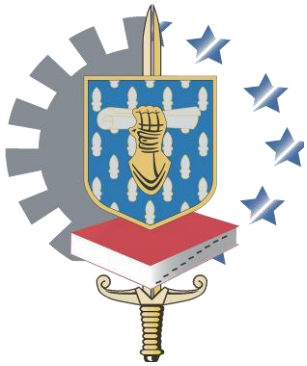
2007

ANALYSE ET GESTION DES RISQUES DANS LES GRANDES ENTREPRISES

Impacts et rôle pour la DSI



IERSE

Institut d'Etudes et de Recherche pour la Sécurité des Entreprises

CIGREF

« Promouvoir l'usage des systèmes d'information comme facteur de création de valeur et source d'innovation pour l'entreprise »

Publications du CIGREF en 2006-2007

Analyse et Gestion des risques dans les grandes entreprises :
impacts et rôles pour la DSI

Baromètre Gouvernance SI :
Evaluer sa démarche de gouvernance du système d'information

Changement et transformation du SI :
Note de synthèse

Exemples d'offshoring :
Retours d'expériences et leçons apprises au sein de grandes entreprises

Faire face aux changements de périmètre d'entreprise :
guide de survie à l'usage des dirigeants en cas de changement de périmètre d'entreprise

Gestion des actifs immatériels :
kit de démarrage et études de cas

Les dossiers du Club Achats :
Synthèse des activités 2007

Management d'un Centre de Services Partagés informatiques :
Quels modèles ? Quels bénéfices pour l'entreprise ? Quels impacts sur le métier de DSI ?

Marketing de la DSI :
Cadre de mise en œuvre

Outil de scénarisation prospective des besoins Ressources Humaines de la SI :
Facteurs clés de l'évolution des métiers et des compétences

Pilotage économique du Système d'information :
Présentation des coûts informatiques et fiches d'amélioration par processus

Plan Stratégique Système d'Information

Tableau de bord des Ressources Humaines :
Indicateurs clefs

Tableau de bord Sécurité :
Indicateurs clefs de la sécurité système d'information

Ce rapport a été réalisé dans le cadre du partenariat de recherche liant le CIGREF et l'IERSE

Par

Jérémie LACROIX
Membre des groupes de recherche de l'IERSE

L'étude a été pilotée par **Patrick ANGLARD**, DSI de Thalès
et **Frédéric LAU**, chargé de mission au CIGREF

Ce rapport a bénéficié des apports de l'activité « Gestion des risques » du Comité de Pilotage « performance durable du SI ». Il a été rédigé en s'appuyant sur les contributions des personnes et entreprises suivantes :

Christine MILLET	Agence Informatique pour les Finances de l'Etat
Cyrille ROY	AGF-I
Alain DELBOY	Air Liquide
Pascal BUFFARD	AXA France Service
Robert ZEITOUNI	Crédit Agricole SA
François-Xavier TUAL	DCNS
Jean-Yves BIGNON	Euro Disney Associés S.C.A.
Yves SPIELMANN	Euro Disney Associés S.C.A.
Eric VERTOUT	Groupe Les Mousquetaires
Alain BOUILLE	Informatique CDC
Jean-Pierre VUILLERME	Michelin
Jean-Jacques CASSE	Pfizer France
Rachelle BALMADIER	Renault SA
Muriel ROI	SAFRAN
Bruno BIGUET	THALES

Sommaire

Listes des figures

Préambule

En 2006, les DSI membres du CIGREF se sont interrogés sur la gestion des risques dans les grands groupes. En effet, il ressortait de leurs réflexions que la notion de risque n'était pas comprise de la même façon suivant la stratégie de l'entreprise, son secteur d'activité, l'organisation dans laquelle la DSI se trouve ….

De ces visions différentes ressortaient des méthodes de management différentes : les DSI venant du monde de l'assurance sont naturellement très au fait de la gestion des risques parce c'est leur cœur de métier, d'autres DSI, comme par exemple ceux du secteur industriel ont une sensibilité différente vis-à-vis de la gestion des risques.

Pour répondre à ce besoin d'investigation, le comité de pilotage du CIGREF « Performance durable des SI » a mis en place une activité autour de ce thème.

Afin d'avoir une vision opérationnelle des pratiques, la méthode de l'entretien a été retenue. Ces derniers ont été majoritairement réalisés avec des gestionnaires de risque[1] d'entreprise et des DSI d'entreprises membres du CIGREF.

La réflexion s'est structurée autour de deux aspects : le rôle de la DSI dans la démarche globale de gestion des risques de l'entreprise et l'impact de cette démarche sur le fonctionnement de la DSI.

[1] Dans la suite de ce document nous pourrons utiliser aussi le terme anglais *risk manager* ou l'abréviation RM

1 Quelques notions avant toutes choses…

Le *risk management* au sens moderne du terme est une matière assez nouvelle en France. Suivant qu'il est utilisé par la doctrine, dans le monde de l'entreprise, ou dans le langage courant, il ne revêt pas la même signification. Il est donc important de définir les termes de risque, gestion des risques et *risk manager* avant de poursuivre.

Le vocabulaire propre à cette discipline n'est pas encore standardisé voici donc quelques définitions tirées de la littérature sur ce sujet.

1.1 Qu'est-ce qu'un risque ?

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

« Le risque est constitué par tout événement susceptible de faire perdre de l'argent à l'entreprise. Un incendie dans un atelier, la perte de parts de marché, un mauvais positionnement stratégique sont des risques qui peuvent affecter la santé financière d'une entreprise. »
« Les risques sont les évènements qui empêchent [l'entreprise] d'atteindre ses objectifs stratégiques : la gestion des risques ou *risk management* doit être une logique d'entreprise. »
Ecole des Mines

«[Le risque est la] probabilité qu'un effet spécifique se produise dans une période donnée ou dans des circonstances déterminées. »
Directive n° 96/82 du Conseil de l'Europe[2].

«[Le risque est la] combinaison de la probabilité et des conséquence(s), de la survenue d'un événement dangereux spécifié. »
OHSAS *18001*[3]

« [Le risque est] la menace qu'un événement , une action, ou une inaction affecte la capacité de l'entreprise à atteindre ses objectifs stratégiques et compromette la création de valeur ».
Cabinet Ernst & Young[4]

[2] Directive n° 96/82 du Conseil de l'Europe du 9 décembre 1996 concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses.
[3] OHSAS ou *Occupational Health and Safety Assessment*, certification qui précise les règles pour la gestion de la santé et la sécurité dans le monde du travail. Elle a une valeur internationale.

1.2 Qu'est-ce que la gestion des risques ?

« *The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects*. (La culture, les processus et structures qui sont dirigés vers la gestion efficace d'opportunités potentielles ou d'effets défavorables). »
Standard australien et néo-zélandais de risk management AS/NZS 4360 :1999

« [Le risk management] vise à identifier et anticiper les évènements, actions ou inactions susceptibles d'impacter la mise en œuvre de la stratégie dans un horizon donné, définir les options de traitements et s'assurer qu'une option optimale est choisie, mettre en œuvre cette option et contrôler l'efficacité de la solution retenue par rapport aux attentes ».
Cabinet Ernst & Young

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

La gestion des risques dans l'entreprise passe par l'identification du risque résiduel[5], son évaluation, le choix d'une stratégie de maîtrise et un contrôle.

Aujourd'hui en 2007, l'attention portée à la gestion des risques dans l'entreprise s'est accrue. Ceci se traduit simultanément par un cadre réglementaire renforcé et par une pression grandissante des marchés pour une prise de conscience des entreprises de la nécessité de maîtriser leurs risques.

[4] Cette définition est issue de l'ouvrage « Comprendre et gérer les risques » de Franck Moreau, qui reprend les définitions conçues et admises au sein du cabinet Ernst Young.
[5] Le risque zéro n'existe pas : la part de risque qui n'est pas toujours soit maîtrisée, soit identifiée, est cette part de risque « résiduel »

1.3 Qui est le risk manager ?

« *A person hired to identify significant pure risks that a company faces and prescribe effective techniques to deal with them*. *(*Le risk manager est une personne engagée pour identifier les risques purs significatifs que rencontre une société et pour prescrire des techniques efficaces pour les manager*). »*
Glossaire du Credit Research Foundation

1.4 Comment peut-on classer les risques ?

Il existe de nombreuses classifications de risques dont l'utilisation diffère suivant les entreprises.

Par exemple, les risques peuvent être classés suivant leur nature :

- De nature économique, ils résultent d'un brusque changement dans l'environnement économique de l'entreprise
- S'ils sont opérationnels, ils sont liés à un dysfonctionnement dans les processus industriels ou de production de l'entreprise
- Ils peuvent aussi survenir d'un évènement naturel
- Ou bien être liés à une action volontaire ou involontaire de l'homme.

Mais les risques peuvent aussi être classés selon qu'ils touchent aux actifs financiers ou qu'ils sont opérationnels ou de conformité.

Par exemple, parmi les **risques financiers**, nous pouvons trouver :

- Ceux liés aux crises monétaires et financières : les risques pays.
- Les risques de contrepartie, liés au non respect d'une obligation par un cocontractant.
- Ceux de taux de crédit s'ils évoluent défavorablement
- Ceux de change avec la variation des cours des monnaies
- Ceux de marché et de la loi de l'offre et de la demande
- Les risques sur la facilité à acheter ou à revendre un actif : c'est-à-dire de liquidité.

Le comité de Bâle[6] a sa propre définition du **risque opérationnel** : c'est un « risque de pertes provenant de processus internes inadéquats ou défaillants, de personnes et systèmes ou d'événements externes ». Dans ce cadre particulier les risques opérationnels ont donc un champ d'application très large. Les accords de Bâle les classent en 8 catégories :

1. Fraude interne
2. Fraude externe
3. Sécurité de systèmes
4. Pratiques en matière d'emploi et sécurité sur le lieu de travail
5. Clients, produits et pratiques commerciales
6. Dommages aux actifs corporels
7. Dysfonctionnement de l'activité et des systèmes
8. Exécution, livraison et gestion des processus

Les risques de **conformité**, concernent :

- Les aspects légaux et règlementaires
- Les risques de sanction : administrative, judiciaire, disciplinaire
- Le risque de réputation
- Le non respect de la déontologie

[6] Le Comité de Bâle ou « Comité de Bâle sur le contrôle bancaire » est une institution créée en 1974 par les gouverneurs des banques centrales du « groupe des Dix » (G10) au sein de la Banque des règlements internationaux à Bâle.

2 Une nouvelle ère : le « *risk management* »

De plus en plus confrontées aux problématiques de risques, les entreprises sont aujourd'hui progressivement devenues plus sensibles à la nécessité d'une gestion efficace des risques, à tel point qu'on peut désormais parler d'une nouvelle « ère » dans la prise en compte des menaces de l'entreprise : celle du *risk management*.

La compréhension et l'application des concepts de *risk management* dans leur acception anglo-saxonne est assez récente dans les entreprises françaises. Il en résulte une maturité des entreprises inégale, des stratégies de prise en compte différentes et des choix organisationnels dissemblables.

2.1 La prégnance nouvelle du risk management *dans les entreprises françaises*

La gestion des risques « moderne » est née aux États-Unis entre les années 1950 et 1960. A cette époque elle ne se faisait que par le transfert des risques vers un assureur. Dominée par la question de l'assurance et la prise en compte des pertes financières, cette notion a évolué. Seuls les accidents d'hygiène et du travail faisaient l'objet d'une anticipation et d'une prévention. La prise en compte d'éléments financiers comme moyen de couverture des risques, conduisait au rattachement des « *risk managers* » à la direction financière de l'entreprise.

Dans les années 1980, en raison de la sophistication des outils financiers et de la prise de conscience par les entreprises de l'importance des plans de continuité, la démarche de gestion des risques s'est étendue à d'autres domaines. C'est à cette époque que l'on s'interroge sur son application au management des projets informatiques.

Depuis les années 2000, la gestion des risques a pris une importance capitale dans la vie des entreprises. Elle procède d'une approche globale et d'une prise en compte de plus en plus complète de toutes les vulnérabilités pouvant entraver la bonne marche de l'entreprise. Elle tend à être intégrée dans la stratégie globale de l'entreprise et devient un élément qui peut influer sur les principes d'organisation de l'entreprise.

