

APIA

Administrateurs Professionnels
Indépendants Associés

Cahier n°27

Le rôle de l'administrateur indépendant dans la gestion du risque

SATEC
COURTIER EN ASSURANCES

 **SIACI SAINT HONORE**


LAMY LEXEL
avocats d'entreprises

Table des matières

Introduction	2
1 Les enjeux de la Gestion des risques	
1.1 Comment concilier l'esprit d'entreprise et la gestion du risque ?	3
1.2 Une nécessité : se doter d'une méthodologie	3
2 Comment optimiser le traitement des risques ?	
2.1 Les risques assurables et leurs préventions	6
2.1.a Les contrats d'assurance méconnus	7
2.1.b Les contrats d'assurance liés aux « risques nouveaux »	8
2.2 Les risques non assurables	9
2.3 Les erreurs à ne pas commettre	10
3 Rôle de l'administrateur indépendant	11
Conclusion	12
Annexes	13

1 Les enjeux de la Gestion des risques

Introduction

L'entreprise est par définition un espace de création de valeur conforme à l'objet social : « *La prise de risque fait partie intégrante de l'entreprise. Contrepartie inévitable de la création de valeur, au cœur même de l'activité entrepreneuriale, la question n'est évidemment pas de chercher à supprimer le risque mais d'arriver à le connaître et à le maîtriser* » (in P. Cabane : Manuel de Gouvernance d'Entreprise).

Les assureurs et leurs actuaires ont depuis longtemps cherché à mesurer la valeur du risque, en corrélant son intensité financière, son occurrence et la durée considérée. Les financiers se sont emparés des travaux des actuaires pour établir des calculs de valorisation d'actifs pondérés par les risques.

Le dirigeant et les administrateurs qui l'entourent cherchent en conséquence à maîtriser les choix donc les risques.

Une mission essentielle de l'administrateur est de conformer le risque stratégique à l'appétence au risque acceptée par les actionnaires. À ce titre, il est fait obligation au Conseil d'administration de rendre compte des risques dans le rapport de gestion, au visa de l'article L 225-100 de code de commerce, encadré par la loi qui a confié au Conseil d'administration quatre missions :

- déterminer la stratégie et en suivre la mise en œuvre,
- se saisir de toute question relative à la bonne marche de l'entreprise et régler par ses débats les affaires la concernant,
- nommer les dirigeants et en fixer la rémunération,
- assurer la qualité de l'information communiquée aux actionnaires.

Dans le cadre des deux premières missions, le Conseil d'administration a bien l'obligation de se poser la question : « *Que se passerait-il si, par exemple, tel risque n'est pas pris en*

compte, telle opportunité n'est pas saisie, tel changement se confirme, tel nouveau concurrent se développe ? ».

Au surplus, il appartient au Conseil et aux administrateurs de s'assurer de la création de valeur, de connaître les écarts par rapports aux objectifs, d'en connaître les raisons, d'en suivre les corrections et de la pérenniser. Afin de maintenir ou même de promouvoir la vision entrepreneuriale, donc de la prise de risque, les administrateurs ont pour missions et devoirs de :

- s'assurer d'un plan de gestion des risques, des règles de gestion des risques, et d'en vérifier la constance, la validité des modifications portées,
- la mise en place de retour d'informations fiables sur le suivi opérationnel des décisions prises donc des risques pris.

Ces missions, faut-il le rappeler, sont accomplies dans un univers d'informations biaisées par nature, par celui qui les transmet et par celui qui les reçoit, même si l'un et l'autre sont d'une grande honnêteté intellectuelle : le trop fameux « *traduttore traditore* » et « *on entend ce qu'on veut bien entendre* ». Ce sont les biais cognitifs.

En résumé, avant et après le choix, à l'heure de la décision, quand les modalités de décision sont définies aussi bien que les modalités de sa mise en œuvre, le suivi doit être précis, les résultats d'étape doivent être fiables, le piège abscons (jusqu'où ne pas aller trop loin, savoir s'arrêter) doit être repéré et banni. Diriger, c'est risquer et construire la valeur de l'entreprise, mais aussi prévoir : la création pérenne de valeur doit être le fil rouge de la conduite de l'administrateur avec l'intérêt social comme boussole.

Il nous semblait donc intéressant d'apprécier la notion de gestion des risques et du traitement efficace de ces derniers, de l'angle de vue de l'administrateur indépendant.

1.1 Comment concilier l'esprit d'entreprise et la gestion du risque ?

Qu'est-ce que la gestion du risque ?

Dans l'économie mondiale et globale du 21^{ème} siècle, les échanges de l'entreprise avec son environnement (environnement physique, technique, juridique, économique, social, médiatique...) sont incessants et les dépendances inévitables et souvent imprévues (fournisseurs, conjoncture économique et politique, opinion publique, intempéries...).

Cet environnement dans lequel interviennent des acteurs variés aux logiques divergentes, est instable, partiellement prévisible ou souvent imprévisible. L'entreprise doit savoir en faire un allié. Elle sera d'autant plus forte qu'elle saura entrer en symbiose avec lui, l'apprivoisant, anticipant ses mouvements, s'adaptant tout en sachant y puiser les opportunités de création de valeur indispensable, dans une économie hyper concurrentielle.

Dans ce contexte, la prise de risques peut être génératrice de valeur mais ces mêmes risques peuvent en même temps affaiblir voire anéantir une entreprise. L'analyse et la maîtrise des risques deviennent incontournables.

La gestion du risque est une opportunité... Et non une contrainte

Toutes les entreprises ne sont pas égales face à l'adversité ; seules celles qui adoptent une posture proactive leur permettant une adaptation continue et audacieuse face à l'incertain pourront rester dans la course. Dès lors, la gestion du risque n'est pas un luxe mais un choix stratégique fort, une

opportunité plutôt qu'une contrainte. Bien comprendre les risques, c'est bien comprendre le « business model » de l'entreprise, ses facteurs de création de valeur et le dispositif de contrôle qui en découlent qui doit aboutir à un outil d'aide à la décision.

C'est une préoccupation forte des dirigeants d'entreprise

Une enquête menée par Ipsos en juin 2014 auprès d'un échantillon représentatif de 500 chefs d'entreprise de 10 à 500 salariés fait ressortir :

- un sentiment croissant de vulnérabilité dans un contexte de concurrence et de judiciarisation croissante de la société. A nouveaux risques, nouvelles préoccupations :
 - 80% des chefs d'entreprise sont préoccupés par le risque de mise en cause du dirigeant et sa responsabilité civile et pénale ;
 - 61% craignent pour l'image/réputation de leur entreprise et près de la moitié sont préoccupés par le risque de crise médiatique ou les cyber-risques ;
- une sensibilité toujours réelle aux risques « classiques » : le niveau de trésorerie de l'entreprise, les pertes de marchés, la défaillance d'un homme clé, les impayés, le conflit social...

Mais a contrario, cette étude souligne également un point majeur : le sentiment des dirigeants d'être plutôt bien couverts pour les risques relatifs à leur entreprise (95%) ou à eux-mêmes (76%)... alors que 75% d'entre eux n'ont jamais réalisés une analyse poussée ou une cartographie des risques.

1.2 Une nécessité : se doter d'une méthodologie

La gestion du risque est un processus en plusieurs étapes :

- identifier les risques auxquels est exposée une entreprise. On parle alors de cartographie des risques.
- classer les risques selon leur intensité, leur impact sur la vie de l'entreprise et la maîtrise qu'elle en a. Il s'agit là d'une hiérarchisation des risques.
- limiter les risques par la mise en place d'un plan d'action :
 - instaurer une politique de prévention,
 - décider de transférer ou non certains risques à un tiers (assureurs, banquiers...),
 - définir des responsabilités au sein du management par type de risque,
 - voire parfois prendre le risque de ne rien faire car les moyens à mettre en œuvre pour le maîtriser représentent une contrainte trop grande pour l'entreprise.

