, la pénétration est un élément effectif du processus de l'agression).

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

EFFET (Effect)

Ce qui est produit par la cause. Nous retiendrons la définition restrictive suivante : c'est le résultat direct, tangible, de ce qu'un événement, une action, un auteur, un contexte... matérialisant la cause, produit au premier degré sur l'environnement physique, logique et organisationnel de la donnée et de l'information.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

ELEMENTS DE PILOTAGE DE RISQUES (Risk Drivers)

Facteurs justifiant le besoin de gestion des risques. Les éléments de pilotage de risques comprennent souvent le rythme de changement, le besoin de diligence raisonnable, les attentes des parties en matière de bonne gouvernance, etc.

Source Fonction : Risk Manager aux Editions DUNOD

ENJEU (Stake)

Ce que l'on peut perdre ou gagner. Ils peuvent être de différents niveaux. L'enjeu majeur de l'entreprise sera le dépôt de bilan.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

ESTIMATION DU RISQUE (Risk Estimation)

Processus utilisé pour affecter des valeurs à la probabilité et aux conséquences d'un risque.

Note :

L'estimation du risque peut considérer le coût, les avantages, les préoccupations des parties prenantes, et d'autres variables requises selon le cas pour l'évaluation du risque.

Source ISO/IEC Guide 73:2002

EVALUATION DU RISQUE (Risk Evaluation)

Mesurer l'impact de la réalisation de l'aléa sur les objectifs de l'entreprise ou du groupe.

Processus de comparaison du risque estimé avec des critères de risque donnés pour déterminer l'importance d'un risque.

Note: L'évaluation du risque peut être utilisée pour appuyer la décision d'accepter ou de traiter un risque.

Source ISO/IEC Guide 73:2002

EVALUATION QUANTITATIVE DES RISQUES (Risk Evaluation, Risk Measurement)

Processus quantitatif de mesure d'une fréquence ou d'une gravité en vue de calculer le poids financier d'un risque.

Source Fonction : Risk Manager aux Editions DUNOD

EVALUATION QUALITATIVE DES RISQUES (Risk Assessment)

Processus d'identification, de mesure de l'impact et de la probabilité d'un risque et de ses composantes, en général par score.

Source Fonction : Risk Manager aux Editions DUNOD

EVENEMENT (Event – Occurrence)

Phénomène (naturel ou non), accident, incident, tendance, résultat, circonstance, décision.

Occurrence d'un ensemble particulier de circonstances.

Note 1 :

L'événement peut être certain ou incertain.

Note 2 :

L'événement peut être une seule occurrence ou une série d'occurrences.

Note 3 :

La probabilité associée à l'événement peut être estimée sur une période de temps donnée.

Source ISO/IEC Guide 73:2002

EVENEMENT DE RISQUE (Risk Event)

Occurrence d'un risque, d'une circonstance ou situation réelle.

Source Fonction : Risk Manager aux Editions DUNOD

EVENEMENT LIE A LA SECURITE DE L'INFORMATION (Information Security event)

Occurrence identifiée d'un état d'un système, d'un service ou d'un réseau, indiquant une brèche possible dans la politique de sécurité de l'information ou un échec des moyens de protection, ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité.

Source ISO/IEC/TR 18044:2004

EVITEMENT DE RISQUE (Risk Avoidance)

Décision de ne pas prendre un risque, c'est-à-dire de choisir une autre voie qui ne fait pas intervenir ce risque.

Source Fonction : Risk Manager aux Editions DUNOD

EXCLUSION (Exclusion)

Clause de la police par laquelle l'assureur manifeste son intention de ne pas couvrir un risque ou un événement. Celle- ci doit être formelle et limitée. La charge de la preuve d'une exclusion appartient toujours à l'assureur.

EXPERT DU RISQUE (Expert of the Risk)

Spécialiste dans un domaine de compétence liée à la gestion de risque, apportant conseil et méthodologie au niveau des méthodes ou des processus.

FACTEURS DE RISQUES (Risk Factors)

Sources ou initiateurs de risques (voir initiateurs de risques).

Sources de risque qui sont classées en risques inhérents génériques probables dans le but de faciliter l'évaluation ou l'atténuation des risques.

Source Fonction : Risk Manager aux Editions DUNOD

FACTEUR DE RISQUE DE VERIFICATION (Audit Risk Factor)

Risque que le vérificateur tire les mauvaises conclusions, par exemple, en déclarant que les sujets vérifiés sont en conformité alors qu'ils ne le sont pas, ou en déclarant qu'ils ne sont pas en conformité alors qu'ils le sont.

Source Fonction : Risk Manager aux Editions DUNOD

FAIT GENERATEUR (Trigger Event)

Evénement qui est la cause génératrice du dommage.

FINANCEMENT DES RISQUES (Risk Financing)

Dispositif visant à faire supporter tout ou partie du risque à un tiers externe (assurance, captive,…).

Réserve de fonds pour couvrir les coûts de mise en œuvre du traitement du risque et les coûts associés.

Note : Dans certaines industries, le financement du risque consiste à provisionner uniquement les conséquences financières relatives au risque.

Source ISO/IEC Guide 73:2002

FINITE (Finite)

Le « finite » est une technique de financement *a priori* de pertes futures de type pré-identifié avec des techniques qui relèvent plus du domaine bancaire que du domaine de l'assurance. Ce n'est plus l'aléa en tant que tel qui est couvert, mais plutôt les conséquences financières de l'aléa lorsqu'il est survenu.