Contrairement aux grands groupes français, les entreprises anglo-saxonnes ont adopté depuis de nombreuses années la gestion globale des risques comme élément clé de la stabilité de l'entreprise. Néanmoins, depuis quelques années, les grandes entreprises françaises ont rattrapé leur retard. Pour cette raison on peut parler de « prégnance nouvelle » pour traduire le niveau

actuel d'imprégnation de la notion de risque dans les entreprises françaises.

Nous allons voir dans ce chapitre qu'un certain nombre de facteurs d'influence ont conduit les dirigeants d'entreprise à rendre visible et organiser le *risk management*. Cette volonté de transparence est en relation directe avec le phénomène de gouvernance d'entreprise. En effet, afin de rassurer les principales parties prenantes dans la vie de l'entreprise (les clients, les actionnaires, les employés, les pouvoirs publics…), les dirigeants ont décidé de montrer d'une part que les risques sont pris en compte et d'autre part que leur gestion est intégrée dans la stratégie de l'entreprise.

2.1.1 La prise de conscience

Quatre évènements majeurs ont résonné dans l'écosystème informatique et se sont traduits par une prise de conscience de la nécessité d'anticiper la vulnérabilité des entreprises : le bogue de l'an 2000, les attentats du World Trade Center, l'explosion de l'usine AZF à Toulouse, les scandales financiers Enron et WorldCom.

Le bogue de l'an 2000 a fait prendre conscience à tous que le système d'information est partout et qu'un simple dysfonctionnement peut paralyser des entreprises ou des secteurs économiques entiers. Dans beaucoup d'entreprises, un management des projets informatiques par les risques a été mis en place pour vérifier, corriger, anticiper et réorganiser les systèmes d'information ainsi que pour coordonner la veille et les éventuelles actions au moment du changement de date.

Le 11 septembre 2001, les attentats du World Trade Center à New –York ont un impact majeur sur l'économie américaine et sur de nombreuses entreprises. Cette catastrophe sans précédent par ses conséquences et son *modus operandi* a mis en exergue la fragilité des entreprises vis-à-vis de risques qui n'avaient jamais été envisagés. Ces attentats ont été un élément révélateur de la nécessite de mener une réflexion globale[7] sur les risques.

L'explosion de l'usine AZF à Toulouse, 10 jours plus tard, le 21 septembre 2001, a conduit les entreprises à s'interroger sur la nécessité de communiquer sur les risques et de mieux prendre en compte les risques technologiques.

En décembre 2001, Enron, société américaine de distribution d'énergie, fait faillite en raison des pertes occasionnées par des opérations spéculatives maquillées en bénéfices via des

[7] Au sens effets globaux, mondialisation, entraînant plus de prospective sur les risques

manipulations des comptes pourtant certifiés par le cabinet d'audit Arthur Andersen. Moins d'un an plus tard, durant l'été 2002 la société de télécommunications américaine Worldcom dépose son dossier de faillite à la suite de manipulations comptables révélées au grand jour. Ces deux scandales ont conduit les pouvoirs publics américains à légiférer sur la communication en matière de trésorerie, sur l'approche processus et l'approche risque des entreprises.

Ce sont ces quatre évènements majeurs qui marquent la prise de conscience des entreprises de leur fragilité vis-à-vis des risques : en premier lieu de leur vulnérabilité, en second lieu de leur carence dans la gestion de ces vulnérabilités et enfin de la nécessité d'intégrer la gestion des risques dans leur stratégie.

2.1.2 Les législations

A la suite des scandales financiers énoncés précédemment, les pouvoirs publics ont aussi pris conscience que les vulnérabilités des grands groupes pouvaient avoir de graves conséquences en dans le cas d'un risque avéré, sur les économies nationales. C'est pourquoi, des législations destinées à garantir la stabilité de l'économie en imposant aux entreprises de prendre certaines mesures relatives à la gestion de leurs risques financiers, ont été adoptées.

The Sarbanes-Oxley Act (SOX)

En réponse aux scandales Enron et Worldcom, les autorités fédérales américaines votent le 31 juillet 2002 le « *Sarbanes-Oxley Act* », loi qui organise la transparence de la comptabilité, ainsi que la gestion des risques financiers de l'entreprise.

Cette loi s'applique à toutes les entreprises cotées à la bourse de New-York. Elle a donc un rayonnement fort et touche de nombreuses entreprises hors des frontières des Etats-Unis. La loi SOX a été élaborée dans le but d'apporter une réponse rapide à la crise de confiance sur la communication financière des entreprises. Elle est centrée sur la fiabilité des informations.

La loi sur les nouvelles régulations économiques (NRE)

Dans le cadre de la lutte contre les fraudes et la gestion des risques financiers de l'entreprise, la France anticipe le problème qui est à l'origine des scandales de type Enron et Worldcom : en mai 2001, la loi sur les nouvelles régulations économiques (loi NRE) est votée. Elle impose la dissociation des fonctions exécutives des fonctions de contrôle au sein des entreprises. Par cette obligation, elle renforce l'indépendance des administrateurs par rapport au président et accroit la transparence vis-à-vis des actionnaires. La loi NRE impose aussi aux entreprises de

communiquer sur les conséquences sociales et environnementales de leurs activités.

La loi de sécurité financière (LSF)

La loi de sécurité financière (LSF) a été adoptée par le Parlement français le 17 juillet 2003 afin de renforcer les dispositions légales en matière de gouvernance d'entreprise. Tout comme la loi Sarbanes-Oxley, la LSF organise une modernisation des autorités de contrôle des marchés financiers, la sécurité des épargnants / assurés et le contrôle légal des comptes.

Les accords de Bâle II

Les accords de « Bâle II» sont un dispositif règlementaire élaboré par le comité de Bâle depuis 1998 et publié en 2004. Ce dispositif concerne les établissements financiers européens et vise à améliorer leur capacité de mesure, de gestion et de couverture de leurs risques afin de préserver leur solvabilité et ainsi renforcer leur stabilité financière. Les accords de Bâle II apportent une méthodologie décomposant les risques suivant leur nature et précisant les axes d'amélioration.

La principale innovation des accords de Bâle II par rapport à ceux de Bâle I est la prise en compte des risques opérationnels dans le calcul des fonds que les banques doivent immobiliser pour couvrir leurs propres risques

Le projet de directive Solvency II

« *Solvency II* » ou Solvabilité II est le nom donné au projet de directive européenne déposé auprès du parlement le 10 juillet 2007. Cette directive doit concerner les sociétés d'assurance et de réassurance. Équivalent des accords Bâle II pour les établissements financiers, *Solvency II* est à la fois un principe et un processus : chaque assureur et réassureur doit allouer suffisamment de capital pour couvrir les risques inhérents à son activité. Le calendrier prévoit que ce projet aboutira à une directive en 2008, directive dont l'application effective n'est prévue que pour 2010.

2.2 Cultures d'entreprise en matière de gestion des risques

La culture du risque d'une entreprise se traduit par le niveau de prise en compte des risques dans la stratégie de l'entreprise et dans son organisation. D'une manière globale, il apparait au cours de nos entretiens, que ce niveau de culture tend à augmenter dans les grands groupes français, même s'il existe encore de grandes différences entre les entreprises. Deux facteurs permettent d'expliquer ces différences : le niveau de culture du risque dépend en très grande partie de l'activité et de la réglementation applicable à l'entreprise.

2.2.1 La culture fonction de l'activité de l'entreprise

Les disparités de culture s'expliquent en partie par l'activité des entreprises. Sur l'échantillon observé (15 entreprises), il est possible de classer les entreprises en cinq groupes, selon leur secteur d'activité, avec pour chacun un niveau de culture différent :

1. Les sociétés d'assurance et de réassurance ont toutes une sensibilité particulière vis-à-vis du risque. Leur activité est basée sur le transfert des risques, c'est le cœur de leur métier. Expertes dans la gestion des risques de leurs clients, ces sociétés sont également très expérimentées dans le management de leurs propres risques.
2. La sensibilité à la gestion du risque des banques et des établissements financiers assimilables est très proche de celle des assurances, mais pour des raisons différentes : ils doivent se couvrir vis à vis du risque de retrait massif des avoirs de leurs clients. D'où les accords de Bâle II.
3. Les grands groupes de défense ou ceux qui participent à la défense nationale sont très sensibles aux problématiques de risk management. De par leur activité confidentielle qui revêt souvent un caractère stratégique pour leur pays, ces grandes entreprises ont très tôt été obligées de prendre en compte les risques comme composants essentiels de leur stratégie.
4. Il existe de très fortes disparités en matière de prise en compte des risques dans les entreprises du secteur industriel. Certains groupes pratiquent le *risk management* depuis de nombreuses années, tandis que d'autres n'en sont qu'au stade embryonnaire. Ces inégalités dépendent en grande partie de l'histoire de l'entreprise et de sa concurrence.
5. La gestion de risque parait embryonnaire dans les administrations. La plupart du temps elle se réduit à sa plus simple expression, à savoir le transfert des risques vers un assureur. Néanmoins dans certains cas, il est apparu qu'elle pouvait être mise en œuvre efficacement comme méthode de management des projets « à risque ».

2.2.2 Règlementation et culture du risque

La réglementation a un très fort impact sur le niveau de culture du risque des entreprises :

- Les établissements financiers astreints au respect des accords de Bâle II sont légalement obligés de prendre en compte les risques de crédit, de marché et les risques opérationnels.
- De la même manière, les sociétés d'assurance et de réassurance qui ont déjà une très forte culture du risque, vont

devoir réorganiser leur propre démarche de gestion de risque en fonction des obligations qui découleront de *Solvency II*.

- Les entreprises françaises qui sont cotées à la bourse de New York doivent appliquer les dispositions de SOX depuis déjà 6 ans.

2.2.3 Nationalité et culture du risque

Historiquement, les entreprises anglo-saxonnes ont toujours été en avance sur les entreprises françaises en matière de *risk management*. Leurs filiales françaises et les entreprises françaises qui ont des liens forts avec les entreprises américaines ont bénéficié de cette avance. Par exemple, l'entreprise EuroDisney a bénéficié et bénéficie toujours de la culture de risque de l'entreprise World Disney Company.

2.3 Organisation et méthodes pour la gestion des risques

La mise en place d'une démarche « moderne » de *risk management* implique une adaptation de l'organisation de l'entreprise et modifie les relations entre les différents acteurs. Des formations sont fréquemment mises en place afin de sensibiliser les collaborateurs de l'entreprise aux changements amenés par la gestion de risque dans l'organisation.

2.3.1 L'organisation de la démarche de risk management

La mise en œuvre d'une fonction de *risk management* pose la question de sa place dans l'organisation et l'entreprise.

Tous les grands groupes français n'ont pas choisi de mettre en place une fonction de *risk manager*, ni même adopté une organisation similaire en la matière. Pourtant, la prise en compte des risques a conduit dans la majeure partie des entreprises, à rendre visible la démarche de gestion des risques dans la répartition des responsabilités de haut niveau.

Le choix de la fonction gestion des risques dépend de la stratégie d'entreprise

Différentes fonctions de l'entreprise peuvent exercer les missions et activités liées aux risques :

- Le responsable de l'audit interne peut exercer des fonctions de gestion des risques par le biais de l'action de *reporting* qu'il exerce dans toutes les branches de l'entreprise.
- Dans les entreprises où la production dépend essentiellement de l'informatique, la plupart des risques du groupe sont liés aux systèmes d'information. La gestion des risques intègre donc une forte composante relative à la sécurité des systèmes d'information. Le responsable de la sécurité des systèmes

d'information peut jouer dans ce cas un rôle majeur dans la démarche de *risk management*.

- Le transfert des risques vers un assureur est la méthode la plus anciennement utilisée en matière de gestion des risques. Actuellement, la gestion des risques ne se limite plus uniquement à cette méthode même si cette méthode est encore largement utilisée. Le responsable assurances de l'entreprise a donc encore une place prépondérante dans la démarche de gestion des risques.
- La responsabilité de la démarche de gestion des risques implique une réelle compétence financière. Un des directeurs (financier, opération, organisation selon le cas) de l'entreprise peut aussi être amené à exercer des fonctions de gestion des risques. Avant que la fonction de *risk manager* ne soit créée dans les entreprises, le directeur financier, du reste, a souvent exercé des activités relatives à la gestion des risques.
- Le Directeur Général délègue le plus souvent cette responsabilité.

