PME et ETI : la gestion des risques est aussi pour vous !

Préface

La prise de risque est inhérente à la démarche entrepreneuriale. Les chefs d'entreprise de PME-ETI le savent bien ! Ils en gèrent quotidiennement, dans un maelstrom d'urgences qui les empêche généralement de construire une stratégie de gestion des risques et, plus encore, de la réinterroger régulièrement : manque de temps, absence de collaborateur dédié, sous-estimation pensant que cela n'arrive qu'aux autres, mauvaise hiérarchisation des risques… Les priorités vont bien évidemment au développement de l'activité et l'analyse des risques est renvoyée à une période plus calme qui n'arrive, en réalité, jamais. La prise de conscience peut n'apparaître que lors de l'entrée d'investisseurs ou après une « catastrophe », dont l'impact ébranle la croissance de l'entreprise voire met en cause sa survie.

Pourtant, les retours d'expériences de dirigeants ayant investi dans la mise en place de tels dispositifs démontrent les avantages réels obtenus, en termes de pilotage stratégique, d'anticipation, de meilleure allocation des ressources, d'un dialogue plus construit avec ses parties prenantes…

La gestion des risques protège et renforce au final la valeur de l'entreprise et, corrélativement, celle du patrimoine personnel investi. C'est tout l'enjeu : sécuriser la prise de décision et la mise en œuvre de la stratégie par une vision partagée et rationnalisée.

Ainsi, développer une stratégie de gestion des risques est bien un outil d'aide au pilotage et est source de création de valeurs dans les PME-ETI ; mais elle nécessite une méthodologie adaptée à leurs spécificités et notamment aux moyens que les dirigeants peuvent allouer à cette démarche.

C'est pourquoi le Medef Deux-Sèvres et l'AMRAE proposent ce guide méthodologique ; c'est un outil de sensibilisation et d'appui au déploiement d'une stratégie de gestion des risques. Son ambition est de convaincre les dirigeants de PME-ETI de l'intérêt de s'engager dans une telle aventure.

Élaboré avec des chefs d'entreprises, il est pragmatique et concret et présente tant les facteurs de succès que des outils d'analyse adaptés.

La gestion des risques renforce certainement l'art de prendre des risques, mais en toute intelligence et conscience : c'est bien un sujet majeur pour les dirigeants de PME-ETI !

Brigitte Bouquot
Présidente de l'AMRAE

Paul-François Arrighi
Président du Medef Deux-Sèvres

Les auteurs

Coordinateurs :

Hélène Dubillot, directrice de la coordination scientifique de l'AMRAE

Xavier Migeot, délégué général du Medef Deux-Sèvres

Contributeurs :

Laurence Jouve, juriste en droit du travail et ressources humaines

Marie-Elise Lorin, responsable de la gestion des risques (SMACL Assurances) et pilote de l'antenne Grand Ouest de l'AMRAE

Pierre Lainé, chargé des affaires économiques et financières (Medef Deux-Sèvres)

Jean-Christophe Rodier, responsable risques et assurances, (Groupe CNIM).

Et les 13 chefs d'entreprise et collaborateurs des Deux-Sèvres ayant participé au groupe de travail : Christine Foulon (Secrétaire général, Darva), Jean-Pierre Barthole (Directeur, Dupont), Pierre Cordier (Directeur général, Groupama Centre Atlantique), Joël Gasnier (Président, C2E), Patrice Labaeye (PDG, Boton Merlet), Bertrand de La Porte du Theil (Président, Doc Emballages), Emery Jacquillat et Laurent Micouin (PDG et RRH, Camif Matelsom), Dominique Pluviaud (Président, Marcireau), Denis Papin (Président, Denis Papin Collectivités), Jean-Claude Rousseau (Président, Rousseau), Philippe Rullier (Président, Rullier) Emmanuel Saux (Président, Favid).

À propos ...

... de l'AMRAE

L'AMRAE (**A**ssociation pour le **M**anagement des **R**isques et des **A**ssurances de l'**E**ntreprise) est l'association professionnelle de référence des métiers du risque et des assurances en entreprise. Elle rassemble plus de 1300 membres appartenant à 700 organisations privées ou publiques.

L'AMRAE aide ces organisations dans l'atteinte de leurs objectifs stratégiques et opérationnels pour leur permettre d'améliorer leurs performances et de maîtriser leurs risques.

AMRAE l'Association rassemble les acteurs majeurs des lignes de maîtrise du risque (Risk Management, contrôle et audit internes, assurance et juridique). A travers ses comités scientifiques, ses publications et ses nombreuses manifestations, l'AMRAE produit pour ces experts les contenus qui nourrissent leurs compétences, leur évolution dans leur métier et leur contribution à la réussite de la stratégie de l'entreprise.

Avec **AMRAE Formation,** elle répond à leurs besoins de formation professionnelle tout au long de la vie en dispensant des formations certifiantes de haut niveau.

AMRAE Les Rencontres organise le congrès annuel de référence des métiers du risque et des assurances (plus de 2800 participants en 2018). Ces trois jours constituent le rendez-vous métier incontournable des acteurs de la maitrise des risques et de son financement.

... du Medef Deux-Sèvres

Le Medef Deux-Sèvres, **1er syndicat patronal**, représente plus de 500 entreprises de toutes tailles – 90 % de TPE-PME – et de tous secteurs d'activités, industrie, services, commerce, BTP..., ainsi que 16 fédérations professionnelles.

Acteur incontournable de la vie économique, le Medef Deux-Sèvres **accompagne ses dirigeants au quotidien** à toutes les étapes de la vie de leur entreprise : droit du travail, économie et finances, accompagnement des entreprises en difficulté, relations avec les pouvoirs publics et parlementaires... Il les représente et les défend aussi dans plus d'une soixantaine d'organismes (Conseils de prud'hommes, Urssaf, CPAM...).

Il est par ailleurs membre fondateur de #FrenchAssurTech, accélérateur de start-up qui associe les grandes mutuelles niortaises et NiortAgglo.

En 2018, le Medef Deux-Sèvres **renforce ses services** auprès de ses adhérents PME et ETI **en déployant le dispositif sur la gestion des risques** présenté dans ce guide.

Sommaire

TRAITEMENT

TROIS POINTS DE VIGILANCE

ANNEXES

AVANTAGES

I. Les avantages de la démarche « gestion des risques » pour les PME-ETI

Définition :

Le risque est défini par la norme ISO 31000 comme l'effet de l'incertitude sur les objectifs. La gestion des risques vise donc à réduire les menaces qui pèsent sur l'atteinte des objectifs opérationnels, stratégiques de l'entreprise.

Entreprendre, c'est prendre des risques consciemment.

Au-delà d'une formalité de respect de la conformité et de la réglementation, piloter son activité par les risques permet d'avoir un formidable outil d'aide à la décision, de se concentrer sur les réalisations les plus importantes pour l'entreprise, de mieux allouer les ressources, gérer les coûts, négocier ses contrats avec les parties prenantes qui sont rassurées par cette maîtrise.

Les principaux avantages habituellement reconnus par les entreprises qui se sont lancées dans la démarche sont :

- **Anticiper les opportunités** par une stratégie construite : analyser et hiérarchiser les risques majeurs avant qu'ils ne surviennent et passer d'une gestion des risques « perçus » à une gestion des risques « réels » ;
- **Piloter avec une plus grande efficience** l'entreprise au quotidien : mettre en place des outils qui rendent visibles des risques qui n'apparaissent pas dans le radar habituel et/ou mieux évaluer les risques déjà connus ;
- **Identifier des risques émergents** et leur impact sur l'entreprise (pandémie, nouveaux types de fraude, bouleversements issus de la révolution technologique en cours…) ;
- **Se préparer en engageant des plans préventifs,** à un coût souvent moins élevé que les plans de traitement. Maîtriser les enjeux financiers et mieux allouer les ressources ;
- **Disposer d'un outil de management** impliquant et mobilisant ses équipes ;
- **Renforcer le dialogue constructif avec ses instances de gouvernance,** son commissaire aux comptes… ;
- **Renforcer sa capacité de négociation** avec ses parties prenantes, notamment les institutions financières, qui apprécient l'approche par les risques ;
- **Valoriser le pilotage de l'entreprise auprès des tiers** et mieux négocier les conditions partenariales (conseils, courtiers, financeurs, investisseurs, assureurs…) ;
- **Alimenter sa stratégie RSE** (responsabilité sociale des entreprises) ;
- **Avoir une longueur d'avance :** anticiper pour chercher des solutions innovantes vers les partenaires. Valoriser son entreprise en cas de cession de l'entreprise.

Les PME-ETI, du fait de leur taille et de l'élan qui les animent, sont souvent naturellement mieux armées que les grandes entreprises pour faire face à l'inconnu. Elles ont plus d'agilité pour mener des actions correctives et adapter leur offre. En termes d'organisation, leur souplesse leur permet de réagir efficacement en situation de crise : les collaborateurs se connaissent mieux et l'information circule plus rapidement.

Tout en se caractérisant par cette faculté d'adaptation et de réactivité, les PME-ETI connaissent une plus grande vulnérabilité, ayant une surface financière plus réduite que celle des grandes entreprises et une structure plus fragile. **Leur survie peut donc être engagée très rapidement. C'est tout l'intérêt de mettre en place une gestion des risques.**

PAROLES DE

CHEFS D'ENTREPRISE DU MEDEF DEUX-SÈVRES

« Où sera mon entreprise dans 3-5 ans si je n'ai pas de stratégie de gestion des risques ? »

« À la recherche d'un outil permettant de gérer les risques et de ne pas les subir. »

« Nécessité de bâtir une stratégie pour ne pas disparaître face à des ruptures structurelles. »

« Repérer les risques, les anticiper, mettre en place une stratégie de contre pour limiter les menaces sur mon entreprise. »

« Après les risques chimiques qui sont mes risques majeurs, je sens qu'il faut que j'ai un vision 360° de tous les risques auxquels je peux être confronté. »

« J'ai été confronté à des risques export, à des risques sanitaires. Mais je suis bien conscient que je suis aussi confronté à d'autres risques que je maîtrise moins car je n'en ai pas mesuré l'impact et l'occurrence. »

« J'ai subi un cyber risque : une bonne entrée en matière pour se dire qu'une stratégie de gestion des risques est indispensable et qu'il faut prendre le temps de s'en préoccuper en amont ! »

« Je suis convaincu que le risque est au cœur de la création de valeurs. »

« Comment instiller constamment une culture des risques et une politique de prévention efficace au sein de mon entreprise, et *auprès de tous mes collaborateurs ? »*

PAROLES DE

GESTIONNAIRES DE RISQUES

« La démarche de gestion des risques est un formidable outil de pilotage des risques majeurs et prioritaires de l'entreprise. Elle est également le meilleur moyen d'implémenter la culture du risque (maîtrisé) dans l'entreprise. Le rôle moteur de la direction et la transversalité permettent d'impliquer efficacement et concrètement l'ensemble des forces vives de l'organisation, afin de devenir un projet global d'entreprise à la fois permanent et évolutif. C'est une méthode essentielle pour être en mesure de déterminer les risques majeurs, les évaluer/quantifier et les prioriser.

C'est donc une aide précieuse à la prise de décision sur les sujets essentiels et/ou structurants de l'entreprise. »

Jean-Christophe Rodier, responsable risques et assurances, Groupe CNIM

« Il y a quelques années, ma direction a souhaité mettre en place une organisation permettant de mieux maîtriser les risques liés à notre activité, caractérisée par une forte croissance et des exigences de plus en plus fortes provenant de notre environnement.

Mon poste de manager de risques a été créé pour répondre à ce besoin. L'objectif, bien entendu, n'était pas d'arrêter de prendre des risques. Bien au contraire : nous devions continuer à en prendre, mais de façon consciente, partagée et mieux maîtrisée.