Nous vous proposons un exemple de méthodologie volontairement généraliste qui ne prétend pas couvrir l'intégralité des risques. Il reviendra bien entendu à l'utilisateur de cet outil, de l'adapter en fonction du marché de l'entreprise, de ses spécificités et de son environnement.

Etape 1 : Identification des risques : cartographie

L'objectif de la cartographie des risques est de recenser les activités susceptibles de générer des risques. Il s'agit d'un travail préparatoire conduit à tous les niveaux hiérarchiques de l'entreprise, dont les principaux responsables opérationnels et responsables des fonctions support concernés doivent établir une synthèse. Acquérir une sorte

« d'intimité » avec l'entreprise grâce à la connaissance des marchés, des produits, des modalités d'exécution et de l'organisation interne. Cette intimité doit être formalisée pour

qu'elle puisse être partagée avec les différents interlocuteurs et faciliter les arbitrages le moment venu.

Exemple (non exhaustif) de cartographie des risques

Risques stratégiques		Risques opérationnels	
1	Crise sur un marché CLE	13	Sinistres : accident majeur sur un site
2	Perte d'un client CLE	14	Carence fournisseur
3	Perte d'un partenariat stratégique	15	Perte d'un équipement critique
4	Défaut de Gouvernance	16	Rupture de la chaîne logistique
5	Défaut d'innovation	17	Perte d'un SI critique
6	Erreur de développement produit	18	Accident du travail / Maladies professionnelles
Risques financiers		19	Pollution accidentelle ou graduelle
7	Fraude interne	20	Défaut qualité majeurs
8	Fluctuations fortes des prix des matières premières	21	Vol ou corruption de données sensibles ou confidentielles
9	Risque de change	22	Perte d'hommes clés
10	Risque fiscal	23	Mise en cause responsabilités dirigeants
11	Défaillance dans la maîtrise des stocks et du BFR	24	Cyber attaque
12	Défaut de paiement d'un client	25	Sécurité du personnel en déplacement
		26	Dégradation du climat social
		Risques juridiques	
		27	Non-respect des règles de concurrence
		28	Non-respect de la réglementation et des lois en vigueur
		29	Engagements contractuels non tenus
		30	Accords commerciaux non-conformes (LOI LME)
		Risques de réputation	
		31	Processus de gestion de crise non coordonné au niveau du groupe

Étape 2 : Classifier les risques : évaluation et priorisation

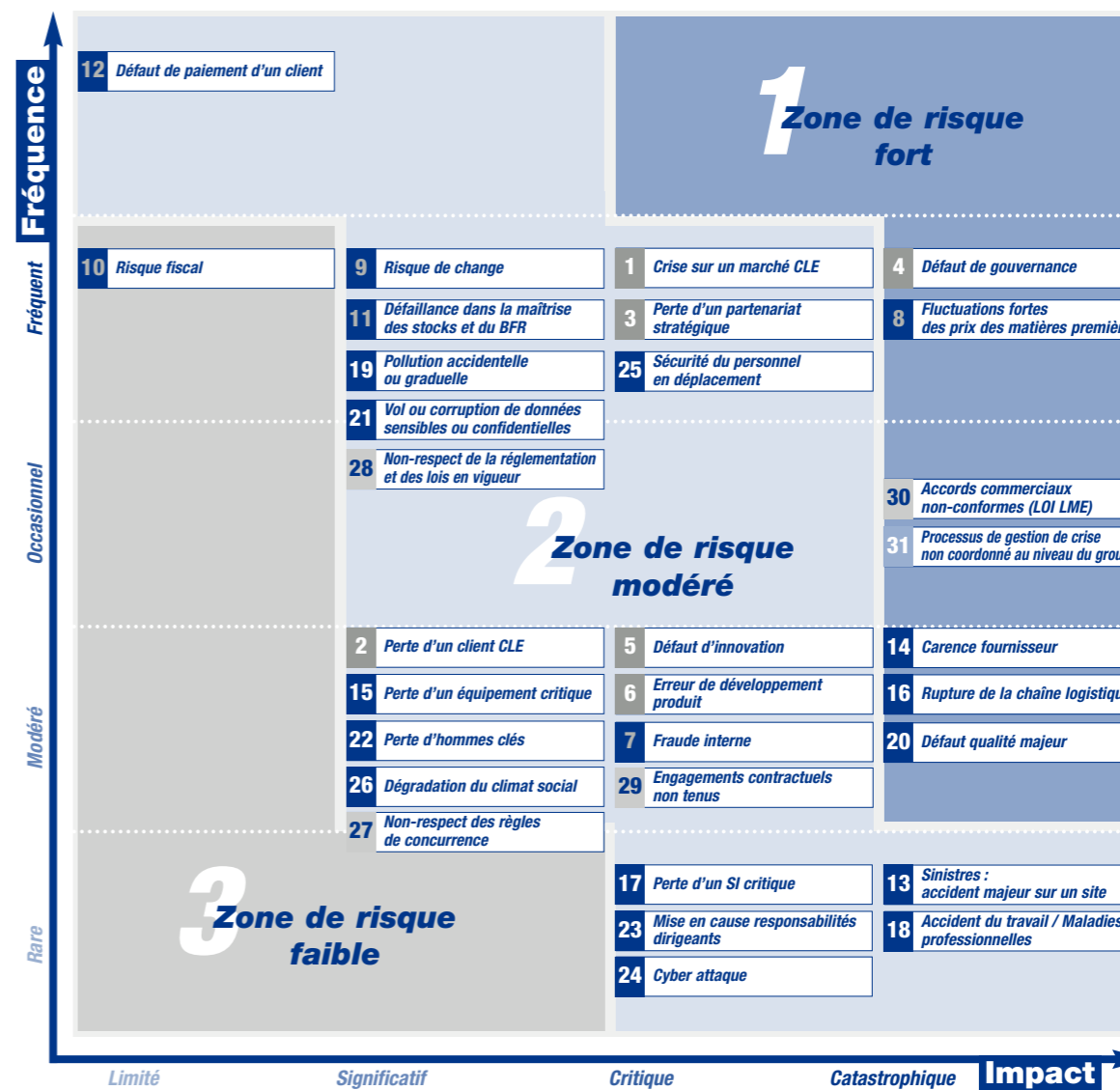
Une fois que les principaux risques inhérents à l'activité de l'entreprise ont été recensés, un travail de hiérarchisation est nécessaire.

Afin d'évaluer un risque, la méthodologie souvent retenue

consiste à positionner les risques sur les deux axes qui sont : la fréquence et l'impact. Cette évaluation peut être fondée sur l'historique, sur des éléments chiffrés, sur l'expérience...

L'évaluation combinée de ces deux facteurs permet d'établir une matrice de criticité des risques allant de « faible » à « fort ».

Matrice de criticité



Étape 3 :

Limiter les risques : plan d'action

En préambule, il paraît essentiel de souligner l'importance de constituer un groupe de travail interne à l'entreprise impliquant les opérationnels, la direction et un chef de projet désigné. Ce groupe de travail pourra être aidé de consultants externes et devra veiller au bon déroulement du processus. Ainsi, pour chaque risque identifié, un responsable en charge

du plan d'action devra être nommé.

Les zones de risque fort doivent être traitées dans le plan d'action.

Les zones de risque faible peuvent faire parties du plan d'action.

Les zones de risque modéré doivent être analysées au cas par cas par le groupe de travail pour les inclure ou les exclure du plan d'action.

