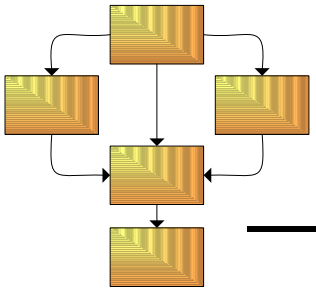

Club EBIOS

La gestion des risques

Analyse des pratiques dans différents secteurs

Date	:	18 novembre 2008
Statut	:	Approuvé
Nombre de pages	:	37
Responsable des travaux	:	Nicolas MAYER
Validation	:	Cercle opérationnel concerné
Approbation	:	Cercle stratégique

Club EBIOS, 72 avenue Gaston Boissier, 78220 VIROFLAY

Ce document a été réalisé par le Club EBIOS

Responsables des travaux :

- Nicolas MAYER

Contributeurs :

- Jean-Luc ALLARD
- Cyril DEMONCEAUX
- Emmanuelle DIOLOT
- FRANCE TÉLÉCOM (Paul RICHY)
- Matthieu GRALL
- Jean-Louis FLEISCH
- Serge LEBEL
- Gérard MOLINES
- Cyril MOURLON
- RATP (Jean CAIRE)

Participants invités :

- Didier CHARPIAT
- Sébastien POGGI
- Didier SEVRIN

Les commentaires et suggestions sont encouragés et peuvent être adressés à l'adresse suivante (voir formulaire de recueil de commentaires en fin de document) :

Club EBIOS
72 avenue Gaston Boissier
78220 VIROFLAY

contact[at]club-ebios.org

Table des matières

Introduction

La notion de gestion des risques

Le concept de gestion des risques (ou *risk management*) a fait son apparition à la fin des années 50 aux États-Unis dans le secteur financier, en relation avec des questions d'assurance [Dubois 1996]. La gestion des risques a donc longtemps été considérée comme la dimension probabiliste d'une perte financière au regard de la question d'assurance. Par la suite, la notion de gestion des risques a été étendue à d'autres secteurs, citons notamment l'environnement, la gestion de projet, le marketing, ainsi que la sécurité informatique (ou plus généralement des systèmes d'information) dans lequel se cadre [EBIOS]. L'objectif de ce document est de présenter des secteurs autres que celui de la sécurité des systèmes d'information dans lesquels on pratique la gestion des risques, afin d'en obtenir une vision plus générale.

L'organisation internationale de normalisation (ISO) s'est attachée à définir la gestion des risques de manière générale et applicable à tous les secteurs, en particulier au sein de l'[ISO Guide 73]. Le risque y est défini comme la "combinaison de la probabilité d'un événement et de ses conséquences". La gestion du risque est quant à elle identifiée comme l'ensemble des "activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque".

Dans la suite de ce document nous allons nous attacher à dépasser ces définitions très générales et investiguer dans plusieurs secteurs pratiquant la gestion des risques, afin de rechercher les points de convergence et de divergence entre les différentes pratiques et plus particulièrement les caractéristiques propres de la gestion des risques de sécurité des systèmes d'information (SSI) vis-à-vis des autres secteurs.

Un instrument essentiel dans la prise de décision…

Si la gestion des risques est un outil indispensable pour le secteur financier sur lequel repose une partie du modèle économique de ce secteur (risques de crédit, couverture d'assurance, performances boursières…), son institutionnalisation à d'autres secteurs a permis de rationaliser la prise de décisions. La fonction de gestionnaire de risque (*risk manager*) a suivi cette même évolution. Principalement dédié aux risques financiers, elle tend désormais à intégrer d'autres secteurs afin de fournir à la direction, à qui elle reporte directement, une vue globale pour guider la stratégie de l'entreprise. De ce fait, le *risk manager* a besoin de comprendre et de s'adapter aux différents secteurs qu'il est censé couvrir. Un cadre commun lui alors est nécessaire pour lui permettre de dialoguer avec les experts de la gestion des risques d'un secteur particulier.

… mais géré différemment dans les secteurs qui l'utilisent

Ce document vous présente les secteurs où la gestion des risques joue un rôle majeur afin d'en éclairer les ressemblances et les dissemblances. La gestion des risques n'est pas réservée à l'informatique mais concerne un nombre croissant de secteurs qui réfléchissent à leurs stratégies de survie et d'expansion. L'actualité aidant, la gestion des risques pénètre ainsi les esprits et élargit son champ d'activité, nous détaillerons donc les secteurs suivants :

- la sécurité des systèmes d'information ;
- la sûreté de fonctionnement ;
- l'environnement ;
- la gestion de projet ;
- les risques professionnels ;
- les risques juridiques ;
- les risques financiers.

On identifie un secteur cohérent comme un champ d'activités remplissant une ou plusieurs des caractéristiques suivantes :

- Un système spécifique au secteur
  (ex : système d'information pour la SSI, écosystème pour l'environnement…)
- Des risques spécifiques
  (ex : risque de dépassement de ressources ou de délai dans un projet)
- Un nombre conséquent de méthodes et d'outils dédiés

Certains secteurs, tels que celui des risques opérationnels (notamment dans le cadre de Bâle II), constituent une agrégation d'autres secteurs.

Ce document retient donc une approche dissociative entre les secteurs cohérents et les cas d'agrégations de secteurs.

Prenons l'exemple des accords règlementaires Bâle II. Ce règlement vise la gestion des risques opérationnels. Or la gestion des risques opérationnels ne se cantonne pas un secteur particulier mais regroupe un ensemble de secteurs : informatique, finance, gestion de projet… qui sont regroupés au sein d'un même concept. Bâle 2 hérite donc d'une part des concepts liés à chacun de ces secteurs, ainsi qu'un certain nombre, plus limité, qui lui sont spécifiques.

En agissant ainsi, il est inutile de réinventer des outils déjà présents dans d'autres sphères. Il faut cependant bien comprendre que la frontière entre plusieurs secteurs de risques peut être tenue et ne constitue qu'une vue de l'esprit. Finalement les risques des uns ne s'arrêtent pas précisément là où commencent ceux des autres !

1 Analyse des pratiques dans différents secteurs

Cette partie présente le résultat de l'étude des pratiques de gestion des risques dans différents secteurs (sécurité des systèmes d'information, finances, gestion de projets…), ainsi qu'une synthèse des points communs et spécificités de ces approches.

Les secteurs étudiés ci-après ont été mis en évidence du fait de la spécificité des concepts qu'ils manipulent, du sujet sur lequel ils portent, des risques et de leur gestion, ou bien des méthodes et outils dédiés.

Les résultats de l'étude de chaque secteur sont tous présentés sous la forme suivante :

- la délimitation du secteur ;
- la description du concept de risque dans le secteur, avec une décomposition basée sur l'[ISO Guide 73] en événement, incertitude et conséquences ;
- l'usage de la gestion des risques dans le secteur ;
- la manière dont est mis en œuvre le processus de gestion des risques dans le secteur, avec une décomposition basée sur l'[ISO Guide 73] :
  - l'établissement du contexte : les éléments recueillis pour décrire le sujet d'étude ;
  - l'appréciation des risques : la mise en évidence des risques et l'estimation de leur importance ;
  - le traitement des risques : la sélection et la mise en œuvre de mesures visant un refus (évitement de la situation à risque), une optimisation (réduction ou augmentation), un transfert (vers des tiers) ou une prise de risque ;
  - l'acceptation des risques : la décision d'accepter formellement les choix effectués lors du traitement des risques ;
  - la communication relative aux risques : l'échange ou le partage d'informations concernant les risques ;
  - le contrôle et le suivi : la vérification de la mise en œuvre des mesures et la collecte des éléments utiles à l'amélioration ;
  - l'amélioration : la prise en compte des éléments collectés pour tenir à jour et améliorer le processus.
- les références, méthodes et outils utilisables.

1.1 La sécurité des systèmes d'information (SSI)

1.1.1 Délimitation du secteur de la SSI

La sécurité des systèmes d'information (SSI) vise à protéger les éléments essentiels (biens du patrimoine informationnel : les informations et les processus les utilisant) contre toute atteinte de leurs besoins de sécurité (disponibilité, intégrité, confidentialité…), qu'elle soit accidentelle ou délibérée. De ce fait, la SSI est bien distincte voire assujettie aux autres risques relatifs aux SI, que l'on pourrait qualifier de stratégiques, tels que la politique de maintenance, l'installation d'un nouveau logiciel, l'organisation du *workflow*…

Ces éléments essentiels reposent sur des systèmes d'information (SI), organisés pour accomplir des fonctions de traitement d'information (processus métiers), et composés d'entités techniques (logiciels, matériels, supports, réseaux, téléphonie…) et d'entités non techniques (organisations, lieux, personnes…).

1.1.2 Le risque dans le secteur de la SSI

La terminologie et le niveau de détail des descriptions de risques SSI varient selon la méthode employée. Mais les concepts restent globalement les mêmes.

1.1.2.1 L'événement

L'événement considéré en SSI est un scénario (souvent appelé menace) décrivant si possible :

- l'élément menaçant, à l'origine de la menace, généralement humain ou naturel, agissant de manière fortuite ou délibérée, comme un pirate informatique, un employé, un concurrent, une forêt inflammable, une rivière à proximité… ; son potentiel peut être estimé (selon par exemple sa motivation, ses compétences et ses ressources) ;
- l'incident ou le sinistre (souvent appelé méthode d'attaque) comme un incendie, une crue, un vol de matériel, une divulgation, un piégeage de logiciels… ; sa plausibilité ou sa fréquence est parfois estimée ;
- les vulnérabilités des entités, exploitables par l'élément menaçant pour réaliser l'incident ou le sinistre ; leur importance peut être estimée.

1.1.2.2 L'incertitude

En SSI, l'incertitude de l'événement représente l'estimation de la possibilité de réalisation de la menace (essentiellement en fonction de la plausibilité de l'incident ou du sinistre et de l'importance des vulnérabilités). Elle peut être appelée opportunité, faisabilité, fréquence…

1.1.2.3 Les conséquences

Les conséquences dans le secteur de la SSI n'évoquent que les aspects négatifs.
Ces pertes (ou impacts) décrivent généralement :

- l'atteinte des besoins de sécurité (disponibilité, intégrité, confidentialité…) des éléments essentiels ; ils sont exprimés selon des échelles de besoins ;
- les impacts sur l'organisme (interruptions de service, pertes d'image de marque, infractions aux lois, pertes financières …) ; ils peuvent être quantifiés ou évalués selon une échelle.

1.1.3 L'usage de la gestion des risques dans le secteur de la SSI

La gestion des risques SSI peut être considérée comme un support à la gestion globale de la SSI. Elle est employée pour des SI en conception et pour des SI existants, ponctuellement, régulièrement ou systématiquement selon le niveau de maturité des organismes.
De plus en plus d'organismes du secteur public et du secteur privé imposent la réalisation d'études de risques SSI à la création de nouveaux SI.
En France, la réglementation ([IGI 1300]) oblige à étudier les risques de tout système traitant des informations classifiées de défense.
Par ailleurs, quatre des neuf principes des lignes directrices de l'OCDE relatives à la SSI ([OCDE]) concernent la gestion des risques SSI.