Source Fonction : Risk Manager aux Editions DUNOD

FONCTION (Function)

Terme générique désignant un ensemble d'activités ou processus d'une entreprise, d'un secteur ... voire d'un poste. Chaque fonction peut se décomposer hiérarchiquement en un certain nombre de sous fonctions.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

FORME DU CONTRAT (Form)

Elle peut être fondamentalement différente :

- « périls dénommés » : liste finie de cas de figure assurés ;
- ou « tout sauf » : le champ de la couverture est défini ou limité par les exclusions.

Source Fonction : Risk Manager aux Editions DUNOD

FRAIS SUPPLEMENTAIRES D'EXPLOITATION (Increased Cost of Working)

Frais supplémentaire engages après un sinistre pour réduire la perte de bénéfice et permettre le redémarrage rapide des activités.

FRANCHISE (Deductible)

Somme d'argent ou fraction de dommage laissée contractuellement à la charge de l'assuré.

FRAUDE (Fraud)

Utilisation non autorisée des ressources du système d'information, conduisant à un préjudice évaluable sur le plan monétaire pour la victime, essentiellement induit par le détournement de biens et de fonds au profit du criminel.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

FRÉQUENCE D'APPARITION (Frequency of Appearance)

Paramètre pris en compte dans l'appréciation de l'impact et quantifié par des nombres de 0 à 4 qui donneront cette fréquence : **(0)** une fois, **(1)** une fois par an, **(2)** une fois par mois, **(3)** une fois par semaine, **(4)** plusieurs fois par jour.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

GAREAT

Gestion de l'assurance et de la réassurance des risques attentats et actes de terrorisme. GIE crée en décembre 2001 agissant en qualité de pool obligatoire de réassurance pour les risques de terrorisme survenant sur le territoire français.

GESTION DES INCIDENTS (Incident Management)

Identification et maîtrise des incidents par une analyse de leurs causes, impacts et coûts, sur un périmètre à la fois interne et externe. L'objectif est de réduire de façon significative le nombre d'incidents en développant des plans d'actions (notamment de prévention des causes de ces incidents).

GESTION DES RISQUES (Risk Management)

Application générale des politiques, processus et pratiques de traitement des risques. La gestion des risques peut inclure l'identification, l'évaluation, les mesures de réduction et de financement, la surveillance, le pilotage et la communication.

Source Fonction : Risk Manager aux Editions DUNOD

GESTION GLOBALE DES RISQUES (Total Management of the Risks)

Processus itératif d'identification, d'évaluation et de hiérarchisation des risques facilitant la mise en place d'outils de contrôle et d'optimisation de l'activité permettant d'atteindre les objectifs fixés dans le cadre de la stratégie de l'entreprise ou du groupe.

GESTION GLOBALE DES RISQUES DE L'ENTREPRISE (Total Management of the Risks)

GESTIONNAIRE DU RISQUE (Risk Manager)

Responsable - par délégation - de la mise en œuvre des actions arrêtées par le propriétaire dans son domaine, il a les moyens de cette gestion (en totalité ou partiellement pour les moyens humains et financiers, en totalité pour les moyens hiérarchiques). Agissant au nom du propriétaire du risque, il ne peut subdéléguer cette gestion.

GLOBALE DE BANQUE (Blanket Bankers Bond – Fidelity – Computer Crime)

Police d'assurance garantissant les dommages aux fonds et valeurs détenues par un établissement financier et au sein de la même police la fraude interne et externe et la malveillance informatique.

GRANDS RISQUES (Major Risks)

Définis par l'art.L111-6 du code des assurances en fonction de critères énoncés à l'art. R 111-1 du même code. Un grand risque réuni au moins deux des critères ci-dessous :

- total du dernier bilan > 6,2 millions d'euros
- chiffre d'affaire du dernier exercice > 12,8 millions d'euros
- effectifs moyen du dernier exercice > 250

GRAVITÉ DE L'IMPACT (Gravity of the Impact)

C'est l'appréciation du niveau de gravité (pondéré par fréquence d'apparition) des impacts quantifiés de 0 à 4 et signifiant : **(0)** sans gravité, **(1)** peu grave, **(3)** très grave, **(4)** extrêmement grave.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

GRAVITE DES RISQUES (Severity)

Ensemble des conséquences (financières, humaines…) d'un risque. Mots équivalents : intensité, sévérité.

Source Fonction : Risk Manager aux Editions DUNOD

GRILLE DE COTATION DES RISQUES (Risk Scorecard)

Outil de cotation qualitative des risques permettant d'en obtenir un classement et d'identifier des zones de risques essentielles. La cotation peut porter sur la fréquence et la gravité.

Source Fonction : Risk Manager aux Editions DUNOD

IDENTIFICATION DES RISQUES (Risk Identification)

Processus ayant pour objet de recenser l'ensemble des risques liés à un groupe ou une entreprise, un processus, un projet, une entité,… ainsi que leurs sources et leurs conséquences.

Processus permettant de trouver, lister et caractériser les éléments du risque.

Note 1 :

Les éléments peuvent inclure les sources ou les phénomènes dangereux, les événements, les conséquences et la probabilité.

Note 2 :

L'identification des risques peut également refléter les préoccupations des parties prenantes.

Source ISO/IEC Guide 73:2002

IDENTIFICATION DES SOURCES (Source Identification)

Processus permettant de trouver, recenser et caractériser les sources.

Note :

Dans le domaine de la sécurité, l'identification des sources est appelée identification des phénomènes dangereux.