Exemple d'un plan d'action de suivi des risques

N°	Risque	Responsable	Action	Délai
4	Défaut de gouvernance / Règles de délégation de pouvoir			
7	Fraude interne			
8	Fluctuations fortes des prix des MP			
9	Risque de change			
16	Rupture de la chaîne logistique			
17	Perte d'un SI critique			
20	Défaut qualité majeur			

N°	Risque	Responsable	Action	Délai
21	Vol ou corruption de données sensibles			
27	Non-respect des règles de la concurrence			
29	Engagements contractuels non tenus			
30	Accords commerciaux non conformes			
31	Processus de gestion de crise non coordonné au niveau du groupe			

2 Comment optimiser le traitement des risques ?

Pour traiter un risque, l'entreprise dispose de plusieurs alternatives :

- la diminution du risque : mise en place des mesures de prévention et suivi des mesures correctives,
- l'évitement du risque : décision de stopper une activité, de ne pas se développer sur un pays ou de renoncer à un produit, au regard du couple « rendement/risque » de l'option choisie mais également du coût de traitement du risque qui peut être prohibitif pour l'entreprise,
- l'acceptation du risque : lorsque le risque est inférieur au niveau d'appétence de l'entreprise qu'elle considère pouvoir maîtriser en cas de réalisation, ou pouvoir traiter à un coût acceptable. Il faut alors intégrer cette donnée dans le financement de l'activité,
- le partage du risque : décision d'externaliser le risque en le partageant avec un partenaire ou un sous-traitant. Pour

2.1 Les risques assurables et leur prévention

Du point de vue de l'assureur, les risques assurables sont ceux pour lesquels il est possible de recueillir, de calculer et d'estimer les pertes futures. Les risques assurables disposent de statistiques qui sont utilisées comme base pour l'estimation de la prime. Les risques assurables peuvent être prévus et mesurés. Le risque doit rester aléatoire et ne pas dépendre de la volonté de l'assuré dans sa réalisation.

Lorsque les risques sont assurables, un passage en revue systématique des contrats d'assurance s'impose, en vérifiant la définition exacte des événements assurés ou non, ainsi que les niveaux de garanties. Ce faisant, tel industriel découvrira, par exemple, que des stocks de matières premières lui appartenant et hébergés chez des sous-traitants ne sont pas assurés ou inversement, assurés deux fois.

Nous suggérons la réalisation d'un audit des assurances, par un courtier ou un audit indépendant avec pour principaux objectifs :

- identifier les principaux risques auxquels est exposée l'entreprise, et vérifier l'adéquation entre les couvertures de l'entreprise et les risques encourus par celle-ci ;
- vérifier que les couvertures en place sont conformes à la législation en vigueur ;
- proposer des améliorations aux couvertures en place compte tenu des possibilités des compagnies d'assurances ou bancaires.

Attention, cet audit d'assurance couvre la revue des risques assurables, qui concerne une très large partie des risques encourus par l'entreprise, mais n'exonère pas un travail plus large de revue globale des risques mené par un groupe de travail interne ou un éventuel prestataire.

Une telle revue est, suivant les cas, réalisée :

- à la prise de fonction de l'administrateur indépendant,
- en complément des autres diligences réalisées au moment

autant, l'entreprise ne doit pas s'exonérer de contrôler le dispositif de gestion du risque par le tiers, sauf à en subir ultérieurement et indirectement la mauvaise maîtrise,

- le transfert du risque : décision de couvrir le risque par un tiers (assureur ou banquier), ce qui suppose une interrogation sur l'étendue et le coût de transfert, exercice simple pour les assurances classiques de dommages telles que l'incendie, le vol ou les catastrophes naturelles ou pour les couvertures de taux ou de change mais fort compliqué lorsqu'il s'agit de risques émergents comme certains risques politiques ou les risques d'atteinte aux systèmes de traitement des données (cyber risques). Toutefois, tous les risques ne sont pas assurables...
- la délégation de pouvoir permet de minimiser les risques par une gestion au plus près des opérations et également de responsabiliser les collaborateurs. Cf cahier Apia n°14 « Les délégations de pouvoirs ».

d'une acquisition,

- dans la perspective d'un projet de cession à titre d'informations complémentaires à la disposition des candidats acquéreurs (*vendor's due diligence*),
- dans une perspective de renégociation périodique des contrats de couvertures et d'une mise en concurrence régulière des tiers (tous les trois ans est raisonnable, en général très productif pour l'entreprise).

L'administrateur indépendant aura par une connaissance détaillée des risques connus, assurés ou non, une vision exhaustive de l'exposition de l'entreprise et pourra le cas échéant prendre les décisions qui s'imposent en matière de couverture des risques.

Nous vous présentons ici, à titre purement indicatif, des exemples de contrats d'assurance avec les primes estimées. Nous ne pouvons évidemment pas recenser tous les types de contrats d'assurance (Responsabilité Civile, Multirisque Immeuble, Flotte Automobile, Dommage Ouvrage...) qui sont, dans une très large majorité des entreprises, souscrits et connus et très souvent « de droit ». Nous avons plutôt choisi de vous présenter les contrats méconnus et également les contrats couvrant les nouveaux risques.

Focus sur l'Audit d'Assurance :

Afin d'aider l'entreprise dans sa démarche de gestion des risques, un audit des Risques peut être réalisé par un prestataire externe (courtier, conseil spécialisé...). L'approche se déroule généralement en 4 étapes : évaluation des risques, analyse et hiérarchisation, recommandation sur le plan d'action et suivi. Le coût estimé pour cet audit se situe entre 5 000 € et 12 000 € HT pour une PME d'environ 50 M€ de chiffre d'affaires.

2.1.a Les contrats d'assurance méconnus

I - en lien avec la protection des dirigeants / administrateurs / collaborateurs

► La RCMS (Responsabilité Civile des Mandataires Sociaux ou Responsabilité des Dirigeants)

Ce contrat d'assurance est destiné aux entreprises quelle que soit leur taille. Il garantit tous les dirigeants de droit et de fait (administrateurs, dirigeants, délégués de pouvoirs, personnes physiques et morales), ainsi que l'ensemble des employés en cas de réclamations directes et personnelles y compris en cas de réclamations liées au droit du travail.

En tant que mandataire social, qui plus est dirigeant d'entreprise, la loi vous rend personnellement responsable, au titre de vos fonctions, dans les 3 cas suivants :

- le non-respect des dispositions légales et/ou réglementaires ;
- le non-respect des statuts ;
- la faute de gestion encadrée par le code de commerce et ses conséquences financières qui doivent être motivées par le juge, en total et en part de responsabilité entre les responsables éventuels.

Dans ces cas, vous devrez alors assumer le coût de votre défense et de l'indemnité éventuellement due au plaignant

Quel coût ?

Pour une PME générant un chiffre d'affaires annuel de 20 M€ et avec un niveau de garantie de 2 M€, le montant de la prime payée par l'entreprise au profit des bénéficiaires sera de l'ordre de 2 000 € / 4 000 € par an au total.

sur votre patrimoine personnel.

Ainsi, en souscrivant ce contrat, l'entreprise protège toutes les personnes qui engagent leur responsabilité au quotidien et dont la responsabilité personnelle, et donc le patrimoine, peut être mis en jeu. Aujourd'hui, seulement 20% des entreprises en France ont souscrit ce contrat.

► La perte d'emploi du dirigeant

Ce contrat, souscrit par l'entreprise au profit de son dirigeant, garantit un revenu fixe en cas de perte d'emploi, pour protéger le dirigeant et sa famille.

Sauf s'il a un contrat de travail avec un lien de subordination reconnu par Pôle Emploi, le dirigeant et le mandataire social perdent leur emploi « ad nutum » et ne peuvent prétendre à aucune indemnité de chômage.

► La Perte d'homme clé

Ce contrat « Homme-clé » assure toute personne ayant un rôle stratégique dans l'entreprise (dirigeant, collaborateurs proches), mais également ceux dont le savoir-faire ou les compétences spécifiques sont indispensables au bon fonctionnement de l'activité. Les garanties de ce contrat permettent en cas de perte d'homme clé :

- de se prémunir contre une perte d'exploitation ou une baisse brutale du chiffre d'affaires, de la marge brute ou des bénéfices ;
- de disposer de trésorerie immédiate pour faciliter la réorganisation, le recrutement et la formation d'un nouveau collaborateur ;
- de garantir le versement d'un capital à l'entreprise, en cas de décès, d'invalidité, de perte totale et irréversible d'autonomie de l'Homme clé.