Dans les mois qui ont suivi, nous avons réalisé une cartographie des risques majeurs de notre groupe en impliquant très fortement le top management et le directoire mais aussi les directions opérationnelles. Après cette 1ère phase, nous avons mis en place une organisation qui permette de travailler sur les risques prioritaires en termes d'enjeux. Nous avons nommé pour cela des propriétaires de risques. Ce sont généralement des managers opérationnels de haut niveau capables de faire travailler de façon transversale des équipes de différents départements. Leur rôle est de définir, mettre en œuvre et piloter des plans d'action sur les risques dont ils ont la responsabilité.

Aujourd'hui, l'investissement des propriétaires de risques dans les plans d'actions est un facteur clé de succès et constitue le socle de notre dispositif. Le manager de risques se positionne comme un fédérateur, garant de la cohérence des démarches mises en œuvre et de l'avancement des travaux.

Il a également pour rôle majeur de diffuser une culture de gestion des risques dans l'entreprise *via* de la formation ou de l'assistance aux opérationnels. »

Max Giumelli, manager de risques d'un groupe pharmaceutique (ETI)

VOS OBJECTIFS, EN SYNTHÈSE

BASIQUES

II. Les basiques de la démarche de gestion des risques

1. Les grandes étapes

La gestion des risques visant à réduire les menaces qui pèsent sur les objectifs que se fixent les entreprises, il faut, dans une première étape, bien définir ses objectifs pour bien identifier ses risques, les deux étant intrinsèquement liés.

1) Formaliser et partager la connaissance des objectifs, de la stratégie, avec l'équipe dirigeante, même *a minima*, est utile dès le début

Toute l'équipe sera ainsi mobilisée sur les mêmes points d'attention, en particulier la place de l'entreprise dans sa filière. Elle a de plus en plus d'interactions avec l'ensemble des parties prenantes (clients, fournisseurs, sous-traitants…), renforcées si elle travaille à l'international (filiale, exportations…). Un risque majeur frappant l'entreprise peut aujourd'hui nuire à toute la filière, par un effet de ricochet.

2) Construire son « univers des risques »

L'univers des risques désigne l'ensemble des risques, quelle que soit leur nature, à laquelle une entreprise peut être exposée et susceptibles de porter atteinte à la réalisation de ses objectifs et enjeux. Il est spécifique à une organisation car intrinsèquement attaché à sa culture, ses traditions, son organisation, ses valeurs, son écosystème et sa filière. Les principales catégories de risques à prendre en considération sont :

- les risques stratégiques et les risques externes, parmi lesquels ceux liés à la concurrence, à la RSE, les risques pays, les risques de discontinuité des opérations ou de réputation ;
- les risques opérationnels, comme les risques fournisseurs, les risques clients, les risques de supply-chain ou les risques liés aux bâtiments ;
- les risques supports, par exemple liés aux ressources humaines ou au système d'information, les risques juridiques, de non-conformité, financiers…

Ces catégories ne sont pas rigides. Elles sont à adapter au contexte de chaque entreprise (cf. l'univers de risques proposé pour les PME-ETI en partie III).

3) Cartographier et traiter les risques

A partir de cet univers pourra être réalisée et retravaillée régulièrement une **cartographie des risques**, représentation visuelle des risques et de leur positionnement sur une échelle impact / probabilité de survenance ou impact / maîtrise interne. Elle pourra être partagée par l'équipe dirigeante et sera un véritable outil de pilotage au service du dirigeant pour gérer son activité efficacement par les risques et les plans d'actions associés. C'est un document qui peut facilement remplacer de longs rapports, synthétiser les actions prioritaires sur l'ensemble de l'organisation et faire gagner un temps précieux au dirigeant.

Principes généraux de gestion des risques (GUIDE AMF 2010) – Définition

La gestion des risques est l'affaire de ***tous les acteurs de la société.*** *Elle vise à être* ***globale*** *et doit couvrir l'ensemble des activités, processus et actifs de la société.*

La gestion des risques est un ***dispositif dynamique*** *de la société, défini et mis en œuvre sous sa responsabilité.*

La gestion des risques comprend un ensemble de moyens, de comportements, de procédures et d'actions adaptés aux caractéristiques de chaque société qui permet aux dirigeants de maintenir les risques à un niveau acceptable pour la société.

Le risque représente la possibilité qu'un événement survienne et dont les conséquences seraient ***susceptibles d'affecter les personnes, les actifs, l'environnement, les objectifs de la société ou sa réputation.***

2. À quel moment se lancer?

Avant de vous lancer

Le chef d'entreprise doit être prêt vis à vis de lui-même, puis de tiers :

- à une réelle transparence sur la situation actuelle de l'entreprise et sa vision stratégique du devenir de son activité ;
- à une remise en cause éventuelle de son fonctionnement d'entreprise ;
- à un vrai partage avec son équipe de direction autour de ce sujet, pour plus de performance.

LE BON TIMING

IL FAUT TROUVER LE BON MOMENT ET LE BON RYTHME POUR ENGAGER LA DÉMARCHE.

LA BONNE PÉRIODE

La démarche de gestion des risques demandant un réel investissement collectif, il est important que chaque entreprise et, *a fortiori*, chaque PME, s'interroge quant à la **meilleure période pour engager une telle démarche.** Selon l'activité de l'entreprise, sa saisonnalité et les projets déjà en cours, il sera préférable de reporter la réflexion.

LA DÉCLINAISON STRATÉGIQUE

La déclinaison temporelle du projet peut se faire avec deux indicateurs, pouvant se cumuler :
1- les décisions budgétaires : le plan d'action coïncide avec les budgets sans attendre l'exercice suivant.
2- le plan stratégique de l'entreprise : la maîtrise des risques étant intimement liée à la stratégie, la démarche d'analyse des risques/opportunités et son actualisation, doivent être rythmées par les évolutions du plan stratégique.

UN CALENDRIER SERRÉ

Une fois la période choisie, il conviendra de trouver le rythme compatible avec la vie de l'entreprise : rendre les acteurs suffisamment disponibles pour que la démarche soit approfondie et pertinente mais sans s'étendre trop dans le temps.
Un calendrier "serré" permet de **garder le dynamisme et l'implication** de chaque acteur et évite que les travaux de début de démarche soient obsolètes en fin de démarche.

IL FAUT TROUVER LE BON TIMING, TOUT EN CONSIDÉRANT QUE CERTAINES CIRCONSTANCES PEUVENT DÉCLENCHER LE PROCESSUS OU LE PROVOQUER :

- Après un changement d'organisation (fusion, acquisition, réorganisation...) ;
- Dans un contexte de forte croissance (chiffre d'affaires, géographique...) ;
- En réponse aux attentes réglementaires ;
- Suite à des accidents majeurs ;
- Dans le cadre d'une période de crise...

3. Focus sur l'analyse des risques et la cartographie

La gestion des risques vise à **identifier les principaux événements et situations susceptibles d'affecter de manière significative la réalisation des objectifs de l'entreprise.** Une telle démarche, pour être efficace, n'a donc pas pour objectif d'identifier et de traiter tous les risques mais doit se concentrer sur les risques majeurs. Le risque zéro n'existe pas et la maîtrise totale des risques est une illusion. Il faut aussi garder cela en tête.

3.1 L'esprit de la démarche d'analyse des risques

La gestion des risques doit être conçue comme une démarche collective. Elle permet de décider collégialement des hiérarchisations de risques et des priorités de plans d'actions.

C'est un outil d'aide à la décision. Ce n'est donc pas tant le recensement des risques que leur hiérarchisation, qui permettra l'action. Cette étape est particulièrement importante. Dégager un consensus sur une vision construite de l'entreprise et de ses enjeux par l'équipe de direction et non par le chef d'entreprise seul, permet d'assurer une vraie pertinence à la démarche.

D'une entreprise à l'autre, les choix seront très variables. Le principe fondateur de la démarche est qu'il n'y a pas de bonne ou de mauvaise hiérarchisation. Celle émanant du travail collectif approfondi sera la meilleure. Elle tiendra compte des composantes de l'entreprise, de sa maturité face aux risques, de sa stratégie, de son appétence aux risques (et donc leur acceptation), de son environnement réglementaire, de sa capacité au changement, de sa culture d'amélioration continue, de ses spécificités culturelles, organisationnelles et opérationnelles...

La notion d'appétence aux risques recouvre l'acceptation d'un certain niveau de risque.

Il est essentiel de bien cerner les différences d'appétence aux risques des acteurs de la démarche afin de ne pas aboutir à une hiérarchisation biaisée. En effet, la démarche ayant pour seul objectif d'être un outil d'aide à la décision, il s'agit donc de déterminer les 4/5 axes prioritaires d'action sur lesquels l'entreprise travaillera. Le positionnement de chaque risque sur la cartographie a cette ambition. Mais peu importe, au final, si presque tous les risques sont positionnés en partie verte (forte appétence aux risques) ou tous positionnés en rouge (peu d'appétence aux risques) : des priorités se dégageront tout de même. L'essentiel est qu'il n'y ait pas une appétence non consciente qui viendrait décaler le positionnement de certains risques sur la cartographie et fausser leur hiérarchisation. Il faudra donc aligner l'appétence aux risques des dirigeants avec le plan d'actions qui sera élaboré.

L'appétence ne sera naturellement pas homogène, pour trois raisons :

- on accepte mieux les risques que l'on connaît bien. Ils peuvent même être sous-estimés car considérés comme faisant partie de l'univers habituel dans lequel l'entreprise a toujours su évoluer ;
- on peut sous-estimer les risques que l'on ne connaît pas du tout, dont les enjeux ne sont pas perçus ;
- le dirigeant devra déterminer l'appétence acceptable pour chaque risque selon sa structure et ses valeurs. Ainsi une entreprise pourra déterminer, par exemple, qu'un retour produit pour non-conformité est inacceptable du fait des conséquences financières et d'image qu'il induit, lorsqu'une autre estimera de son côté ce risque acceptable.

L'appétence aux risques influe donc le positionnement des risques. Une réflexion collective au sein de l'entreprise, aux expériences et visions croisées, permettra de mieux discerner les approches individuelles.

De même, il sera pertinent de mesurer son appétence aux risques en s'ouvrant sur l'extérieur. Les orientations de choix stratégiques de maîtrise des risques seront utilement mises en lumière lors de partages d'expériences entre pairs, d'échanges au sein d'un syndicat professionnel, salons professionnels...

La gestion des risques est aussi un outil de management et de mobilisation du collectif de travail par le travail en commun, la vision partagée des contraintes, tant internes qu'externes, les enjeux de chaque service, de chaque composante de la structure.

Le consensus à obtenir permettra une valorisation du collectif, une nouvelle implication de chacun dont les bénéfices dépassent notoirement la démarche de gestion des risques.

3.2 Le processus d'analyse des risques

Le processus d'analyse des risques se décompose en plusieurs étapes, listées ci-dessous.

3.2-1 Identification des risques majeurs

Il s'agit d'identifier, lister, décrire le plus précisément les risques majeurs susceptibles de menacer l'atteinte des objectifs stratégiques. Il faut s'assurer que l'ensemble des acteurs de la démarche utilisent les mêmes mots avec le même sens (collaborateurs bien évidemment, mais aussi assureurs, courtiers...). Il faudra également mettre à jour régulièrement cette liste au regard des objectifs et des enjeux de l'entreprise.

3.2-2 Appréciation/évaluation/hiérarchisation des risques majeurs

L'évaluation d'un risque est la condition fondamentale pour permettre la prise de conscience de ses impacts. L'évaluation de l'impact du risque ou de son coût de survenance est très complexe. En effet, elle intègre toutes ses conséquences, non seulement l'impact matériel immédiat (financièrement calculable) mais également les impacts indirects et/ou immatériels, qui sont plus difficiles à évaluer.