Par rapport aux fonctions citées précédemment, la fonction de *risk manager* est une fonction récente. Elle a été définie spécifiquement pour prendre en charge la démarche de gestion de risque dans son ensemble. Elle apparait donc comme étant la plus adaptée à la vision contemporaine des risques. Néanmoins, il n'existe pas de *risk manager* ou directeur des risques dans toutes les entreprises.

Il est aussi possible de cumuler la fonction de *risk manager* avec une fonction traitant de problématiques similaires comme par exemple un directeur assurance ou un responsable sécurité des SI.

Ce cumul de fonction est motivé par la volonté de communiquer autour de la démarche de gestion des risques et de la rapprocher de disciplines connexes partageant les mêmes enjeux.

Le rattachement du risk manager

Le niveau de rattachement du *risk manager* dans le groupe est un indicateur représentatif du niveau de maturité de l'entreprise face au risque.

Généralement, le *risk manager* est rattaché à la direction financière de l'entreprise. Ce rattachement permet la déclinaison d'une politique globale de gestion des risques de par l'appartenance du directeur financier au comité exécutif. Néanmoins, il peut aussi traduire une priorité donnée aux risques financiers par rapport aux autres risques.

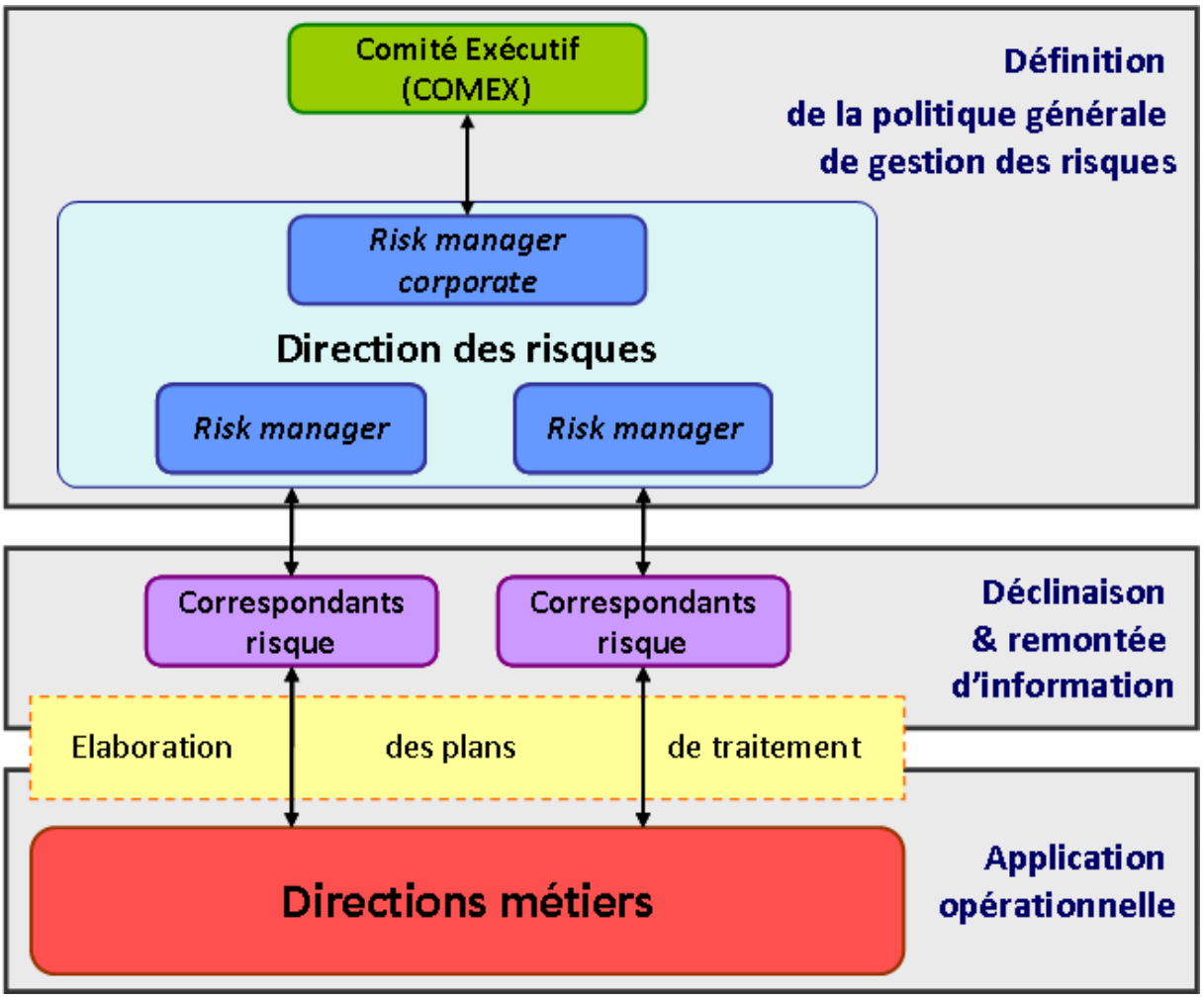
Dans certaines entreprises, le *risk manager* est membre du comité exécutif de l'entreprise. Ce rattachement s'exerce par le biais d'un *reporting* direct au comité exécutif ou par l'existence d'un comité de maitrise des risques composé du *risk manager* et de directeurs membres du comité exécutif. Ce choix favorise la prise en compte du risque par l'ensemble des métiers.

Les organigrammes possibles en matière de gestion des risques

Lors des entretiens, nous avons observé quatre modes principaux d'organisation mise en place dans les entreprises.

Organisation « globale »

Certains groupes ont adopté une organisation « globale » en matière de *risk management*. C'est-à-dire qu'elle est liée à l'adoption d'une politique globale et intégrée de gestion des risques d'entreprise. Elle est appelée *Enterprise risk management* ou ERM.



Source CIGREF

Figure 1 : Organisation globale

Cette politique propose l'utilisation de méthodologies et d'outils communs à l'ensemble des branches, directions et filiales de l'entreprise afin de structurer et de rendre cohérente la participation de ces entités à la démarche de gestion des risques. Elle permet d'avoir une vision complète des risques du groupe et des risques métiers tout en les hiérarchisant.

La mise en œuvre de cette politique est sous la responsabilité d'un *risk manager* le plus souvent rattaché au comité exécutif qui définit avec son aide, les éléments de la politique générale de gestion des risques. Ce *risk manager* « *corporate* » a un rôle de coordination et de supervision de la démarche. Par conséquent, il va dans certains cas avoir la responsabilité de la direction de l'assurance ou du contrôle interne.

Le directeur des risques est assisté par des correspondants risques qui déclinent la politique générale de *risk management* dans les différentes branches et filiales de l'entreprise. Ces correspondants participent à la remonté des informations nécessaires à la cartographie des risques du groupe. Ce sont les interlocuteurs privilégiés des métiers avec lesquels ils élaborent les plans d'action de traitement des risques. En effet, les directions métiers sont compétentes pour l'application opérationnelle de la politique de *risk management*, car elles sont expertes dans les activités qu'elles exercent.

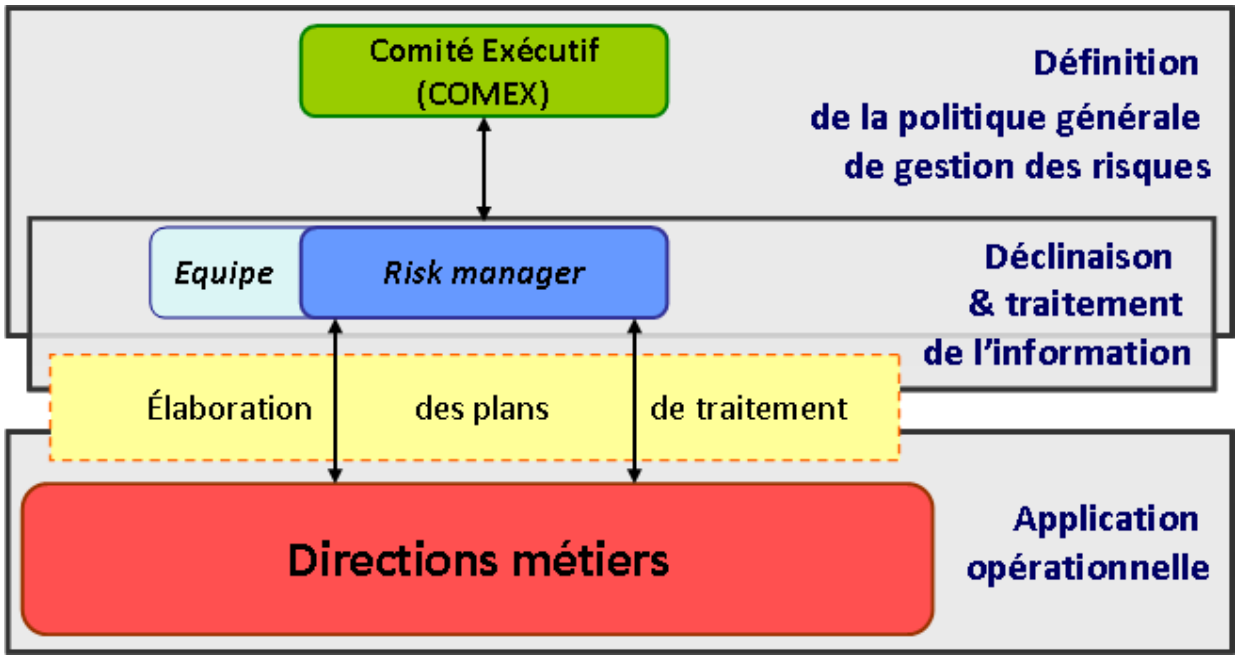
L'organisation « globale » en matière de *risk management* est un schéma qui convient bien à des groupes décentralisés.

Organisation « centrale réduite »

Les entreprises fortement centralisées ou mono-sites adoptent plus généralement une organisation « centrale réduite » en matière de *risk management*. Assisté d'une petite équipe, le *risk manager* du Groupe (*Chief Risk Officer*) définit la politique générale de gestion des risques.

Ce *risk manager* a pour interlocuteurs directs, les directeurs métiers et les opérationnels avec lesquels il établit la cartographie des risques et les plans d'action nécessaire à leur traitement.

Il n'y a pas de correspondants risques ou équivalents dans les filiales et dans les différentes divisions du groupe.



Source CIGREF

Figure 2 : Organisation centrale réduite

Organisation en « électron libre »

L'absence de *risk manager* dans une entreprise ne signifie pas l'absence d'une démarche de gestion des risques. La mise en œuvre d'une telle démarche peut être initiée par une direction métier ou une direction fonctionnelle qui donne les impulsions nécessaires à cette démarche.

Cette organisation peut dans certains cas provoquer un manque de visibilité de la démarche et donc des difficultés en parler. Relayée par l'absence d'une politique globale et intégrée de gestion des risques, elle peut aussi conduire à moins d'efficacité et de cohérence dans la démarche.

Absence d'organisation

Lorsqu'il n'existe ni *risk manager* ni démarche structurée de *risk management*, les différents métiers assurent au niveau local l'identification et le traitement de leurs propres risques. Par conséquent, les métiers gèrent leurs risques en totale indépendance.

Cette indépendance ne permet pas une gestion centralisée des risques au niveau du Groupe. La somme des risques métiers ne correspondant pas à la totalité des risques groupe il y a perte d'efficacité dans leur traitement.

Gestion des risques et organisation de la DSI

En matière de gestion des risques, les DSI des entreprises peuvent adopter plusieurs schémas organisationnels.

Dans certaines entreprises, l'informatique prend la forme d'un GIE dans lequel il existe le plus souvent une personne en charge de la gestion des risques du GIE. Ce *risk manager* ne traite quasiment que des risques liés aux SI.

Du reste, il n'est pas rare de voir le responsable sécurité groupe piloter la gestion des risques liés aux systèmes d'information. Dans ce cas, son action est relayée par la DSI groupe et par les DSI des filiales.