La garantie des hommes clés dépend de l'âge, de l'état de

santé de l'assuré et des montants assurés. Pour un homme clé de 40 ans, non-fumeur, et avec un niveau de garantie de 1 M€, la prime sera de l'ordre 4 500 € / 6 000 € par an en garantie Décès / Perte Totale et Irréversible d'Autonomie. Ce contrat ne couvre pas une perte partielle d'autonomie inférieure à 100% reconnue par le corps médical.

Le dirigeant a également la possibilité d'organiser son indisponibilité temporaire ou définitive dans le cadre de la rédaction d'un Mandat de Protection Future (voir cahier Apia n°21)

► Le personnel en déplacement

Ce contrat permet aux dirigeants de couvrir la responsabilité de l'entreprise en cas d'utilisation par ses collaborateurs de leur véhicule personnel à des fins professionnelles en cas d'accident responsable. La prime annuelle par collaborateur est comprise entre 60 € et 100 € en fonction des zones géographiques, de la durée et de la fréquence des déplacements.

II - en lien avec l'activité

► Le risque fiscal

Ce contrat couvre pour partie les frais d'assistance juridique en cas de contentieux après un contrôle fiscal.

Généralement, il s'agit d'une option incluse dans les contrats d'assurance dits « de Protection Juridique ». Ce dernier couvre alors les frais de contentieux en cas de contrôle. La pénalité fiscale n'est en revanche jamais prise en charge.

► L'assurance de la garantie de passif

Ce contrat garantit les obligations réciproques de l'acheteur et du vendeur d'actifs, au surplus des garanties habituelles. Lors de la cession d'une entreprise, les engagements du vendeur sont consignés dans un document généralement intitulé la « convention de garantie », annexe ou partie de l'acte de cession, constituant l'engagement du vendeur sur l'exactitude, l'exhaustivité et la sincérité des informations communiquées. Le prix de la cession n'est définitif uniquement lorsque toutes les clauses de garanties sont purgées dans le temps prévu par la convention :

- l'acheteur peut solliciter le vendeur pour compenser toute augmentation de passif ou diminution d'actifs se révélant postérieurement à la cession mais trouvant son origine antérieurement ;
- l'engagement reçu par l'acheteur n'a de valeur que pour autant qu'il puisse être exécuté en cas de besoin ; d'où la mise en place de dispositifs dits de « garantie de la garantie » tels que les cautions bancaires, les comptes séquestre ou les compléments de prix.

Dans sa version « vendeur », l'assurance est la seule technique permettant à ce dernier, s'il est de bonne foi, de se

Quel coût ?

À titre d'exemple, pour un dirigeant dont le salaire brut annuel (y compris dividendes) est de 150 K€, le montant de la prime se situerait dans une fourchette de 3%-4% (4 500 € / 6 000 €) du salaire brut (sans révocation) et de 5%-6% (7 500 € / 9 000 €) du salaire brut (avec révocation) pour une garantie de maintien de 70% de son salaire pendant une durée de 12 à 24 mois.

Quel coût ?

Pour une PME de 20 M€ de CA l'option complémentaire engendre un coût de 2 000 € / 5 000 € annuel.

prémunir des conséquences d'un appel en garantie, les autres moyens (tels que cautions, séquestres ou compléments de prix) ne protégeant que l'acquéreur. Dans sa version « acheteur », l'assurance vient compléter, sans recours sur le vendeur, le premier niveau de protection consenti par ce dernier.

Ces avantages originaux, distincts des autres techniques de « garantie de la garantie » tel que le séquestre bancaire, présentent un intérêt dans des situations très variées dont nous ne citons que quelques exemples à titre d'illustration :

- objectif de prévoyance personnelle du dirigeant cédant (transfert du produit de la cession aux héritiers sans transférer le passif potentiel constitué par la garantie de passif),
- en cas de présence d'un fonds d'investissement, clôture d'un fonds et libération du « *carried interest* »,
- rapatriement de la garantie (quand le cédant est hors de France),
- garantie limitée donnée par le cédant du bloc de contrôle dans une opération « *public to private* ».

► Le défaut de paiement d'un client

Quel coût ?

Ainsi pour une PME réalisant un Chiffre d'Affaires de 20 M€ et qui souhaite assurer 50% de ses revenus, la prime variera entre 30 000 € et 50 000 €. Certains assureurs crédits proposent des formules forfaitaires selon la tranche de chiffre d'affaires (ex : pour un CA compris entre 1 M€ et 3 M€, la prime sera comprise entre 5 000 € et 8 000 € / pour un CA compris entre 3 M€ et 8 M€, la prime sera comprise entre 9 000 € et 15 000 €).

0,3% à 0,5% du chiffre d'affaires assuré. Il varie en fonction de la qualité des clients assurés et de l'historique de la sinistralité.

2.1.b Les contrats d'assurance liés aux « risques nouveaux »

Ces contrats garantissent les conséquences d'une cyber-attaque, d'accident sur les données, de fraude (en général) ou de malveillance.

► Les cyber-attaques

Les risques d'atteinte aux systèmes d'information et aux données informatiques sont devenus une réalité incontestable, quel que soit le secteur d'activité : simple virus informatique, piratage informatique, espionnage, vol de données, malveillance d'un employé ou tentative de cyber extorsion de fonds, voire de cyber espionnage économique ou industriel... Les contrats de couverture dédiés à ce type de risques couvrent les frais de consultants et d'experts pour la gestion de crise, les frais de communication pour protéger l'image de l'entreprise, les frais de notification en cas d'atteinte aux données personnelles des clients, les frais et pertes d'exploitation, les frais de procédures CNIL ainsi que les conséquences de la responsabilité de l'entreprise en cas de dommages causés aux tiers.

L'assureur-crédit est extrêmement bien renseigné sur les entreprises, dispose souvent d'une connaissance fine et historique de nombreux paramètres autres que financiers, il est aussi le moyen le moins cher pour sélectionner les clients.

► La couverture du risque de change

Ce contrat garantit le taux de change à terme et sécurise la rentabilité des transactions.

De même, il garantit le montant de remboursement d'une transaction financière à terme.

Lorsqu'une entreprise intervient sur les marchés internationaux pour exporter, importer ou investir, les règlements s'opèrent généralement en devise locale ou en dollar. L'une des préoccupations lors de ces transactions sera de connaître le cours de conversion de ces devises en euro.

Or, durant le délai plus ou moins long qui peut exister entre la date de négociation, le prix convenu et son règlement, le cours de conversion de ces devises va fluctuer et un mouvement défavorable peut compromettre la rentabilité de l'opération, voire se traduire par une opération à perte. Ce risque est appelé risque de change.

Les banques proposent divers schémas de couverture plus ou moins complexes : change spot ou à terme, tunnel d'options...

Toutefois les instruments de couvertures de change sont exactement les mêmes que les instruments spéculatifs, et il est du rôle de l'administrateur de vérifier que de tels instruments ne sont utilisés à d'autres fins que la couverture de contrats liés à l'intérêt social de l'entreprise.

► La couverture du risque du taux d'emprunt

Ce contrat permet à une entreprise, lorsqu'elle a mis en place un contrat long terme à taux variable de se couvrir contre une hausse du taux, en payant une « prime ». Le montant de cette prime est payable en une fois en fonction du plafond souhaité et de la durée du prêt (pour la valeur totale ou partielle de la dette). Il est conseillé de mettre en concurrence les banques prêteuses sur cette prime forfaitaire.

Le cas Domino's PIZZA : La chaîne de livraison à domicile Domino's Pizza a été victime en juin 2014 d'une tentative de racket de la part de pirates informatiques affirmant avoir volé les données de 650 000 clients et réclamant une rançon de 30 000 euros, sous peine de les publier.

La société a fait le choix de ne pas payer et de contacter l'ensemble de ses clients.