Il s'agit bien de tout ce qui résulte de la survenue de l'événement jusqu'à la restauration de la situation de départ : perte d'image ou de réputation, perte d'exploitation, désorganisation de l'activité…

Cette évaluation doit se caler le plus possible sur une évaluation financière pour objectiver et rendre concrètes les conséquences du risque. La gestion des risques doit permettre ainsi de sécuriser la valeur de l'entreprise et décrire tous les types d'impacts en cas de survenance du risque.

Nous pouvons définir trois étapes :

1 - Construire une échelle de gravité adaptée à l'entreprise, pour aider à calibrer le niveau de gravité en cas de survenance et tenter de quantifier les conséquences humaines, financières, juridiques, perte de clients, perte d'image… (qui peuvent être ramenées en nombre de jours et de K€ perdus).

2 - Les lier à une échelle de fréquence/survenance estimée.

3 - Préciser le niveau de maîtrise actuel ou en cours (plan de prévention, actions de formation, actions de contrôle, audit interne ou externe, capacité de mobilisation rapide des ressources en cas de survenance…).

Ex : Echelle de fréquence. Source « La cartographie : un outil de gestion des risques ». Collection Maîtrise des risques ©AMRAE.

		Description de la réalisation	Réalisation calendaire	Probabilité de réalisation
4	**Quasiment certain**	Événement attendu dans la plupart des cas	Immédiat	> 50 %
3	**Possible**	Événement probable dans la plupart des cas	12 mois	> 20 %
2	**Peu probable**	Événement devant se produire à un moment donné	3 ans	< 10 %
1	**Rare**	Événement risquant de se produire à un moment donné	5 ans	< 10 %

Autre exemple de hiérarchisation et d'évaluation financière des risques : Source « La cartographie : un outil de gestion des risques ». Collection Maîtrise des risques ©AMRAE.

N°	Nom / Description du risque	Estimation du risque		Évaluation du risque	
		Fréquence	Gravité	Fréquence	Gravité
1	Échec à la mise en place du SI de gestion	Moyenne	**Financier** → Fort **Réputation** → Moyen	Moyenne	**Financier** → Fort - Absence de Chiffre d'affaire sur 3 mois = environ 80 M€ **Temps de panne système** → Très fort - incapacité du système à fonctionner pendant 3 jours minimum
2	Entente illicite	Fort	**Financier** → Très fort **Réputation** → Moyen	Fort	**Financier** → Fort - 10 % du CA **Réputation** → Moyen
3	Défaillance qualité	Moyenne	**Financier** → Moyen **Réputation** → Moyen	Peu probable	**Financier** → Moyen - CA maxi par produit 10 M€ **Réputation** → Très fort - Crédibilité du groupe basée sur la qualité et la confiance

Ce tableau est en général enrichi :

- des sources ou causes des risques analysés,
- des mesures ou actions décidées pour en assurer la maîtrise,
- de l'évolution des risques constatée à l'issue de la réitération de la démarche.

L'estimation sera complétée ultérieurement par une véritable évaluation. Les méthodes les plus fréquemment utilisées par les entreprises ont été répertoriées dans la publication AMRAE « La cartographie des risques » :

EXTRAITS

Une **méthode qualitative** qui consiste à suivre une échelle décrite et détaillée qui est la résultante d'un travail de groupe et non d'une étude d'expert ou représentative d'une vérité absolue. Il n'y a donc pas de niveau critique de risque universel qui serait identifié par la méthodologie. C'est à chaque entreprise de définir son échelle de risques. C'est une étape importante dans le processus de gestion des risques car elle permet de donner une gravité potentielle à la réalisation d'un risque. Néanmoins, la hiérarchisation des risques est plus importante que leur évaluation. En effet, pour un manager de risques, il est plus urgent de pouvoir communiquer sur les priorités de l'entreprise plutôt que sur une évaluation potentielle « exacte » des risques.

Il existe aussi une autre approche qui n'est pas fondée sur la notion de niveau de risque mais sur celle de **scénarios**. L'impact est alors évalué non par rapport à l'intensité d'un risque spécifique mais par rapport à une corrélation de risques qui, en soi, peuvent être d'une intensité faible ou moyenne mais dont le cumul dans une chaîne de causalité produira un événement critique. Cette méthode est empruntée au secteur des assurances. Elle consiste à estimer le sinistre raisonnablement escomptable (SRE) ou le sinistre maximum possible (SMP) pour choisir les actions à mener.

L'entreprise peut aussi opter pour une **évaluation quantitative** des risques (non détaillée dans le présent ouvrage) qui consiste à utiliser des bases historiques (incidents, sinistres...) pour évaluer d'une manière plus « statistique » les risques de l'organisation. En résumé, cela revient à « se servir du passé pour prévoir l'avenir ».

Dans des cas spécifiques, **l'évaluation « à dire d'experts »** peut aussi être utilisée. Il s'agit d'une évaluation faite par ... des experts. Par exemple, lors de l'évaluation de l'impact d'un tremblement de terre, il peut être utile pour un manager de risques de s'en remettre à l'évaluation d'experts dans ce domaine.

Enfin, le manager de risques peut aussi avoir recours au **modèle « bayésien »***. Les réseaux bayésiens sont un outil d'aide à la décision pour le manager de risques. A travers une représentation graphique des sources du risque, des actions de réductions / de transferts, le manager de risques peut calculer, sur la base de probabilité attachée à chaque élément, l'exposition, la survenance ou la gravité du risque mais également le coût du financement ou de la réduction du risque. Les réseaux bayésiens sont utilisés dans l'analyse de risques mais également dans le diagnostic médical et industriel et dans la détection des spam et de data mining. » cf Réseaux Bayésiens, Eyrolles, 2007, 3eme édition.

Le **théorème de Bayes est un résultat de base en théorie des probabilités.*

3.3 La cartographie

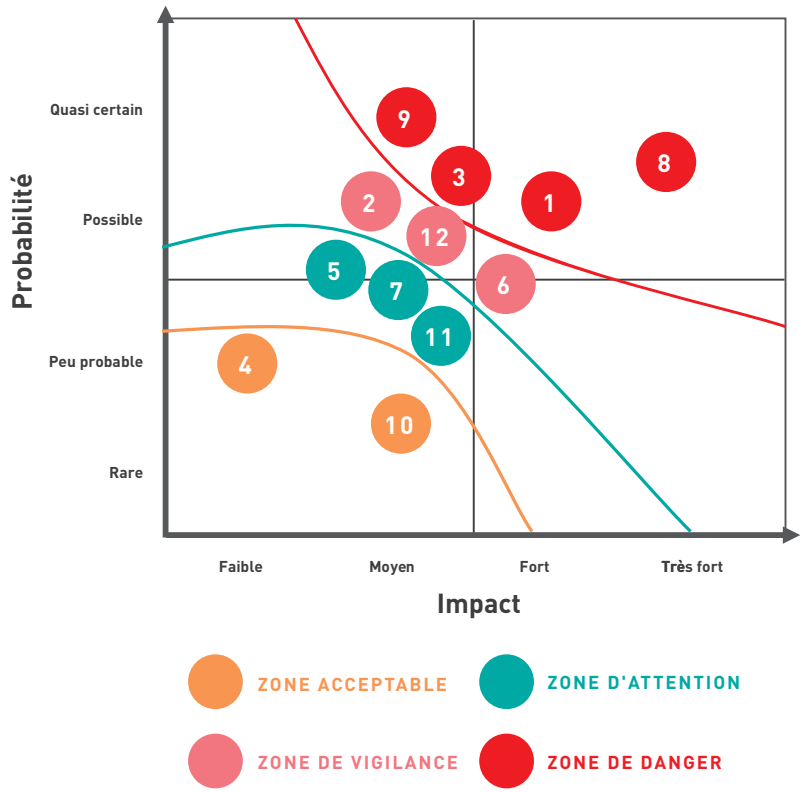
La cartographie des risques doit permettre au dirigeant de se **représenter visuellement et synthétiquement les risques majeurs susceptibles d'affecter gravement les objectifs et enjeux de son entreprise.** C'est une image à un instant T qui représente d'une manière globale et hiérarchisée les principaux risques de l'entreprise, quelle que soit leur nature. Elle devient ainsi un véritable outil de pilotage par les risques.

Sa forme dépend des éléments que l'on souhaite mettre en valeur (probabilité/impact, échéances, part de chaque entité de l'entreprise, nature de risque...). Il n'y a pas de modèle unique.

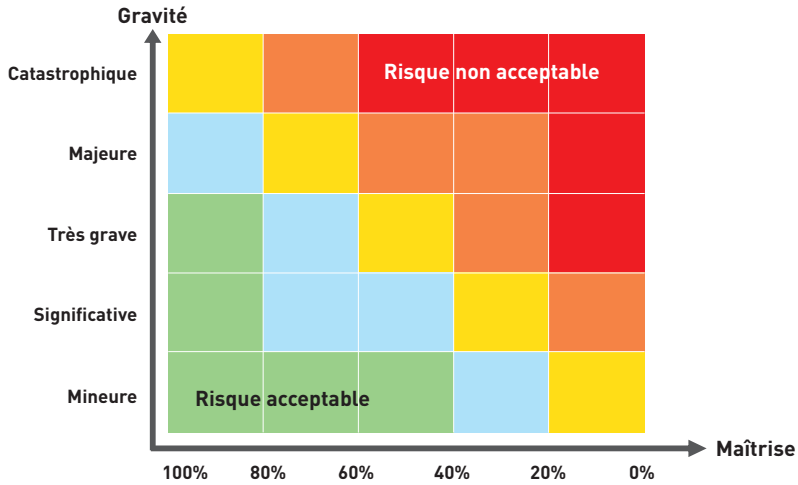
Dans le 1er exemple ci-dessous sont combinés les critères de gravité de l'impact du risque (faible, moyen, fort, très fort) et ceux de sa probabilité d'occurrence (rare, peu probable, possible, quasi certain).

Exemple 1 : Cartographie Gravité / Impact.

Source « La cartographie : un outil de gestion des risques ». Collection Maîtrise des risques ©AMRAE.



Exemple 2 : Cartographie Gravité / Maîtrise



Cette seconde représentation est axée sur le niveau de maîtrise/contrôle interne et le niveau de criticité de l'impact.

Dans ces représentations, le risque est le plus souvent, pour des raisons de confidentialité, représenté par le numéro qui lui est attribué lors de la constitution de la liste des risques majeurs.

Principes de la cartographie des risques : hiérarchisation, partage et alignement

- **Hiérarchisation**

L'objectif de la cartographie est de faire ressortir **un nombre limité de risques prioritaires** d'un portefeuille de risques **majeurs.** Ces risques identifiés doivent faire l'objet d'un suivi et d'un traitement spécifique. Il revient à chaque entreprise d'élaborer les échelles de graduation, de décider si l'évaluation de l'impact peut rester qualitative ou si elle sera traduite financièrement, ou les deux. Plus le risque a un impact concret, plus il doit être pris au sérieux...

- **Partage et alignement**

Il conviendra de susciter un échange ouvert et transversal au sein de l'équipe dirigeante pour **dégager un consensus sur les risques et les priorités d'actions.** Cette démarche sera initiée à partir d'entretiens avec les collaborateurs et les dirigeants.

Les avantages :

- **Obtenir une vision globale :** connaissance des menaces sur les enjeux majeurs,
- **Échanger sur une vision transverse des risques** (risques dans et hors de la sphère de responsabilité),
- **Partager au plus haut niveau la même compréhension globale des risques.** Cela permet une implication et une prise de décision du niveau le plus élevé de la hiérarchie jusqu'aux directions opérationnelles ou fonctionnelles de l'entreprise. Il en est de même avec les instances de gouvernance de l'entreprise, où la gestion des risques doit devenir un sujet traité au minimum lors d'une réunion spécifique dans l'année.