Cette prise en compte de la gestion des risques par la DSI n'implique pas une influence forte de la démarche de *risk management* sur son organisation. C'est au niveau des processus et du fonctionnement de celle-ci que la démarche a le plus d'influence.

Dans les groupes d'inspiration anglo-saxonne, il peut exister une fonction d'IT *risk manager*, spécialiste des risques liés aux systèmes d'information. Il conduit la politique de gestion des risques informatiques et peut être assisté par des correspondants risques ou sécurité au niveau des filiales. Ces correspondants sont chargés d'une part, de la remontée des informations, d'autre part, de la déclinaison des préconisations émises par l'IT *risk manager* au niveau des DSI des filiales.

2.3.2 *Relations entre les acteurs de l'entreprise*

Paradoxalement, la mise en place d'une politique globale et intégrée de gestion des risques déclinée par un *risk manager* conduit dans un premier temps à une complexification des relations entre les acteurs de l'entreprise et dans un second temps à une rationalisation de la démarche de gestion des risques.

Des relations complexes

Nature des relations entre le *risk manager* et les autres fonctions de l'entreprise

La nature des relations entre le *risk manager* et les autres fonctions de l'entreprise varie suivant qu'elles soient métiers ou fonctions d'évaluation et de contrôle.

La présence d'un *risk manager* a progressivement conduit les métiers à intégrer les risques dans le management de leurs projets et dans la continuité de leur activité. Cette prise en compte n'a pas été immédiate : les directions métiers ont eu tendance à privilégier leurs objectifs opérationnels immédiats, d'autant plus

que, la mise en œuvre des plans d'action de traitement des risques nécessitent souvent de mobiliser des budgets qui pourraient être affectés à la conduite de projets propres à leur activité. La gestion des risques n'était pas une priorité pour les métiers chargés de la mettre en œuvre.

Le *risk manager* a donc été dans un premier temps considéré comme une source de gêne pour les opérationnels, mais l'appui de sa hiérarchie et les opérations répétées de sensibilisation ont démontré aux directions métiers son importance pour la maîtrise des risques dans l'entreprise.

Il y a eu moins de tensions avec les fonctions d'évaluation et de vérification de la sécurité (qualité, sécurité, audit interne). Par nature, il existe une complémentarité entre ces dernières et la fonction de *risk manager*. Cette complémentarité se traduit par la mise en place de mécanismes de contrôle qui verrouillent la démarche.

Il apparait alors qu'une démarche de gestion des risques encourage les mécanismes de contrôle même s'ils apparaissent en premier lieu comme un handicap à la flexibilité. Ces contrôles sont porteurs de valeur car ils poussent les métiers à s'industrialiser, et la démarche à se rationaliser.

Types de relations entre ces acteurs

Il existe naturellement des relations hiérarchiques classiques entre le directeur des risques, les *risk manager*s et les éventuels correspondants risques présents dans les filiales.

Néanmoins, l'efficacité de la démarche est garantie par la transversalité des relations entre tous les acteurs impliqués dans cette démarche. Dans ce cadre transversal, tous les acteurs de l'entreprise sont concernés et doivent contribuer : la gestion des risques implique un travail en réseau où une relation collaborative est toujours préférée à une relation hiérarchique.

Le rôle du *risk manager* n'est donc pas d'imposer la politique de gestion des risques mais d'assister et de coordonner les différentes directions opérationnelles dans la maîtrise de leurs risques. C'est un facteur d'optimisation, de mise en cohérence et de rationalisation du réseau d'acteurs participant à la gestion des risques de l'entreprise

La rationalisation des relations

Les entreprises qui ont participé à cette étude indiquent fréquemment que les conflits éventuels qui existaient entre le *risk manager* et les autres acteurs de l'entreprises se transforment progressivement : d'abord critiquée, la démarche est maintenant acceptée pour quatre raisons majeures :

- Le *risk manager* peut aider les directions métiers à obtenir des budgets pour des aménagements relatifs au risque ou à la sécurité.
- Le *risk management* permet aux directeurs métiers de justifier leurs échelles de priorités dans la mise en œuvre de certaines mesures. En effet des priorités doivent se dégager pour traiter d'abord les risques les plus importants. Cela permet de justifier, sur une base rationnelle confortée par la méthode de gestion des risques, que le traitement de risques secondaires soit reporté.
- Le *risk manager* qui a entériné le choix fait par une direction métier en matière de risque peut assumer la responsabilité de l'absence de traitement d'un risque métier réalisé.
- La gestion des risques peut être utilisée par les métiers comme standard de management des projets.

Cette acceptation de la démarche par les métiers a conduit à rendre cohérentes les relations entre les acteurs impliqués dans la démarche de gestion des risques.

Au centre du dispositif de gestion des risques, le *risk manager* agit donc aussi comme un coordinateur : c'est le point central du réseau d'acteurs participant à la gestion des risques de l'entreprise.

Les relations entre le risk manager et la DSI

On constate qu'en général les directives du *risk manager* (ou de son équivalent) prises en compte par la DSI se concentrent en priorité sur la sécurité des systèmes d'information (DICP[8], continuité d'activité…), laissant de côté d'autres risques (par exemple les risques sur les projets) que le risk manager souhaiterait voir traités. Néanmoins, les relations entre la DSI et le *risk manager* prennent la forme d'une coopération. En définitive ils n'ont pas une relation de prescripteur à exécutant pour les raisons suivantes :

- Ces deux directions sont parfois rattachées au même directeur

[8] DICP : Disponibilité, Intégrité, Confidentialité et Preuve

- Elles ont une culture de la sécurité commune
- Les préconisations du *risk manager* vis à vis de la DSI viennent plutôt en complément d'actions déjà identifiées car la DSI a une forte culture en matière de gestion des risques.

Il peut aussi exister des « *IT* » *risk manager*s au sein de la DSI. Dans ce cas les relations entre le *risk manager* « Groupe » et la DSI sont simplifiées : chacun a son propre domaine d'intervention. Les *IT risk manager*s appréhendent le risque informatique de manière extrêmement fine alors que le *risk manager* Groupe va se concentrer sur les risques informatiques principaux : leurs priorités ne sont donc pas nécessairement les mêmes. Cependant il n'y a pas de cloisonnement total, la supervision de la sécurité des systèmes d'information est par exemple une préoccupation commune que les deux entités font avancer ensemble.

Dans certaines entreprises, le *risk manager* dicte les niveaux de protection. La DSI se charge de mettre en œuvre les mesures adéquates pour atteindre les objectifs de réduction des risques qui lui ont été assignés. Dans ce cas, la démarche peut avoir un impact fort dans la professionnalisation du travail de la DSI. Dans ce cadre, le *risk manager peut* être assisté d'un collaborateur qui connait les éléments de la politique globale et qui a une compétence en matière de système d'information, afin de faire le relais entre la politique de gestion des risques et la pratique de la DSI.

Lorsqu'il n'existe aucune démarche globale et structurée de *risk management*, les risques sont le plus souvent traités par les métiers. Dans ce type d'organisation, la DSI peut se voir alors fixer des objectifs de gestion pour des vulnérabilités qui ne sont rattachées à aucun métier. Dans d'autres cas, elle va se substituer à certains métiers, en particulier lorsque la sécurité des systèmes d'information est en jeu.

Enfin on note que dans une démarche bien comprise d'allocation, par la fonction *risk manager*, du traitement des risques aux métiers concernés, certains risques pourtant liés à l'informatique sont assez logiquement traités par d'autres métiers. Par exemple les risques juridiques liés à l'utilisation non éthique de l'informatique par le personnel sont traités par la DRH, avec le conseil de la DSI, mais c'est la DRH qui prend les mesures nécessaires (règlement intérieur, engagement individuel…)

2.3.3 Développement de la formation en matière de gestion des risques

La prise en compte des risques dans l'entreprise conduit le plus souvent à la mise en place de formations et de sensibilisations relatives au *risk management*. Ces actions ont pour but d'insuffler une réelle culture du risque au sein de l'entreprise.

Formation, sensibilisation et compétences en matière de gestion des risques

La formation

Suivant les entreprises, il existe de fortes différences en matière de formations et de sensibilisations sur la gestion des risques :

- Les entreprises les moins matures en matière de gestion des risques organisent rarement des formations sur ce sujet.
- Dans d'autres entreprises les formations axées sur la sécurité physique ou les systèmes d'information, sont l'occasion d'aborder les problématiques relatives à la maîtrise des risques.
- Enfin, dans les entreprises les plus avancées en matière de gestion des risques des formations et des sensibilisations poussées sont organisées pour les managers, lors de colloques ou dans des universités d'entreprise.

Toutefois, les entreprises ne proposent pas un cycle de formation poussé en la matière pour tous leurs employés. Dans le meilleur des cas, les managers sont formés et le reste des collaborateurs légèrement sensibilisés.

La sensibilisation

La plupart des entreprises privilégient la sensibilisation plutôt que la formation de leurs collaborateurs. Les actions de sensibilisation sont souvent organisées par les *risk manager*s. Elles peuvent prendre différentes formes :

- Campagnes d'affichage,
- applications ludiques sur Intranet,
- responsabilisation par signature de documents,
- questionnaires.

L'intérêt des questionnaires est d'identifier les lacunes afin d'éviter d'organiser des sessions sur des sujets déjà maitrisés par les collaborateurs. Les thèmes de sensibilisation évoluent donc rapidement. Ce principe est particulièrement intéressant pour la DSI puisque les systèmes d'information évoluent très rapidement. Les DRH peuvent appuyer le *risk manager* dans ce sens car elles

sont très intéressées par ce principe de questionnaire de sensibilisation.

La sensibilisation est aussi encouragée par le biais d'une part de la signature d'une décharge de responsabilité et d'autre part du règlement de l'entreprise. De nombreuses entreprises imposent la signature de documents à leurs employés afin d'attester qu'ils ont pris en compte les risques. Ces documents permettent de responsabiliser l'employé et surtout de montrer que l'entreprise a pris les mesures nécessaires pour se prémunir des risques juridiques induits par la faute d'un de ses employés.

Malgré toutes ces mesures, les *risk managers* considèrent que les cadres de l'entreprise ne sont jamais assez sensibilisés ou formés à la gestion des risques. Plus souvent notés sur leur implication dans la performance économique du groupe, que sur la réalité des mesures de protection mises en place, il est difficile de maintenir chez eux, un niveau de motivation élevé.

Les compétences en matière de gestion des risques

Certaines entreprises demandent une compétence spéciale en matière de gestion des risques pour les personnes en charge piloter des projets relatifs au *risk management*. Cette compétence n'est exigée qu'au niveau des managers sous la forme d'un titre ou d'une expérience.

Néanmoins, pour les responsables de projet en général, certaines entreprises se posent aussi la question d'intégrer un niveau de sensibilisation minimum à la gestion des risques dans fiche métier du référentiel RH[9].

Lorsque cette compétence est exigée, elle fait le plus souvent l'objet d'une évaluation. C'est une garantie pour le *risk manager* de la bonne maîtrise des usages par les collaborateurs.

La formation de la DSI en matière de gestion des risques

En général, la démarche de gestion des risques a peu d'impact sur la formation ou la sensibilisation des membres de la DSI. Dans la plupart des entreprises, aucune formation n'est prévue pour la DSI en matière de *risk management.*

Néanmoins, dans de rares entreprises, les cadres nouvellement embauchés, y compris ceux de la DSI, suivent une formation sur l'utilisation de leur outil bureautique. Le but de cette formation est de leur donner une conscience des risques de piratage et d'intrusion et leur rappeler l'éthique liée à l'usage de ces outils.

[9] Les échanges au sein du groupe RH du CIGREF montrent que cette compétence pourrait aussi être étendue à d'autres métiers.