Source ISO/IEC Guide 73:2002

IMPACT DU RISQUE (Impact of the Risk)

Conséquence d'un évènement qui se réalise.

Exprime le niveau des conséquences produites par une atteinte ou une agression.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

IMPACT STRATÉGIQUE (Strategic Impact)

Il exprime les conséquences des autres impacts en terme d'enjeux (le plus important étant probablement le dépôt de bilan.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

IMPUTABILITÉ (Imputability)

Propriété qui permet d'**imputer de façon certaine une opération** à un utilisateur à un moment donné.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

INCIDENT (Incident)

Evénement relevant d'un dysfonctionnement dans le processus, et susceptible, en fonction de sa gravité, de déclencher l'alerte pour la mise en route du processus de gestion de crise. Le dispositif de veille en matière de risques et de crise intègre le suivi des incidents. (Voir aussi 'Base incidents' et 'Gestion des incidents')

INCIDENT LIE A LA SECURITE DE L'INFORMATION (Information security incident)

Un incident lié à la sécurité de l'information est indiqué par un ou plusieurs événement(s) de sécurité de l'information indésirable(s) ou inattendue(s) présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information.

Source ISO/IEC TR 18044:2004

INDICATEUR DE RISQUE (Risk Indicators)

Paramètre de normes, de seuils, d'alertes ou de mesures permettant d'évaluer un risque.

Source Fonction : Risk Manager aux Editions DUNOD

INDUIT (Induced)

Qui est généré au second degré, ou qui est la conséquence de... (Les pertes financières induites par le vol du fichier marketing.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

INFORMATION (Information)

(1) Interprétation d'une donnée en fonction de critères relatifs à un point de vue.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

(2) Elément de connaissance susceptible d'être représenté à l'aide de conventions pour être conservé, traité ou communiqué (J.O. du 17/1/1982).

INITIATEUR DE RISQUE (Initiator of Risk)

Evénement source (situation, réorganisation, évolution sociétale et législative, tendance, fait, caractéristique…) qui est à l'origine d'une situation néfaste ou opportune pour l'organisation. Il a une appréciation positive, neutre ou négative.

INTÉGRITÉ (Integrity)

C'est en général une caractéristique des données et des informations qui les donnes comme étant exemptes de falsification ou de modification liée à des actions malveillantes. Par extension? On y associe parfois les notions de COHÉRENCE, de COMPLÉTUDE, voire de NON-RÉPUDIATION ou de NOTARISATION...

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

INTENSITE DES RISQUES (Severity)

Voir « Gravité ».

Source Fonction : Risk Manager aux Editions DUNOD

LIGNE DIRECTRICE

Description clarifiant ce qu'il convient de réaliser et par quels moyens, en vue d'atteindre les objectifs fixés par la politique de l'organisme.

Source ISO/IEC 13335-1:2004

MAITRISE DU RISQUE (Risk Control)

Actions de mise en œuvre des décisions de management du risque.

Note :

La maîtrise du risque peut impliquer la surveillance, la réévaluation et la mise en conformité avec les décisions.

Source ISO/IEC Guide 73:2002

MALVEILLANCE (Malicious Act)

Origine de certaines menaces sur lesquelles des actions de prévention pourraient avoir avec un effet retardateur (quant à leur naissance) ou éradicateur (suppression totale) sur les risques qu'elles représentent. La malveillance regroupe toutes actions commises directement ou indirectement par des personnes intérieures ou extérieures à l'entreprise ou à l'organisme concerné, y compris les actions commises à l'occasion d'émeutes ou de mouvements populaires, ainsi que les actes de terrorisme et de guerre étrangère.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

L'auteur d'un acte malveillant a eu la volonté de commettre non seulement l'action génératrice du dommage mais également sa conséquence dommageable.

MANAGEMENT DU RISQUE (Risk Management)

Activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque.

Note :

Le management du risque inclut généralement, l'appréciation du risque, le traitement du risque, l'acceptation du risque et la communication relative au risque

Source ISO/IEC Guide 73:2002

MATRICE DE RISQUES (Risk Matrix)

Tableau définissant les critères de l'évaluation de l'impact et de la probabilité, du niveau de maîtrise des risques. La matrice de risques présente un visuel compréhensible pour toutes les parties impliquées.

Source Fonction : Risk Manager aux Editions DUNOD

MAUVAIS USAGE RAISONNABLEMENT PREVISIBLE (Reasonably Foreseeable Misuse)

Utilisation d'un produit, procédé ou service dans des conditions ou à des fins non prévues par le fournisseur mais qui peut provenir d'un comportement humain envisageable.

Source ISO/IEC Guide 51:1999

MENACE (Threat)

"Signe" par lequel se manifeste ce que l'on doit craindre. C'est un indice ou une supposition qui laisse prévoir que quelque chose de dangereux ou de préjudiciable pourrait se produire si certaines conditions se concrétisent. Son état d'origine est **potentiel**, c'est-à-dire qu'elle n'existe que virtuellement. Elle est en puissance de devenir une *agression* tant que certaines conditions ne sont pas réunies pour sa concrétisation. Nous pouvons avoir à faire à des menaces inconnues, des menaces connues mais non maîtrisées et des menaces connues et maîtrisées.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

Cause potentielle d'un incident indésirable, pouvant entraîner des dommages au sein d'un système ou d'un organisme.

Source ISO/IEC 13335-1 :2004

MESURE (Control)

Moyen de gérer un risque, comprenant la politique, les procédures, les lignes directrices, et les pratiques ou structures organisationnelles, et pouvant être de nature administrative, technique, gestionnaire ou juridique.