Le cas TARGET :

Entre le 27 novembre 2013 et le 15 décembre 2013, Target, l'un des plus importants acteurs de la distribution aux USA, s'est fait subtiliser plus de 40 millions de données bancaires, auxquelles s'ajoutent 70 millions de données personnelles. La méthode d'attaque est classique, mais bien orchestrée : les attaquants ont en premier lieu piraté un sous-traitant du distributeur chargé de la surveillance à distance des systèmes de chauffage et de climatisation. Le système de facturation externe de Target auquel le sous-traitant avait accès n'étant pas complètement isolé du réseau interne, les cybercriminels

ont réussi à s'y infiltrer, à voler 70 millions de données personnelles, et à installer un logiciel malveillant sur quelques terminaux de paiements. Les auteurs ont décidé, peu avant Noël où l'affluence est la plus forte, de déployer leur malware sur la plupart des terminaux de paiements des magasins du territoire américain.

Les motivations des attaquants sont purement financières. En effet, une donnée personnelle se vend sur le marché noir entre 0,25 \$ et 2 \$ environ, tandis qu'une donnée bancaire peut rapporter plusieurs dizaines de dollars.

L'expérience industrielle :

Un article de L'Express en date du 29 septembre 2011 nous apprenait que le Groupe Areva a été la cible d'une attaque de grande ampleur. Ces intrusions lancées plus de deux ans avant leur découverte auraient touché aussi bien les sites en France que les filiales à l'international du groupe. Les hackers auraient réussi à s'introduire dans le réseau informatique du groupe et à prendre le contrôle d'ordinateurs. Des préjudices « sur le plan stratégique » sont évoqués, ce qui pourrait signifier le vol de secrets industriels. Nous ignorons aujourd'hui si les activités militaires d'Areva ont été touchées.

À titre d'exemple, en décembre 2014 un industriel allemand, spécialiste de la production d'acier, a été victime d'une attaque informatique réussie ayant conduit à la compromission de son système informatique avec un résultat concret : l'impossibilité de procéder à l'arrêt maîtrisé d'un haut fourneau, avec pour conséquences d'importants dégâts sur le site.

Dans son rapport, le ministère précise que l'attaque a commencé par une infiltration du réseau administratif de l'entreprise visée par hameçonnage ciblé. De là, les pirates auraient réussi à compromettre le réseau de contrôle des installations industrielles.

► Fraude et malveillance (hors cyber attaques)

Quel coût ?

Pour une PME de 20 M€ de CA, une garantie de 150 000 € coûtera entre 2 000 € / 4 000 € et pourra être intégrée en garantie complémentaire dans un contrat d'Assurance RCMS.

En cas de fraude (création de fournisseurs imaginaires, fausses factures, virements frauduleux,...), l'entreprise peut se couvrir avec un contrat d'assurance adapté. Concrètement, l'entreprise se protège contre tout acte frauduleux et malveillant, commis à l'encontre de ses valeurs, biens et documents, y compris les données informatiques. Les coûts indirects de la fraude sont également pris en charge : les intérêts débiteurs facturés, les intérêts créditeurs non perçus, les frais de recours et d'expert, la gestion de crise et l'atteinte à la réputation.

2.2 Les risques non assurables

Certains risques sont non assurables car ils ne répondent pas aux caractéristiques techniques de l'assurance. En effet, les assureurs ne s'engagent pas sur ces risques du fait notamment :

- d'une insuffisance de données statistiques,

Quelques mesures de prévention des fraudes aux virements. Il peut s'agir d'une fraude par détournement des règlements fournisseurs / bailleurs (fraude simple, commise par un tiers ciblant la fonction financière ou comptable d'une société) ou d'une fraude par usurpation d'identité des employés de vos banques partenaires (comme dans le cadre des « escroquerie au Faux président »).

Quelques règles de bonnes pratiques pour vous protéger de ces fraudes :

- en cas d'appel, se renseigner sur l'identité de son interlocuteur en lui demandant des informations précises (nom, prénom, numéro de téléphone) ;
- procéder ensuite par contre-appel de préférence en appelant un numéro de ligne fixe au lieu d'un portable. En cas de doute, demander un écrit de confirmation et les coordonnées téléphoniques ;
- vérifier les renseignements reçus et s'interroger sur la criticité des informations demandées ;
- en cas de changement de références bancaires de vos fournisseurs / bailleurs reçues par courrier, mail ou fax, procéder également à un contre appel ;
- ne jamais communiquer, même auprès de sa banque ou de son fournisseur / bailleur habituel, identifiant, mot de passe, code d'accès par email, téléphone ou sur un site internet. Ils pourraient servir à l'établissement de faux courriers portant mention de vos codes de référencement par exemple ;
- en cas de demande de test des systèmes de virement par télétransmission, ne pas effectuer de tests sur des comptes communiqués par un tiers. Le système EBICTS contient une relation test avec chacune des banques référencées dans le logiciel comptable ;
- contacter votre banque et toujours votre fournisseur/bailleur en cas de demande d'opérations bancaires ou de changement de coordonnées bancaires,

En amont il est recommandé :

- la mise en place d'une procédure de vérification/validation auprès de tiers de confiance identifiés auprès du fournisseur/bailleur ou de votre banque (responsable commercial, direction financière ou chargé de clientèle de la banque) ;
- la mise en place d'une procédure imposant à votre banque de vous alerter en cas de changement de coordonnées bancaires de vos fournisseurs/bailleurs, même lorsque ce changement a été adressé à la banque par un membre de votre entreprise.

L'annexe 1 vous présente des exemples concrets de cas de fraude avec les recommandations en terme de prévention et de solution assurancielles possibles.

- d'une interdiction légale de les assurer (amendes),
- de l'impossibilité de mutualiser le risque comme certains risques émergents tels que le terrorisme,
- d'absence d'aléa.

2.3 Quelques erreurs à ne pas commettre

L'expérience d'un Conseil d'administration est évidemment celle de ses membres. L'administrateur indépendant est l'un d'entre eux.

Les expériences les plus fortes viennent souvent d'erreurs commises, surmontées puis analysées ; elles rendront le Conseil attentifs aux pièges et motiveront son questionnement.

► Les pièges du comportement facteurs de risques

a) la prévision

L'Entrepreneur a confiance en lui, faute de quoi, il ne serait pas entrepreneur. Mais en termes de prévisions, le piège est l'optimisme et la trop grande confiance.

La grande majorité des business plan s'avèrent trop optimistes sur leurs parties recettes, et ne comportent pas souvent de plans alternatifs crédibles.

b) Le statu quo

Le piège de ne pas étudier la modification de ce qui marche bien. Le statu quo est l'expression d'une vision statique d'un système et peut s'analyser comme tous les actifs : plus le temps passe, plus la dépréciation s'accélère.

c) La persistance dans l'erreur

Le piège de ne pas savoir mettre fin aux projets pour sauver coûte que coûte le projet initial au lieu de s'adapter et changer en acceptant une perte.

d) L'instinct grégaire

La peur d'être le seul à commettre une erreur. Ne vaut-il pas mieux se tromper avec tout le monde ?

e) Les faux consensus

Quoi de plus rassurant que les opinions ou les faits bien choisis qui confortent nos idées ?

3 Rôle de l'administrateur indépendant

« Prévenir plutôt que guérir » est simple à dire mais l'art de l'anticipation n'est pas simple en entreprise. Sa bonne pratique va éliminer un certain nombre de risques.

Apprendre à détecter et à interpréter des signaux faibles suppose bien plus d'expérience que la lecture et la compréhension de chiffres, de reportings, qui de toutes façons traduisent un passé et non un futur.

C'est pourquoi la loi a fait du devoir d'anticipation un des rôles fondamentaux du Conseil d'administration. Le rôle de vigie de l'administrateur indépendant prend alors tout son sens.