À noter : Intégrez la démarche aux processus de l'entreprise

Une cohérence avec les démarches déjà menées dans l'entreprise (démarches qualité, développement durable, lean, qualité de vie au travail...) et leurs acteurs, doit être recherchée pour éviter les redondances, les conflits de priorisation. Il faut donner du sens, de la cohérence afin de mettre en perspective les différents projets menés dans l'entreprise.

Les entreprises, y compris PME-ETI, ont très généralement des tableaux de bord de pilotage de la structure. Il peut être pertinent d'intégrer les indicateurs de gestion des risques dans les tableaux existants. Cela permet d'inscrire la démarche comme outil de développement et de rendre lisible l'interaction entre les réflexions menées au sein de la structure.

3.4 Traitement des risques

Après l'identification et l'évaluation des risques, vient la prise de décision quant aux suites à donner. Gérer ses risques, c'est aussi se donner les moyens de décider de leur traitement !

L'objectif ne sera pas toujours de supprimer les risques ; cela n'est pas toujours possible. Et quand la suppression des risques est envisageable, il faudra en mesurer le « prix » (financier et/ou organisationnel). Le choix de la structure pourra être alors de ne pas les supprimer, mais de les gérer.

Il s'agit alors de les prioriser et de les maîtriser en décidant d'actions (les plus adaptées et les mieux proportionnées) qui doivent être prises (réduction, transfert à l'assurance, autres plan d'actions...).

La maîtrise des risques passe par l'élaboration d'un plan d'actions concret, dont il faut veiller à la bonne réalisation dans les conditions définies.

Les actions peuvent être de différents types : organisationnel, technique, juridique, financier, humain...

Pour être efficace, chaque action doit être :

- traduisible en activités concrètes et mesures pragmatiques décidées collégialement ;
- accompagnées de moyens humains et matériels, réalistes ;
- assorties d'un délai de mise en œuvre acceptable ;
- comporter des indicateurs objectifs de réalisation/performance permettant de mesurer la réduction du niveau de risque. Ils peuvent être quantitatifs et directement connectés aux conséquences du risque. Ils peuvent également être qualitatifs et directement liés aux dispositifs de maîtrise du risque mis en place. Ces indicateurs doivent être simples à collecter, objectifs et pragmatiques (ex: % de mise en place, % de formation réalisées, % de réalisation...).
- chaque action mise en œuvre doit être suivie par une personne identifiée, dite « le propriétaire du risque ». Autant que possible le chef d'entreprise ne doit pas être le seul propriétaire des risques. Étant souvent, en PME, le pilote de la démarche, il ne pourra cumuler les casquettes sans risque de s'essouffler et/ou de perdre du recul et de la pertinence.

À défaut de ces conditions, les mesures envisagées ne seront pas prises, la démarche perdra de son efficacité et de sa légitimité (cf chapitre IV).

3.5 Contrôle et suivi des plans d'action : la gestion des risques doit être positionnée comme un process pérenne de pilotage de l'entreprise

Afin de maintenir une dynamique dans la démarche, il convient, idéalement tous les trimestres et au minimum une fois par an, **de faire un point sur l'avancée des 4 ou 5 risques** identifiés comme prioritaires. La régularité du suivi permettra également d'intégrer plus facilement de nouveaux collaborateurs, de les impliquer et de bénéficier de leur recul et de leurs apports. Il convient chaque année de refaire un nouveau travail de cartographie, afin de fixer les nouveaux risques prioritaires de l'année et éventuellement prendre en compte des risques émergents, de vérifier les étapes de réduction des risques antérieurs...

Il faut capitaliser sur les réalisations de l'année et faire un retour d'expérience :

- ce qui a échoué, et bien entendu, ce qui reste à corriger,
- mais aussi ce qui a donné des résultats, afin de le conserver et accorder la reconnaissance aux acteurs, permettant ainsi que la démarche reste positive et mobilisante.
- se fixer des objectifs pour l'année à venir.

Étudier les tendances d'évolution des risques, chaque année, en équipe de direction, est une nécessité. Un risque identifié une année n'aura pas les mêmes impacts l'année suivante.

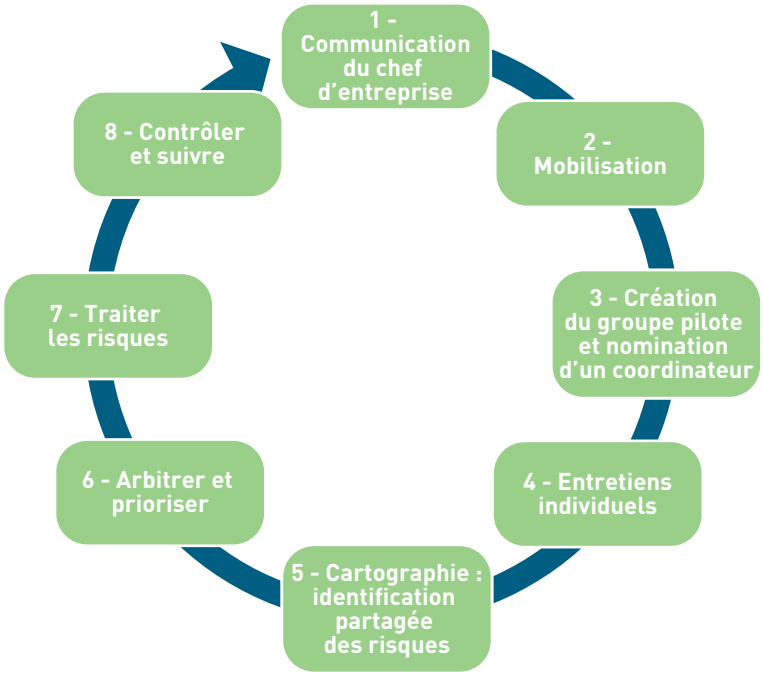
Il faut s'interroger car une cartographie utile est une cartographie vivante.

Il faudra parfois accepter une certaine modestie dans la mise en œuvre du plan d'actions : ne pas tenter de résoudre ou ne pas traiter des risques pour lesquels aucune marge de manœuvre compatible avec les possibilités de l'entreprise n'apparaît clairement. Ces risques ne devront pas être niés mais pourront être traités ultérieurement, quand, par exemple, l'entreprise aura acquis une maturité plus importante en gestion des risques.

À noter : La gestion des risques, sujet de la gouvernance

La gestion des risques est un sujet qui doit être présenté dans les instances de gouvernance (conseil de surveillance, conseil d'administration...) et faire l'objet d'un échange nourri au moins une fois par an et à chaque grande étape de l'entreprise (croissance externe...). Les administrateurs sont de plus en plus intéressés à être informés de cette partie « Risques », non seulement dans le cadre de leur activité de gestion mais aussi au vu des responsabilités qu'ils endossent à ce sujet.

En synthèse, la démarche de gestion de risques a huit grandes étapes que l'on retrouve dans le graphe suivant

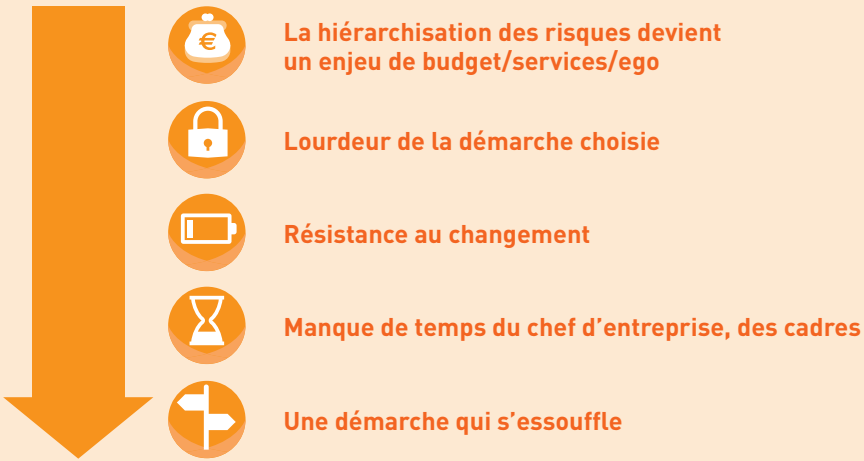


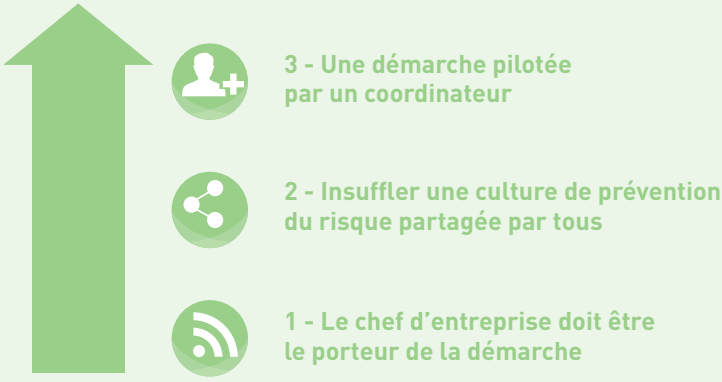
4. Les 3 facteurs de réussite, versus, les faiblesses

Une démarche globale de gestion des risques nécessite la mise en œuvre d'une approche construite, d'une méthodologie rigoureuse, jalonnée d'étapes progressives, une analyse en évolution perpétuelle adaptée au rythme de l'entreprise afin d'être un véritable outil au service du développement de la structure.

Chaque étape a ses règles propres et ses exigences méthodologiques afin d'en garantir le succès. Loin d'être une démarche uniforme, l'appropriation réussie de la démarche de gestion des risques sera celle qui prend en compte la culture de l'entreprise (dirigeant et collaborateurs), son appétence aux risques, ses valeurs partagées, ses modes de management et de communication, son organisation, ses contraintes spécifiques...

Pour autant des principes généraux se dégagent, conditionnant la réussite du projet.





Concentrons-nous sur les facteurs de succès !

1. Le chef d'entreprise doit être le porteur de la démarche

Le chef d'entreprise, spécifiquement de PME-ETI, doit donner l'impulsion par son implication dans la démarche et la communication claire qu'il fera à ce sujet. Cette démarche doit être présentée comme un process collectif d'entreprise, visant à une meilleure performance globale.

Spécialement en PME, c'est l'implication et la conviction du chef d'entreprise qui en fera son succès. La communication doit être claire, largement partagée, succincte pour être lisible. Selon la culture de l'entreprise, cet engagement pourra prendre la forme d'un point à l'ordre du jour de la réunion de direction, d'une réunion spécifique, d'une communication orale puis écrite. L'étape de la formalisation du lancement de la démarche constitue un ancrage utile.

Une communication renouvelée aux différentes étapes essentielles permettra de maintenir voire d'élargir l'adhésion.

Exemples :

- Communication par affichage : donner un nom à la démarche, trouver un logo/symbole visuel, écrire l'engagement et les objectifs poursuivis, actualiser.
- Communication par réunions de service.
- Communication par les canaux habituels de l'entreprise : journal interne, intranet...

2. Insuffler une culture de prévention du risque partagée par tous et la maintenir

Au-delà de l'étape d'entretiens individuels et si la structure de l'entreprise le permet, le chef d'entreprise doit être prêt à partager sa vision des risques avec l'équipe de direction (DAF, DRH, directeur de production par exemple), en créant un Comité des Risques ou un dispositif aux fonctions similaires. La vision croisée de ces principaux acteurs permettra une analyse plus pertinente et plus fine des risques. Cela permettra aussi un échange sur la hiérarchisation des priorités d'action qui enrichira la réflexion. Au terme de cet échange, le chef d'entreprise reste seul décisionnaire des priorités utiles à sa structure : plus le partage sera grand plus l'adhésion sera forte et donc la performance globale.