1.1.4 Le processus de gestion des risques SSI

1.1.4.1 L'établissement du contexte

Dans le secteur de la SSI, L'établissement du contexte a pour but de délimiter et décrire le périmètre sur lequel la gestion des risques va porter, de garantir une approche systémique (métier - SSI) et de recueillir les éléments qui permettront d'adapter le traitement des risques au contexte particulier.
Le périmètre peut être physique (locaux, bâtiments) ou fonctionnel (applications particulières, domaines de responsabilités…) du fait de la nature impalpable de l'information.

Elle consiste, quand elle est réalisée, à décrire au minimum l'organisme, les enjeux liés au SI étudié, les informations ou processus à protéger, les entités sur lesquelles elles reposent et les contraintes à prendre en compte (notamment les références légales et réglementaires applicables).

Cette phase est principalement réalisée avec des décideurs et des acteurs métiers (maîtrises d'ouvrage quand le SI est à concevoir ou responsables métiers quand le SI existe déjà).

1.1.4.2 L'appréciation des risques

L'analyse des risques SSI consiste à mettre en évidence les risques SSI. Généralement, elle se fait soit par construction des risques (approches exhaustives), soit par ajustement de scénarios de risques (approche génériques), soit de manière informelle (approches par l'expérience).
Les mesures de sécurité existantes peuvent être prises en compte dans l'étude des vulnérabilités.

En ce qui concerne l'évaluation des risques, les éléments quantitatifs (évalués précisément ou via des échelles) permettent de hiérarchiser les risques (généralement en fonction de l'opportunité des menaces et des pertes). Des calculs sont parfois effectués pour les positionner les uns par rapport aux autres (sachant que ces calculs n'ont aucune valeur scientifique…).
Bien qu'elles puissent être quantitatives, l'évaluation est plus souvent réalisée qualitativement ou à l'aide d'échelles permettant de positionner les éléments les uns par rapport aux autres.

Cette phase est principalement réalisée en interaction avec des acteurs métiers (maîtrises d'ouvrage, utilisateurs, responsables d'activités ou équivalents) et des acteurs supports (maîtrises d'œuvre ou équivalents).

1.1.4.3 Le traitement des risques

Le traitement des risques SSI débute par une phase de planification, qui consiste à choisir entre :

- refuser les risques (éviter la situation à risque) ;
- réduire les risques et spécifier (à l'aide d'objectifs et/ou d'exigences de sécurité) les mesures de sécurité à mettre en œuvre ; ces mesures peuvent :
  - porter sur :
    - les éléments menaçants,
    - les vulnérabilités,
    - les besoins de sécurité,
    - l'impact ;
  - et concerner :
    - la dissuasion,
    - la prévention,
    - la détection,
    - la réaction,
    - la récupération…
- transférer les risques (vers des tiers) ;
- prendre les risques.

Cette planification est faite en tenant compte des caractéristiques du contexte et en confrontant l'impact (financier, organisationnel…) des mesures au bénéfice attendu (effet sur les risques).
Elle peut également intégrer les mesures de sécurité existantes.

Le traitement des risques SSI se poursuit par une phase de mise en œuvre des mesures spécifiées.

Les risques résiduels, subsistant après le traitement des risques SSI, sont mis en évidence.

Cette phase est principalement réalisée en interaction avec des acteurs métiers (maîtrises d'ouvrage, utilisateurs, responsables d'activités ou équivalents), des acteurs supports (maîtrises d'œuvre ou équivalents) et des acteurs représentatifs des secteurs impactés par les mesures de sécurité (ressources humaines, finances, juridique…).

1.1.4.4 L'acceptation des risques

L'acceptation des risques SSI est appelée homologation de sécurité. Elle représente la décision d'accepter formellement les choix effectués lors du traitement des risques SSI et les risques résiduels. Elle est prononcée au vu d'un dossier à définir et peut être refusée, provisoire ou définitive.

L'homologation de sécurité est prononcée par une autorité désignée, qui peut s'appuyer sur une commission d'homologation, qui lui fournit les éléments nécessaires à la prise de décision.

1.1.4.5 La communication relative aux risques

La communication relative aux risques SSI représente l'échange ou le partage d'informations concernant les risques. Elle est adaptée à l'objectif et à la cible de communication et permet :

- d'obtenir les éléments nécessaires :
  - à l'établissement du contexte (descriptions, enjeux, contraintes…),
  - à l'appréciation des risques (besoins, vulnérabilités…) ;
- d'échanger les éléments nécessaires au traitement des risques (choix de la stratégie de traitement, "négociation" des mesures…) ;
- de fournir les éléments nécessaires :
  - à l'acceptation des risques (dossier de sécurité, risques résiduels…),
  - au contrôle et au suivi (mise en œuvre des mesures de sécurité, évolutions du SI…),
  - à l'amélioration (état des lieux…).

Elle implique à différents moments tous les acteurs des autres phases.

1.1.4.6 Le contrôle et le suivi

L'effectivité et l'efficacité des mesures de sécurité sont évaluées (vérifications de conformité, audits, inspections, contrôles hiérarchiques, auto-évaluations…).
Par ailleurs, les évolutions du contexte ou du SI sont relevées (éléments essentiels, entités, besoins de sécurité, éléments menaçants…) car elles sont susceptibles de faire évoluer les risques.
Cette phase est principalement réalisée par les personnes en charge de la SSI.

1.1.4.7 L'amélioration

Cette ultime phase vise l'amélioration de la démarche (adaptation du budget et des ressources humaines par exemple) et des mesures par l'identification des problèmes/solutions amenés au cours de la phase précédente.
Cette phase est principalement réalisée par les personnes en charge de la SSI.

1.1.5 Références, méthodes et outils

Il existe de nombreuses approches méthodologiques contribuant à la gestion des risques SSI ([EBIOS], [OCTAVE], [CRAMM] …). Ces démarches peuvent être concurrentes, complémentaires, d'un niveau de détail plus ou moins important, spécifiques à un secteur d'application (santé, défense…), avec des résultats particuliers, plus ou moins outillées, gratuites ou payantes, plus ou moins reconnue…
L'[ISO 27005], en cours de finalisation, décrit les invariants de la gestion des risques SSI.

1.2 La gestion de projets[1]

1.2.1 Délimitation du secteur de la gestion de projet

La norme [ISO 8402] définit un projet comme un "processus unique, qui consiste en un ensemble d'activités coordonnées et maîtrisées comportant des dates de début et de fin, entrepris dans le but d'atteindre un objectif conforme à des exigences spécifiques telles que les contraintes de délais, de coûts et de ressources". Le management de projet comprend la planification, l'organisation, le suivi de la progression et la maîtrise de tous les aspects du projet dans un processus continu, afin d'atteindre ses objectifs.

1.2.2 Le risque dans le secteur de la gestion de projet

La gestion des risques de projet est une démarche faisant partie intégrante du secteur de la gestion de projets. Elle traite des incertitudes tout au long du projet et est présente au sein des principales méthodes de gestion de projet. Les risques sont définis comme la possibilité qu'un projet ne s'exécute pas conformément aux prévisions de dates, de coût ou d'expression des besoins. Le risque en gestion de projet est constitué de deux éléments : la probabilité d'apparition du risque (caractéristique de la cause du risque) et l'impact du risque qui détermine sa conséquence.

1.2.3 L'usage de la gestion des risques dans le secteur de la gestion de projet

Maîtriser les risques est une préoccupation majeure en conduite de projet. Les finalités principales que l'on retrouve dans la gestion des risques d'un projet [Courtot 1998] sont :

- améliorer la pertinence de la définition des objectifs du projet (en termes de coûts, de délais et de spécifications), grâce à l'accroissement et à l'amélioration de la qualité des informations recueillies ;
- accroître les chances de réussite du projet grâce à une meilleure compréhension et identification des risques encourus, une meilleure définition des actions à entreprendre pour s'en prémunir, mais également grâce à un pilotage plus réactif et sensible aux évolutions de son environnement ;
- contribuer à l'amélioration de la communication entre les différents acteurs du projet sur les différentes décisions à prendre.

À noter que la gestion des risques de projet permet d'obtenir des informations utiles à la fois pour la maîtrise d'ouvrage et la maîtrise d'œuvre d'un projet.

La gestion des risques de projet consiste à:

- recenser les risques qui pourraient faire qu'un projet ne s'exécute pas conformément aux prévisions de date d'achèvement, de coût ou de spécifications ;
- préparer des actions correctives ou préventives ;
- exécuter et suivre les actions et les indicateurs de risques.

1.2.4 Le processus de gestion des risques de projet

1.2.4.1 L'établissement du contexte

On remarque ici particulièrement l'absence d'une étape spécifique d'identification du contexte et de définition des frontières de l'étude, au contraire du secteur des SI où elle a une part prépondérante. Il faut toutefois noter que cette démarche est toujours effectuée dans le cadre général d'un projet et des activités de gestion de projet qui l'entourent. On considère donc que cette information est toujours disponible pour le gestionnaire de risques. On évoque simplement dans certaines méthodes [PMBOK] une phase préparatoire de "*Planning*".

[1] Notamment d'après [ADELI].

1.2.4.2 L'appréciation des risques

La phase d'appréciation des risques est composée de 2 étapes de la démarche classique de gestion des risques de projet : l'identification des risques et l'évaluation des risques.

L'identification des risques, qui est le préalable à toute démarche de gestion des risques de projet, consiste à répertorier, de manière la plus exhaustive possible, tous les événements générateurs de risques (sources du risque) pour le projet et pouvant conduire au non respect de ses objectifs.
Une fois cette identification réalisée, il convient d'analyser, de manière plus ou moins détaillée, leurs causes et leurs incidences potentielles, en prenant en compte les interactions et combinaisons éventuelles. Une catégorisation des risques peut être réalisée, sur base de leur cause (causes techniques, politiques, organisationnelles…), afin de définir des traitements adaptés à chaque risque.

L'évaluation des risques va quant à elle s'appuyer sur une analyse quantitative pour mieux appréhender et estimer les impacts sur les coûts, les délais et/ou les spécifications techniques du projet. Cette quantification permet en premier lieu de repérer parmi les risques identifiés ceux qui sont négligeables et qui ne présentent pas de risque réel vis-à-vis de l'organisation étudiée.
Lors de cette étape va être évaluée, dans la mesure du possible, la probabilité d'apparition de chaque risque recensé et à estimer la gravité de leurs conséquences directes et indirectes sur les objectifs du projet. Il va ainsi être possible de hiérarchiser les risques, afin de se focaliser sur les risques prépondérants, de préparer les parades les plus efficaces possibles et de définir les actions à mener en priorité pour les maîtriser.

1.2.4.3 Le traitement des risques

Le traitement des risques est l'étape qui va définir et mettre en œuvre des mesures appropriées pour diminuer les risques et les ramener à un niveau acceptable au vu du projet. Cinq possibilités classiques existent :

- suppression de la cause du risque ;
- transfert du risque (partage de la responsabilité ou du coût du risque) ;
- réduction de sa criticité (en réduisant sa probabilité d'apparition ou la gravité de ses conséquences) ;
- accepter le risque tout en le surveillant ;
- planifier et organiser des actions qui seront lancées en cas d'apparition du risque ou contingence.

1.2.4.4 L'acceptation des risques

Aucune phase spécifique d'acceptation des risques n'est généralement déroulée lors d'une démarche de gestion des risques de projet, celle-ci étant réalisée en fin de traitement des risques.