Note : Le terme « mesure » est également utilisé comme synonyme de « conservation » ou de « contre-mesure »

Source ISO/IEC 17799:2005

MESURES DE SÉCURITÉ (Safety Measures)

Ensemble d'actions correspondant aux grandes fonctions regroupées en prévention, dissuasion, protection, restauration et compensation.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

MÉTHODE (Method)

Manière raisonnée d'agir pour parvenir à un résultat. Elle fait référence à des concepts qui sont des principes fondamentaux intégrés dans une démarche qui est un cheminement jalonné. Pour atteindre les résultats escomptés, elle utilise des outils automatisés (logiciels) ou non (modèles, tableaux, ...).

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

MODELISATION DES RISQUES (Risk Modelling)

Démarche et ensemble de techniques de représentation des risques en vue de leur évaluation statistique et mathématique.

Source Fonction : Risk Manager aux Editions DUNOD

MOYEN DE TRAITEMENT DE L'INFORMATION (Information Processing Facilities)

Tout(e) système, service ou infrastructure de traitement de l'information, ou locaux les abritant.

Source ISO/IEC 17799:2005

NON-RÉPUDIATION (Not-Repudiation)

Preuve qu'un message a été **envoyé par une personne précise à un moment précis**, sans avoir été modifié depuis son envoi. Cette preuve devrait pouvoir être vérifiée à tout moment par un tiers. Sans la non répudiation, des émetteurs et des récepteurs d'informations pourraient nier les avoir reçues ou envoyées.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

OBJECTIF (Objective)

Spécifie, en terme de finalité, le niveau de qualité et de quantité des résultats que doit atteindre un système par son fonctionnement.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

OPTIMISATION DU RISQUE (Risk Optimization)

Processus visant, pour un risque, à minimiser les conséquences négatives et à maximiser les conséquences positives et leurs probabilités respectives.

Note 1 :

Dans le contexte de la sécurité, l'optimisation du risque est focalisée sur la réduction du risque.

Note 2 :

L'optimisation du risque dépend des critères de risque, en incluant le coût et les exigences légales.

Note 3 :

Les risques associés à la maîtrise du risque peuvent être considérés.

Source ISO/IEC Guide 73:2002

PANNES - matérielles et logiques (**Breakdowns** - Material and Logical)

Ensemble de **causes d'origine ou de révélation interne** entraînant l'indisponibilité ou le dysfonctionnement (non-conformité aux fonctionnalités et aux performances nominales) total ou partiel du système.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

PARTIE PRENANTE (Stakeholder)

Toute personne, groupe ou organisme susceptible d'affecter, d'être affecté ou de se sentir affecté par un risque.

Note1 :

Le décideur est également une partie prenante.

Note 2 :

Le terme "partie prenante" inclut, mais à un sens plus large que "partie intéressée".

Source ISO/IEC Guide 73:2002

PERCEPTION DU RISQUE (Risk Perception)

Manière dont une partie prenante considère un risque à partir d'un ensemble de valeurs ou de préoccupations.

Note 1 :

La perception du risque dépend des besoins, questions et connaissances des parties prenantes.

Note 2 :

La perception du risque peut différer des données objectives.

Source ISO/IEC Guide 73:2002

PERTES DE SERVICES ESSENTIELS (Losses of Essential Services)

Ensemble de **causes d'origine externe** entraînant l'indisponibilité ou le dysfonctionnement total ou partiel du système : électricité, télécommunications, eau, fluides divers.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

PERTE D'EXPLOITATION (Loss of Revenue – Business Interruption)

Perte de chiffre d'affaire consécutive à la survenance d'un risqué assuré.

PERTES DIRECTES (Direct Losses)

Elles regroupent les frais d'expertise, de déblaiement, de réparation ou de remplacement des **matériels endommagés**, ainsi que les frais d'expertise et de restauration des **éléments non matériels** du système atteint : système d'exploitation, données, programmes, procédures, documentations et divers.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

PERTES INDIRECTES (Indirectes Losses)

Elles englobent l'ensemble des **frais correspondant à des mesures conservatoires** destinées à maintenir à l'intérieur du système des fonctionnalités ou des performances aussi proches que possible de celles qui étaient les siennes avant le sinistre jusqu'à sa complète remise en état (matériel et non matériel). Les pertes indirectes comprennent également **les pertes d'exploitation** : pertes de marge dues à des frais supplémentaires et/ou à des pertes de revenu directes ou indirectes (pertes d'affaires, de client, d'image, etc.) ; pertes de fonds et de biens (pertes d'informations confidentielles, de savoir-faire, etc.) ; responsabilité civile encourue par l'entreprise ou l'organisme du fait des préjudices causés à autrui, volontairement ou pas, du fait de la survenance d'un sinistre dans son enceinte juridique.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

PLAN DE CONTINUITE D'ACTIVITE – PCA (Business Contingency Plan)

Ensemble de mesures visant à assurer, selon divers scénarios de crises, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services essentielles de l'entreprise puis la reprise planifiée des activités.

Le Comité de Réglementation Bancaire et Financière impose aux établissements de crédit et aux entreprises d'investissement de disposer d'un plan global réunissant l'ensemble des PCA qui soit objectivé et régulièrement évalué sous le contrôle de l'organe délibérant de l'organisation (article 1 du règlement CRBF 2004-02).