Par contre, la DSI participe souvent à la mise en place de sensibilisations dans des domaines liés à la gestion des risques : la sécurité des systèmes d'information et la protection des informations stratégiques de l'entreprise (intelligence économique) :

- L'*IT risk manager* peut être le vecteur de ces sensibilisations. Il émet des recommandations sur la sécurité des systèmes d'information vers les DSI des filiales qui vont diffuser tout au long de l'année un ensemble de documents de sensibilisation sur les risques liés aux systèmes d'information.
- La prise en compte des risques liés à la maitrise de l'information stratégique ou à l'intelligence économique est un enjeu majeur pour l'entreprise. Les entreprises vraiment sensibilisées à ces problématiques proposent des formations organisées le plus souvent avec le concours de la DSI et de différents services de l'état (la DST10 par exemple). Les managers de la DSI peuvent aussi être formés à ces problématiques. Ils les déclineront ensuite auprès de leurs utilisateurs.

La DSI, dans ce cadre, est un élément moteur dans la mise en place de formations sur des sujets liés à la gestion des risques.

2.4 Les outils de gestion des risques

Pour gérer, prévenir, réduire et traiter les risques, des outils et méthodes ont été progressivement développés dans l'entreprise. Ils ont permis d'affiner les procédures de cartographie des risques et de mettre en relief des facteurs clefs, nécessaires à un management optimal des risques.

2.4.1 La procédure de gestion des risques

Même si les procédures de gestion des risques diffèrent selon les entreprises, les étapes qui la composent sont toujours similaires :

- Dans un premier temps, les risques sont identifiés, cartographiés et évalués.
- Une fois les risques majeurs identifiés, des plans d'action destinés au traitement de ces risques sont mis en œuvre. Les risques résiduels font l'objet d'un transfert.
- Les budgets « risque » sont alloués aux entités chargées de les traiter

[10] Direction de la Surveillance du Territoire

- Enfin, les actions correctrices font l'objet d'un suivi et d'un contrôle.

La cartographie des risques

Perception des risques

L'identification des risques dépend de la façon dont ils sont perçus. Les différences de perception dépendent du contexte dans lequel les risques s'exercent. Par exemple :

- on constate que les directeurs des différents métiers ne hiérarchisent pas des risques identiques de la même manière.
- Le caractère stratégique d'un risque dépend aussi de l'entité sur laquelle il s'exerce.
- De la même manière, les risques stratégiques du groupe sont souvent très différents des risques métiers.
- Enfin, suivant que l'on s'attache à regarder pour un risque donné, la sévérité de ses conséquences ou sa probabilité d'occurrence, sa perception sera différente

La définition d'un langage spécifique à la gestion des risques est nécessaire pour réaliser une cartographie aboutie et précise. Il faut définir une terminologie commune avec des référentiels processus communs pour ne pas amplifier les différences de perception entre les entités qui vont participer à l'élaboration de la cartographie.

Toute cartographie des risques nécessite une préparation rigoureuse qui suit certains principes. Elle doit être réalisée auprès d'un échantillon de personnes suffisamment représentatives tout en prenant en compte de facteurs comme le coût et le temps. Comme le plus souvent, les interlocuteurs n'auront pas une démarche menant spontanément à une bonne cartographie des risques, le *risk manager* devra les guider par un dispositif méthodologique adapté.

Certains *risk manager* choisissent de déléguer la cartographie des risques à des consultants. Ce choix dépend du temps imparti, du budget et des personnes à interroger.

Identification des risques

Dans un premier temps, le *risk manager* va réaliser une étude préalable des risques de l'entreprise en fonction de sa propre perception. Cette étude préalable va lui permettre d'identifier l'échantillon qu'il va interroger par la suite. Dans l'absolu, il faudrait interroger toutes les unités et les métiers de l'entreprise ce qui est le plus souvent impossible. L'échantillon de

cartographie sera très différent d'une entreprise à l'autre, car il dépend de la perception du *risk manager*.

Dans un second temps, le gestionnaire des risques va élaborer des questionnaires sur la perception des risques, pour chacun des métiers ou entités qu'il a choisi d'interroger. Généralement ces questionnaires sont destinés à quatre types d'interlocuteurs :

- les opérationnels qui ont un rôle important à jouer car ils ont souvent un degré important de sensibilité aux risques,
- les responsables de processus métier,
- la direction générale lorsque cela est possible,
- les consultants externes et internes.

Evaluation des risques

Pour avoir une liste exhaustive des risques et de leur perception, les questionnaires réalisés précédemment sont croisés avec l'étude préalable réalisée par le *risk manager*.

Les risques sont alors classés et hiérarchisés selon leur importance[11]. Ce classement se fait pour chacune des entités de l'entreprise. Différentes méthodes peuvent être utilisées pour procéder à cette évaluation.

Les personnes interviewées vont noter chaque risque et les placer dans un diagramme en fonction de deux critères : la sévérité et la difficulté à gérer ce type risque. Ces matrices et diagrammes font ensuite l'objet d'un regroupement dans une base de données qui est traitée par le département des risques.

Une autre méthodologie utilise une notation collective des risques et la confrontation des opinions lors d'un débat.

Le *risk manager* groupe va utiliser ces notations pour établir une cartographie globale des risques majeurs pour l'entreprise et mettre en évidence les priorités à examiner en termes de plans d'actions.

Le traitement des risques

L'entreprise a le choix de réduire ses risques ou de les transférer.

La réduction des risques se fait par la prévention[12] ou par la protection[13]. En règle générale, le transfert des risques vers un assureur se fait après réduction de celui-ci.

[11] C'est à dire selon la gravité de leur impact potentiel combinée à leur probabilité d'occurrence
[12] Action sur la fréquence du risque
[13] Action sur la gravité du risque

La réduction des risques prend la forme de plans d'action déduits des priorités dégagées par la cartographie des risques. Dans la majeure partie des cas, les plans d'action sont définis et mis en œuvre par les opérationnels avec l'assistance du *risk manager*. En effet, les personnes en contact direct avec l'activité soumise au risque, sont les plus à même de proposer et de mettre en œuvre des mesures de traitement de ce risques. Ils ont une expertise dans leur activité propre. Chaque responsable de risque désigné, doit définir les plans d'action adéquats et les mettre en œuvre après une éventuelle validation du *risk manager.*

Ces plans ont pour objectif de réduire au maximum les risques jugés majeurs pour le groupe c'est-à-dire d'obtenir un risque résiduel le plus faible possible. La constitution de ces plans comprend en général deux grandes étapes :

- Déterminer la meilleure façon de traiter le risque,
- Sélectionner et planifier un traitement adapté.

Le transfert des risques prend généralement la forme de contrats d'assurances. Il se traduit également par l'existence de contrats types qui définissent clairement les zones de responsabilité de chacune des parties (entreprise / partenaires)

Traitement des risques et décentralisation de l'entreprise

La gestion des risques peut être déclinée dans les différentes entités de l'entreprise sous forme de microprocessus. Structurellement l'analyse des risques peut être décentralisée dans les filiales, pour les rendre les plus autonomes possible. Les éléments déterminants de ce choix sont :

- le nombre de filiales
- et leur distribution internationale.

Il existe différentes méthodes pour coordonner la maîtrise des risques dans ces structures. Par exemple, on peut faire remplir un questionnaire au directeur régional pour déterminer sa vision du risque et de la sécurité. Ses réponses sont ensuite comparées aux faits réels, ce qui permet de mettre en évidence les discordances qui devront être corrigées.

Ce travail permet de définir des macro-processus de gestion des risques garant d'une cohérence au sein des filiales. Des politiques définissant les règles de gouvernance sont alors mises en place pour combler les déficits en matière de gestion des risques. Les différentes entités de l'entreprise vont devoir s'aligner sur ces macro-processus pour atteindre le standard exigé.

L'allocation des budgets liés aux risques

Suivant les entreprises, l'allocation des budgets de gestion des risques peut se faire au niveau de la direction financière ou au sein des conseils d'administration lorsque les entreprises sont fortement décentralisées.

Dans tous les cas cette allocation se fait après concertation avec les entités concernées par la gestion des risques qui justifient leurs projets d'investissement en la matière. Toutes les décisions concernant les risques sont prises en cohérence avec le plan stratégique du Groupe.

L'efficacité économique fait partie intégrante des différents objectifs de tout programme de gestion des risques. L'importance du facteur économique dépend directement de la tolérance de l'entreprise face à l'incertitude : plus cette tolérance est faible, plus les budgets dégagés pour la démarche seront importants. Comme il est impossible de tout protéger en raison des coûts, un arbitrage aura forcément lieu. Il confrontera la criticité avec le coût du risque et des mesures de traitement. Les métiers ne sont pas entièrement libres pour effectuer cet arbitrage qui doit nécessairement s'inscrire dans le plan d'orientation stratégique de l'entreprise[14]. Les plans d'action qui vont être mis en œuvre par les métiers vont devoir respecter cette orientation de l'entreprise.

La gestion des risques n'est pas du pilotage à vue en fonction des marges de manœuvre financières. Elle doit respecter une stratégie d'entreprise préétablie. Le propre de la démarche est d'identifier tous les risques pouvant affecter la bonne marche de l'entreprise et de traiter les plus urgents tout en se fixant comme objectif, à terme, de traiter les autres.

Dans certaines entreprises comme les établissements bancaires, la règlementation impose la couverture financière de certains risques (risques de crédit, risques de marché, risques opérationnels).

Suivi et contrôle des actions de traitement des risques.

La cartographie des risques doit faire l'objet d'une mise à jour régulière. A cette fin, le *risk manager* doit organiser une procédure de remontée de l'information.

Un suivi et un contrôle de la mise en œuvre effective des plans d'action doit également être organisé. Souvent la taille du département de maitrise des risques ne permet pas ce suivi. Lorsque le processus est suffisamment mûr, les fonctions de

[14] Les entreprises matures en matière de gestion des risques intègrent toujours une composante « risque» dans leur plan stratégique

contrôle interne, d'audit ou même le responsable de la sécurité peuvent être amenés à exercer ce suivi et ce contrôle. Cependant ce n'est pas toujours possible et de nombreux *risk manager*s regrettent ne pouvoir assurer le bouclage de la démarche de gestion des risques. Cette notion de bouclage est très importante car elle conditionne l'efficacité de la démarche.

Dans ce cadre, de nombreuses entreprises organisent des contrôles et des audits qui peuvent s'exercer à différents niveaux. Le cas des risques portant sur les systèmes d'information en est un bon exemple.

- Audits sur le fonctionnement interne de la DSI. Certains de ces audits peuvent être certifiés par divers services de sécurité institutionnels (DST, etc.) en particulier pour tout ce qui concerne les risques liés au secret professionnel.
- Des audits sur l'état de la sécurité de tout ou partie des composants informatiques.
- Des audits sur l'incidence de nouvelles applications sur la maitrise des risques.
- Certaines entreprises ont été plus loin en instituant un système de contrôle permanent sur la maitrise des risques liés aux systèmes d'information. L'objectif de ces contrôles est d'avoir en permanence un test du système de sécurité.

Ces processus internes ne doivent pas occulter un élément essentiel de la démarche, la gestion du risque « fournisseur ». Cette exigence vis-à-vis des fournisseurs peut se traduire de différentes manières. La plus importante étant le recours à l'outil contractuel :

- Il existe des clauses types de responsabilités/assurances, validées par la direction juridique de l'entreprise, qui sont insérées dans les contrats cadres avec les sociétés de services. Lorsque les fournisseurs souhaitent modifier des clauses liées à la gestion des risques, la direction juridique peut demander l'avis du *risk manager*. Relativement aux SI, la charte informatique peut être inclue dans les contrats des prestataires.
- Du point de vue des risques opérationnels, les entreprises peuvent prévoir un plan de prévention qui permet d'identifier et de traiter la réalisation d'un risque chez le fournisseur.
- Dans les établissements bancaires la réglementation dicte les mesures à prendre concernant les fournisseurs. La banque doit lister l'ensemble des prestataires essentiels et stipuler contractuellement la qualité, le niveau de service, le niveau de sécurité et de continuité exigés. De plus, elle doit définir

les contrôles qui vont être effectués pour garantir ces exigences. Les contrats doivent aussi stipuler que la Commission Bancaire peut venir contrôler le prestataire.