L'administrateur indépendant, en collaboration totale avec les dirigeants de l'entreprise, doit avoir ce rôle de vigie et donc :

- insuffler cette posture anticipative de la gestion des risques dans l'entreprise.
- anticiper – c'est-à-dire éviter de se laisser surprendre et se donner le temps nécessaire pour adapter les fonctionnalités de l'entreprise à son environnement et à ses mutations internes – est à la fois l'une des premières préoccupations du chef d'entreprise et à la fois celle qu'il peut le moins bien traiter car :
 - il est accaparé par le quotidien des opérations
 - il n'a pas le temps matériel de collecter et de vérifier personnellement l'information.

Interpréter et analyser des éléments d'appréciation pouvant conduire à des décisions très lourdes de conséquences :

- Faire réaliser une cartographie, une hiérarchisation des risques et un plan d'action (surveillance, création de procédures d'urgence et de scénarii...), pour en minimiser les impacts. Il s'appuie sur la parfaite connaissance des dirigeants de leur entreprise, de son environnement, de sa vulnérabilité.
- Veiller à faire actualiser régulièrement la démarche. Son travail s'inscrit autant dans la durée (détection de nouveaux risques) que dans le temps court de la gestion de crise. Cela peut également impliquer des actions d'améliorations continues (organisation, pratiques, infrastructures, procédures de gestion de crise,...). La gestion des risques est un processus itératif qui évolue en fonction des nouvelles activités, de la conjoncture, des réorganisations. Cette démarche doit être portée au plus haut niveau de l'entreprise et efficacement relayée par le management et les opérationnels acteurs essentiels dans l'identification des risques, et qui ne doivent pas pour autant renoncer à l'audace et à l'envie d'entreprendre.

La stratégie est l'art de prendre des risques. Pour autant, l'analyse des risques ne doit pas entraver – mais peut-être uniquement aider à orienter – la décision stratégique. La grande difficulté est de hiérarchiser ces questions, pour éviter de se faire peur en permanence ou de se perdre en conjectures inutiles.

C'est au Conseil d'administration de trouver le juste milieu et de proposer une démarche d'anticipation et de connaissance des risques adaptée.

Un Conseil d'administration doit être capable de construire ses propres convictions sur un sujet, dès lors que la sécurité et le devenir de l'entreprise sont en jeu.

Pour y parvenir, il lui faudra aussi rencontrer des acteurs qu'il n'est pas habituel pour ses membres de rencontrer.

Le chef d'entreprise devra l'accepter et le faciliter, le Conseil respectant, bien sûr, une totale non-ingérence. Il lui faudra identifier les sources d'information et les recouper entre elles, confronter les points de vue du dirigeant et de son comité de direction, des clients (qui exprimeront leurs attentes), des fournisseurs (qui parleront des concurrents), des concurrents (qui exprimeront leurs doléances et leurs visions du futur), d'organismes extérieurs, du commissaire aux comptes qui aura un regard différent et intéressant.

Il est de bonne pratique que le commissaire aux comptes envoie au chef d'entreprise une « Lettre au Management » rédigée à l'issue de sa mission récapitulant les risques qu'il a identifiés. Les Administrateurs peuvent s'enquérir de l'existence d'une telle lettre et en demander une copie au chef d'entreprise.

Un administrateur doit pouvoir connaître et qualifier la façon dont le dirigeant gère ses relations avec ses actionnaires, ses administrateurs, son commissaire aux comptes, les représentants du personnel et les organes du dialogue social, l'ensemble du personnel, son comité de direction, ses banquiers... surtout pas pour juger la façon dont il s'y prend mais pour mieux cerner sa personnalité et mieux comprendre son regard et éventuellement détecter des difficultés à venir.

C'est ainsi que le Conseil pourra, par exemple, aider :

- un chef d'entreprise déterminé et persévérant à s'arrêter plutôt qu'à chercher à sauver coûte que coûte un projet auquel il croyait beaucoup,
- un chef d'entreprise intuitif et visionnaire à ne pas négliger les « détails » car le diable n'est pas dans les bonnes idées mais dans les détails,
- un chef d'entreprise optimiste à prévoir des scénarii de repli,
- un chef d'entreprise qui travaille trop, qui prend trop sur lui, à déléguer.

La présence d'un administrateur indépendant, conscient de cette mission, est une assurance que ces sujets figureront à l'ordre du jour et seront traités par le Conseil d'administration.

Afin d'aider l'administrateur indépendant dans sa démarche, une liste non exhaustive de questions pouvant être posées au Conseil d'administration pour s'assurer d'une bonne gestion des risques au sein de l'entreprise est proposée en Annexe 3.

Conclusion

Le vent, pour le capitaine d'un voilier est synonyme de risque lorsqu'il se déchaîne, lorsqu'il pousse vers les écueils et le naufrage. Néanmoins, maîtrisé, géré, le vent peut également être l'allié qui permet au bon marin d'arriver à bon port sur la route choisie. Fortune de mer, fortune aléatoire !

Il en est de même pour le dirigeant d'une entreprise et son Conseil d'administration.

Pour l'heure, que les risques soient simplement opérationnels ou qu'ils soient stratégiques, que les risques soient assurables ou ne le soient pas, que les risques soient assurés ou non, par tous les moyens dont il dispose ou par tous les moyens qu'il est en droit de réclamer, l'administrateur a une obligation légale de s'impliquer dans la gestion des risques encourus aussi bien par l'entreprise elle-même que par son environnement, son personnel, ses fournisseurs, ses clients et/ou tout ce qu'il est convenu d'appeler les « parties prenantes ».

En veillant à l'actualisation de la cartographie des risques et en associant à une évaluation systématique de la criticité de chacun de ces risques, l'administrateur contribue ainsi à la création de valeur, objet de toute entreprise, en tentant d'éliminer, ou à tout le moins de minimiser toutes les sources incertaines susceptibles de porter atteinte à cette valeur.

Ainsi, pour tous les risques assurables, l'administrateur doit par exemple vérifier que sont sollicitées des évaluations externes, concurrentes des assureurs en place, par des courtiers généralistes ou spécialisés, afin de vérifier la qualité des couvertures mises en œuvre et des moyens mis en place par l'entreprise pour en minimiser les coûts. Il doit aussi sensibiliser le dirigeant sur « l'aléa moral » : sous prétexte de couvertures efficaces, ou supposées telles, des comportements anormaux ne doivent pas apparaître.

La perception et l'analyse fine des risques impliquent une connaissance poussée de l'entreprise à tous les niveaux hiérarchiques, dans tous les services ou départements, ainsi qu'une appréhension précise des processus de travail, de décisions, d'informations ou tout autre. L'administrateur qui entend se saisir de la question des risques, i.e. de leur existence et de leur prévention, satisfait ainsi à son obligation légale de « se saisir de toute question relative à la bonne marche de l'entreprise et régler par les débats qu'il suscite les affaires la concernant ».

La liberté de l'administrateur indépendant permet de questionner, de « challenger » les dirigeants de l'entreprise sur les risques, leurs qualifications, leurs évaluations statistiques et la quantification des conséquences.

Dans l'avenir, les systèmes d'assurances et de couvertures des risques, du fait de l'augmentation exponentielle du nombre de données « Big Data » et à raison de leur instantanéité, vont concerner de nouveaux espaces encore méconnus. En dotant l'entreprise de systèmes efficaces de traitement de ces données, le dirigeant et son Conseil d'administration auront une meilleure maîtrise statistique et financière, donc stratégique, en réduisant la dépendance de l'entreprise aux risques et aléas de son univers. En contribuant à introduire une rationalité croissante dans les processus de décisions, les dirigeants entreprendront progressivement dans un mode de décision prédictif au lieu de subir et d'être le plus souvent dans un mode décision réactif.

Ce cahier peut être résumé en Latin en deux mots : « *praemonitus, praemunitus* », traduit simplement ainsi « prévenu, pré-muni ». La forme latine était une des devises de Francis Drake, mais aussi celle de corps d'armées US ou britanniques, et se traduit en Anglais par « *forewarned, forearmed* », nettement plus offensif !