Source : CRBF, Règlement n° 2004-02

PLAN DE REPRISE DES ACTIVITES/CONTINUITE D'ACTIVITE (Business Recovery Plan)

Plan décrivant avant tout sinistre les moyens de secours à déployer après sinistre pour une reprise des activités.

PLAN DE SAUVEGARDE (Backup-plan)

Ensemble des procédures et des moyens permettant de **disposer de copies des programmes, des fichiers, des procédures**, suffisamment à jour pour redémarrer une application après un incident. Les plans de sauvegardes sont conçus pour autoriser la sélection d'une partie seulement des fichiers et permettant également la **sauvegarde de fichiers volumineux**.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

PLAN DE SECOURS INFORMATIQUE (Computer Emergency Scheme)

Ensemble des procédures et des moyens permettant de **poursuivre l'exploitation avec une interruption minimale**, en cas d'indisponibilité d'un système ou d'une application.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

Plan décrivant avant tout sinistre les moyens de secours informatique à déployer après sinistre pour une reprise des activités.

POLITIQUE (Policy)

Intentions et dispositions générales formellement exprimées par la direction.

Source ISO/IEC 17799:2005

POTENTIELLE (Potential)

Qui qualifie ce qui est en puissance de devenir ! Exemple : la menace est une agression potentielle.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

PRÉVENTION (Prevention)

Mesure de sécurité qui aura une action "réductrice" en évitant la naissance de nouveaux risques, la résurgence d'anciens, et en atténuant ou supprimant ceux qui existent et dont les origines sont de nature malveillante.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

PREVENTION DES RISQUES (Risk Prevention)

Processus de réduction des risques portant sur l'analyse des causes et ayant pour but de diminuer la probabilité d'occurrence du risque.

PRIME (Premium)

Somme que doit payer l'assuré en contrepartie de l'engagement de l'assureur de prendre en charge le sinistre.

PRINCIPE INDEMNITAIRE (Indemnity Principle)

Principe selon lequel l'assureur remet l'assuré dans la situation qui aurait été la sienne si le sinistre ne s'était pas produit. L'indemnité doit être égale à la perte subie et l'assurance ne doit pas être source de profit.

PRISE DE RISQUE (Risk retention)

Acceptation de la charge d'une perte, ou du bénéfice d'un gain, d'un risque particulier.

Note 1 :

La prise de risque inclut l'acceptation des risques qui n'ont pas été identifiés.

Note 2 :

La prise de risque n'inclut pas les traitements effectués par le biais des assurances, ou le transfert par d'autres moyens.

Note 3 :

Il peut exister une variabilité dans le degré d'acceptation et cela dépend des critères de risque.

Source ISO/IEC Guide 73:2002

PRIVILÈGE MINIMUM (Minimum privilege)

Principe qui requiert que chaque utilisateur soit doté des privilèges minimums pour accéder aux ressources dont il a besoin. L'application de ce principe **limite les risques** d'erreurs, d'accidents ou d'utilisation non autorisée des ressources.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

PROBABILITÉ D'APPARITION (Probability of appearance, Likelihood)

Elément d'appréciation des chances de subir une atteinte qui sera exprimé par : l'appréciation de la vraisemblance de la naissance ou de l'existence du risque que la menace peut représenter, l'aspect plausible de sa concrétisation en agression et par le réalisme de son degré de réussite. Cet élément ne relève pas de calculs statistiques mais du ressenti des utilisateurs ou du dire d'experts. Cette probabilité sera exprimée et quantifiée par des nombres de 0 à 4 qui signifieront :

(**0**) ne surviendra jamais

(**1**) surviendra peut être

(**2**) surviendra probablement

(**3**) surviendra sûrement

(**4**) surviendra à court terme

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

PRODUITS DERIVES (Derivatives)

L'exemple le plus connu actuellement pour couvrir un risque est celui des dérivés climatiques.

Le principe général des dérivés est que l'investisseur s'engage à rembourser un montant prédéfini si un

événement précis survient dans une plage de temps limitée et précisée à l'avance.

Source Fonction : Risk Manager aux Editions DUNOD

PROGRAMME DE SAUVEGARDE (Back-up Program)

Programme permettant d'**effectuer une copie de sauvegarde** d'un fichier stocké sur un support de données.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

PROPRIETAIRE DU RISQUE (Risk owner)

Responsable de la maîtrise des risques pour les activités qu'il exerce, il dispose du pouvoir décisionnaire et des moyens financiers, humains et hiérarchiques utiles à cette maîtrise ; il a la capacité de déléguer la gestion de ces risques. (Voir 'gestionnaire de risques').

A ce titre, il est le principal interlocuteur de la Direction des Risques (ou du Risk Manager) pour définir le niveau global de maîtrise, son impact (financier notamment) et sa fréquence, et pour identifier le ou les plan(s) d'action et pour suivre leur mise en œuvre.

PROTECTION (Protection)

Mesure qui détectera, neutralisera ou diminuera les effets de l'agression, évitant ainsi d'avoir à subir une atteinte ou atténuant éventuellement son niveau. Les mesures de protection concerneront les environnements logiques, physiques et organisationnels. Elle regroupe l'ensemble des actions qui ont pour vocation d'assurer la détection et la neutralisation d'une agression ou l'atténuation de ses effets.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

PROTECTION DES RISQUES (Risk Protection)

Processus de réduction des risques portant sur l'analyse des conséquences et cherchant à diminuer la gravité du risque.

PROVISION DE FREQUENCE (frequency Provision)

Réserve comptable faite par l'entreprise pour couvrir un risque et notamment pour la sinistralité de fréquence

PROVISION TECHNIQUE (Technical Provision)

Montant que l'assureur, la captive ou le réassureur doit mettre en réserve pour faire face à l'indemnisation des sinistres.