1.2.4.5 La communication relative aux risques

Il n'y a pas de recommandations spécifiques de communication relative aux risques. A l'image de l'étape d'étude du contexte, la communication des risques est encapsulée au sein de la communication relative au projet dans son ensemble.

1.2.4.6 Le contrôle et le suivi

Le suivi et le contrôle des risques doivent être effectués régulièrement afin de détecter les modifications au sein du panel de risques analysés, certains risques pouvant disparaître, d'autres apparaître ou d'autres encore, considérés initialement comme faibles, pouvant devenir rapidement inacceptables pour l'entreprise dès lors qu'ils n'ont pu être maîtrisés. Une mise à jour de la liste de risques et de leur caractéristique est donc réalisée.

1.2.4.7 L'amélioration

Généralement lors de la phase de clôture du projet, la capitalisation des risques permet de documenter le savoir-faire et les expériences acquises sur les risques associés au projet. Cette étape a pour objectif l'amélioration l'ensemble du processus de gestion des risques dans le cadre d'un autre projet. Les données utiles devront donc être recensées et conservées tout au long du projet, puis formalisées lors de la phase de clôture du projet.

1.2.5 Références, méthodes et outils

Plusieurs techniques existent et peuvent être combinées pour identifier les risques projets : l'analyse de la documentation existante, l'interview d'experts, la réalisation de réunions de brainstorming, l'utilisation d'approches méthodologiques (comme l'[AMDEC], l'analyse préliminaire des risques – APR, les arbres de causes…), la consultation de bases de données de risques rencontrés lors de projets antérieurs ou encore l'utilisation de check-lists ou de questionnaires préétablis et couvrant les différents domaines du projet.

De nombreuses méthodes de gestion de projet, intégrant une partie de gestion des risques de projet, sont disponibles. On peut citer [PMBOK], [PRINCE2] ou [HERMES] comme faisant partie des plus utilisées sur le marché. On peut également citer la norme [ISO 10006] qui a pour vocation de donner des conseils sur le "management de la qualité dans les projets" et dont une section traite des processus relatifs aux risques.

1.2.6 Remarques sur le secteur

De même, il est intéressant de noter l'effort important qui suit le traitement du risque : le suivi des risques ainsi que la capitalisation du risque. Ce qui ressort de ce constat est, très certainement, une très grande variabilité des risques, en termes de déclanchement et de niveau, pour un type de risque donné, qui entraîne un fort besoin de suivi et de contrôle, ainsi qu'un gros effort basé sur la réutilisabilité d'une démarche de gestion des risques pour d'autres projets, lié à la capitalisation lors de la clôture du projet. Pour les étapes de 1 à 3, leur contenu est classique et comparable à ce qui se fait dans les autres secteurs. Les éléments essentiels qu'on retrouve sont les deux types d'analyse des risques (qualitative ou quantitative), la matrice des risques, ainsi que les quatre types de traitement des risques (voir ci-dessous).

Dans le cadre de la gestion de projet, les objectifs à atteindre lors d'une démarche de gestion des risques se déclinent en termes de coût, de délais et de qualité, en lien avec les objectifs généraux du projet qui caractérisent un produit ou un service.

Au niveau du traitement du risque, les quatre cas classiques de traitement du risque : acceptation, contrôle (préventifs ou sur la cause, correctifs ou sur la conséquence [PMBOK]), transfert et évitement sont envisageables. Ses traitements agissent sur les éléments "tangibles" du projet que nous appelons les ressources du projet et qui sont par exemple les ressources humaines, le budget ou le produit du projet.

La norme [ISO 10006], relative à la gestion de la qualité dans les projets, recommande, lors d'une démarche de gestion des risques de projet, de tenir compte également d'autres risques sortant du contexte propre de la gestion de projet, tels les risques relatifs à la sécurité, à la santé ou à la sûreté de fonctionnement.

1.3 L'environnement

1.3.1 Délimitation des secteurs de l'environnement

La conscience de tous envers la nécessité de respecter l'environnement à conduit les entreprises à pousser la gestion des risques de production au-delà des aspects immédiats de santé et de sécurité vers les conséquences sur le long terme pour l'environnement (voir [Bradbury 2004], [Callow 2003]).

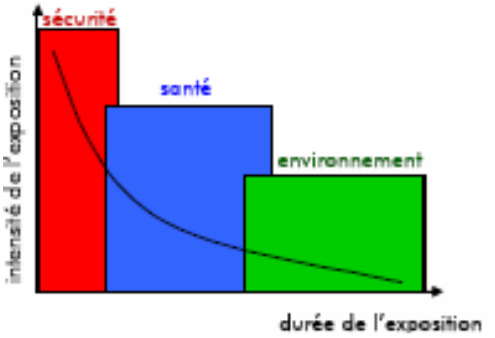

Figure 1 - Le glissement des secteurs de gestion des risques

Cette prise de conscience n'est pas seulement le résultat de pressions règlementaires mais également du marché financier où l'on constate que la considération de l'environnement est un argument supplémentaire pour attirer de nouveaux actionnaires. Les entreprises qui ont ainsi développé une démarche environnementale qui les ont amenés par exemple à une certification [ISO 14001] affichent clairement cet avantage concurrentiel.

L'[ISO 14001] est apparu historiquement comme le premier système de management intégré, avant l'[ISO 9001] et l'[ISO 27001]. Ce système de management a ainsi posé depuis de nombreuses années le processus de gestion des risques environnementaux.

1.3.2 Le risque dans le secteur de l'environnement

Un risque environnemental est composé de la notion d'aspect et d'impact ;

- l'aspect est la cause de l'impact : "Élément d'une activité d'un organisme susceptible d'interactions avec l'environnement"
- l'impact est la conséquence sur l'environnement : "Toute modification de l'environnement, négative ou bénéfique, résultant des activités d'un organisme"

Exemple :

Activité	Aspects		Impacts	
Transport de matières dangereuses	1. Consommation d'essence	=>	1. Épuisement des ressources naturelles	-
	2. Émissions sonores		2. Nuisances sonores	-
	3. Utilisation du chemin de fer		3.Diminution du transport par route => Diminution de la pollution atmosphérique	+

1.3.3 L'usage dans le secteur de l'environnement

L'usage de la gestion des risques dans l'environnement est principalement utilisée afin d'afficher et de prouver les valeurs éthiques d'une organisation. La certification à l'[ISO14001] fait figure aujourd'hui de référence pour ces organisations. Le schéma de management et d'audit environnemental ([EMAS]) suit la même philosophie volontaire, au contraire des entreprises de type SEVESO qui sont légalement obligées de recourir à la gestion des risques selon la directive du même nom.

La norme européenne [EMAS] est un outil de gestion de la performance environnementale. L'amélioration de cette performance passe par la mise en place d'un système de gestion environnemental similaire à celui proposé par l'[ISO 14001], la réalisation d'un audit environnemental et la publication des résultats environnementaux. L'obtention de la certification [EMAS] n'est pas une obligation légale, mais elle témoigne d'un véritable savoir-faire dans la gestion des risques environnementaux. Une certification [ISO 14001] préalable est un pas important mais non suffisant à l'obtention de cette certification.

La directive européenne [SEVESO], a été conçue pour définir une politique commune dans la gestion des risques des risques industriels. Elle fait suite à la catastrophe de l'usine intervenue dans la commune du même nom en 1976. La directive originelle a été remplacée par la directive [SEVESO] qui est en application depuis février 1999. Les sites de production classés à risques doivent respecter cette directive. L'usine AZF de Toulouse, qui a explosée en 2001, en fait partie.
Cette directive impose donc :

- l'inventaire des établissements à risque ;
- la mise en place de plans de prévention et d'urgence ;
- la synergie entre les exploitants pour éviter l'effet domino ;
- l'institution d'autorités de surveillance des établissements à risque.

L'éco-conception est quant à celle une démarche globale centrée sur le produit. Elle consiste à prendre en compte des critères environnementaux dès la phase de conception d'un produit. Ces critères concernent généralement l'ensemble des phases du cycle de vie du produit à savoir sa production, sa distribution, son utilisation et sa fin de vie. Il s'agit tout à la fois de mieux maîtriser les risques et les coûts liés au cycle de vie des produits, d'anticiper les attentes naissantes des donneurs d'ordre ou des consommateurs, favorables à une meilleure prise en compte de l'environnement ou encore de faire de l'environnement un facteur nouveau de dynamisation et de créativité lors des processus de création et de conception de produit. Toutes les entreprises qui peuvent agir directement ou indirectement sur la conception ou l'amélioration des produits sont concernées par l'éco-conception.

1.3.4 Le processus de gestion des risques environnementaux

1.3.4.1 L'établissement du contexte

La première étape vise à définir le périmètre sur lequel la gestion des risques va porter. Dans le cas de l'environnement ce périmètre peut être physique (locaux, bâtiments, chaîne de production) ou orienté flux (flux entrants et sortants), dépendant de la stratégie de gestion de l'entreprise.

1.3.4.2 L'appréciation des risques

La phase d'analyse environnementale est le cœur du processus de gestion des risques. La méthode [AMDEC] est très populaire pour la réalisation de cette phase. C'est une analyse globale, rationnelle, concertée et systématique de toutes les activités de l'entreprise des impacts environnementaux réels ou potentiels spécifiques à l'entreprise. Cette analyse doit prendre en compte le fonctionnement de l'organisme en marche normale ainsi qu'en marche dite incidentelle.

Au vu des résultats de l'analyse environnementale, l'organisation doit déterminer les impacts environnementaux significatifs qu'elle s'occupera de réduire.

1.3.4.3 Le traitement des risques

Pour les risques qu'elle souhaite contrôler elle-même, l'organisation va sélectionner des mesures de sécurité de nature technique et/ou organisationnelle. L'ensemble de ces mesures va constituer une politique environnementale ou un manuel environnemental qui devra être rédigé. Des plans d'actions sont également préparés afin de prévenir les risques car dans le secteur environnemental, encore plus qu'ailleurs, on préfère prévenir que guérir. Des plans d'actions dits "dormants" sont également rédigés pour traiter les éventuels incidents.

L'implémentation des contrôles constitue ensuite la phase de réduction des risques à proprement parler. Les contrôles sélectionnés sont déployés.

1.3.4.4 Communication

La communication a pour objectif de recueillir et de partager les informations relatives aux risques environnementaux entre les différentes parties prenantes. Il n'existe pas de spécificité particulière dans ce secteur.

1.3.4.5 Le contrôle et le suivi

L'effectivité et l'efficacité de la politique environnementale doivent être déterminées pour suivre l'évolution du profil des risques de l'entreprise. S'en suit un état des lieux qui nourrit la phase suivante.

1.3.4.6 L'amélioration

Cette ultime phase vise l'amélioration de la démarche (ex : adaptation du budget et des ressources humaines) et des contrôles (ex : relocalisation des machines de production) par l'identification des problèmes/solutions amenés au cours de la phase précédente.

1.3.5 Références, méthodes et outils

Les principaux outils sont l'AMDEC et l'écotoxicologie.