Annexes

Annexe 1 : Exemples de cas de fraude

Cas de Fraude	Comment s'en prémunir	Réponse Assurance
<i>Falsification de moyens de paiement (chèques, virements) : imitation de la signature du PDG par le comptable historique de la société.</i>	<i>Confier à 3 personnes différentes les fonctions d'enregistrement, de décaissements, de préparation des chèques et traites, et de rapprochements comptables et bancaires. La règle de la double signature doit être pratiquée pour tout paiement supérieur à 5 000 €.</i>	<i>Les pertes sont garanties sous réserve que l'auteur ne soit pas un dirigeant.</i>
<i>Surfacturation : un acheteur se livre à un petit trafic avec des fournisseurs de produits moyennant des commissions en liquide.</i>	<i>Etablir des rapprochements entre les adresses de livraison, les fichiers fournisseurs et les adresses des salariés. Edicter des règles claires de sélection et de suivi des fournisseurs</i>	<i>Les pertes sont garanties sous réserve d'établir l'existence des commissions pour démontrer l'enrichissement de l'employé.</i>
<i>Création de fournisseurs fictifs : une comptable crée des fausses factures au bénéfice de fausses sociétés en collusion avec son conjoint.</i>	<i>Sensibiliser les employés sur les risques de fraude et organiser le classement des documents sensibles.</i>	<i>Les pertes sont garanties sous réserve de démontrer l'enrichissement de l'employé et/ou de son conjoint.</i>
<i>Virement externe frauduleux : fabrication d'un faux ordre de virement après le vol d'une photocopie d'ordre.</i>	<i>Définir avec son banquier des clés secrètes de confirmation d'ordre.</i>	<i>Si la fraude a été commise directement auprès de la banque celle-ci en sera seule responsable et éventuellement fera intervenir son propre assureur. Si en revanche l'auteur est un employé de l'entreprise, le contrat souscrit par celle-ci a vocation à s'appliquer, et ceci même si la responsabilité de la banque peut être engagée, l'assureur conservant un recours à l'encontre de cette dernière.</i>

Annexe 2 : Exemples de risques non assurables

Quelques exemples de risques non assurables	Commentaires
Perte de profits par le biais de la concurrence.	L'entreprise ne peut pas assurer ses chances de gagner ou de perdre dans une compétition commerciale.
Lancement d'un nouveau produit.	Une entreprise qui lance un nouveau produit ne peut pas assurer les chances d'acceptation du nouveau produit puisqu'il n'a pas été testé sur le marché. Il est toutefois possible de s'assurer sur les pertes d'exploitations consécutives à un évènement tel que la destruction des stocks empêchant la commercialisation du bien.
Perte subie à la suite d'une gestion mauvaise et/ou inefficace.	La capacité de gérer avec succès une organisation dépend de nombreux facteurs et le profit ou la perte dépend de l'utilisation judicieuse de ces facteurs, dont un est la capacité de gestion efficace. La perte attendue dans une organisation par suite de l'inefficacité ne peut pas être assurée. Le dirigeant peut en outre en être personnellement comptable.
Perte de profit, à la suite de la chute de la demande	La demande de tout produit varie avec le temps et d'autres facteurs. Un assureur n'assurera jamais la perte prévue due à la diminution de la demande. Les contrats prévoient en outre souvent l'exclusion des conséquences de la perte de clientèle.
Fournisseur unique	L'histoire, le savoir-faire spécifique d'un fournisseur, l'absence d'analyse des risques peuvent conduire à des situations de dépendances critiques vis-à-vis de fournisseurs uniques ou prépondérants (dépendance sur les prix, défaillances financières, logistiques ou qualitatives). S'en prémunir nécessite de conduire ou faire conduire par les services achats une veille détaillée et permanente de cette potentielle dépendance et d'établir des scénarios d'évitement ou de sécurisation.
Changement réglementaire	Le risque de changement réglementaire ne cesse de s'accroître du fait de la complexité croissante des exigences de conformité (réglementation du travail, directives de l'Union Européenne (EU) la législation environnementale, ...). Néanmoins, la réglementation est fondamentale pour protéger les intérêts des entreprises, et son évolution peut avoir un impact positif sur l'activité si elle est gérée efficacement (procédures commerciales plus efficaces, anticipation des changements réglementaires à venir, ...).
Risque d'entente	Le risque d'entente entre entreprises est certainement l'un des plus importants de par son impact financier potentiellement très lourd pour l'entreprise accusée d'avoir enfreint les règles de la concurrence, mais aussi par son impact négatif sur la réputation et donc l'image de l'entreprise. L'entente sur les prix par action concertée de plusieurs entreprises sur leurs tarifs est certainement l'une des plus sanctionnées financièrement, en France comme en Europe, mais aussi la plus médiatisée. La sanction pécuniaire que l'Autorité peut être amenée à prononcer est calculée selon l'importance des dommages causés à l'économie et après analyse de la situation de l'entreprise ou du groupe auquel elle appartient. Le maximum légal est 10% du chiffre d'affaire mondial total de l'entreprise ou du groupe auquel elle appartient. Exemple d'entente dans les produits d'entretien : L'autorité de la concurrence a annoncé en décembre 2014 qu'elle allait infliger pour 345 M€ d'amendes à plusieurs fabricants de produits d'entretien pour avoir coordonnés leurs politiques commerciales auprès de la grande distribution et s'être concertés sur les hausses de prix entre 2003 et 2006.
Perte de chance	La perte de chance due à une erreur d'un tiers n'est généralement pas bien assurée, elle est stratégique et ne se résume pas à la perte d'exploitation. Le nom mal choisi d'un nouveau produit malgré l'intervention d'un cabinet spécialisé, idem pour un défaut de dépôt de brevet ou de marque, essentiellement hors des frontières nationales, un fichier client obsolète bien qu'acheté très cher, une publicité mal comprise, voilà quelques exemples inassurables. Au surplus, la perte de chance est très souvent improuvable devant un tribunal faute d'historique, en particulier pour les produits nouveaux.

Annexe 3 : Check list de questions aux membres du Conseil

L'administrateur pourra s'appuyer sur les questions suivantes pour structurer les discussions sur l'évaluation du système de gestion des risques (= « rôle de l'administrateur » cf. cahier 2 de APIA) :

1) Sur la stratégie en matière de risques :

- quels sont les risques inhérents à la stratégie et aux objectifs de l'activité ?
- la politique de gestion des risques est-elle communiquée de manière claire au sein de l'entreprise ? Si oui, de quelle manière ? Si non, pourquoi ?
- la politique en matière de prise de risques (les risques que l'entreprise est prête à prendre) est-elle définie ?
- les responsabilités en matière de gestion des risques sont-elles clairement établies ? Comment est réparti « l'univers des risques » entre les différents managers de l'entreprise ?
- existe-t-il un comité d'audit interne ? Qui en fait partie ?

2) Sur le pilotage :

- des systèmes de mesure et de contrôle des risques ont-ils été mis en place ?

- quand le Conseil a-t-il été pour la dernière fois informé sur les risques significatifs ?

- de quelle manière les présomptions de réalisation de risques sont-elles transmises aux responsables désignés ?
- de quelle manière le système de gestion des risques est-il lié au système d'assurance de l'entité ?

3) Sur le recensement des risques :

- existe-t-il une cartographie des risques ?
- si oui, qu'en est-il des risques opérationnels, de réputation, réglementaires ou contractuels, financiers, informatiques, ...
- existe-t-il un système de détection des risques émergents ? Quels nouveaux risques pourraient apparaître (nouveaux concurrents, modèles d'activité, récession, politiques et pénaux, sous-traitance, catastrophes) ?
- un « scénario du pire » pouvant affecter l'entreprise a-t-il été envisagé ?

Ont participé à l'élaboration de ce Cahier APIA

APIA

31bis-33 rue Daru - 75008 Paris
Tél. 01 42 27 05 91
Site : www.apia.asso.fr
Contact : contact@apia.asso.fr

Créée fin 2003, APIA est une association dont l'objectif est de promouvoir et de professionnaliser la fonction d'administrateur d'entreprises.