- **L'enjeu est de mobiliser l'ensemble des acteurs de la démarche en créant un climat de confiance**

Une cartographie n'est pas un audit des différents services, c'est un outil d'aide à la décision collective. Une explication claire de l'objectif poursuivi, insistant sur l'intérêt collectif, doit être portée par le chef d'entreprise pour permettre une vraie adhésion au projet.

Il faut rassurer, rappeler régulièrement l'intérêt collectif recherché par cette démarche vertueuse. C'est un processus d'amélioration continue mais qui, pour certains, par crainte ou par refus, peut aussi créer une résistance au changement.

Il faut donc prendre le temps d'un réel partage à cette étape afin de fédérer autour du projet.

Cette étape peut parfois être sous-estimée dans les PME-ETI où l'habitude d'échanges informels fait penser que le "message passe" facilement. Cependant, un tel projet transversal, impliquant l'équipe de direction sur une vision globale de l'entreprise et de sa projection, est un exercice souvent différent du quotidien, qui demande un temps de mobilisation variable.

Il convient de prendre ce temps. De l'adhésion réelle des acteurs, puis de leur implication, dépendent le succès de la démarche.

- **Maintenir l'esprit de la prévention du risque**

C'est avec le temps et les multiples expériences vécues en commun que se forge la culture d'un collectif. Elle ne se décrète pas et doit s'inscrire dans le long terme pour exister.

En PME-ETI, la proximité de contacts quotidiens peut rendre la construction d'une culture des risques plus facile et plus rapide. A l'opposé, une PME-ETI aura une plus grande difficulté à maintenir au fil des mois le dynamisme de la démarche. Il faudra notamment veiller à la formalisation des différentes étapes (entretiens, analyse, cartographie...) par la réalisation de supports écrits synthétiques qui rythmeront la démarche et permettront d'en conserver le caractère itératif.

Enfin, le chef d'entreprise devra également garder à l'esprit qu'il doit y avoir une vraie correspondance entre la culture voulue puis affichée et la pratique managériale réelle qu'il portera. L'implication collective doit être effective au risque de perdre le bénéfice de la démarche.

3 - Un coordinateur de la démarche

Dans les PME-ETI, nécessairement réactives, aux prises avec le quotidien, et aux compétences parfois exclusives, la question de la disponibilité se pose de façon cruciale. Dégager du temps pour une action transversale comme la gestion des risques, quand bien même tous les collaborateurs seraient convaincus de son utilité, peut s'avérer délicat et mettre en cause les objectifs fixés.

Il sera donc utile de nommer un coordinateur de la démarche (directeur financier, juridique…). Il fera vivre la démarche, assurera son suivi et sa progression, en rendant compte au chef d'entreprise et au groupe de travail. Le coordinateur doit être légitime auprès des équipes, reconnu par sa connaissance de l'organisation et de la filière. Il doit avoir la capacité de faire adhérer, de diffuser la culture du risque, de faire jouer chaque niveau, d'écouter et recueillir les propositions. Il aura en charge la mise en place d'une méthodologie souple, adaptée à la culture et au niveau de l'entreprise, des outils efficaces, la construction de l'univers des risques et de la cartographie en collaboration avec l'équipe dirigeante, sa mise à jour, le suivi des plans d'actions, le suivi de l'agenda de présentation au conseil d'administration, de surveillance…

Il pourra être utile de s'interroger quant à la possibilité d'intégrer la gestion des risques dans les instances de pilotage déjà existantes de l'entreprise (comité de direction, réunion des cadres…). L'objectif de la démarche reste l'efficacité et non de créer une strate supplémentaire.

Enfin, si la taille de la structure ne permet pas de déléguer cette mission, le chef d'entreprise devra assumer ce rôle.

AUTO-DIAGNOSTIC

III. Auto-diagnostic d'analyse des risques en PME-ETI

Il est habituellement admis que seuls 25% à 30% des risques sont assurables. Et quand bien même certains le sont, la survenance du risque, pourtant assuré, n'est jamais complètement couverte (désorganisation, image/réputation de l'entreprise, impact clients...). La gestion des risques est donc un véritable outil de la stratégie de l'entreprise.

Le Medef Deux-Sèvres et l'AMRAE sont convaincus de l'intérêt pour les PME-ETI de se doter d'une démarche pragmatique de gestion des risques, et ce quels que soient la taille de l'entreprise et son secteur d'activité. C'est la raison pour laquelle ils ont mis en place un groupe de travail constitué essentiellement de chefs d'entreprise de PME-ETI afin de construire un auto-diagnostic d'analyse des risques utilisable, simplement, par toute entreprise.

L'objectif poursuivi est de sensibiliser à cette thématique par un premier niveau d'appréciation instantané et synthétique de la structure face à sa gestion des risques.

1. Les objectifs du groupe de travail

1) Construire un univers des risques, spécifique aux PME-ETI qui a permis de sensibiliser les entreprises à la force que cet outil de gestion des risques peut être pour le développement de leurs structures.

Cet univers a été élaboré à partir des expériences croisées de l'ensemble des chefs d'entreprise. Les risques identifiés ont été regroupés en grandes famille de risques.

2) Produire un questionnaire, issu de cet univers des risques permettant d'effectuer un auto-diagnostic de la situation de la structure et ainsi apporter une aide opérationnelle concrète à tous ceux qui voudraient s'engager dans ce projet.

Le questionnaire, outre l'intitulé du risque et ses conséquences possibles, comportera une série de questions permettant au chef d'entreprise de mieux se positionner quant au risque et d'envisager des pistes de plan d'action.

Le chef d'entreprise appréciera et cotera deux critères :

- l'impact en cas de survenance du risque : limité / significatif / critique / catastrophique ;
- la probabilité de survenance du risque : improbable / rare /occasionnelle / fréquente.

3) Le questionnaire dans sa forme numérique est un outil excel de mesure de la gravité de chaque risque relevé qui alimente automatiquement **une cartographie** et donnera au chef d'entreprise une vision synthétique et instantanée de son auto-évaluation des risques.

2. Questionnaire d'auto-diagnostic

Lancez-vous!

Vous retrouverez le fac-similé du questionnaire PME-ETI dans le rabat de la 3ème de couverture.

Pour faire votre auto-diagnostic en ligne rendez-vous sur **www.macartodesrisques.fr** !

La matrice d'analyse des risques a été conçue et testée pour être simple d'utilisation. Elle est constituée par un questionnaire qui est le seul document nécessitant une saisie de données. Ce questionnaire est composé de 7 colonnes, dont 4 à renseigner pour 54 questions. Un fac-similé du questionnaire se trouve dans le rabat de 3ème de couverture.

Le chef d'entreprise peut la remplir seul ou lors de réunions collectives avec un ou des collaborateurs. La démarche sera ainsi enrichie par le croisement des analyses. Elle peut être aussi administrée par un tiers (Medef territorial...).

Les risques sont divisés en 7 univers distincts : stratégiques, financiers, opérationnels, sûreté/sécurité, gestion de crise, réglementation/ conformité et RH.

Chaque univers est segmenté en différents « risques décelés ». Pour renseigner au mieux le questionnaire, des exemples de cause et de conséquences du risque sont proposés.

Pour chaque risque décelé, il est proposé à celui qui renseigne :

- D'identifier si son entreprise est exposée au risque : par exemple, une entreprise qui n'exporte pas n'est pas exposée à des risques liés à l'exportation... Réponse OUI/NON.
- De rédiger la réponse à la question (texte libre), ce qui permet de conserver ses analyses, très utiles pour retravailler régulièrement sur la cartographie des risques de son entreprise.
- De coter l'impact en cas de survenue du risque, suivant une échelle à 4 niveaux : 1-limité ; 2-significatif ; 3-critique ; 4-catastrophique.
- De coter la probabilité estimée de survenance du risque, suivant une échelle à 4 niveaux : 1-improbable ; 2-rare ; 3-occasionnelle ; 4-fréquente.

À la fin du renseignement de chaque univers, il est proposé de s'autoévaluer sur l'ensemble de cet univers (cotation de 1 à 4).

Le site **www.macartodesrisques.fr**, permet une saisie et une cotation en ligne des différentes questions. Ce site est sécurisé, conforme à la RGPD et les données sont anonymisées. A l'issue de cette saisie, le chef d'entreprise pourra télécharger un rapport (sous format pdf) qui contiendra :

- ses réponses au questionnaire,
- le niveau de maîtrise des risques de l'entreprise sur les 7 univers de risques, sous la forme d'un radar. Elle se renseigne automatiquement à partir des données saisies dans le questionnaire.
- la cartographie des risques de l'entreprise en croisant l'impact et la fréquence de chaque risque.

TRAITEMENT

IV. Traitement des risques

Après la phase d'identification et d'évaluation des risques, vient la phase de prise de décisions. Connaître ses risques réels permet de mieux les sélectionner et de mettre en œuvre les mesures appropriées. En effet, la sélection du mode de traitement va tenir compte du degré de maîtrise des risques identifiés et de son appétence aux risques.

En général les PME-ETI vont choisir un traitement sélectif, se concentrant sur les risques prioritaires, majeurs, indispensables à la survie de leur entreprise. La cartographie permet d'appréhender facilement les zones « rouges », prioritaires à traiter.

1. Les options de traitement des risques

LA NORME ISO 31000, NOUVELLE VERSION DE FÉVRIER 2018, ABORDE LONGUEMENT LA PARTIE TRAITEMENT DES RISQUES

Les formes de traitement énumérées sont :

- un refus du risque marqué par la décision de ne pas commencer ou poursuivre l'activité porteuse du risque ;
- la prise ou l'augmentation d'un risque afin de saisir une opportunité ;
- l'élimination de la source de risque ;
- une modification de la vraisemblance ;
- une modification des conséquences ;
- un partage du risque (par exemple par le biais de contrats, de souscription de couvertures d'assurance) ;
- un maintien du risque fondé sur une décision éclairée.

Traiter un risque correspond à un chemin de réflexion comprenant des étapes progressives. Un parallèle peut être fait avec les démarches réglementaires de prévention des risques professionnels en santé au travail, auxquelles sont habituées les PME-ETI.

Traiter un risque revient donc à choisir, successivement, l'une des solutions suivantes, voire des combinaisons de plusieurs d'entre elles :

1 - **Supprimer la source du risque, par exemple :** cession d'une activité, fusion, changement d'outil informatique, suppression d'un produit…

2 - **Réduire les causes et/ou les conséquences d'un risque.** C'est à ce stade que seront décidées la mise en place :

- de plans de prévention (pour éviter la survenance) : interdiction de fumer sur un site, mise en place de permis de feu…
- mais également des mesures de protection (réduire les effets) : détection incendie et désenfumage des locaux, sprinklers…

3 - **Transférer le risque à un tiers, souvent par contrat,** comme un prestataire, un fournisseur ou un assureur.

4 - **Accepter le risque en l'état,** mais après avoir jugé qu'il restait acceptable financièrement au regard de ses effets sur les résultats de l'entreprise. Sinon il n'est pas considéré comme traité (ex. : garder des infrastructures telles quelles car le sinistre maximum possible est jugé supportable par l'entreprise).

Il pourra alors être étudié l'opportunité de provisionner les conséquences financières prévisibles de la survenue du risque.

2. Évaluer l'acceptabilité du risque pour l'entreprise et choisir son option

LES PRINCIPES GOUVERNANT LA PRISE DE DÉCISION

La norme ISO 31000 rappelle le principe suivant :

« Le choix de la ou des options de traitement du risque les plus appropriées implique de comparer les avantages potentiels en termes d'atteinte des objectifs par rapport aux coûts, aux efforts et aux inconvénients de leur mise en œuvre »

Les travaux de l'AMRAE sur la cartographie des risques soulignent :

« La part d'irrationalité dans l'approche d'une politique d'acceptation rend indispensable une réflexion profonde des décideurs et mandataires sociaux au plus haut niveau de l'entreprise. Il n'est pas possible, dans le cadre d'une saine gestion des risques, de faire l'économie d'une telle réflexion, parce qu'elle conditionne l'identification des priorités de traitement et donc de maîtrise recherchée des risques ».