L'AMDEC a été développée par l'armée américaine vers la fin des années 40 en tant que technique d'évaluation de la fiabilité afin d'évaluer les effets des défaillances sur les systèmes et les équipements. Actuellement l'AMDEC est devenue une technique de base pour la maîtrise des risques environnementaux, car cette méthode simple permet d'évaluer rapidement et quantitativement les aspects et impacts significats :

$$C = F \times G \times E$$

F = Fréquence d'apparition / Probabilité d'occurrence
G = Gravité
E = Efficacité des moyens de prévention, de détection et de protection actuels
C = Criticité

Les valeurs de F, G et E sont fixées par une échelle qui est à déterminer en amont. En aval, on déterminera un seuil à partir duquel la criticité (C) rendra le traitement du risque environnemental nécessaire. Par ailleurs, la conformité règlementaire peut amener l'obligation de traiter certains impacts, en dehors de toute considération des résultats de l'analyse. La fixation de l'échelle peut également reposer sur des données écotoxicologiques, notamment en ce qui concerne la gravité.
On appelle écotoxicologie l'évaluation des risques chimiques pour les écosystèmes basée sur la relation entre les effets indésirables des substances chimiques et leurs niveaux de présence connus ou prédits dans l'environnement. L'écotoxicologie est là pour appuyer quantitativement l'analyse des risques environnementaux, c'est-à-dire fournir une base mathématique pour évaluer et gérer les effets potentiels des produits chimiques. Cette base statistique est typiquement basée sur les mesures de survie, de croissance et de reproduction d'espèces animales et végétales à ces produits. L'écotoxicologie joue donc une part importante pour la détermination des risques en apportant la preuve expérimentale que la concentration *x* d'un produit *y* peut avoir des effets néfastes sur un écosystème. L'analyse des risques écotoxicologiques revient à déterminer la concentration maximale des substances rejetées dans l'environnement sans qu'elle en affecte sa structure ou son fonctionnement : la PNEC (*Predicted No-Effect Concentration* / Concentration prédite sans effet). Cela peut se faire selon trois approches : l'approche par substance (qui fonctionne par identification des substances et détermination de leur degré de toxicité via des bases de connaissances), l'approche par matrice (qui repose sur une analyse comparative in vitro entre un échantillon contaminé et un échantillon non contaminé selon un scénario de référence) et l'approche *in situ* (qui repose sur un test en conditions réelles dans le milieu). [Thybaud 2005]

1.3.6 La réglementation dans l'environnement

La législation et la règlementation qui touchent à l'environnement et en particulier à l'écotoxicologie sont complexes et demandent un investissement important pour une organisation qui doit effectuer une veille juridique assez lourde pour déterminer quels sont les règlements qui s'appliquent à son cas. Il serait donc bien trop fastidieux de les énumérer toutes. Voici cependant quelques réglementations européennes importantes : [UE 67], [UE 156], [UE 271], [UE 676], [UE 793], [UE 1488].

1.4 La sûreté de fonctionnement

1.4.1 Délimitation du secteur de sûreté de fonctionnement

On définit généralement la sûreté de fonctionnement comme le secteur cherchant à réduire les risques ayant des causes accidentelles et pouvant nuire aux éléments du système à protéger, en particulier les êtres humains. Par analogie, la sécurité est définie comme le secteur cherchant à réduire les risques d'attaques ayant des causes malveillantes et pouvant nuire aux éléments du système à protéger (malgré la définition de la section 1.1 qui a inclus dans la SSI les menaces ayant des causes accidentelles). Pourtant, les méthodes et techniques liées à la sécurité de fonctionnement couvrent, de la même manière que les méthodes de SSI avec les risques à cause accidentelle, également certains risques en lien avec la sécurité, tout en gardant majoritairement comme cible les risques propres au secteur. Par conséquent, on trouve un recouvrement partiel entre la sûreté de fonctionnement et la SSI lorsqu'un SI est système cible. Notre attention se portera ici uniquement sur des méthodes dédiées à la sûreté de fonctionnement et applicable à tout type de système.

La sûreté de fonctionnement est un secteur qui touche tout type de système automatisé.
Dans chaque grand secteur industriel (aéronautique, espace, ferroviaire), il existe un ensemble de normes définissant les concepts, les principes, les méthodes et quelquefois aussi les techniques à appliquer pour garantir la sûreté de fonctionnement du système à développer. Ces normes peuvent être nationales ou internationales. Le monde militaire possède également ses propres normes.

1.4.2 Le risque dans le secteur de la sûreté de fonctionnement

Nota : le vocabulaire peut varier d'une norme à l'autre, néanmoins on retrouve – éventuellement sous des noms différents – les mêmes concepts.

L'événement considéré comme une atteinte à la sûreté de fonctionnement est appelé une défaillance. Cet événement intervient dès que le service fourni n'est plus délivré ou qu'il dévie du service correct attendu. Cet événement intervenant sur le comportement externe du système, l'événement interne causant la défaillance est appelé erreur. Il faut toutefois noter qu'une erreur peut être gérée et ne conduit donc pas forcément à une défaillance. La cause d'une erreur est appelée faute et une vulnérabilité est une faute interne au système. Une mauvaise interaction homme-machine est un exemple de faute externe, qu'une vulnérabilité du système peut faire aboutir à une erreur. A noter qu'on parle généralement de panne pour désigner l'état du système qui résulte d'une défaillance.

Les conséquences d'une défaillance sur le système sont caractérisées par le niveau de sévérité (encore appelée gravité) de la défaillance et les causes par la probabilité d'occurrence. Un exemple de mesure de la cause du risque est le taux de défaillance ou inverse du MTTF (*Mean Time To Failure*, temps moyen jusqu'à l'occurrence de la première défaillance). Les niveaux de gravité et les taux d'occurrence sont quantifiés, entraînant la quantification des niveaux de risque. Le risque est alors considéré comme le produit de la sévérité par la fréquence d'occurrence. Les niveaux de gravité et les taux d'occurrence sont quantifiés, entraînant la quantification des niveaux de risque.

La sécurité est alors définie comme l'absence de niveaux de risques inacceptable.

De plus, les normes définissent généralement un ensemble de méthodes et moyens dont la mise en œuvre garantit l'assurance que le produit ou système obtenu satisfera ses objectifs de sécurité. Le degré d'assurance est dans certaines normes européennes ([EN 61508], [EN 50126]…) quantifié par un ensemble discret de niveau d'intégrité de la sécurité. Ce concept est analogue aux niveaux d'assurance de l'[ISO 15408].

1.4.3 L'usage de la gestion des risques dans le secteur de la sûreté de fonctionnement

La gestion des risques de sûreté de fonctionnement est généralement entièrement insérée au sein du processus de conception d'un système, voire du cycle de vie complet d'un système, depuis sa définition jusqu'à sa dépose.

Ce processus doit permettre d'identifier les risques, les évaluer et déterminer ceux qui sont inacceptables (le seuil correspondant pouvant être défini dans la norme ou laissé à l'appréciation de l'Autorité d'exploitation du futur système). En général de tels systèmes font l'objet d'une homologation formelle, réglementaire, qui s'appuie sur la démonstration de l'atteinte du niveau de sécurité requis, c'est-à-dire la démonstration de l'absence des niveaux de risques inacceptables.

D'autre part, les normes ne sont pas rétroactives et ne peuvent pas s'appliquer a posteriori sur des systèmes qui n'ont pas été initialement développées selon les normes. Par contre, les évolutions font l'objet d'analyse et de vérifications particulières en fonction du niveau d'intégrité (c'est-à-dire le degré d'assurance) recherché.

1.4.4 Le processus de gestion des risques de sûreté de fonctionnement

1.4.4.1 L'établissement du contexte

L'établissement du contexte dans le secteur de la sûreté de fonctionnement s'effectue en deux temps. En premier lieu, une première phase de présentation des concepts est nécessaire, afin de développer un niveau suffisant de compréhension du système, nécessaire pour appréhender les phases ultérieures du processus. Cette étape laisse transparaître la diversité des systèmes pouvant être l'objet d'une telle étude.
Cette phase est suivie d'une phase de définition du système et des conditions d'application qui l'influencent. On y retrouve principalement les éléments permettant de caractériser le système (mission, frontières), notamment sous forme de contraintes et conditions qui s'appliquent (contraintes imposées par l'infrastructure existante, conditions d'exploitation, de maintenance). Lors de cette phase sera également délimité le champ d'analyse des situations dangereuses du système.

1.4.4.2 L'appréciation des risques

Lors de la phase d'appréciation des risques, appelée ici analyse des risques, on va tout d'abord identifier les situations dangereuses, puis évaluer et quantifier les conséquences de ces situations dangereuses, enfin identifier les évènements à la source de ces situations dangereuses.
Le niveau du risque sera ensuite déterminé. Un management des risques est ensuite mis en place, nécessitant de déterminer et de classer l'acceptabilité du risque associé à chaque situation dangereuse identifiée.
En général, la phase d'évaluation des conséquences d'une situation dangereuse repose sur une analyse inductive, tandis que la phase de recherche des événements initiateurs repose sur une analyse déductive.

1.4.4.3 Le traitement des risques

Une fois les risques analysés et évalués, les exigences du système sont déterminées au niveau fonctionnel, accompagnées de critères de démonstration et d'acceptation de ces exigences. Un programme de conduite des tâches est établi afin d'implémenter ces exigences dans les phases suivantes du processus. Ces exigences seront allouées aux sous-systèmes, aux composants et aux éléments externes au système. Les moyens de réduction du risque se divisent en techniques d'évitement des fautes et techniques de tolérance aux fautes.

1.4.4.4 L'acceptation des risques

Lors de la phase de validation et d'acceptation du système, on évalue et valide la conformité de l'ensemble combiné des sous-systèmes, des composants et des dispositifs externes de réduction des risques. Si cette évaluation se révèle positive, le système sera accepté en l'état.

1.4.4.5 La communication relative aux risques

La communication relative au risque est effectuée tout au long du processus de gestion des risques, au travers de livrables. Elle ne représente pas une étape spécifique du processus. Comme document support à la communication des risques, on peut citer par exemple le "registre des situations dangereuses", dans lequel est consigné l'ensemble des situations dangereuses, et qui est mis à jour régulièrement tout au long du processus, comme par exemple après le traitement et l'acceptation des risques où l'on va y intégrer les risques résiduels identifiés.
La communication repose aussi sur le dossier de sécurité final qui sert à l'homologation du système.

1.4.4.6 Le contrôle et le suivi

Le contrôle et le suivi des risques sont réalisés lors des phases d'exploitation et maintenance ainsi que de surveillance des performances du système. L'objectif est d'assurer la continuité de la conformité aux exigences de sûreté de fonctionnement définies sur le système tout au long du cycle de vie de ce dernier

1.4.4.7 L'amélioration

Une phase de modification et remise à niveau du système permet de maintenir à niveau les exigences déterminées. Il faut noter que l'[EN 50126] qui a servi, entre autres, de référence, présente d'autres phases, non représentées dans le cadre de la gestion des risques, car entrant uniquement dans le cycle de vie général du système qui est le sujet général de la norme. On y retrouve les phases de conception et réalisation, de fabrication, d'installation et de retrait du service et dépose.

1.4.5 Références, méthodes et outils

Les principales références utilisées dans le secteur sont les suivantes : [Avizienis], [Laprie], [Villemeur].

Les principales normes utilisées dans le secteur sont les suivantes : [EN 61508], [EN 50126], [EN 50129], [ECSS Hazard], [ECSS Safety], [IDS 56].