Initiée par un groupe de dirigeants d'entreprises de taille moyenne, APIA s'est élargie depuis à d'autres dirigeants et à de nombreux partenaires, experts reconnus des métiers proches de l'entreprise.

Les membres et les partenaires travaillent ensemble sur des thèmes liés aux fonctions et responsabilités des administrateurs pour enrichir leur pratique professionnelle, mieux aider les chefs d'entreprises et contribuer à la pérennité et au développement de celles-ci.

GROUPE SATEC

24 rue Cambacérés 75008 Paris
Tel. +33 (0)1 42 80 81 02
Site : www.satecassur.com

Contacts : Pierre Le Morzadec - lemorzadec@groupe-satec.com - + 33 6 45 74 04 34

Le Groupe SATEC, 10^{ème} courtier d'assurance, décline une large gamme de produits d'assurance. Son savoir-faire lui permet de concevoir différents programmes d'assurance sur mesure, tant dans le domaine affinitaire que sur les risques d'entreprise.

Nous accompagnons nos clients en France et à l'international dans le choix des solutions les plus adaptées pour protéger leurs activités ainsi que leurs salariés : Dommages aux biens (bâtiments, matériels, stocks...) et pertes d'exploitation, Responsabilité civile, Flotte automobile Risque client, Marchandises transportées, Fraude, malveillance, Construction, Collectives, prévoyance et retraite,

Le Groupe SATEC a ainsi su gagner la confiance de nombreuses entreprises et organisations dans des secteurs aussi variés que l'automobile, le médical, la construction, l'immobilier, le luxe, le monde associatif et sportif, la grande distribution et la distribution spécialisée, les institutionnels et les collectivités.

Le groupe représente un chiffre d'affaires de 40M€ et compte près de 300 collaborateurs.

SIACI SAINT HONORE

18, rue de Courcelles 75008 Paris
Tel. + 33 (0)1 44 20 94 53
Site : www.s2hgroup.com

Contact : Mickaël ROBART - Département Lignes Financières - mickael.robart@s2hgroup.com

Un des leaders français du courtage et du conseil en assurance, accompagne les grandes entreprises et les ETI dans le management de leurs risques en assurances de biens et de personnes en France et à l'international. Le Groupe conçoit et développe pour ses entreprises clientes des solutions sur-mesure en IARD, Transport, Mobilité internationale, Protection sociale, Retraite, Stratégie RH & Rémunération globale. Les services de SIACI SAINT HONORE couvrent l'ensemble de la chaîne de valeur, du conseil en gestion des risques au pilotage et gestion de programmes d'assurance. Le cabinet compte aujourd'hui près de 1600 collaborateurs à travers le monde, assure 1,3 million de personnes en France et à l'international, et réalise un chiffre d'affaires de 259 millions d'euros en 2014.

LAMY LEXEL Avocats Associés

25 rue de Choiseul - 75002 Paris
Tél. 01 55 27 24 00
Contact : Jérôme Saleur - jsaleur@lamy-lexel.com
91 cours Lafayette - 69455 Lyon cedex 06
Contact : Vincent Médail - vmedail@lamy-lexel.com
Tél. 04 72 74 53 00
www.lamy-lexel.com
Twitter : @LamyLexel

Cabinet d'avocats d'affaires « full services » intervenant en conseil et en contentieux, implanté à Lyon et à Paris, appuyé par les réseaux internationaux PLG International Lawyers et First Law International, LAMY LEXEL est le partenaire des entreprises et des équipes dirigeantes dans la mise en place de leurs projets stratégiques.

Un cabinet pluridisciplinaire de 95 collaborateurs avec des valeurs et une relation client fortes.

Nos avocats allient l'innovation des solutions juridiques à une approche « terrain » portée par leur connaissance de l'environnement économique pour délivrer le conseil le plus approprié : pragmatique, technique, rapide et efficace.

Nos équipes pluridisciplinaires conjuguent leurs expertises pour donner vie aux projets en s'assurant de leur pérennité, en anticipant les risques et en optimisant les process.

Maitriser les risques pour les transformer en opportunités.

Les avocats de LAMY LEXEL sont à même de saisir les enjeux et contraintes des entreprises, d'identifier, auditer et mesurer les risques potentiels, pour proposer des solutions juridiques adaptées. Un développement sécurisé avec une vision patrimoniale long terme, pour que le risque ne soit pas un frein aux ambitions des entreprises...

Les cahiers APIA

Déjà parus :

- **Cahier APIA n°1** : « Quelques conseils en matière d'assurance de la responsabilité des dirigeants et des mandataires sociaux ».
- **Cahier APIA n°2** : « Rôle des administrateurs en matière de contrôle interne et de gestion des risques ».
- **Cahier APIA n°3** : « Un administrateur Indépendant dans les Sociétés par Actions Simplifiées (S.A.S.) ? ».
- **Cahier APIA n°4** : « L'administrateur d'entreprises : un facteur de succès d'une transmission d'entreprise ».
- **Cahier APIA n°5** : « Administrateur et Chef d'Entreprise, une alchimie gagnante ».
- **Cahier APIA n°6** : « Anticiper ! Dépasser l'approche traditionnelle ».
- **Cahier APIA n°7** : « Un administrateur indépendant dans les entreprises patrimoniales ».
Partie 1 : hors cession ou transmission de l'entreprise.
- **Cahier APIA n°8** : « Un administrateur indépendant dans les entreprises patrimoniales ».
Partie 2 : En cas de cession ou transmission de l'entreprise.
- **Cahier APIA n°9** : « Les enjeux de la gouvernance dans les jeunes entreprises en croissance ».
- **Cahier APIA n°10** : « Vous avez dit indépendant ? ».
- **Cahier APIA n°11** : « Les ressources humaines : un facteur stratégique de succès ».
- **Cahier APIA n°12** : « Repères pour la rémunération des Administrateurs Indépendants ».
- **Cahier APIA n°13** : « La logistique et l'Administrateur ».
- **Cahier APIA n°14** : « Les délégations de pouvoirs ».
- **Cahier APIA n°15** : « Les procédures amiables ».
- **Cahier APIA n°16** : « Challenger la stratégie ou pourquoi et comment l'administrateur doit, en permanence, susciter son élaboration ».
- **Cahier APIA n°17** : « Le risque de fraude dans les entreprises : le rôle des administrateurs dans sa prévention ».
- **Cahier APIA n°18** : « Le rôle de l'Administrateur Indépendant dans un processus d'externalisation ».
- **Cahier APIA n°19** : « Apport, dans une PME, d'un Administrateur issu d'une ETI ou d'un grand groupe ? ».
- **Cahier APIA n°20** : « L'Administrateur Indépendant et la Responsabilité Sociétale des Entreprises (RSE) en PME-ETI ».
- **Livre bleu APIA** : « Pour une gouvernance d'entreprise choisie, la réponse d'APIA : l'Administrateur Indépendant ».
- **Cahier APIA n°21** : « Indisponibilité du dirigeant actionnaire, les nouveaux outils pour s'y préparer ».
- **Cahier APIA n°22** : « Développer ou transmettre avec un investisseur financier, Bonnes pratiques pour le dirigeant et l'administrateur ».
- **Cahier APIA n°23** : « Le risque de sanctions pour le dirigeant et les administrateurs en cas de liquidation judiciaire ».
- **Cahier APIA n°24** : « Comment ouvrir son Conseil à un Administrateur Indépendant ? ».
- **Cahier APIA n°25** : « Inscrire l'innovation dans l'ADN de l'entreprise ».
- **Cahier APIA n°26** : « Gouvernance et rupture numérique, opportunité stratégique et risque majeur : c'est un sujet de gouvernance ».
- **Cahier APIA n°27** : « Le rôle de l'administrateur indépendant dans la gestion du risque ».
- **Cahier APIA n°28** : « Auto-évaluation des Conseils ».

Sur simple demande à : contact@apia.asso.fr