2.4.2 Méthodologies de gestion des risques à l'usage des DSI

Lorsque les Directions des SI s'interrogent sur les risques qui pourraient frapper l'entreprise et plus particulièrement la DSI, elles s'appuient en général sur un référentiel à trois niveaux :

- La politique globale de sécurité et de gestion des risques menée au niveau groupe.
- Les standards : normes ISO[15], le plan de continuité informatique (PCI), les réglementations, etc.
- Les méthodologies : le directeur des risques peut en effet décider d'appliquer certaines méthodologies du marché pour appréhender le risque lié aux systèmes d'informations (MEHARI, EBIOS, ITIL etc.). Ce choix peut aussi lui être imposé par la direction de l'entreprise ou par les usages. Néanmoins pour certains RSSI ou *risk manager*, ces outils s'apparentent le plus souvent à du contrôle de conformité qu'à de la gestion des risques.

2.4.3 Les facteurs clefs pour une bonne gestion des risques

Les entretiens réalisés, notamment avec les *risk manager* Groupe nous ont permis de déterminer plusieurs facteurs clefs utiles pour une bonne gestion des risques d'entreprise :

- **Une prise de décision doit suivre la réalisation de la cartographie des risques**. Lorsqu'aucune vulnérabilité n'est identifiée, une simple validation de la cartographie est suffisante. Quand elle n'est pas suivie d'une prise de décision, la cartographie des risques n'est pas génératrice de valeur ajoutée. De plus les personnes interrogées pour réaliser cette cartographie seront moins enclines à participer dans le futur.
- Il est plus intéressant de **faire une cartographie rigoureuse des risques « a minima »**, plutôt qu'une cartographie exhaustive qui ne permettrait pas un traitement efficace des risques de l'entreprise.

[15] Voir en annexe la liste des normes concernées

- **Le *risk manager* doit organiser la responsabilité de la mise en œuvre des plans d'action**. En effet, en cas de dysfonctionnement dans le traitement des risques, les opérationnels vont souvent se retourner vers le *risk manager* en mettant en avant sa compétence d'expert en la matière. De manière plus générale il ne faut pas confondre le rôle du *risk manager* qui est de piloter et de cadrer la gestion des risques, de la responsabilité de réalisation des actions correctives qui revient le plus souvent à des responsables opérationnels ou métier.

3 Le rôle de la DSI dans la démarche de gestion des risques de l'entreprise

La DSI peut contribuer fortement à la démarche de *risk management*. Cette contribution s'exerce alors généralement sous la forme d'une influence directe lors de la mise en œuvre d'une politique globale et intégrée de gestion des risques dans l'entreprise, ou indirectement par la mise en place d'outils, de méthodes ou de formations en support aux activités du *risk manager*. Enfin, la DSI participe toujours à la démarche d'entreprise par la gestion de ces propres risques liés aux systèmes d'information.

3.1 La contribution directe de la DSI dans la gestion des risques

Le niveau de contribution de la DSI dans la démarche de gestion des risques dépend généralement de trois critères :

- l'importance pour l'entreprise de « l'information » et du système qui lui est associé.
- le niveau de maturité de la démarche de gestion des risques mise en œuvre dans l'entreprise.
- L'existence et le rattachement d'un éventuel Responsable de la sécurité des Systèmes d'Information (RSSI) dans l'entreprise

3.1.1 Le rôle de l'information et de l'informatique dans l'entreprise

Au fil des entretiens, il est apparu que plus la production ou l'activité d'une entreprise sont liées à son système d'information, plus la DSI contribue à la démarche de gestion des risques. *A contrario,* cette participation devient plus faible dans les entreprises où la production est moins dépendante du système d'information.

Les entreprises où la production dépend beaucoup du système d'information

Il faut distinguer les entreprises où la production dépend directement du système d'information, des entreprises où l'information est le produit de l'entreprise.

Dans les entreprises où « l'information » est un produit en tant que tel (banques, assurances, opérateurs de télécommunication, grande distribution, industries à flux tendus), une grande partie des risques du groupe sont, par définition, liés au système d'information. La DSI joue alors un rôle important dans la démarche de gestion des risques de l'entreprise qui se traduit par des actions dans les domaines suivants :

- La défense anti-intrusion du périmètre logique de la société.
- La protection de l'information stratégique de l'entreprise contre l'accès, l'utilisation, la diffusion, la destruction, ou la modification non autorisée. Ce domaine concerne, bien évidemment, les organisations où « l'information » est le cœur de métier de l'entreprise. Dans ce domaine, le rôle de la DSI est d'autant plus important que le correspondant CNIL de l'entreprise est directement rattachée à la DSI : il est pénalement responsable des informations qui lui sont confiées par les clients, partenaires ou collaborateurs.
- La définition du *Disaster recovery plan* (DRP) ou plan de secours. Ce plan définit les actions qui vont permettre, en cas de crise grave, de redémarrer le plus efficacement possible, le système d'information, avec une perte minimale de données, de temps et de matériel et pour un coût acceptable.

Dans les entreprises industrielles, la gestion des risques des systèmes de production est de plus en plus souvent pilotée par la DSI qui y étend son savoir-faire acquis dans un premier temps dans l'informatique de gestion.

Il apparaît que les deux types de systèmes d'information (production et gestion) sont de plus en plus interdépendants. Des attaques menées sur l'informatique de production risquent donc d'impacter le système informatique de gestion. D'autant que l'informatique de production est de plus en plus fréquemment sous-traitée à des prestataires dont les standards de gestion des risques doivent alors être systématiquement contrôlés.

Les risques liés à l'informatique de gestion sont en général bien maitrisés grâce à la sécurité des systèmes d'information (pare-feu, identification, antivirus, contrôle d'accès..). L'extension de ces mesures aux systèmes d'information de production, est d'autant plus critique que la sécurité du système dépend de celle de son élément le plus faible.

Les industriels ont longtemps conçu et piloté leur propre informatique en toute indépendance. Ils ont appris à résoudre opérationnellement la plupart des risques qu'ils rencontrent. Cependant, on constate en interne, une propension à peu communiquer et partager le savoir-faire sur ce sujet et une grande réticence vis à vis de mesures de sécurité préconisées par la DSI ou le RSSI.

C'est le rôle du *risk manager* ou du RSSI d'agir et de résoudre ces désaccords entre l'informatique de gestion et l'informatique de production. Il en a la légitimité, ce qui lui permet d'imposer la

cohérence de la gestion des risques à travers tous les systèmes de l'entreprise.

Les entreprises où la production dépend moins de l'informatique.

Dans les entreprises qui ne fonctionnent pas en flux tendu, et dont l'informatique ne joue pas un rôle direct dans la production ou les ventes, la DSI gère également les risques informatiques.

Cependant l'impact des risques sur l'activité étant moindre, les exigences vis à vis des systèmes de réduction des risques seront inférieures ou de nature différente. Par exemple dans le cas des plans d'action du risque de pandémie, les DSI chercheront des solutions pour faire travailler leur personnel à distance alors que dans les entreprises de la première catégorie[16] préfèreront des solutions permettant la présence sur leur site des personnels indispensables à la production informatique.

3.1.2 Impact du niveau de maturité de l'entreprise en gestion des risques

Le rôle de la DSI dans la démarche de gestion des risques est inversement proportionnel au niveau de maturité de l'entreprise en matière de *risk management*.

Nous allons voir que dans les entreprises les moins matures, la DSI peut être amenée à jouer un rôle majeur. En effet elle agit souvent comme un moteur dans la mise en place d'une démarche globale de gestion des risques. Une fois que l'entreprise a atteint un niveau de maturité suffisant, la DSI n'est plus alors un acteur majeur du processus, ce qui est positif.

Entreprises moins matures

Dans les entreprises qui n'ont pas de *risk manager* ou de département en charge de la maitrise des risques, on constate que la DSI joue un rôle important dans la gestion des risques de l'entreprise. Lorsque ni l'organisation de la démarche de *risk management*, ni la répartition des taches ne sont structurées, la DSI peut aussi jouer ce rôle moteur. Dans ce cadre, elle peut alors être à l'origine de la mise en place d'une démarche moderne de *risk management*.

Ce rôle d'initiateur est plus souvent volontaire que statutaire. Il s'exerce en général via le responsable sécurité des systèmes d'information (RSSI) qui possède souvent des compétences et une mission proches de celles qu'aurait un *risk manager*. De part ces compétences, la DSI est parfois invitée à participer aux

[16] Celles dont la production dépend fortement de l'informatique

analyses des risques métiers. Elle agit alors comme un service de conseil et de support qui peut aider les directions métiers dans l'évaluation de leurs propres risques en appliquant des concepts issus des systèmes d'information : disponibilité, intégrité, confidentialité et preuve.

Mais paradoxalement si la DSI veut contribuer à une bonne gestion des risques dans son entreprise elle doit viser à ne pas en être le gestionnaire principal mais simplement un élément moteur ou déclencheur d'une démarche globale et structurée. En effet, si cette participation active de la DSI conduit l'entreprise à se concentrer en priorité sur les risques liés à l'informatique, il se peut que certains risques majeurs pour l'entreprise ne soient alors pas traités.

Le cas des plans de secours (DRP) est un bon exemple de ce paradoxe apparent : en effet, la mise en place par la DSI d'un DRP efficace n'implique pas forcément la définition d'un bon plan de reprise d'activité dont la valeur dépend de procédures et de mesures préventives touchant tous les métiers ainsi que la direction générale de l'entreprise (cellule de crise, sites de repli, stocks, procédure de communication etc.).

Entreprises matures vis-vis de la gestion des risques

Dans les entreprises matures vis-à-vis de la gestion des risques, il n'est donc pas nécessaire que la DSI ne soit pas un acteur majeur du processus. Même si la DSI n'est plus aujourd'hui considérée comme un service purement support et que ses compétences en matière de sécurité et *a fortiori* en matière de gestion des risques sont reconnues, elle ne participe qu'à une partie de la démarche de *risk management*.

En effet, les risques informatiques, de conformité (*compliance*), légaux, vis à vis des consommateurs[17] sont traités par le *Risk Manager* ou le RSSI lorsqu'il existe. Les directions métiers responsables de ces risques sont directement en charge de leur traitement, la DSI n'intervenant que pour ses risques propres.

En général la DSI gère de manière autonome ses propres risques. Cependant dans certaines entreprises, cette prérogative lui a été retirée et confiée, ou *a minima* partagée, avec le *risk manager* de l'entreprise pour mieux garantir l'indépendance des décisions importantes telles que le choix des risques prioritaires ou l'allocation des budgets de réduction des risques.

[17] Si on est dans une relation métier / consommateur (B to C)

3.1.3 *Le Responsable de la Sécurité des Systèmes d'Information*

Le niveau de contribution de la DSI à la démarche de gestion des risques est largement influencé par l'existence d'un RSSI qui peut lui être rattaché.

Lorsque le RSSI n'est pas rattaché à la DSI et qu'une direction des risques est en place, la DSI contribue à la gestion des risques au même titre que les autres directions métiers, experts dans leur domaine de compétence. Elle se focalise surtout sur la mise en place des plans de traitement des risques liés aux systèmes d'information. Dans ce cas, c'est le RSSI qui va jouer un rôle important dans la démarche de gestion des risques.

Lorsque que le RSSI est rattaché à la DSI, elle eut avoir en tant que telle une importance majeure dans la démarche de gestion des risques. En particulier grâce à ces méthodes d'analyse de risque ou son expertise dans le domaine des plans de reprise d'activité ou des plans de secours informatique. Grâce à son RSSI, la DSI est souvent en avance sur ces sujets.

3.2 *La contribution indirecte de la DSI dans la gestion des risques*

3.2.1 *Typologie des contributions indirectes*

Comme il a été vu précédemment, les entreprises ont évolué de la gestion des risques par le transfert (assurances) à une obligation de traitements par réduction des risques (plans d'actions). Dans cette évolution, la DSI a souvent été un précurseur : le transfert de risque est rarement une solution acceptable en matière de système d'information.