Source Fonction : Risk Manager aux Editions DUNOD

RATIO COMBINE (Combined Ratio)

Somme des frais généraux, des commissions encourues et des sinistres survenus rapportés aux primes acquises par l'assureur, le réassureur ou par la captive.

Source Fonction : Risk Manager aux Editions DUNOD

RATIO SINISTRES A PRIMES (S/P) (Loss Ratio)

Coût des sinistres survenus rapportés aux primes versées.

Source Fonction : Risk Manager aux Editions DUNOD

REASSURANCE (Reinsurance)

Opération par laquelle un assureur s'assure lui-même auprès d'un tiers (le réassureur) pour une partie ou la totalité des risques qu'il a garantis, moyennant le paiement d'une prime.

Source Fonction : Risk Manager aux Editions DUNOD

REDUCTION DES RISQUES (Risk reduction)

Politique visant à l'atténuation de la fréquence ou de la gravité du risque par divers processus : protection, prévention, transfert.

Actions entreprises en vue de diminuer la probabilité, les conséquences négatives, ou les deux, associées à un risque.

Source ISO/IEC Guide 73:2002

REFUS DU RISQUE (Risk avoidance)

Décision visant à ne pas être impliqué dans une situation à risque, ou se retirer d'une situation à risque.

Note :

La décision peut être prise sur la base du résultat de l'évaluation du risque.

Source ISO/IEC Guide 73:2002

RESILIENCE (Resilience)

Capacité, face aux grands risques, de reprise et de retour à la normale des activités essentielles et des systèmes critiques, notamment en vue d'éviter l'apparition d'un risque systématique.

Source Fonction : Risk Manager aux Editions DUNOD

RESSOURCES DE L'ENTREPRISE (Enterprise resources)

Ensemble de ce que doit disposer une entreprise ou un groupe pour atteindre ses objectifs :

- ressources humaines
- ressources techniques
- ressources informationnelles
- ressources financières

RESSOURCES INFORMATIONNELLES (Informational resources)

Ensemble des ressources liées directement à la possession, au traitement et à la transmission d'informations.

RESTAURATION (Restoration)

Mesure de sécurité dont l'ensemble des actions mises en œuvre a pour but de faire retrouver, pour le système, des conditions normales de fonctionnement dans des délais raisonnables et à des coûts supportables. En général, elle se traduira d'abord par des mesures palliatives permettant d'assurer un fonctionnement temporaire avant de pouvoir reconstituer ou restaurer les ressources altérées. Sous le vocable restauration, sont inclus les aspects "plan de secours et sauvegarde", ainsi que le "back up" et tous les éléments contribuant à un retour à une situation normale.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

RETENTION (Retention)

Part du risque conservée pour son propre compte.

RETOUR A LA NORMALE (Resumption)

Capacité d'une entreprise, après un choc extrême, à accepter et traiter de nouvelles opérations, à un rythme au moins égal à celui précédent la catastrophe.

Source Fonction : Risk Manager aux Editions DUNOD

RISQUE (Risk)

Dans le cadre d'une organisation, évènement ou séquences d'évènements susceptibles d'affecter la bonne réalisation des objectif de l'entreprise ou du Groupe, de mettre en péril sa pérennité et de compromette la création de valeur.

Combinaison de la probabilité d'occurrence d'un dommage et de sa gravité.

Source ISO/IEC Guide 51:1999

Combinaison de la probabilité d'un événement et de ses conséquences.

Note1:

Le terme "risque" est généralement utilisé uniquement lorsqu'il existe au moins la possibilité de conséquences négatives.

Note2:

Dans certaines situations, le risque provient de la possibilité d'un écart par rapport au résultat ou l'événement attendu.

Source : Guide ISO/IEC 73:2002

Danger plus ou moins probable émanant d'une menace et pouvant se traduire en terme de probabilité d'apparition et de niveau d'impact. La probabilité d'apparition sera fonction de l'existence de ce risque en terme d'enjeu et de la probabilité de concrétisation de menace en agression, puis des chances de réussite de cette agression qui produira une atteinte.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

RISQUE ASSURABLE (Insured Risk)

- objet de l'assurance (personnes ou biens) ;
- probabilité de survenance d'un sinistre ;
- événement qui déclenche la garantie (incendie, vol, etc.).

Source Fonction : Risk Manager aux Editions DUNOD

RISQUE AVERE (Risk proven)

Risque déjà constaté dans un contexte donné.

RISQUE CATASTROPHIQUE - Risque de Gravite(Catastrophic risk)

Evénement imprévisible ou de faible fréquence mais dont l'impact est majeur.

RISQUE DE FREQUENCE (Expected Risk)

Risque se produisant régulièrement avec un impact faible ou moyen.

La prévention s'applique à leur réduction.

Source Fonction : Risk Manager aux Editions DUNOD

RISQUE DE GRAVITE (Unexpected Risk)

Risque à très faible fréquence mais dont les conséquences sont très importantes. La protection s'applique à leur réduction. Pour les gravités les plus fortes, synonymes : choc extrême, catastrophe, risques majeurs.

Source Fonction : Risk Manager aux Editions DUNOD

RISQUE DE MISE EN ŒUVRE (Implementation Risk)

Risque lié aux choix des conditions de mise en œuvre.