LES INCONTOURNABLES DE LA PRISE DE DÉCISION

Le processus d'arbitrage de ressources : on ne pourra jamais couvrir les risques aussi totalement qu'on le souhaiterait. Le risque zéro n'existe pas. Néanmoins, il faut quand même arriver à séparer les risques les plus inacceptables des autres et décider de l'allocation des ressources que l'on est prêt à dédier à leur maîtrise.

L'évaluation complète de l'impact du risque est difficile car pour être complète, elle doit intégrer toutes les conséquences, non seulement l'impact matériel immédiat mais également les impacts indirects et immatériels beaucoup plus difficiles à évaluer.

La période d'évaluation : l'évaluation doit se faire sur une période longue qui prend naissance à la survenance du risque et prend fin au retour définitif à la situation antérieure à la réalisation du risque. Il faudra prendre en compte les différentes conséquences : la perte d'image ou de réputation, les pertes d'exploitation, la désorganisation de l'activité, la désaffection de la clientèle...

Le choix du traitement pourra se fonder sur une combinaison d'appréciations :

- par approche financière du risque ;
- par niveau d'acceptabilité du risque : un risque jugé inacceptable (ex : un accident corporel de clients ou d'employés) sera traité à un niveau maximum, même si sa probabilité de survenance est extrêmement faible ou que le coût du traitement paraît très élevé ;
- par l'adaptation et l'adéquation du traitement à la culture de l'entreprise.

2.1 Appréciation par l'approche financière

On pourra prioriser les options de traitement des risques en fonction de l'analyse d'impact financier qui aura été faite. Il est donc essentiel que l'analyse ait été faite avec précision (voir étape analyse des risques en chapitre II).

On ne peut que travailler sur des appréciations subjectives. Le plus souvent, les entreprises travaillent sur des estimations de « tranches » financières, en fonction de *scenarii* concrets de sinistres. Par exemple : si le feu prend dans une usine, le responsable de l'usine sera le plus à même d'estimer le risque maximum possible en fonction des mesures et plans d'actions déjà mis en œuvre, comme le remplacement récent des systèmes de sprinklage, les résultats des contrôles des appareils existants...

Néanmoins, la décision du mode de traitement d'un risque dépasse la seule considération financière. Chaque entreprise a son propre « appétit aux risques » ou sa propre aversion, même si elle n'est pas toujours formalisée.

Par exemple : « Je ne prends aucun risque d'incendie sur cette usine car son fonctionnement est au cœur de ma stratégie. Son arrêt entraînerait un risque d'image vital pour mon entreprise. »

Principe du "Just enough": Restez attentif à la pertinence des options retenues !

Le coût du traitement doit être en rapport avec l'enjeu (ne pas dépenser 50 pour éviter un risque de 10), d'où la nécessité de bien évaluer en amont l'impact éventuel du risque.

2.2 Appréciation par le niveau d'acceptabilité du risque

Il faut vérifier les risques tolérables par l'entreprise, compte tenu de son secteur d'activité, des réglementations qui la gouvernent, de son éthique, de ses valeurs, de sa culture du risque, des accords avec certaines parties prenantes (clients, fournisseurs, collectivités…). Il en est de même pour les risques qu'elle décide de ne pas tolérer (sécurité ou intégrité des personnes, qualité des produits, risques de réputation…). Dans certains cas, les obligations légales auxquelles l'entreprise est soumise vont déterminer une forme spécifique de traitement. L'entreprise n'aura donc pas le choix. Il en va ainsi de réglementations sectorielles qui imposent des solutions quel que soit le contexte (chimie, télécoms…).

2.3 Appréciation par l'adaptation et l'adéquation du traitement à la culture de l'entreprise

Outre l'impact financier et la cohérence avec le niveau d'acceptabilité du risque, le traitement sera approprié s'il est adapté sur le plan qualitatif. Différents facteurs sont à prendre en compte, qui, pour un même risque, peuvent entraîner des décisions différentes d'une entreprise à l'autre :

- la cohérence avec les objectifs stratégiques de l'entreprise et avec ses valeurs ;
- les habitudes dans la manière d'aborder les problèmes et la résistance au changement au sein de l'entreprise ;
- la prise en compte de la dimension culturelle notamment celles des filiales à l'étranger, qui ne sera pas forcément en adéquation avec les valeurs et les objectifs de la maison mère ;
- …

Les PME-ETI n'ont pas moins de choix pour traiter leurs risques que les entreprises de plus grande taille. Néanmoins, du fait de l'impact souvent plus fort d'un risque sur leur structure, elles doivent sélectionner plus finement les risques prioritaires à traiter et les solutions adaptées à leur taille et à leurs moyens.

3. Suivre le traitement du risque

Dans les PME-ETI, en l'absence de collaborateur dédié ou spécialisé, l'appréciation des risques et de leur maîtrise sera avant tout une approche terrain, pragmatique, visant à répondre aux problématiques métiers, sans sous-évaluer les risques immatériels (cyber, réputation…).

Chaque risque dont le traitement nécessite un plan d'actions doit être pris en charge par un responsable nommément désigné. Son rôle sera de définir le plan d'actions, en lien avec toutes les directions concernées, de mettre en place et de suivre ce plan, y compris l'aspect budgétaire et le reporting.

Ce suivi d'un risque ou d'un processus sera d'autant plus effectif et efficace que l'on fonctionnera en intégration, c'est-à-dire que cette mission s'intégrera logiquement dans les fonctions de la personne, et en contribution/concertation avec les acteurs concernés par ce plan d'actions.

Par exemple, un plan d'actions de sécurisation d'une usine reviendra au responsable de l'usine. Il rendra compte de son avancée au pilote du dispositif de gestion de risques dans l'entreprise (s'il existe) ou au dirigeant de la PME-ETI lui-même.

La direction de l'entreprise devra donc aussi s'impliquer et pourra demander régulièrement à connaître les avancées du plan d'actions au manager opérationnel concerné. Ce dernier devra évidemment rendre compte régulièrement de son action.

Traiter ses risques, c'est ainsi choisir et mettre en œuvre des mesures qui vont permettre d'agir sur la probabilité de survenance et/ou sur l'impact des risques, et donc d'augmenter le niveau de la maîtrise interne.

La prévention joue un grand rôle, notamment dans la maîtrise de la survenance du risque.

OUTIL PRATIQUE
PLAN DE SUIVI DE TRAITEMENT DES RISQUES : RECOMMANDATIONS DE LA NORME ISO 31000

- Les décideurs et les autres parties prenantes sont informés de la nature et de l'étendue du risque résiduel après le traitement du risque.
- Le risque résiduel est documenté et soumis à suivi et revue et, le cas échéant, fait l'objet d'un traitement supplémentaire.
- Les informations fournies dans le plan de traitement comportent :
  - la justification du choix des options de traitement, y compris les avantages attendus ;
  - les personnes responsables de l'approbation et de la mise en œuvre du plan ;
  - les actions proposées ;
  - les ressources nécessaires, en tenant compte des impondérables ;
  - les mesures des performances ;
  - les contraintes ;
  - les rapports et le suivi requis ;
  - le moment où les actions sont censées être entreprises et achevées.

4. Focus sur les assurances

Il existe des activités (aviation, construction, médecine ...), des pays, où les responsabilités sont telles qu'il faut absolument s'assurer. Bien souvent aussi, les clients l'exigent .

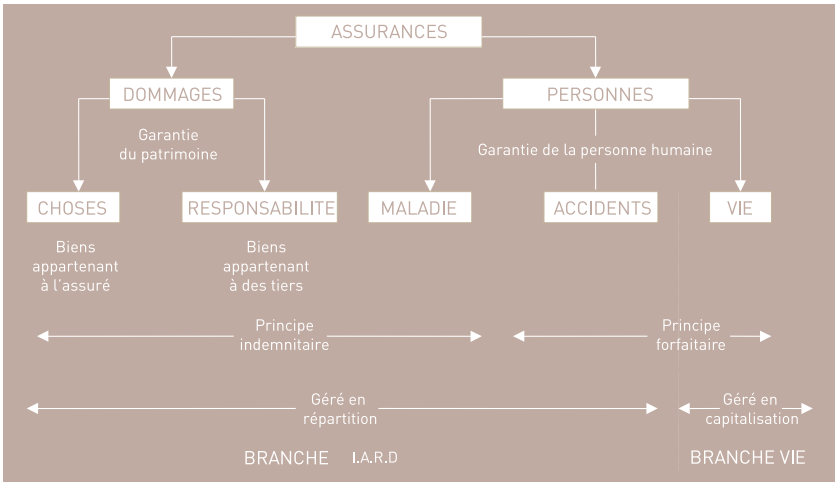
Enfin, parce qu'un incendie, entre autres peut causer la mort d'une PME, il est fortement conseillé aux dirigeants d'investir dans l'assurance pour couvrir leurs risques. C'est le plus souvent lorsque le risque survient que l'on se rend compte de l'utilité de cet investissement. Alors mieux vaut y allouer un budget avant qu'il ne soit trop tard...

4.1 Les différentes branches d'assurance

On distingue les assurances de Personnes et les assurances de Dommages.

Les premières sont principalement constituées (en entreprise) des frais de santé d'une part et de la prévoyance d'autre part.

Les assurances de Dommages (IARD) sont constituées des assurances de la branche Responsabilité Civile (RC) et des assurances de Dommages aux Biens.



4.2 Fondamentaux du transfert des risques à l'assurance

Pour qu'un risque soit assurable, il doit être :

- Aléatoire (soudain et imprévu) ;
- Maîtrisable ;
- Quantifiable financièrement : l'assureur doit *a minima* pouvoir déterminer un impact financier maximum que le risque soit de nature « matériel » ou « immatériel » (ex : cyber risque).

Il existe deux grandes formes de contrat d'assurance :

- **Les contrats tous risques « sauf » :** toutes les garanties sauf celles spécifiquement exclues (certaines exclusions sont « rachetables ») sont couvertes. C'est la forme contractuelle la plus souvent retenue par exemple en assurance de responsabilité civile.
- **Les contrats dit en périls dénommés :** c'est l'inverse, car le contrat précise ce qui est couvert, tous les autres événements étant exclus. C'est très souvent le cas par exemple dans les polices Cyber, pour lesquelles l'assureur souhaite bien définir l'étendue de sa garantie pour mieux maîtriser et quantifier son exposition.

En assurances Dommages aux Biens, ces deux formes de contrats peuvent être utilisées.

4.3 Seules quelques assurances sont obligatoires (du strict point de vue juridique) :

- **L'assurance des véhicules pour la partie responsabilité civile automobile** (communément dénommée « assurance aux tiers ») ;
- **L'assurance responsabilité civile (RC),** mais uniquement pour certaines professions réglementées (ex : architectes. bureaux d'études...). Elle couvre les dommages aux tiers (clients, fournisseurs, prestataires, mais également toutes autres personnes même sans lien contractuel) ;
- **Les assurances spécifiques pour certains secteurs d'activité.** Par exemple, les entreprises du BTP ont l'obligation de souscrire une assurance de responsabilité décennale qui couvre les dommages matériels à l'ouvrage, en cas d'atteinte à la solidité ou à la destination de l'ouvrage, constatés dans les dix ans suivant la réception des travaux.

4.4 Même non obligatoire, il est cependant judicieux d'investir dans l'assurance pour assurer la pérennité de la société.