Cette antériorité lui permet de contribuer indirectement de plusieurs façons :

- La DSI peut participer localement à l'identification des risques de l'entreprise. Dans les sociétés de grande distribution par exemple, la DSI en tant que plaque tournante de l'entreprise va percevoir et identifier des risques opérationnels qu'elle va se charger de signaler afin qu'ils soient traités.
- Lorsqu'un risque n'a pas encore été rattaché à un métier, la DSI peut se voir fixer des objectifs de gestion pour ce risque. Dans d'autres cas, il arrive qu'elle se substitue à certains *métiers* lorsque la sécurité des systèmes d'information est en jeu.
- Elle peut aussi fournir les outils techniques et les méthodologies nécessaires au traitement des risques. Cependant la fourniture de supports informatiques pour la gestion des risques (outils d'audit, d'enregistrement des

classements de risques, de suivi des plans d'action, de traçabilité....) ou la mise en place d'une application informatique de gestion des risques sont relativement rares. Les *risk manager* préfèrent communiquer directement avec les entités opérationnelles. Seules les entreprises qui ont de nombreuses filiales à l'international commencent à mettre en place ce type d'outils avec l'aide de la DSI.

- Dans la mise en œuvre des plans d'action de traitement des risques par les métiers, la DSI peut accompagner les directions métiers sur notamment : la description des processus, la mise en place de points de contrôles et des dispositifs de contrôle interne.
- La prise en compte par les directions métiers de risques qu'elles n'ont pas envisagé peut être aussi favorisée par un questionnement des différents services de l'entreprise lors de la définition d'un plan de secours informatique.

Cette liste n'est pas exhaustive. Les moyens par lesquels la DSI peut participer indirectement à la démarche de gestion des risques sont nombreux et l'on peut encore citer rapidement:

- Le renforcement ou la création d'applications informatiques destinées à diminuer certains risques de l'entreprise
- La vérification du bon fonctionnement de la gestion intégrée (ERP)18 vis à vis de la LSF19
- La mise en place d'outils anti-fraude (traçabilité des achats des paiements....)
- L'élaboration des indicateurs de « *compliance* » requis selon le secteur d'activité
- La contribution au contrôle des exportations sous leur aspect immatériel (risque de sortie du territoire national des données relevant du patrimoine industriel ou scientifique national sous forme de document électronique)
- Le développement de contenu consacré à la gestion des risques au moyen des outils d'*e-learning* sur l'intranet.
- La mise à disposition de personnels de maîtrise d'ouvrage déléguée auprès des directions métier pour les aider dans leur démarche de gestion des risques.
- Etc.

[18] Enterprise resource planning

[19] Loi de Sécurité Financière

3.2.2 Méthodologies, outils

Pour l'identification, l'analyse et le traitement des risques liés aux systèmes d'information, nous avons vu précédemment qu'il existe de nombreuses méthodologies à la disposition de la DSI.

Ces méthodologies (Méhari, Ebios…) proposent un déroulé pas à pas du processus de gestion des risques liés aux systèmes d'information.

Néanmoins, ces méthodes d'analyse apparaissent aux yeux de certains DSI, trop lourdes et difficilement adaptables aux contraintes et spécificités de leur entreprise. Initialement développées pour un secteur d'activité donné, leur application dans un environnement nouveau implique des ajustements difficiles à mettre en œuvre. Pour cette raison, de nombreuses entreprises n'appliquent pas *stricto* sensu ces méthodes. Néanmoins, elles peuvent s'en inspirer pour mettre en place leurs propres procédures d'analyse et de traitement des risques.

3.2.3 La gestion des risques liés aux systèmes d'information

On peut procéder à une mise en perspective temporelle des risques pris en compte par la DSI en proposant de distinguer quatre familles d'activités apparues successivement :

Le traitement préventif des limites du système informatique :

La lutte contre l'obsolescence est une des activités permanentes et de fond de la DSI. Dans un certain sens le traitement du bug de l'an 2000 relevait de cette catégorie. De manière plus moderne on trouve les calculs d'ingénierie du SI et les tests de capacité de système à absorber des pointes d'activité ou des pertes partielles de certains de ses éléments (ex redondance des moyens de communication, calculs de MTBF, dimensionnement et architecture de la génération électrique des data centers).

La protection des données (seconde moitié des années 90)

Dans la protection des données on retrouve typiquement la lutte anti-intrusion, la mis en place de systèmes de protection contre les virus informatiques…etc. De manière plus contemporaine on intègre aussi dans cette catégorie, la gestion des identités, la protection des données à la source, la protection des exportations immatérielles,…

La continuité d'activité (années 2000)

La continuité d'activité est assurée par les sauvegardes de données et désormais par les DRP[20].

La continuité d'activité a évolué. Désormais, elle prend en compte dans sa composante informatique, les grandes catastrophes "systémiques" affectant un pays ou une région géographique. C'est le cas du risque de pandémie aviaire ou de crue centennale de la Seine.

On constate à travers ces problèmes que ce n'est plus le seul "redémarrage" des applications qui prime mais la capacité d'apporter « l'énergie » informatique à tous les secteurs de l'entreprise qui sont encore en état de pouvoir l'utiliser. Typiquement, la DSI s'interroge sur les moyens à mettre en œuvre pour permettre au personnel de continuer à travailler depuis chez lui en cas de grippe aviaire.

La conformité (période actuelle)

Actuellement, la DSI se penche sur la conformité des systèmes d'information. En voici quelques exemples : Auditabilité de la gestion des licences logiciel, éthique de l'utilisation des moyens informatiques…

3.2.4 La participation par le biais de la sécurité des systèmes d'information (SSI)

La sécurité des systèmes d'information est un élément de prévention et de protection contre les risques liés aux systèmes d'information. Dans la plupart des grands groupes, il existe un Responsable de la Sécurité des Systèmes d'Information (RSSI) ou AQSSI pour les administrations chargé des aspects sécuritaires des systèmes d'information. Le RSSI est souvent directement rattaché à la DSI ou en étroite relation avec elle. Lorsqu'il n'existe pas, c'est la DSI dans son ensemble qui assure la sécurité des systèmes d'information, ce qui peut être considéré comme un élément majeur de sa participation à la démarche de gestion des risques.

La sécurité des systèmes d'information agit en prévention. Elle va bien entendu privilégier les risques liés à son propre domaine :

- Dans de nombreuses entreprises, les projets majeurs qui impliquent le recours aux systèmes d'information doivent faire l'objet d'un bilan sécurité. Les avant-projets font l'objet de bilans express par les équipes de pilotage. Dès qu'une

[20] *Disaster Recovery Plan*

faille est détectée, des mesures de sécurité sont mise en œuvre en suivant le processus définit dans le projet.

- La protection de l'information.
- La gestion des identités et des droits (authentification, identification, répudiation, *network operating systems*…)
- Les télécommunications : sécurisation des réseaux locaux et à grande distance, des accès pour les collaborateurs mobiles et des infrastructures d'échange entre l'entreprise et le monde extérieur.

3.2.5 Formation et sensibilisation

Dans nos entretiens, il est apparu que la DSI est un acteur majeur de la sensibilisation et de la formation des collaborateurs de l'entreprise sur les risques. En particulier pour les problématiques de sécurité des systèmes d'information et d'intelligence économique. Néanmoins certains de nos interlocuteurs regrettent que l'action de la DSI ne soit pas plus avancée dans ce domaine.

La formation et la sensibilisation par la DSI aux problématiques de sécurité des systèmes d'information peuvent prendre plusieurs formes :

- La DSI peut publier sur intranet des textes de sensibilisation sur la sauvegarde des données personnelles ou sur le choix des mots de passe et leur utilisation.
- La sensibilisation peut aussi se faire par l'affichage de posters, ou la projection de vidéos lors des réunions de groupe.
- Certaines DSI développent aussi des applications ludiques mises à disposition des collaborateurs, pour qu'ils se testent sur leurs connaissances des règles applicables en matière de sécurité des systèmes d'information.

En termes de sensibilisation, l'explosion des moyens de communication et l'information numérique conduit les entreprises à considérer que la protection des connaissances stratégiques est un enjeu majeur dans la maitrise des risques et que la DSI est un des meilleurs acteurs dans la mise en œuvre de cette protection :

- De la remise d'un mot de passe au respect des clauses de confidentialité dans les contrats, tout doit être strictement encadré afin de s'assurer que les personnes qui vont manipuler des informations stratégiques pour l'entreprise soient conscientes du fort niveau de criticité qu'elles représentent.

- De la même manière, la DSI doit s'assurer que les entreprises nouvellement acquises ou que les prestataires qui viennent dans les locaux respectent bien la politique de sécurité des systèmes d'information.
- La DSI peut et sait aussi mettre en place un programme de protection de l'information destiné à sensibiliser les directions métiers afin qu'elles prennent leurs décisions en respectant l'esprit de la politique générale de sécurité.

C'est donc un des rôles de la DSI de s'assurer que les actions de sensibilisation sont déployées, respectées et régulièrement mises à jour.

Pourtant certains obstacles demeurent : même si la diffusion de l'information est assurée, il n'existe pas encore, dans certaines entreprises, de véritable mesure de l'efficacité de la formation et de la sensibilisation aux risques. Connaître la portée et l'efficacité de la politique de sensibilisation aux risques est la principale piste d'amélioration qui a été exprimée par nos interlocuteurs. Le principal point à améliorer reste la définition d'indicateurs clefs permettant de mesurer l'impact de la sensibilisation aux risques et se fondant sur des éléments objectifs.

Conclusion

Depuis quelques années, de nombreuses entreprises françaises ont organisé une démarche de gestion des risques. La prise en compte des risques dans le fonctionnement de l'entreprise n'est pas nouvelle, néanmoins, depuis les années 2000, leur gestion a beaucoup progressé et s'est professionnalisée.

Pourtant, il existe encore de fortes différences de maturité face au risque entre les entreprises. Le niveau de maturité de l'entreprise face aux risques dépend de plusieurs facteurs, tels que son activité ou le respect de la règlementation, qui les poussent à mettre en place une démarche de *risk management*. Avec les spécificités de l'entreprise (organisation centralisée ou décentralisée), ils influent sur son organisation en matière de gestion des risques. Il apparait par exemple que le *risk manager* est la fonction la plus adapté à la mise en œuvre d'une politique de gestion des risques au sein de l'entreprise, mais qu'elle peut, néanmoins, être assurée par d'autres entités dans l'entreprise.

Mais lorsqu'aucune démarche n'est organisée au sein de l'entreprise, la DSI est souvent la plus à même de l'initier. En effet, le rôle de la DSI dans la démarche de gestion des risques est inversement proportionnel au niveau de maturité de l'entreprise en matière de *risk management*. Quand il est faible, la DSI est souvent l'élément moteur de son initialisation. De même lorsque la production de l'entreprise est essentiellement liée à son système d'information, la DSI jour un rôle majeur dans la démarche de gestion des risques. Dans ce cadre, le rôle du RSSI devient prédominant : s'il est rattaché à la DSI, il amplifie l'impact de la DSI sur la démarche.

Il peut arriver que la DSI ne soit pas pleinement intégrée dans la démarche de gestion des risques d'entreprise. Néanmoins, elle y joue toujours un rôle par le biais de contributions indirectes. En particulier dans les domaines de la formation et de la sécurité informatique. Enfin, elle participe toujours au traitement de ses propres risques liés aux systèmes d'information en utilisant des méthodologies qui ont été développées pour satisfaire aux besoins de la sécurité des systèmes d'information.

Quelle que soit le niveau de maturité de l'entreprise ou son organisation face au risque, la participation de la DSI à la démarche de gestion des risques est amenée à se généraliser pour trois raisons majeures :

1. Les DSI dont l'entreprise n'a pas encore mis en place une réelle démarche de gestion des risques sont en train de se rendre compte que leur technicité et leur expérience en la matière peuvent être utilisées pour donner l'impulsion

nécessaire à la mise en œuvre d'une telle démarche au sein de l'entreprise.

2. L'activité des entreprises dépend de plus en plus de leur système d'information. C'est sa qualité d'expert dans ce domaine qui rend la DSI plus à même, avec l'aide ou non d'un RSSI, de mettre en place les mesures destinées à traiter des risques qui tendent à devenir majeurs pour l'ensemble des entreprises.
3. Enfin, les attentats du World Trade Center et les hypothèses de pandémie grippale ou de crue centennale de la Seine, ont amené les entreprises à s'interroger sur le concept de continuité d'activité. La DSI est l'acteur majeur dans la continuation d'activité, en particulier dans la définition et la mise en œuvre des plans de secours informatique. Dans ce domaine, son influence a tendance à se généraliser.