De nombreuses méthodes ont été développées pour conduire les analyses de risques et déterminer les moyens de réduction à mettre en œuvre. On peut notamment citer les suivantes :

- Analyse préliminaire des dangers : analyse de type inductif qui vise à identifier les dangers d'un système (ou d'une installation industrielle) ainsi que ces causes puis évaluer la gravité des conséquences liées à ces situations dangereuses. Ce type d'analyse est effectué lors de la définition du système, préalablement à la mise en œuvre d'autres méthodes. Cette technique née dans les années 60 est utilisée dans de nombreuses industries comme le nucléaire, l'aéronautique, le ferroviaire ou l'industrie chimique.
- Analyse de modes de défaillance, de leurs effets et de leur criticité (AMDEC) : analyse de type inductif qui consiste à évaluer les effets de chaque mode de défaillance des différents composants d'un système pour identifier les défaillances qui auront des effets importants. Une AMDEC est une analyse de modes de défaillance et de leurs effets (AMDE) quantifiée par une criticité. Une AMDE se divise en quatre phases successives pour un système donné :
  - définition des fonctions et des composants,
  - détermination des modes de défaillance des composants, identification de leurs causes,
  - analyse des effets des défaillances,
  - l'identification des mesures en place pour réduire la défaillance.

  L'AMDE, qui a vu le jour dans les années 60, est issue du monde aéronautique. C'est une méthode extrêmement employée et réglementaire dans plusieurs secteurs industriels.
- HAZOP : méthode inspirée des AMDE qui a été développée par l'industrie chimique dans les années 70 pour l'analyse des risques des systèmes thermohydrauliques. HAZOP utilise une liste de mot-guides ("pas de", "plus de", "moins de", "trop de") afin d'aider à l'identification exhaustive les différents types de dérives potentielles.
- Arbres de cause (arbres de défaillance) : méthode déductive qui vise à identifier les diverses combinaisons d'événement susceptibles d'entraîner un certain événement (qui est unique pour l'arbre), le résultat étant représenté sous la forme d'un arbre. L'analyse déductive est réalisée sur plusieurs niveaux jusqu'à l'obtention d'événements "de base". Le passage d'un niveau à son raffinement se fait par des opérateurs logiques, principalement le ET et le OU, bien que d'autres opérateurs soient possibles. Ceci permet ensuite de faire d'une part des calculs logiques sur les opérateurs afin de déterminer des "coupes minimales" d'autre par de procéder à des évaluations probabilistes.
  Cette méthode qui est issue des laboratoires Belle est considérée comme très efficace et beaucoup utilisée (nucléaire, aéronautique, spatial…).

De nombreuses autres méthodes sont également mises en œuvre. Il faut noter l'importance croissante des modèles probabilistes de fiabilité qui reposent sur des modélisations des systèmes et des événements de plus en plus sophistiquées.

1.5 La maîtrise des risques professionnels[2]

1.5.1 Délimitation du secteur des risques professionnels

La maîtrise des risques dits professionnels englobe tous les risques liés à la protection de la santé (intégrité physique et psychique) des salariés d'un établissement, y compris les salariés temporaires.

1.5.2 Le risque professionnel

1.5.2.1 L'événement

L'événement considéré dans le risque professionnel est sa cause. Par exemple, il peut s'agir de causes techniques (état des équipements, conformité…), organisationnelles (information aux risques, temps de travail, ergonomie…), managériales (consignes de l'encadrement, évaluation…) ou comportementales (respect des procédures, équipements de protection individuelle…).

1.5.2.2 L'incertitude

L'incertitude des risques professionnels est liée à leur fréquence (F) et à leur gravité (G). Il est même admis que le risque (R) peut être calculé ainsi :

$$R = F * G$$

La fréquence peut être calculée en fonction de la dangerosité (D) et du niveau de protection ou de prévention (P) : $F = D / P$.
La gravité peut être calculée en fonction du temps d'exposition (T) et du nombre de personnes exposées (N) : $G = T \times N$.

$$\text{Soit : } R = (D / P) * (T \times N)$$

1.5.2.3 Les conséquences

Les conséquences d'un risque professionnel sont des impacts uniquement négatifs qui peuvent être directs ou induits. Les impacts directs peuvent être des accidents du travail (AT) ou des maladies professionnelles (MP). Les impacts induits peuvent être économiques (coûts directs et indirects), juridiques (pour la personne physique et pour la personne morale), sociaux (actions des salariés ou des représentants du personnel, dégradation du climat social) ou sur l'image de marque (dégradation des relations internes et externes).

1.5.3 L'usage de la gestion des risques professionnels

L'[UE 391] a été déclinée en France dans la Loi [FR 1414], qui impose d'identifier et d'évaluer les risques professionnels, et de mettre en œuvre les actions appropriées (obligation de résultat). Le décret [FR 1016] impose de formaliser tous les ans le résultat de cette évaluation. La circulaire [FR DRT-6] précise que l'évaluation devrait être faite avec méthode, traçable et planifiée dans le cadre d'un processus d'amélioration continue.

La véritable gestion des risques professionnels par une obligation de résultat est relativement novatrice et requiert encore des évolutions culturelles et comportementales.

D'une part, elle répond aux exigences réglementaires, et d'autre part, elle répond à une obligation de performance contribuant à la satisfaction des clients, des salariés, des investisseurs et des partenaires..

1.5.4 Le processus de gestion des risques professionnels

D'une manière générale, il est souhaitable que la gestion des risques professionnels soit réalisée de manière interactive en interne (avec les bureaux d'études et des méthodes, les achats, les ressources humaines, le management de la qualité, le système d'information…) et en externe (avec les organismes d'État, les clients, les sous-traitants, les fournisseurs…).

[2] Essentiellement d'après l'ouvrage [Degobert 2004].

1.5.4.1 L'établissement du contexte

Un ensemble d'informations relatives au contexte particulier de l'organisme peut être recueilli afin d'améliorer la pertinence de l'appréciation des risques vis-à-vis de la culture de l'organisme, de sa réalité, de son environnement et de sa stratégie. L'organisme est également présenté de façon macroscopique (unités ou postes de travail) et/ou détaillée (établissements, bâtiments, ateliers, corps de métier). Les obligations réglementaires et normes en vigueur doivent être connues.

1.5.4.2 L'appréciation des risques

Une évaluation globale, macroscopique, peut être réalisée par unité ou poste de travail. L'évaluation des risques se fait alors de manière maximaliste. Elle peut ensuite être pondérée (par les volumes de salariés concernés) et raffinée (par établissements, bâtiments, ateliers, corps de métier…), surtout pour les organismes de taille importante.

Concernant l'analyse des risques professionnels, la recherche des causes peut être réalisée à l'aide d'un arbre des causes ("méthode des 5M" ou "diagramme d'Ishikawa" – Milieu, Matériel, Matières, Méthodes et Main d'œuvre, auxquels s'ajoute le Management) suivi d'une étude des causes techniques, organisationnelles, managériales et comportementales ("critères TOMC") ; les impacts pour les salariés et pour l'organisme sont également étudiés selon les axes économique, juridique, social et sur l'image de marque.

S'agissant de l'évaluation des risques professionnels, leur fréquence et leur gravité sont estimées en tenant compte des actions de prévention mises en œuvre. Le risque peut être la résultante de la multiplication de la fréquence et de la gravité. Il peut être pondéré par le dimensionnement des unités ou des postes de travail. Une cartographie par risque et par unité ou par poste de travail peut être réalisée en mettant en évidence l'évolution de la situation.

1.5.4.3 Le traitement des risques

Dans un premier temps, la politique de prévention doit faire l'objet d'un engagement de la Direction à s'impliquer dans la prévention des risques professionnels et de la définition d'objectifs (axes de progrès) régulièrement révisés. Par ailleurs, la gestion de la continuité et des crises doit systématiquement être traitée.

Dans un second temps, des actions sont déterminées. Ces actions diffèrent selon leur nature (solutions managériales, d'apprentissage, organisationnelles ou techniques), leur type (palliatives, curatives ou préventives), leur priorité (selon la priorité des projets sur lesquels elles portent et en se basant sur une décision, une démarche d'analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC), le *benchmarking*, la loi de PARETO ou le calcul de rentabilité) et leur terme (court, moyen ou long, selon les projets sur lesquels elles portent).
Les actions sont destinées à agir soit sur la fréquence (réduction du danger, augmentation du niveau de protection ou de prévention), soit sur la gravité (réduction du temps d'exposition ou du nombre de personnes exposées) des risques professionnels.

Le traitement des risques professionnels est réalisé de manière cohérente avec L'établissement du contexte. Il est généralement intégré dans le cadre d'un projet (avec une organisation, des responsabilités, un budget, des étapes et des livrables définis).

1.5.4.4 L'acceptation des risques

L'acceptation des risques professionnels est faite sur la base des phases précédentes après tests et éventuelles corrections.

1.5.4.5 La communication relative aux risques

La communication concerne essentiellement le lancement d'un projet de gestion des risques professionnels et ses résultats (par exemple à l'aide d'indicateurs), qui doivent être communiqués à l'ensemble du personnel (ex : durée depuis le dernier accident). Elle intègre également les échanges nécessaires aux autres phases de la gestion des risques professionnels.

La communication relative aux risques professionnels est un facteur essentiel de réussite pour induire des changements de comportements de façon durable (motiver les acteurs, légitimer les décideurs…).

1.5.4.6 Le contrôle et le suivi

Les contrôles peuvent être des audits, des évaluations par unité ou poste de travail, des contrôles quotidiens, des inspections inopinées ou des observations croisées.

Le suivi des opérations doit faire l'objet d'une traçabilité rigoureuse, utile sur le plan juridique et au bon fonctionnement de l'ensemble de la démarche. Ce suivi est axé sur la performance.

1.5.4.7 L'amélioration

L'amélioration du processus de gestion des risques professionnels se base sur l'organisation (structures, fonctions…) et la gestion de la connaissance.
Le but est de mettre en œuvre un processus pérenne, en amélioration continue.

1.5.5 Références, méthodes et outils

Le référentiel le plus répandu pour la gestion des risques professionnels est la norme [OHSAS 18001] sur la gestion de la santé et de la sécurité au travail. Elle permet aux organismes de se faire certifier et est complétée par l'[OHSAS 18002], un guide décrivant sa mise en place. Il existe plusieurs outils d'assistance à la mise en œuvre de la gestion des risques professionnels, tels que PRAXISME® (société AD'APTUS), Objectif QSE© (société AQSE Conseil Formation), EVALURISQUE©…

1.6 La maîtrise des risques juridiques[3]

1.6.1 Délimitation du secteur des risques juridiques

Est ici considérée la gestion des risques juridiques au sein d'une organisation.

1.6.2 Le risque juridique

1.6.2.1 L'événement

Le risque juridique résulte de la conjonction d'un événement et d'une norme juridique (à caractère général – prescription légale telle que loi, règlement, jurisprudence… – ou relatif – obligation contractuelle telle que contrat, décision…).