- **Une assurance des biens matériels de l'entreprise et des pertes d'exploitation consécutives.** Les risques à transférer sont d'abord ceux qui vont affecter les biens de l'entreprise : immobiliers (ex : incendie de site), matériels (ex : bris de de machines), et les marchandises (ex : incendie de stocks). Egalement, les pertes d'exploitation, entraînant un arrêt d'activité consécutif à ces dommages matériels, sont au moins tout aussi dramatiques. **C'est pourquoi les PME ont intérêt à investir dans une police Dommages aux biens et pertes d'exploitation consécutives.** En attendant la reprise totale de la production ou mieux encore le retour à une activité équivalente à celle antérieure au sinistre (rétablissement du chiffre d'affaires), cette garantie prend en charge la perte de marge brute, à savoir la perte de chiffre d'affaires moins les charges variables. Egalement, elle couvre les frais supplémentaires pour revenir plus rapidement au nominal : frais de sous-traitance, intérimaires, location de nouveaux sites... L'entreprise définit une période nécessaire pour revenir à la situation initiale à savoir un délai de 12, 18 voire 24 mois. L'indemnisation des dommages matériels sera basée sur la valeur des biens endommagés et les pertes d'exploitation évaluées sur la base des pertes de marge subies, sans recherche d'une quelconque responsabilité. Il est donc très important de revoir annuellement la valeur des stocks et des biens assurés, et cela de préférence en valeur à neuf (en valeur de reconstruction à neuf pour les bâtiments et en valeur de remplacement à neuf pour les autres

biens matériels). Enfin, du moment où l'entreprise souscrit une assurance de Dommages pour ses sites, elle bénéficie en France de la garantie Catastrophes Naturelles ;

- **L'assurance responsabilité civile** n'est pas obligatoire (sauf cas mentionnés supra) mais elle est indispensable car elle permet de couvrir les conséquences des dommages causés à des tiers. Par exemple, vous ne pouvez livrer un de vos clients importants suite à une cause extérieure à votre entreprise (un incendie dans l'usine d'un de vos fournisseurs essentiel et unique) mais vous êtes quand même responsable des conséquences financières qui en découlent vis-à-vis de votre client (pertes d'exploitation de ce dernier, image…) ;
- **Une couverture « Atteinte à l'environnement et risques environnementaux »,** soit en extension de votre police RC, soit par une police dédiée à ce risque. En effet, tout entreprise peut causer des préjudices aux tiers et ou à l'environnement. Nul n'est par exemple à l'abri d'une fuite d'hydrocarbure en raison d'une cuve fuyarde, d'un raccordement mal réalisé, du heurt d'une conduite… ;
- **L'assurance Responsabilité Civile des Mandataires Sociaux (RCMS) :** elle est très importante, en particulier pour les dirigeants et mandataires sociaux des PME-ETI. Elle couvre les dommages causés aux tiers par les mandataires sociaux du fait de leur qualité de représentant et responsable de l'entreprise. La RCMS n'est pas obligatoire mais fortement conseillée, sinon le dirigeant peut être engagé sur son patrimoine personnel et perdre tous ses biens personnels (privés). Le second but de la RCMS est de payer les frais de défense de l'avocat (s'ils sont payés par l'entreprise, c'est considéré comme un abus de bien social puisqu'il s'agit d'une défense de la personne privée et non de l'entreprise) ;
- **L'assurance transport :** elle est nécessaire pour compenser financièrement la perte ou la détérioration de marchandises transportées (ex : renversement d'un camion contenant des biens précieux et/ ou coûteux, défaut de calage…) ;
- **L'assurance Tous Risques Chantiers (TRC) :** c'est une assurance de dommages qui couvre pendant la phase de travaux (début des travaux jusqu'au PV de réception) tous types de dommages (vol, pertes, destruction…) sur tous les biens matériels, sauf exceptions dénommées. Elle couvre également certains des dommages survenant au cours de la garantie constructeur pendant 12 mois voire 18 à 24 mois, si cette option a été souscrite ;

- **L'assurance cyber risques :** de la malveillance ou la négligence d'un employé à la cyberattaque venant de l'extérieur, elle permet de couvrir un grand nombre de risques cyber à l'origine exclus ou insuffisamment assurés dans les polices traditionnelles (Dommages et RC). Les garanties peuvent couvrir : un acte de malveillance informatique, un virus informatique, le piratage informatique, le vol de données personnelles, la malveillance d'un employé, des diffamations ou dénigrements sur internet, l'usurpation d'identité... Cf Cahier Technique AMRAE, en partenariat avec le CESIN : « Cyber risques : outil d'aide à l'analyse et au traitement assurantiel »- 2015.
- **Assurance Fraude :** les fraudes aux faux présidents/faux virements /faux fournisseurs sont des risques de plus en plus prégnants dans les PME. Des assurances spécifiques Fraude existent pour garantir le montant dérobé.
- **Assurance perte d'emploi des dirigeants d'entreprise :** elle permet aux entrepreneurs et mandataires sociaux de percevoir un revenu en cas de perte d'emploi.

Le traitement des risques a globalement un fort enjeu financier, qui nécessite bien souvent un transfert à l'assurance. En l'absence de spécialiste, l'assurance est souvent dévolue à un DAF, un directeur financier, voire un directeur juridique. Le soutien technique et les conseils d'un intermédiaire d'assurances (courtier, agent général) sont essentiels pour avoir une bonne vision des solutions d'assurances, et plus généralement de financement de risques, disponibles sur le marché et adaptées au besoin spécifique de l'entreprise.

La cartographie des risques devient alors un outil business pour optimiser la négociation de ses contrats d'assurance :

- Elle permet de montrer que les risques sont bien connus et identifiés par le chef d'entreprise, qu'il a réalisé le travail en amont, ce qui rassure les parties prenantes ;
- Elle clarifie les discussions sur les risques à couvrir en priorité et permet au chef d'entreprise de savoir exactement quel budget et quelles assurances il doit prendre ;
- Elle permet aussi de négocier plus finement les polices et les primes.

TROIS POINTS DE VIGILANCE

V. Les 3 points de vigilance spécifiques aux PME-ETI

1 *Capacité du chef d'entreprise à accepter les remises en cause induites par la démarche*

Le chef d'entreprise, spécialement en PME-ETI, est le porteur de sa structure. **L'identification personnelle est habituellement très forte, souvent depuis de nombreuses années.** C'est une force, notamment dans les rapports avec les partenaires de l'entreprise comme les banques, les donneurs d'ordre..., ceux-ci tenant largement compte, dans leurs engagements, de la personnalité du chef d'entreprise, de son ancrage dans l'économie locale, de son vécu entrepreneurial. Il y a donc une construction dans la continuité, avec une prise de risques financiers corrélatifs, que le chef d'entreprise assume seul. Il est très habituellement responsable sur son patrimoine personnel, ayant engagé des cautions bancaires. Il se sent un devoir moral de réussite, garant d'un équilibre et parfois d'une tradition familiale.

Or la gestion des risques est aussi une remise en cause des modèles passés, une interrogation sur la position actuelle et les choix pris, une projection sur un avenir aux évolutions qui deviennent rapides et qui peuvent imposer des choix structurants. **Il faudra au chef d'entreprise un recul suffisant pour accepter de partager une lecture pragmatique, parfois de remise en cause, avec une équipe de direction,** qui n'aura ni porté les réflexions, ni tranché en faveur de décisions parfois difficiles, et n'assumera pas financièrement les choix pris.

2 *Les relations interpersonnelles dans la gouvernance des PME*

Un point complémentaire essentiel, très spécifique aux PME, tient à la gouvernance de ces structures. De nombreuses entreprises sont patrimoniales et familiales. On peut retrouver plusieurs générations qui se succèdent à la tête de ces entreprises mais aussi un consortium familial à la direction. **La difficulté tient au fait que la gouvernance est alors centralisée, sans l'équilibre habituel permettant que chaque fonction de la gouvernance joue son rôle, contre balancier des autres.**

Il est usuellement recommandé que la gouvernance s'articule autour de trois "pouvoirs". Le premier est le "pouvoir souverain", exprimé notamment lors des assemblées générales par les actionnaires. Le second est le "pouvoir de surveillance", d'orientation ou de contrôle, tenu par les administrateurs. Le troisième pouvoir est le "pouvoir exécutif" tenu par les dirigeants. Un juste articulation entre ces trois pouvoirs permet de légitimer, prendre et assumer les décisions durables pour l'entreprise.

Dans les PME, ces trois pouvoirs sont habituellement concentrés et/ou non répartis. Cette concentration peut être un atout : elle permet alors une communauté d'intérêt plus facile, un dialogue direct, le leadership naturel du chef de famille, une confiance réciproque... Mais elle peut aussi soulever des difficultés particulières comme des relations personnelles exacerbées, un passage de témoin intergénérationnel délicat, la place des conjoints...

La question de la loyauté est alors très prégnante et ne doit pas être occultée. **La conduite d'une démarche de gestion des risques peut se heurter, en partie au moins, à la nécessité de devoir prendre en compte cette particularité.** Elle sera susceptible d'interpeller de nombreux sujets délicats tels la pertinence de la gouvernance (place des parents, oncles, tantes, grands-parents, fondateurs et usuellement encore détenteurs de parts sociales), la remise en cause de choix industriels familiaux, l'abandon d'activités de l'entreprise non rentables ou aux process en déclin, portés par un frère, une soeur, un cousin... **Il faudra mesurer quelles marges d'acceptabilité dans la remise en cause du modèle existant sont possibles,** la gestion des risques pouvant conduire le chef d'entreprise à des décisions particulièrement cornéliennes....

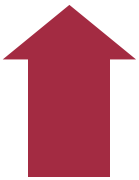
Il est nécessaire d'intégrer cet élément très en amont de la démarche et d'orienter la mise en œuvre de toute action en gardant en tête cet élément. Il est alors préférable de recourir à un tiers extérieur, consultant en gestion des risques, pour conduire la démarche. Ce dernier pourra interpeller et orienter afin de conduire à un constat, factuel, peut-être mieux accepté car posé par un tiers. Si le constat ne parvient pas à être partagé, l'intervention du tiers permettra au chef d'entreprise dirigeant, *a minima*, de s'écarter du lien affectif biaisant l'analyse et la recherche de solutions. Assumer ces dernières restera sa responsabilité...

3 *Confidentialité et anonymisation des renseignements échangés au cours des entretiens*

Les acteurs de la démarche doivent pouvoir exprimer librement leurs idées pour garantir une "matière" importante dans les échanges. Un équilibre délicat et propre à chaque entreprise en fonction de sa culture, sera à trouver entre le partage spontané et la remontée mesurée d'informations. Il semble préférable de convenir entre les acteurs, au début de la démarche, du niveau de partage attendu.

Il sera utile que la personne en charge de la démarche de maîtrise des risques veille, lors des entretiens individuels, à relativiser les informations recueillies qui pourraient être porteuses de doléances ou être utilisées à titre personnel ou de service. Le rappel des objectifs de la démarche en début d'entretien sera nécessaire pour limiter ce risque. De même, la priorisation des risques, décidée en collectif, tempérera également les éventuelles dérives.

Deux points spécifiques aux PME: confidentialité et anonymisation.



Confidentialité

Il est possible que le chef d'entreprise, spécialement dans les PME de petite taille, garde pour lui une part des informations recueillies lors des entretiens. **Cette attitude est le fruit spontané d'une habitude de concentration du lieu de décision mais peut être aussi liée à son doute relatif quant aux capacités de son équipe de direction à se positionner sur des décisions** concernant la stratégie de l'entreprise (les deux facteurs interagissant très certainement).

Ce comportement, si naturel qu'il puisse paraître au regard de la culture de l'entreprise, peut nuire à la pertinence de la démarche. Il faudra veiller à ce que la part d'informations non partagées, si elle doit exister, ne réduise pas l'ambition potentielle de l'étude.