Source Fonction : Risk Manager aux Editions DUNOD

RISQUE INHERENT (Inherent Risk)

Impact d'un événement ou d'une circonstance qui existait avant l'utilisation de moyens d'atténuation des risques (l'atténuation peut agir sur l'impact ou la probabilité d'occurrence ou les deux).

Source Fonction : Risk Manager aux Editions DUNOD

RISQUE OPERATIONNEL (Operational risk)

Risque avéré ou potentiel prévisible suivi par les opérationnels au niveau local.

RISQUE OPERATIONNEL BANCAIRE (Risk banking operationnel)

Risque, y compris juridique, résultant d'une inadaptation ou d'une défaillance imputable à des procédures, personnels et systèmes internes ou à des évènements extérieurs / à l'exclusion des risques stratégiques et des risques de réputation.

Source : Accord de Bâle II

RISQUE POTENTIEL (Risk potential)

Risque non constaté mais dont la potentialité peut être démontrée.

RISQUE RESIDUEL (Residual risk)

Risque restant à la charge de l'organisation après une mesure d'atténuation des risques.

Risque subsistant après le traitement du risque.

Source ISO/IEC Guide 73:2002

RISQUE TOLERABLE (Tolerable risk)

Risque accepté dans un certain contexte et fondé sur les valeurs admises par la société.

Source ISO/IEC Guide 51:1999

RSI (IT Security Operational)

C'est le **R**esponsable de la **S**écurité **I**nformatique e charge de procédures opérationnelles comme les mises à jour des anti-virus, les procédures d'habilitation, de sauvegarde, etc.

RSSI (IT Security Officer)

C'est le **R**esponsable de la **S**écurité des **S**ystèmes d'**I**nformation. Il sera l'expert de l'entreprise chargé de l'ensemble des problèmes de sécurité se rapportant aux systèmes d'information.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

SAUVEGARDE DE RECOURS (Safeguard help)

Seconde copie externalisée des **données** sur **disquette** ou sur un autre support permettant de **restaurer** les données en cas de perte ou destruction du média original.

SCÉNARIO D'ATTEINTE (Scenario of attack)

Récit du déroulement préétabli d'une action conditionnée par l'apparition d'événements, et dont la réalisation des processus pourrait se traduire par diverses atteintes sur les systèmes d'information de l'entreprise. C'est aussi l'ensemble des descriptions concernant : la menace, le risque, l'agression, l'atteinte et l'impact, c'est-à-dire la composition de l'ensemble des éléments et de leurs relations ayant contribué à porter un préjudice à l'entreprise via son système d'information.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

SÉCURITÉ (Security)

C'est un état caractérisant un système dans lequel il n'est exposé à aucun danger. La sécurité des données et des informations pourra être exprimée par leurs "qualités" en terme de niveau de disponibilité, d'intégrité ou de confidentialité.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

SECURITE DE L'INFORMATION (Information Security)

Protection de la confidentialité, de l'intégrité, et de la disponibilité de l'information ; en outre, d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité, peuvent être concernées.

Source ISO/IEC 17799:2005

SEVERITE DES RISQUES (Severity)

Voir gravité.

Source Fonction : Risk Manager aux Editions DUNOD

SIGR – Système d'Information de Gestion des Risques (Information system of risk management))

Application informatique permettant de disposer et d'exploiter à tout moment les données et informations sur les risques liés aux différentes activités du Groupe ainsi que les incidents constatés, afin, notamment, de fiabiliser le pilotage des activités et de mieux connaître le coût des risques.

SINISTRALITE (Claims Record)

Montant correspondant aux sinistres réglés pendant une période donnée, majoré de la variation des provisions pour sinistres survenus mais non encore payés.

Source Fonction : Risk Manager aux Editions DUNOD

SINISTRE ASSURE (Insured Loss)

Evénement déclenchant la garantie du contrat.

SMP (Maximum Forseable Loss or Maximum Possible Loss) : Sinistre maximum Possible.

SRE (Normal Loss Expentency) : Sinistre Raisonnablement Escomptable.

Source Fonction : Risk Manager aux Editions DUNOD

SOUSCRIPTEUR (Insured)

C'est le preneur d'assurance, selon une terminologie récente.

Source Fonction : Risk Manager aux Editions DUNOD

SOUSCRIPTION (to Write)

Décision prise par un assureur et un réassureur d'accepter, moyennant la perception d'une prime, de couvrir un risque.

Source Fonction : Risk Manager aux Editions DUNOD

SYSTÈME DE GESTION (Management system)

Ensemble de règles, procédures, moyens, organisés en vue de maximiser la réalisation des objectifs définis par l'entreprise en tant que système.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

SYSTÈME D'INFORMATION (Information System)

(1) Ensemble organisé de moyens de toute nature qui assurent la survie, le stockage, le traitement, la distribution des informations au sein du système de gestion.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

(2) Ensemble des informations et des opérations de collecte, de conservation, de transformation et de distribution de ces informations liées aux activités de l'entreprise. Les opérations peuvent être manuelles ou automatisées. Un système d'information comprend :

- ✓ Un modèle de fonctionnement (modèle des traitements et modèles des données),
- ✓ Un ensemble de données nécessaires au fonctionnement (la base d'information),
- ✓ Un ensemble d'acteurs (processeurs) capables de faire fonctionner le système.

SYSTÈME INFORMATIQUE (Information processing system)

Ensemble organisé des moyens de toute nature qui assurent la saisie, le traitement, le stockage, la diffusion et la transmission "automatiques" des données au sein d'un système d'information.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

TANGIBLE (Tangible)

Que l'on peut constater (un matériel détruit, un fichier écrasé).