La circonstance à l'origine du risque juridique peut être :

- une infraction pénale (crime, délit et contravention) ;
- une faute / un comportement transgressif intentionnel ou non intentionnel : acte positif contrevenant à une interdiction ou l'omission alors que la norme oblige à des actes positifs ;
- un dommage objectif, ne résultant pas d'un comportement transgressif ;
- une norme juridique nouvelle entraînant une obligation de changer ou une insécurité juridique (avant les premières décisions de jurisprudence ou de la Cour de cassation, permettant de fixer une interprétation) ;
- une évolution de la norme (nouveaux droits, nouvelles opportunités) ;
- l'exploitation d'une norme nouvelle ou existante pour faciliter l'atteinte des buts de l'organisation.

Cet événement dépend de l'organisation elle-même, notamment de son positionnement, et de son activité, pouvant engendrer des risques endogènes ou exogènes.

1.6.2.2 L'incertitude

La "qualification des risques juridiques" est basée sur des critères quantitatifs. La notion d'incertitude comprend en effet :

- la fréquence d'occurrence des risques (basée sur des calculs statistiques réalisés après observation sur une durée déterminée, pouvant être représentée en mois, mais cette approche est contestable pour les actes transgressifs ou les normes nouvelles) ;
- leur gravité, reflétant l'importance de la réalisation d'un risque (pénal, condamnation financière ou médiatique, et susceptible de rendre totalement ou partiellement indisponible une ressource).

1.6.2.3 Les conséquences

Le risque juridique peut avoir des conséquences négatives :

- l'organisation peut se trouver en position de victime :
  - elle subit un préjudice du fait d'une inexécution contractuelle ;
  - elle est victime d'un délit civil ou d'une infraction pénale ;
  - elle est confrontée au changement de la norme juridique qui lui est applicable ;
- l'organisation et/ou ses agents peuvent se trouver en position de coupables et supporter des conséquences :
  - pénales : l'organisation en qualité de personne morale ou les dirigeants ou leurs délégataires en qualité de personne physique supportent une sanction pénale qui peut limiter les droits des personnes (peines privatives de liberté pour les personnes physiques, restriction des droits ou mesures pouvant menacer directement l'existence des personnes morales, ex : interdiction de soumissionner aux marchés publics), condamner à des amendes au coût financier prohibitif et à la publication du jugement aux frais de la personne condamnée ;

[3] Essentiellement d'après l'ouvrage [Verdun 2006].

- financières : dommages et intérêts à payer à la victime (difficilement évaluable car fixé par le juge sauf au cas où ils seraient contractualisés) ;
- d'image : contradiction d'un comportement transgressif de l'organisation avec sa communication ou condamnation judiciaire sur le fondement de la Convention européenne des droits de l'homme (pour une collectivité publique).

Il peut également avoir des conséquences positives (changement de la norme juridique ou exploitation d'une norme juridique favorable à l'organisation, dédommagement suite à un préjudice…).

1.6.3 L'usage de la gestion des risques juridiques

La gestion des risques juridiques prend tout son sens dans la complexité des organisations actuelles, qui oblige à considérer globalement ces risques afin d'appréhender de manière cohérente et pertinente le lien entre les personnes impliquées, les différentes ressources, les différentes normes juridiques applicables et les différents risques.

1.6.4 Le processus de gestion des risques juridiques

1.6.4.1 L'établissement du contexte

La phase d'étude du contexte de la gestion des risques juridiques doit mettre en évidence les buts et stratégies (marché, contraintes, objectifs stratégiques) de l'organisation.

Elle consiste également à identifier les ressources clés de l'organisation, indispensables à la réalisation de sa stratégie : capitalistiques (moyens matériels et immatériels pour acquérir d'autres ressources), financières, humaines, corporelles (meubles et immeubles), fournisseurs (biens ou services), partenaires (opérations communes), clients, environnementales (naturelles et artificielles), immatérielles (propriété intellectuelle, ressources informationnelles, ressources de notoriété).

Il convient enfin d'identifier les parties prenantes susceptibles d'être affectées ou de se sentir affectées par des risques, notamment les dirigeants et l'encadrement intermédiaire.

1.6.4.2 L'appréciation des risques

Analyser les risques juridiques consiste à :

- identifier les normes juridiques applicables aux ressources de l'organisation (obligations absolues, normes juridiques de portée générale ou relative, contrats innommés…) ; difficilement exhaustive, cette appréciation est généralement concentrée sur les normes juridiques applicables à l'organisation et usitées en son sein et celles relatives à la responsabilité sans faute (qui résulte, le cas échéant, d'obligations contractuelles de résultat) ;
- analyser le contexte juridique, selon la raison sociale, la domiciliation, l'activité et les ressources ;
- identifier les juridictions compétentes en fonction de la nature du risque juridique et de ses conséquences (compétence juridictionnelle et géographique) ;
- identifier les comportements transgressifs en étudiant les choix stratégiques de l'organisation, en analysant les décisions de justice rendues, en réalisant des audits et en étudiant les processus conduisant à ces comportements ;
- surveiller le droit en gestation (veille sur l'évolution des normes sensibles et stratégiques pour l'organisation, leurs auteurs, la jurisprudence, les réformes législatives nationales et européennes, les ordonnances, les programmes des partis politiques, la sensibilité de l'opinion publique) ;
- identifier les vulnérabilités et les mesures existantes.

Évaluer les risques juridiques consiste à déterminer les risques de nature à compromettre les stratégies et buts de l'organisation, et donc de nature à menacer sa pérennité. L'occurrence et les conséquences des risques seront donc étudiées. Cela permet notamment de faire émerger les risques qui peuvent atteindre les ressources clés et ceux les plus difficiles à traiter, qualifiés de risques majeurs ou stratégiques. Les responsables des risques juridiques doivent également être identifiés.

1.6.4.3 Le traitement des risques

Certains risques, liés notamment à des comportements transgressifs intentionnels, et dont l'organisation est consciemment à l'origine, sont refusés systématiquement : l'organisation doit faire en sorte de ne plus être en situation à risque (illégalité).

L'organisation optimise, transfère ou prend tout ou partie des risques négatifs qui lui sont imposés, qu'elle ne peut éviter par son activité (résultant d'un comportement transgressif non intentionnel ayant donné lieu à une sanction ou non, d'une responsabilité sans faute, ou d'une norme juridique nouvelle). Ces risques peuvent être traités de manière curative (termes d'une sanction, prescription, amnistie, transaction, réparation, assurance, optimisation…) ou préventive (amélioration des processus, sensibilisation, mise en place de mesures, assurance, lobbying), et en fonction du coût de traitement.

Une politique juridique peut être élaborée pour formaliser le traitement global du risque négatif et l'exploitation du risque juridique positif.

Les conséquences des risques juridiques résiduels (pris, partiellement réduits ou difficilement appréciables) doivent être financées par l'organisation par l'autofinancement (provision ou société captive) ou par recours à l'assurance quand cela est possible.

1.6.4.4 L'acceptation des risques

Cette phase doit être préparée par les personnes qui ont en charge la responsabilité des risques juridiques. En principe, l'acceptation des risques proprement dite doit être décidée en connaissance de cause par les dirigeants, ou ils doivent au moins en être dûment informés.

1.6.4.5 La communication relative aux risques

Les cibles de communication relative aux risques sont principalement les parties prenantes identifiées, qui seront responsables des conséquences de la réalisation de risques (pénalement ou civilement, directement ou par délégation).
La cartographie des risques constitue un outil de communication (mais aussi un outil de gestion des risques juridiques), le but étant de les rendre plus intelligibles et plus tangibles.
L'amélioration de la culture juridique des agents de l'organisation, indissociable de la prise en charge de responsabilités et de l'exercice du pouvoir, passe essentiellement par une implication de la direction (concrétisée par des codes de bonne conduite, des chartes, des politiques) et par une formation aux risques juridiques adaptée aux responsabilités des opérationnels.

1.6.4.6 Le contrôle et le suivi

Les risques juridiques doivent être anticipés et repérés à l'instar des autres types de risques.
C'est pourquoi, des contrôles réguliers des actes juridiques passés au sein de l'organisation (contrats cadre, contrat fournisseur, contrat de travail, règlement intérieur, obligations relatives à la Loi informatique et libertés…) doivent être mis en place. Le responsable des risques juridiques travaillera dans ce cadre en étroite collaboration avec l'équipe de juristes. Un contrôle de la conformité légale et réglementaire doit être mis en place. De même, un suivi de l'actualité juridique concernant l'organisation et son activité devra être conduit. Ce suivi, pour être efficace, devra être régulier. Il permettra à l'organisation de s'assurer qu'elle est en conformité avec les normes juridiques.

1.6.4.7 L'amélioration

Comme dans de nombreux autres secteurs, la partie amélioration du processus de gestion des risques est là pour mettre en place des actions correctives et palliatives suite à la veille continue.

1.6.5 Références, méthodes et outils

La gestion des risques dans le secteur juridique ne semble pas reposer sur des références formelles. Il ne semble pas non plus exister d'outillage particulier. Une connaissance extensive des textes de lois et une approche personnelle sont ici les meilleures armes du juriste. On remarque en effet qu'imaginer de prendre des risques juridiques n'est parfois jamais envisagé, au moins officiellement.

1.7 La maîtrise des risques financiers

1.7.1 Délimitation du secteur des risques financiers

Les risques financiers sont inhérents aux activités humaines qui impliquent des échanges monétaires asynchrones. Ils sont présents dans les activités de financement, exercées par nature par les établissements de crédit et les entreprises d'investissement mais aussi, par usage, par les entreprises non financières lorsque, dans le cadre de la gestion d'excédents de trésorerie par exemple, elles deviennent créanciers financiers.
Ils sont également présents dans toutes les activités qui requièrent des échanges sur les marchés d'instruments financiers.
De cet ensemble très vaste d'activités émergent deux grands types de risques financiers :

- le risque dit "de crédit" ou, selon une acception plus récente et plus large, "de contrepartie" ;
- le risque dit "de marché" : risque de taux d'intérêt, risque de taux de change, risque de prix (actions, matières premières…).

1.7.2 Le risque financier

Dans le secteur financier, peut-être plus que dans tout autre secteur, la définition du risque associe intimement l'événement redouté (le "danger") aux conséquences préjudiciables qu'il entraîne pour l'entité qui le subit.
C'est en effet en termes financiers qu'on cherche à exprimer le produit de la probabilité de survenance de l'événement redouté (à un horizon prédéfini de temps) et de son champ d'impact -qu'en finance, on appelle simplement "exposition" ou "engagement"-.

1.7.2.1 L'événement

En matière de risque de crédit/contrepartie, l'événement redouté est le défaut du débiteur, entendu comme son incapacité à remplir ses obligations contractuelles envers son créancier.
Le défaut survient lorsque le créancier constate l'inexécution d'un paiement, prévu dans le contrat établi avec le débiteur, au-delà d'un délai de temps qui exclut tout retard "technique".
À titre d'exemple, en matière de prêts bancaires aux entreprises, ce délai est de trois mois.

En matière de risque de marché, l'événement redouté est une variation défavorable du(des) paramètre(s) qui conditionne(nt) la valeur de l'instrument financier sur lequel l'entité est contractuellement exposée.

1.7.2.2 Les conséquences

Les conséquences sont financières : ce sont les pertes que le défaut du débiteur ou la variation défavorable de valeur de l'instrument entraînent dans la comptabilité de l'entité, soit sous forme de pertes d'exploitation, soit sous forme d'ajustements de valeur entraînant une diminution des fonds propres.