Annexes

Synthèse des normes portant sur les risques (ISO, BS…)

ISO 17799

ISO 17799 est une norme internationale concernant la sécurité de l'information, publiée en décembre 2000 par l'ISO dont le titre est *Code de pratique pour la gestion de sécurité d'information*. La deuxième édition a été publiée en juin 2005. Cette norme a pour origine la première partie du British Standard BS 7799

L'ISO 17799 est un ensemble de bonnes pratiques destinées à être utilisées par tous ceux qui sont responsables de la sécurité de l'information et des systèmes d'information. Elle part du constat que l'information est un actif important qu'il convient de protéger.

- La sécurité de l'information telle qu'elle est décrite dans la norme est décomposée en trois aspects
- La confidentialité (s'assurer que les informations sont accessibles des seules personnes autorisées)
- L'intégrité (conservation de la validité et de l'intégralité des informations et méthodes de traitement)
- La disponibilité (les utilisateurs autorisés doivent avoir accès aux informations à chaque fois que nécessaire) ».

Cette norme s'appuie sur deux principes et dix chapitres de recommandations sur les aspects techniques et organisationnels de la gestion de la sécurité

- Principe 1 : Définir les exigences de sécurité
- Principe 2 : Choisir des références de contrôle

Chapitres :

- La politique de sécurité.
- L'organisation de la sécurité.
- Classification et contrôle
- Sécurité du personnel.
- Sécurité physique et environnementale
- Gestions des tâches et communications
- Contrôles d'accès.
- Développement et maintenance des systèmes.

- Gestion de la continuité
- Conformité

Pour chacun des éléments référencés, la norme décrit les objectifs à atteindre et les contrôles à mettre en place. Cependant, la norme ne détaille pas ces contrôles qui diffèrent selon l'identification des besoins faites par l'entreprise

ISO 27001

L'ISO 27001 est une norme internationale qui traite de la gestion de la sécurité de l'information. Elle a été publiée en octobre 2005 et porte le titre : « Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information – Exigences ».

La norme ISO 27001 décrit comment mettre en place un Système de Gestion de la Sécurité de l'Information (SGSI) qui permet de choisir les mesures à mettre en place afin de protéger les actifs de l'entreprise.

L'ISO 27001 est un standard international pour la gestion de la sécurité de l'information. Il standard préconise l'utilisation du modèle de qualité : Plan, Do, Check, Act (PDCA) pour établir un SGSI. Ce principe vise à créer un cercle vertueux et un cycle d'amélioration continu. Il se décompose en 4 phases

- P : Planification de la réalisation
- D : Production, réalisation
- C : Contrôle, audit, vérification
- A : Planification d'une nouvelle réalisation, mise en œuvre d'actions correctrices

L'ISO 27001 est une approche basée sur les processus qui définit l'ensemble des tests et contrôles à effectuer pour s'assurer du bon respect d'ISO 17799.

ISO 13335

La norme ISO 13335 est une norme de sécurité des systèmes d'information. C'est un guide de management de la sécurité des systèmes d'information qui trouve son origine dans des rapports techniques décomposés en 4 documents considérés comme des références pour toutes personnes s'intéressant aux systèmes d'information :

- Définitions et concepts de base,

- Informations sur l'organisation à prévoir dans toute entreprise,
- Approches de gestion du risque,
- Guide de choix des mesures préventives selon les circonstances de l'environnement.

La norme se décompose en cinq parties :

- ISO 13335-1 : Concepts et modèles pour la gestion de la sécurité des technologies de l'information et de la communication
- ISO 13335-2 : Techniques pour la gestion des risques pour les technologies de l'information et de la communication
- ISO 13335-3 : Techniques pour la gestion de la sécurité des systèmes d'information
- ISO 13335-4 : Sélection de sauvegardes
- ISO 13335-5 : Guide pour la gestion de sécurité du réseau

Méthodes

MEHARI

MEHARI (Méthode harmonisée d'analyse des risques) est une méthode crée par le CLUSIF (Club de la Sécurité de l'Information Français) dans le but d'aider les Responsables de la Sécurité de Système d'Information dans leurs attributions managériales. Bien que développée pour ce type de fonction spécifique, cette méthode peut aussi être utilisée par les toutes les fonctions qui traitent de problématiques similaires (*risk managers*, etc.).

Cette méthode a vocation à fournir tout un ensemble d'outils adaptés au management de la sécurité des systèmes d'information. La force de cette méthode est la cohérence. A chaque étape du développement de la sécurité correspond un outil cohérent avec les autres. Cette cohérence permet un « feedback » des résultats. Enfin, tous ces outils peuvent être utilisés indépendamment les uns des autres, dans différents types de management. Il existe trois outils majeurs dans cette méthode

- Les diagnostics de sécurité, préalables à l'analyse de risque : Ils sont présentés sous la forme de modules rapide ou approfondi et ont pour objectif d'évaluer le niveau de sécurité en fonction de deux paramètres : le coût et la fiabilité. Le diagnostique rapide permet d'identifier les faiblesses majeures et la mise en œuvre effective de mesures sécuritaires sur un système de sécurité donné, il ne permet

pas de mettre en exergue les points faibles de ces mesures. Le module approfondi, nécessite plus de ressources mais il permet une identification efficace de touts des faiblesses de chaque service de sécurité.

- L'analyse des enjeux permet de mettre en balance les mesures et les objectifs de sécurité à atteindre, ce qui va permettre une prise de décision conforme à la politique sécuritaire de l'entreprise. Cette analyse va permettre de déterminer la juste proportion entre les mesures sécuritaires et les enjeux de sécurité à atteindre. Ce module d'analyse permet de dégager une description des dysfonctionnements possibles et une classification de ces dysfonctionnements.
- L'analyse des risques. En fonction de l'analyse qualitative et quantitative de deux types facteurs : les facteurs structurels (qui ne dépendent pas des mesures de sécurité) et les facteurs de réduction des risques (qui dépendent des mesures de sécurité, la méthode permet une évaluation des risques. Cette évaluation des risques permet la définition et la mise en œuvre de plans de sécurité.

Un des avantages de cette méthode réside dans le fait qu'elle est compatible avec les principales normes ISO sur la sécurité des systèmes d'information. A savoir les normes ISO 13335, 17799, 27001.

Pour plus de renseignements voir le site du CLUSIF: *http://www.clusif.asso.fr*

EBIOS

EBIOS (Expression des Besoins et Identifications des Objectifs de Sécurité) est le nom donné à une méthode développée en 1995 par la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) rattachée au SGDN (Secrétariat Général de la Défense Nationale).

Cette méthode est un outil de :

- gestion des risques liés à la sécurité des systèmes d'information
- de communication sur les risques liés aux systèmes d'information
- d'arbitrage qui permet de justifier la prise de décisions.
- de sensibilisation pour les acteurs d'un projet qui uniformise le vocabulaire.

La méthode EBIOS a de nombreux avantages. Elle est compatible avec les normes internationales et il existe un logiciel libre d'assistance à l'utilisation de la méthode. Cette méthode est applicable aussi bien dans des systèmes simples que des systèmes complexes. Elle se décompose en quatre étapes :

- L'étude du contexte : Dans un premier temps, il s'agit d'identifier précisément le système dans son ensemble, c'est à dire comme la somme des éléments qui le composent, et dans un second temps, le contexte d'utilisation de ce système.
- L'expression des besoins de sécurité : Cette étape a pour but de déterminer le besoin de sécurité pour chacun des éléments identifiés dans l'étape précédente. Tous ces éléments sont priorisés en fonction du facteur de criticité évalué en fonction de la sévérité des impacts dont ils pourraient être victimes. Ces impacts sont évalués en fonction des critères traditionnels des SI. Cette étape permet de déterminer quels sont les éléments les plus critiques.
- L'étude des menaces ou analyse des risques consiste à identifier les risques qui peuvent peser sur le système. Ces risques sont caractérisés par leur type et leur cause (accidentelle, délibérée ou naturelle). A ce stade, on donne des probabilités de réalisation de risques pour chacun des éléments critiques. Cela permet ensuite d'imaginer des scénarios d'attaques avec une probabilité associée. On en déduit les risques spécifiques au système étudié.
- L'expression des besoins de sécurité : Plus le niveau de criticité de l'élément du système est important, plus le besoin de sécurité est fort. Ces besoins de sécurité se pensent en termes techniques ou fonctionnels (organisation, procédure, sécurité physique). L'expression des besoins de sécurité est immédiatement suivie par la mise en œuvre de ces besoins et par une démonstration que le niveau d'exigence sécuritaire a été atteint.

Pour plus de renseignements voir le site de la DCSSI : *http://www.ssi.gouv.fr/fr/dcssi/*

MARION

La méthode MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux) conçue par le CLUSIF (Club de la Sécurité de l'Information Français) n'est plus mise à jour depuis 1998. Le CLUSIF propose désormais la méthode MEHARI (Méthode d'harmonisation et d'analyse des risques).

La méthode MARION permettait d'évaluer les niveaux de sécurité d'une entreprise grâce à des questionnaires portant sur

différents éléments relatifs à la sécurité. L'objectif de cette méthode était d'obtenir un audit de l'entreprise conforme à l'indicateur proposé dans la méthode. Cette méthode se décomposait en 4 phases :

- La préparation
- L'audit des vulnérabilités
- L'analyse des risques
- La mise en place de plans d'actions.

L'intérêt de cette méthode était de pouvoir situer son entreprise en termes de sécurité, par rapport aux autres entreprises françaises utilisant cette même méthode. Depuis que MARION est tombée en désuétude au profit MEHARI, cette méthode n'a plus grand intérêt.

Pour plus de renseignements voir le site du CLUSIF: *http://www.clusif.asso.fr*

COBIT

Le référentiel COBIT (*Control objectives for information & related technology*) est une méthode de Maîtrise des Systèmes d'Information et d'audit éditée par l'ISACA (*Information System Audit & Control Association*) en 1996. C'est un cadre de contrôle qui vise le pilotage des risques liés aux Systèmes d'Information.

Ce référentiel utilisable aussi bien par les manager qu'aux utilisateurs permet de faire des liens entre les risques métiers, les mesures de contrôle et les questions techniques relatives aux SI. Ce référentiel orienté processus permet aux utilisateurs d'obtenir des informations pour des processus qui les intéressent

Le référentiel COBIT est divisé en cinq parties :

- Une synthèse des concepts et principes du référentiel. Elle présente les objectifs et processus de la démarche. C'est un balayage général de la méthode.
- Un cadre de référence qui se décline en quatre domaines et qui présente pour chacun d'eux, les objectifs de contrôle :
- Planification & Organisation
- Acquisition & Mise en place
- Distribution & Support
- Surveillance
- Un guide d'audit qui permet d'une part d'évaluer les vulnérabilités et les risques correspondant aux objectifs de

contrôle et d'autre part, de mettre en place des actions correctrices.

- Le guide de management fournit les indicateurs clefs de succès du management. Il donne aussi une modélisation de la maturité, grâce à une évaluation des objectifs à atteindre.
- Les outils de mise en œuvre. Il d'agit d'outils permettant d'analyser la sensibilisation au management, et de diagnostiquer les contrôles informatiques.

Pour plus de renseignements voir le site de l'ISACA: *www.isaca.org/cobit/*

Le CIGREF, Club Informatique des Grandes Entreprises Françaises, est une association d'entreprises. Sa mission est de promouvoir l'usage des systèmes d'information comme facteur de création de valeur et source d'innovation pour l'entreprise.

Le CIGREF regroupe des grandes entreprises de tous secteurs (assurance, banque, distribution, énergie, industrie, services, services sociaux et santé et transport).

Le CIGREF favorise le partage d'expériences et l'émergence des meilleures pratiques. C'est un interlocuteur des pouvoirs publics français et européens sur les domaines des technologies de l'information.

Le CIGREF fait valoir les attentes légitimes des grands utilisateurs d'informatique et de télécommunications. Les thématiques d'échanges du CIGREF sont *le SI au service des métiers de la DG*, *la performance durable du SI* et le *management de la fonction SI*.

CIGREF
21, avenue de Messine
75008 Paris

Tél. 01 56 59 70 00
Fax 01 56 59 70 01

E-mail : cigref@cigref.fr
www.cigref.fr