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

TARIF (Tarification)

Barème dans lequel figurent les différents taux de prime applicables aux risques entrant dans le cadre d'une catégorie d'assurance (tarif automobile, tarif incendie).

Source Fonction : Risk Manager aux Editions DUNOD

TEST DE PÉNÉTRATION (Intrusion test – test of penetration)

Tests pratiqués par des consultants internes ou externes pour **analyser la solidité des mécanismes** de sécurité.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

TIERS (Third party)

Personne ou organisme reconnu(e) comme indépendant(e) des parties concernées.

Source ISO/IEC Guide 2:1996

TITRISATION (Securization)

Technique consistant à transférer des portefeuilles d'actifs (souvent des créances) à un véhicule « *ad hoc* » chargés de les gérer ou de les revendre sur un marché secondaire.

Source Fonction : Risk Manager aux Editions DUNOD

TOLÉRANCE AUX PANNES (Fault-tolerance)

(1) Capacité que possède un système à continuer à fonctionner en cas d'erreur ou de panne. Les systèmes tolérants les pannes sont basées sur des

composants qui contrôlent leur état de fonctionnement à l'aide d'algorithmes spécifiques.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

(2) Aptitude d'un système informatique à demeurer fonctionnel malgré certaines pannes de ses composants. (J.O. du 07/03/1993).

TRAÇABILITÉ (Traceability)

Eléments de l'activité d'un utilisateur qui peuvent être retenus pour **détecter des changements anormaux** par rapport à ses habitudes.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

TRAITEMENT DU RISQUE (Risk treatment)

Processus de sélection et de mise en œuvre des mesures visant à modifier le risque.

Note 1 :

Le terme "traitement du risque" est parfois utilisé pour les mesures elles-mêmes.

Note 2 :

Les mesures de traitement du risque peuvent inclure le refus du risque, son optimisation, son transfert ou sa prise.

Source ISO/IEC Guide 73:2002

TRANSFERT DU RISQUE (Risk Transfer)

Transmission de tout ou partie de l'impact d'un risque à un tiers, externe ou interne.

Partage avec une autre partie de la charge de la perte, ou du bénéfice du gain, d'un risque.

Note 1 :

Les exigences légales ou réglementaires peuvent limiter, interdire ou imposer le transfert de certains risques.

Note 2 :

Le transfert du risque peut être effectué par des assurances ou d'autres accords contractuels.

Note 3 :

Le transfert du risque peut créer de nouveaux risques ou modifier les risques existants.

Note 4 :

Le déplacement de la source n'est pas un transfert du risque.

Source ISO/IEC Guide 73:2002

Transfert des risques à d'autres parties qui les acceptent et qui sont éventuellement rémunérées en contrepartie. Le transfert est technique et/ou contractuel (pour réduction), ou financier (assurance, etc.).

Source Fonction : Risk Manager aux Editions DUNOD

VALEUR A NEUF (Full Replacement Value)

Valeur de reconstruction / reconstitution à neuf au jour du sinistre.

VALEUR VETUSTE DEDUITE (Depreciated Replacement Value)

Valeur du bien au jour du sinistre. Application d'un coefficient de dépréciation selon la vétusté du bien.

VIRUS (Virus)

Programme, souvent de très petite taille qui possède la faculté de s'introduire dans un programme hôte et de s'auto reproduire, soit à l'identique, soit en se modifiant (virus polymorphe), chaque fois que celui-ci démarre ou est exécuté.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

VRAISEMBLANCE (Probability)

Qualificatif qui caractérise la naissance ou l'existence d'un risque que peut représenter une menace. Elle est quantifiée par des nombres de 0 à 4 qui signifieront : **(0)** n'existera jamais, **(1)** a peu de chance d'exister, **(2)** peut exister mais pas pour le moment, **(3)** existera à court terme, **(4)** existe.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

VULNÉRABILITÉ (Exposure – Vulnerability)

En tant que faiblesse, la vulnérabilité est *ipso facto* relative au couple [menace, enjeu]. Cela se traduira par le fait qu'un risque (et donc la menace qui l'a fait naître) et une faiblesse (des impacts potentiels tangibles, de niveau logique ou stratégique) existent simultanément.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

Faiblesse d'un bien ou d'un groupe de biens pouvant faire l'objet d'une menace.

Source ISO/IEC 13335-1:2004

Point faible d'une organisation pouvant être défini par un objet de risques, des causes et des conséquences.

Source Fonction : Risk Manager aux Editions DUNOD

VULNÉRABILITÉ LOGIQUE (Logical vulnerability)

Elle sera la conséquence de l'impact logique pour le système de gestion. Ce sera, par exemple, l'impact représenté par une atteinte à la disponibilité, le système sensible au retard de certains traitements informatiques qui se traduiront par des retards de production.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

VULNÉRABILITÉ STRATÉGIQUE (Strategic vulnerability)

Elle traduira des conséquences qui pourront être de nature financière et "activer" des enjeux majeurs. Cette vulnérabilité sera plus une caractéristique de l'entreprise qu'une particularité de son système d'information.

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK

VULNÉRABILITÉ TANGIBLE (Tangible vulnerability)

Elle traduit une faiblesse physique, logique ou organisationnelle de l'environnement informatique. Cette fragilité donnera la possibilité à une agression de faire subir au système d'information une atteinte qui aura des impacts tangibles (destructions physiques, logiques et organisationnelles).

Source : AFNOR – Management de la sécurité des systèmes d'information – J GONIK.