En univers incertain, la notion de risque financier peut donc être appréhendée par la formule générale suivante :

Perte financière estimée à un horizon prédéfini de temps
=
Probabilité de survenance de l'événement redouté à cet horizon
*
Montant estimé de l'exposition

1.7.3 L'usage de la gestion des risques financiers

Les effets conjugués de la mondialisation de l'économie et de la complexification des produits et circuits d'échange ayant contribué à fragiliser les agents économiques et donc à accroître les risques (l'augmentation des "sinistres" bancaires durant les vingt dernières années est là pour en témoigner), la gestion des risques financiers est devenue une des clés du pilotage des entreprises financières vers un développement pérenne.

Sous la poussée des contraintes réglementaires (accords de Bâle, textes du Comité Consultatif de la Législation et de la Réglementation Financières en France….), des dispositifs sont mis en place afin de mieux identifier et mesurer les risques, et de mieux les accepter, les prévenir et les gérer une fois acceptés.

Ces dispositifs entrent désormais pour une part de plus en plus importante et structurante dans la gestion des entreprises financières et leur usage vise à dépasser les contraintes et à en faire des sources de compétitivité et de développement.

1.7.4 Le processus de gestion des risques financiers

1.7.4.1 L'établissement du contexte

Le contexte dans lequel s'inscrivent les risques financiers est aujourd'hui largement inspiré par la réglementation.
En instituant des exigences minimales de fonds propres pour la couverture des risques, un dispositif de contrôle interne et une discipline de marché commandant la transparence à l'égard des tiers, la réforme Bâle II conduit en effet les entreprises financières à revoir leur organisation et leurs processus.

1.7.4.2 L'appréciation des risques

L'appréciation des risques financiers fait appel à des modèles de connaissance de l' "écosystème" propre à l'opération envisagée.

Ces modèles suggèrent le recours à des indicateurs de risque.

Le risque de crédit/contrepartie s'apprécie essentiellement à travers un indicateur représentatif de la qualité de crédit du débiteur : la note pour les personnes morales, le score pour les personnes physiques. C'est un indicateur instantané de la qualité de crédit du débiteur et prédictif de son défaut en ce que les analystes le traduisent sous forme de probabilité de défaut.

Le risque de marché s'apprécie à travers quelques indicateurs qui combinent des connaissances "fondamentales" (dynamique macro-économique) et "techniques" (statistiques, comportementales) : la volatilité dite "implicite" -comme mesure prédictive de variabilité des paramètres de marché : taux d'intérêt, taux de change… - la '*value at risk*' - comme mesure prédictive de la perte financière maximale encourue sur un horizon temporel et un intervalle de confiance prédéfinis-…

1.7.4.3 L'acceptation des risques

D'une manière générale, l'acceptation du risque se fait à l'aune de l'aversion au risque. Cette aversion trouve son expression dans la politique des risques définie par l'entreprise financière.

1.7.4.4 Le traitement des risques

Le traitement des risques s'inscrit dans un dispositif global qui couvre une chaîne de décisions et d'actions. Il suppose donc une architecture décisionnelle efficace, un système d'information robuste et fiable et des procédures bien documentées et respectées.

La chaîne des traitements inclut :

- la prévention du risque, par la fixation d'un "plafond" qui s'exprime en termes, soit de montant d'exposition, soit de perte financière estimée ;
- le transfert partiel ou total du risque auprès d'une partie tierce qui l'accepte, par exemple lors de la dégradation de la notation d'un débiteur ou de l'augmentation de la variabilité anticipée des paramètres de marché ;
- la gestion des incidents, par la mise en œuvre de procédures spécifiques de recouvrement d'impayés ;
- la simulation de situations de crise, par la mise en place de programmes intégrant la survenance d'événements à probabilité très réduite mais aux conséquences très préjudiciables.

1.7.4.5 Le contrôle et le suivi

Les risques et les processus et modèles (de notation/*scoring*, de valorisation de positions de marché…) destinés à les gérer sont contrôlés par des unités internes indépendantes des unités opérationnelles qui engagent les opérations vecteurs des risques.
Le contrôle vise tant le respect des règles et principes de gestion que la validation ex post des modèles (procédé dit de "*back-testing*").
Il fait l'objet de *reportings* réguliers auprès des instances décisionnelles.

1.7.4.6 La communication relative aux risques

La communication relative aux risques financiers s'inscrit aujourd'hui dans l'exigence de transparence à l'égard des parties tierces à l'entreprise requise par le législateur et les organes institutionnels de supervision (Commission Bancaire…).
Elle donne lieu à divers types d'états normalisés destinés à l'information publique : document dit "de référence", qui, outre les comptes de l'entreprise, détaille en particulier les facteurs de risques et leur contrôle ; états COREP…

1.7.5 Références, méthodes et outils

S'il n'existe pas, en matière de gestion des risques financiers, de références à proprement parler, il existe des méthodes et des outils.

On considérera que les indicateurs de risque évoqués supra sont les outils privilégiés pour la gestion des risques :

- note/score pour le risque de crédit/contrepartie ;
- *value at risk* pour le risque de marché.

Alors que les méthodes d'établissement des notes/scores restent assez largement spécifiques à chaque entreprise, les méthodes de calcul de la *value at risk* sont partagées : approche RiskMetrics™, approche historique, approche Monte-Carlo…

2 Synthèse des secteurs étudiés

2.1 Points communs

Grâce à l'[ISO Guide 73], il a été possible de dresser un panorama des différents secteurs de la gestion des risques. A fortiori cela nous amène à constater que ces derniers suivent donc un certain nombre de principes communs. On note que ces principes sont repris dans l'[ISO 31000].

Premièrement au niveau des concepts, un noyau dur est toujours présent dans chaque secteur : un risque est composé d'une cause et d'une conséquence. Il va cibler des objectifs de l'organisation dans le secteur du risque étudié. Des mesures de traitement du risque vont être prises afin de protéger ces objectifs et de mitiger les risques, qui peuvent être de l'un des quatre types définis dans l'[ISO Guide 73] (acceptation, contrôle, transfert, évitement).

Ensuite, le processus de gestion des risques de l'[ISO Guide 73] est généralement déroulé dans son intégralité. Ce processus est constitué des éléments suivants :

1. Établissement du contexte
   - Organisation
   - Périmètre de l'étude
   - Objectifs
   - Paramètres à prendre en compte

2. Appréciation des risques
   - Quels sont les risques ?
   - Quel est le niveau des risques ?
   - Classement des risques

3. Traitement des risques
   - Choix pour traiter les risques : réduction, transfert, évitement ou prise de risques
   - Mise en place de mesures pour traiter les risques

4. Acceptation des risques
   - Validation formelle de la manière dont les risques sont traités
   - Validation formelle des risques résiduels

5. Communication relative aux risques
   - Activités de consultation des parties prenantes
   - Activités d'information des parties prenantes

2.2 Particularités des secteurs

2.2.1 SSI

La SSI est un secteur relativement récent dans lequel une notion supplémentaire apparaît : la vulnérabilité. De plus les menaces dans ce secteur sont volatiles. L'outillage méthodologique et logiciel disponible pour la gestion des risques est important et a vu notamment l'apparition d'un système de management intégré [ISO 27001]. La SSI est également un secteur où de nombreuses réglementations ont émergé, rendant l'analyse des risques obligatoire.

2.2.2 Environnement

L'environnement se démarque notamment par les notions d'aspects et d'impacts, ces derniers pouvant s'avérer positifs. [AMDEC] est le principal outil utilisé dans ce secteur pour l'analyse macroscopique, tandis que l'écotoxicologie est utilisée pour la partie microscopique. La réglementation est lourde et contraignante pour certains secteurs (directive SEVESO). Pour y répondre un système de management intégré [ISO 14001] permet de globaliser la démarche.

2.2.3 Les risques professionnels

La gestion des risques professionnels se focalise principalement sur la prévention des risques. On y retrouve la notion de cartographie des risques. [AMDEC] est également régulièrement utilisé pour l'analyse des risques. Il faut noter que les risques professionnels sont souvent soumis à des sanctions pénales. Le secteur des risques professionnels dispose également de son système de management dédié [OHSAS 18001].

2.2.4 Les risques juridiques

Un risque juridique est une conjonction entre un évènement et un référentiel légal (code civil, réglementation sectorielle, contrat entre parties…). Les responsables sont particulièrement sensibles à ce secteur car les sanctions pénales peuvent mettre en danger la survie d'une organisation. La réglementation est complexe, répartie sur différentes juridictions (européen, national, sectoriel, communal…), et qui de plus varie en permanence selon notamment la jurisprudence, imposant un véritable travail de veille continu qui peut vite s'avérer très coûteux.

2.2.5 Gestion de projet

La gestion des risques de projet se distingue par l'absence d'une étape spécifique d'étude du contexte (réalisée généralement lors de la gestion de projet dans son ensemble). L'étape d'acceptation du risque est quant à elle absente des méthodes classiques de gestion des risques de projet. De plus, la gestion des risques de projet peut également déboucher sur des impacts positifs. Les plans de continuité et les plans de reprise sur incident de la SSI rejoignent la notion de contingence en gestion de projet : on accepte le risque tout en le surveillant.

2.2.6 Sûreté de fonctionnement

La gestion des risques de sûreté de fonctionnement s'inscrit clairement dans le cycle de vie complet du système étudié. Il se distingue principalement par son approche spécifique du risque, décrite en termes de faute, erreur et défaillance. Au cours des dernières années, on a constaté un rapprochement entre la SSI et la sureté de fonctionnement.

2.2.7 Les risques financiers

Les risques financiers sont partie intégrante des activités des entreprises financières. Leur gestion est donc une des clés du développement pérenne (on préfère dire "durable" aujourd'hui) de ces entreprises. S'ils présentent une particularité, elle est peut-être à chercher dans les possibilités originales mais aussi hautement complexes de leur transfert à l'économie et donc sans doute en une montée de la vulnérabilité d'ensemble de cette même économie…

Conclusion

La finalité de l'activité de gestion des risques reste dans tous les secteurs la recherche de la meilleure balance des coûts (directs ou indirects) entre la prise de risque et le traitement du risque. Certains secteurs (environnement et professionnels par exemple) jouent sur des effets en longue durée voire irréversible, à la différence d'autres secteurs plus immédiats.

Il existe trois grands types de risques :

- les risques stratégiques (ou risques métiers). Par exemple la création d'une entreprise, d'un produit ou un investissement dans les technologies de l'information ;
- les risques opérationnels sous-jacents à la réalisation de l'activité (technologies de l'information, juridique, professionnel, environnement…) ;
- les risques financiers : insolvabilité, perte de trésorerie, volatilité des cours, fraude, défaut de paiement…

Le but de gestion des risques est de créer un cycle vertueux. On peut considérer que la gestion elle-même a un impact positif. Cependant elle dépend directement de celui qui la réalise et de l'endroit où on la réalise. Par exemple, considérer l'incendie dans la SSI ne se fait pas de la même manière que dans la sécurité physique.

Bien que le processus de gestion des risques soit souvent commun entre les secteurs dans ses grandes lignes, les divergences apparaissent plus dans la terminologie, qui peut souvent être très diverse, même au sein d'un même secteur. Par ailleurs, certaines étapes du processus global sont plus fournies selon les secteurs. Au niveau de la réglementation, cette dernière joue un rôle important dans la gestion des risques de nombreux secteurs, car elle donne aux gestionnaires de risque (*risk manager*) les règles nécessaires à respecter.

Les systèmes de management sont apparus comme une solution pertinente pour différents secteurs, qui se sont rapprochés via cet outil, en vue de réaliser une gestion des risques globale et intégrée.

Annexes

Acronymes

AMDE	Analyse des Modes de Défaillance et de leurs Effets
AMDEC	Analyse des Modes de Défaillance, de Leurs Effets et de Leur Criticité
APR	Analyse Préliminaire des Risques
EMAS	*Environmental Management and Audit Scheme* (schéma de management et d'audit environnemental)
HAZOP	*HAZard OPerability* (analyse de risque et d'opérabilité)
ISO	*International Organization for Standardization* (organisation internationale de normalisation)
MTTF	*Mean Time To Failure* (temps moyen jusqu'à l'occurrence de la première défaillance)
OCDE	Organisation de Coopération et de Développement Économique
OHSAS	*Occupational Health and Safety Management System*
PNEC	*Predicted No-Effect Concentration* (concentration prédite sans effet)
SI	Système d'Information
SSI	Sécurité des Systèmes d'Information

Bibliographie

Les références suivantes apparaissent entre crochets dans le présent document :

[ADELI] *Maîtriser les risques des projets informatiques*, Rapport du groupe de travail "Les risques du projet ", ADELI, PERILoscope 97 (1997).

[AMDEC] *Procedures for performing a failure mode, effects and criticality analysis (FMECA)*, MIL-P-1629, US Army (1949).

[Avizienis] Avizienis, A., et al., *Basic concepts and taxonomy of dependable and secure computing*, IEEE Trans. Dependable and Secure Computing. 1(1): p. 11-33 (2004).

[Bradbury 2004] Bradbury, S.B., Feijtel, T.C.J., Van Leeuwen, C.J., *Meeting the scientific needs of ecological risk assessment in a regulatory context, Environmental science & technology* (2004).

[Callow 2003] Callow, P., Forbes, V.E., *Does ecotoxicology inform ecological risk assessment ? Environmental science & technology* (2003).

[Courtot 1998] Courtot, H., *La gestion des risques dans les projets*, Economica (1998).

[CRAMM] *CCTA (Central Computer and Telecommunications Agency) Risk Analysis and Management Method*, Insight consulting, Royaume-Uni (2003).

[Degobert 2004] Degobert, É., Le Ray, J., *Maîtrise des risques professionnels – Mettre en œuvre une démarche d'amélioration continue*, AFNOR (2004).

[Dubois 1996] Dubois, C., *L'analyse du risque : Une approche conceptuelle et systémique*, Chenelière / McGraw-Hill, Montréal (1996).

[EBIOS] *Expression des Besoins et Identification des Objectifs de Sécurité* – SGDN – version 2 (2004).

[ECSS Hazard] *Space Product Assurance, Hazard Analysis*, European cooperation for space standardization (ECSS), ECSS-Q-40-02A (2003).

[ECSS Safety] *Space Product Assurance, Safety*, European cooperation for space standardization (ECSS), ECSS-Q-40B (2002).

[EMAS] *Réglementation 761/2001 du 19/03/2001 du Parlement et Conseil européen permettant la participation volontaire d'organisations à un système de management environnemental et d'audit* (2001).

[EN 50126] *Applications ferroviaires, Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité*, norme européenne (2000).

[EN 50129] *Applications ferroviaires, Systèmes de signalisation, de télécommunications et de traitement, Systèmes électroniques de sécurité pour la signalisation*, norme européenne (2003).

[EN 61508] *Sécurité fonctionnelle des systèmes électriques/ électroniques/électroniques programmables relatifs à la sécurité*, norme européenne (2002).

[FR 1016] *Décret n°2001-1016 du 5 novembre 2001 portant création d'un document relatif à l'évaluation des risques pour la santé et la sécurité des travailleurs, prévue par l'article L. 230-2 du code du travail et modifiant le code du travail* (2001).

[FR 1414] *Loi n°91-1414 du 31 décembre 1991 modifiant le code du travail et le code de la santé publique en vue de favoriser la prévention des risques professionnels et portant transposition de directives européennes relatives à la santé et à la sécurité du travail* (1991).

[FR DRT-6] *Circulaire DRT n°6 du 18 avril 2002 pris pour l'application du décret n°2001-1016 portant création d'un document relatif à l'évaluation des risques pour la santé et la sécurité des travailleurs, prévue par l'article L. 230-2 du code du travail et modifiant le code du travail* (2002.)

[HERMES] *HERMES (Handbuch der Elektronischen Rechenzentren des Bundes, Methode für die Entwicklung von Systemen)*, Unité de stratégie informatique de la Confédération (USIC), Suisse (1995).

[IDS 56] *Safety management requirements for defence systems, Def Stan 00-56*, Ministry of Defence, Royaume-Uni (1989).

[IGI 1300] *Instruction générale interministérielle n°1300/SGDN/PSE/SSD sur la protection du secret de la défense nationale*, Secrétariat général de la défense nationale (SGDN) (2003).

[ISO 10006] *Systèmes de management de la qualité, Lignes directrices pour le management de la qualité dans les projets,* International Organization for Standardization (ISO) (2003).

[ISO 14001] *Environmental management systems, Requirements with guidance for use,* International Organization for Standardization (ISO) (2004).

[ISO 15408] *Critères Communs pour l'évaluation de la sécurité des Technologies de l'Information,* International Organization for Standardization (ISO) (2005).

[ISO 27001] *Information technology, Security Techniques, Information security management systems, Requirements,* International Organization for Standardization (ISO) (2005).

[ISO 27005] *Information technology, Security Techniques, Information security management systems, Information security risk management,* International Organization for Standardization (ISO) (2008).

[ISO 31000] *Risk management, Guidelines on principles and implementation of risk management,* International Organization for Standardization (ISO) (en cours d'élaboration).

[ISO 8402] *Management de la qualité et assurance de la qualité, Vocabulaire,* International Organization for Standardization (ISO) (1994).

[ISO 9001] *Systèmes de management de la qualité, Exigences,* International Organization for Standardization (ISO) (2000).

[ISO Guide 73] *Management du risque, Vocabulaire, Principes directeurs pour l'utilisation dans les normes,* International Organization for Standardization (ISO) (2002, en cours de révision).

[Laprie] Avizienis, A., Laprie, J.-C., Randell, B., *Fundamental Concepts of Dependability*, Research Report N°1145, Centre national de la recherche scientifique (CNRS), Laboratoire d'analyse et d'architecture des systèmes (LAAS) (2001).

[OCDE] *Lignes directrices régissant la sécurité des systèmes et réseaux d'information, Vers une culture de la sécurité,* Organisation de Coopération et de Développement Économiques (OCDE) (2002).

[OCTAVE] *OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)*, Carnegie Mellon University, Software Engineering Institute, États-Unis (2001).

[OHSAS 18001] *Systèmes de management de la santé et de la sécurité au travail, Spécification*, Occupational Health and Safety Assesment Series (OHSAS) (2007).

[OHSAS 18002] *Systèmes de management de la santé et de la sécurité au travail. Lignes directrices pour la mise en œuvre de OHSAS 18001*, Occupational health and safety assesment series (OHSAS) (2002).

[PMBOK] *PMBOK (Project Management Body of Knowledge) – Management de projet, un référentiel de connaissances*, Project management institute (PMI), Association française de normalisation (AFNOR) (2000).

[PRINCE2] *PRoject IN Controlled Environnements*, Prince 2™, Office of Government Commerce, Royaume-Uni (1996).

[SEVESO] *Directive européenne 96/82/CE du Conseil du 9 décembre 1996 concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses, dite directive SEVESO* (1996).

[Thybaud 2005] Thybaud, É., *Rejets chimiques des installations nucléaires : Évaluation des risques pour les écosystèmes*, Institut national de l'environnement industriel et des risques (INERIS) (2005).

[UE 1488] *Règlement n°1488/94 de la Commission du 28 juin 1994, établissant les principes d'évaluation des risques pour l'homme et pour l'environnement présentés par les substances existantes, conformément au règlement n°793/93 du Conseil* (1994).

[UE 156] *Directive n°91/156/CEE du Conseil du 18 mars 1991, modifiant la directive 75/442/CEE relative aux déchets* (1991).

[UE 271] *Directive n°91/271/CEE du Conseil du 21 mai 1991, relative au traitement des eaux urbaines* (1991).

[UE 391] *Directive européenne 89/391 du 12 juin 1989 sur l'amélioration de la sécurité et de la santé des salariés* (1989).

[UE 67] *Directive n°93/67/CEE de mise sur le marché des substances chimiques* (1993).

[UE 676] *Directive n°91/676/CEE du Conseil du 12 décembre 1991 concernant la protection des eaux contre la pollution par les nitrates à partir de sources agricoles* (1991).

[UE 793] *Règlement n°793/93 du Conseil concernant l'évaluation et le contrôle des risques présentés par les substances existantes* (1993).

[Verdun 2006] Verdun, F., *La gestion des risques juridiques*, Éditions d'organisation (2006).

[Villemeur] Villemeur, A., *Sûreté de fonctionnement des systèmes industriels*, Éditions Eyrolles (1997).

Formulaire de recueil de commentaires

Ce formulaire peut être envoyé à l'adresse suivante :

Club EBIOS
72 avenue Gaston Boissier
78220 VIROFLAY
contact[at]club-ebios.org

Identification de la contribution
Nom et organisme (facultatif) : .....
Adresse électronique : .....
Date : .....

Remarques générales sur le document
Le document répond-il à vos besoins ? Oui ☐ Non ☐

Si oui :

Pensez-vous qu'il puisse être amélioré dans son fond ? Oui ☐ Non ☐

Si oui :

Qu'auriez-vous souhaité y trouver d'autre ?
.....
.....

Quelles parties du document vous paraissent-elles inutiles ou mal adaptées ?
.....
.....

Pensez-vous qu'il puisse être amélioré dans sa forme ? Oui ☐ Non ☐

Si oui :

Dans quel domaine peut-on l'améliorer ?
- lisibilité, compréhension ☐
- présentation ☐
- autre ☐

Précisez vos souhaits quant à la forme :
.....
.....

Si non :

Précisez le domaine pour lequel il ne vous convient pas et définissez ce qui vous aurait convenu :
.....
.....

Quels autres sujets souhaiteriez-vous voir traiter ?
.....
.....

Remarques particulières sur le document

Des commentaires détaillés peuvent être formulés à l'aide du tableau suivant.

"N°" indique un numéro d'ordre.

"Type" est composé de deux lettres :

La première lettre précise la catégorie de remarque :

- O Faute d'orthographe ou de grammaire
- E Manque d'explications ou de clarification d'un point existant
- I Texte incomplet ou manquant
- R Erreur

La seconde lettre précise son caractère :

- m mineur
- M Majeur

"Référence" indique la localisation précise dans le texte (numéro de paragraphe, ligne…).

"Énoncé de la remarque" permet de formaliser le commentaire.

"Solution proposée" permet de soumettre le moyen de résoudre le problème énoncé.

N°	Type	Référence	Énoncé de la remarque	Solution proposée
1				
2				
3				
4				
5				

Merci de votre contribution