Anonymisation

L'anonymisation des informations collectées est un des fondements de la démarche. On ne cherchera pas "qui a fait", "qui a dit", questions qui ne reposent que sur une recherche de la faute, contraire à l'esprit de la démarche, mais on s'interrogera sur le "pourquoi", qui est la porte d'entrée vers la recherche de solutions, transposables quels que soient les acteurs.

Cependant, en PME, compte tenu du nombre réduit de personnes engagées dans la démarche, le croisement des informations permettra rapidement d'en identifier l'auteur. Il faudra veiller à garantir un recul de chacun, une écoute non accusatrice, au risque de voir la démarche se transformer en prises de positions conflictuelles et stériles.

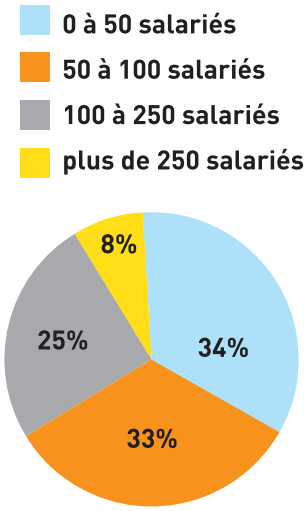
ANNEXES

Annexe 1

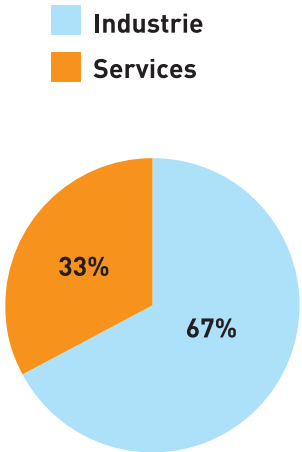
Groupe de travail et méthodologie

Le groupe de travail était composé de 12 entreprises de tailles et de secteurs d'activité variés, adhérents du Medef Deux-Sèvres. L'AMRAE et le Medef Deux-Sèvres remercient chaque membre du groupe pour son implication et sa contribution à ce travail collectif.

Effectifs



Secteurs d'activité



La méthodologie du groupe de travail

1 - Le référent de chaque entreprise a été contacté personnellement pour une présentation du projet général, des objectifs du groupe de travail et afin de recueillir son adhésion.

2 - Des réunions collectives ont été tenues

- Le groupe de travail s'est réuni 4 demi-journées. Un échange de type brainstorming a permis de définir les grandes familles de risques, puis d'analyser, par famille de risque, les différents risques auxquels l'entreprise pouvait être exposée.
- Une liste de points de vigilance, par risque, a été identifiée lors des échanges. Ces points permettent de cerner avec plus de précision le risque évoqué et ses conséquences. Ils peuvent également être des pistes d'action correctrices.

3 - Un questionnaire permettant l'auto-évaluation reprenant l'ensemble des échanges a été établi à la suite de ces réunions collectives. L'outil excel de cartographie des risques a été intégré, s'alimentant automatiquement par la mesure du risque, donnant une vision synthétique en fin d'auto-diagnostic.

4 - Le questionnaire a été testé et amendé auprès de certains membres du groupe de travail puis auprès d'entreprises n'ayant pas participé au groupe de travail. La passation du questionnaire se fait en moyenne en trois heures en face à face.

Annexe 2

Les risques cyber

Les PME et ETI doivent particulièrement être vigilantes car se pensant moins visées par ces risques, elles sont des cibles moins protégées que les entreprises de plus grande taille, donc plus facilement attaquables.

Tous concernés par les risques cyber ! Quelques exemples :

– Perte accidentelle : erreur humaine, panne informatique ;
– Perte intentionnelle :
• Malveillance informatique de concurrents ;
• Intrusion physique dans les locaux ;
• Vols supports numériques (ordinateurs…) ;
• L'hameçonnage (phishing) : leurre envoyé via un faux message, SMS ou appel téléphonique de banques, de fournisseurs… pour voler des informations (comptes, mots de passe, données bancaires…) pour en faire un usage frauduleux ;
• Rançongiciels : pièce jointe ou lien piégé. En cliquant, un cryptage aléatoire des informations s'enclenche, une rançon est demandée pour restauration ;
• Craquage des mots de passe par l'action d'un hacker pour piratage des informations qui peut être récurrent (souvent pas de traces de l'intrusion) /destruction.

Cyber risques en PME : un chiffre à savoir, une question à se poser et un plan d'actions !

1) **Le chiffre :** 80 % du risque cyber est liée à la négligence des salariés → il est donc essentiel de les sensibiliser et de les former régulièrement. Les salariés sont les premiers relais et doivent jouer leur rôle d'alerte.

2) **La question à se poser :** Quelles sont mes données vitales ? → tout n'est pas à protéger mais il faut construire un vrai plan sur l'essentiel.

3) **Plan d'action : points incontournables en PME**

• Avoir **un vrai système de sauvegarde,** voire un PRA (Plan de Reprise d'activité) afin de pouvoir restaurer rapidement ses données et poursuivre l'activité. Tester régulièrement les sauvegardes afin de s'assurer du bon dispositif. Enjeu : quel délai j'accepte d'attendre pour un retour au fonctionnement normal de ma structure et avec quelles pertes ?

• Cloisonnement **des informations** afin que la faille n'impacte que le service concerné ;

- Sécuriser particulièrement les **données jugées « précieuses »** ;
- Sécuriser **les services informatiques mais aussi les locaux et annexes** (vols dans les bureaux, intrusions, vols des clefs usb, ordinateurs dans les voitures…) ;
- Sécuriser **les accès extérieurs par les collaborateurs** au réseau de l'entreprise (smartphone, connexion à distance, ordinateur du domicile…) ;
- **Former et informer** tous les salariés notamment mails, usurpation d'identité, rançongiciels, FOVI (faux ordres de virement) fraude au dirigeant… et instaurer une charte informatique dans l'entreprise sensibilisant aux risques.

Pour aller plus loin et mettre en place une stratégie pour contrer les cyber risques, l'AMRAE a rédigé en 2015, en partenariat avec le CESIN, une publication intitulée « Cyber risques : outil d'analyse et de traitement du risque cyber. »

Cette publication a débouché sur une matrice Excel qui a pour vocation d'être un outil de travail au service du chef d'entreprise et de son équipe (directeur système d'information, manager de risques, DAF…), lui permettant de poser les bases d'une analyse précise de l'univers des risques cyber de son entreprise.

Elle est structurée autour de 5 étapes clefs :

L'étape #1 : Identification des risques

Elle se matérialise dans la matrice par la description précise d'**une liste indicative de scénarios de risques « Cyber »,** à laquelle l'entreprise est susceptible d'être exposée. Cette liste, fruit des échanges du groupe de travail, doit bien évidemment être personnalisée, amendée ou complétée, en fonction de l'univers de risque propre à chaque entreprise, ses métiers et les territoires où elle réalise ses activités.

Chaque risque doit être objectivé pour être compréhensible de manière identique par les différents acteurs impliqués dans l'analyse.

Pour comprendre au mieux les scénarios de risques proposés, nous recommandons que chaque terme utilisé soit expliqué et partagé entre les métiers « SI » et Gestion des risques » via un vocable commun. Les échanges du groupe de travail ont en effet montré combien il est important d'arriver à une lecture et une compréhension commune de chaque terme employé, afin de partager le scénario.

Exemples :

- Fraude due à la vulnérabilité des SI hébergés et /ou managés par l'infogérant.
- Indisponibilité du SI et du service fourni par l'infogérant à l'entreprise suite évènement accidentel sur équipement.
- Panne, dérangement (sans dommage matériel) des installations informatiques et/ou des installations d'infrastructures annexes de l'assuré, pouvant entrainer altération ou destruction de données tiers par l'entreprise
- Doutes sur la sécurité des données suite à un dommage matériel à l'outil de production chez l'entreprise ou chez un prestataire/infogérant.
- Grève, émeute, mouvement populaire générant la destruction des infrastructures de l'entreprise, d'un prestataire de service. d'hébergement désigné ou infogérant désigné.
- Erreur de l'assuré générant une compromission de la sécurité de données personnelles.
- Erreur de programmation de la part de l'entreprise.
- Défaillance d'une prestation de service technologique (installation d'applicatif, administration de serveurs....) ou défectuosité d'un système développé et opéré par l'entreprise pour un client.
- Pénétration dans le système de l'entreprise avec destruction des données de l'assuré + données clients, dont des données personnelles.
- Doutes sur la sécurité des données suite à intrusion dans les systèmes. Coupure/isolation par (décision assuré) du système pour limiter le risque de fraude.

L'étape #2 : Evaluation des impacts

Elle vise à lister **les typologies d'impacts** de chacun des risques. Cette description des impacts est scindée en deux :

- impacts sur l'entreprise (ie. l'entité objet de l'étude),
- impacts sur les tiers.

Cette description sera ensuite complétée par une **évaluation financière** des typologies d'impacts identifiés.

L'étape #3 : Traitements en place

Cette étape s'intéresse aux mesures de gestion et de réduction des risques déjà en place et/ou jugées nécessaires et demande de les décrire.

Cette étape n'est pas présente dans la matrice dans sa version actuelle mais pourrait facilement être ajoutée sous la forme d'une colonne supplémentaire.

Il s'agit essentiellement de lister **les mesures de prévention et ou protection** mises en place dans l'entreprise. Ceci permet « d'affiner » l'analyse de l'intensité de l'impact, de passer à la quantification d'un impact des risques résiduels, puis de faire le lien avec la couverture assurantielle actuelle décrite en étape #4.

L'étape #4 : Polices d'assurances actuelles

Elle permet au chef d'entreprise ou au gestionnaire de risques de décrire la ou les réponses apportées par les polices d'assurance en place au sein de l'organisation. Les polices qui doivent être décrites ici sont par exemple les polices :

- Dommages aux Biens et/ou Pertes Financières Consécutives,
- Responsabilité Civile Générale,
- Fraude,
- Autres types (à décrire selon l'entreprise objet de l'analyse),
- Cyber.

Cette étape se réalise par une description, par risque identifié et pour chaque police listée :

- des frais et postes de dépenses couverts,
- des frais qui ne seraient pas couverts par ces polices mais qui pourraient l'être en étendant une garantie,
- des niveaux « idéaux » de garantie,
- des limites des programmes actuels.

L'étape #5 : Résultats actuels et besoins d'adaptation

Non formalisée dans la matrice Excel, cette étape est la synthèse de l'analyse. Cette synthèse permet le questionnement de l'efficacité des solutions de traitement et de financement en place : ce système est-il adapté et aussi efficace que prévu ?

La réponse à ces questions peut, le cas échéant, déboucher sur la définition d'un ou plusieurs plans d'actions, que ce soit pour compléter ou faire évoluer des mesures de gestion ou de réduction du risque, pour ajuster les garanties et limites des polices en place, ou pour souscrire une garantie dédiée « Cyber » dont les contours seront définis par le résultat de l'analyse décrite plus avant.

Pour aller plus loin : Cahier technique AMRAE/CESIN : « Cyber risques : outil d'aide à l'analyse et au traitement assurantiel ». 2015

Annexe 3

Gestion de crise et PCA :

AVANT LA CRISE :

Mettre en place un dispositif de gestion de crise. Attention : chaque crise est un cas particulier.

- Préparer les procédures (et la liste des collaborateurs en astreinte, avec leur n° de téléphone…), les scénarios de risques majeurs et leur déroulé.
- Définir quand passe-t-on en mode crise ? Quels indicateurs ? Qui et quand décide de passer en crise ?
- Nommer un coordinateur de la crise : relais, porteur des scénarios établis avec la direction générale. Il implique, organise les exercices de gestion de crise, tests et simulations adaptés à l'objectif visé.
- Nommer celui qui communiquera (si besoin) aux médias. Le meilleur ! Pas forcément le DG…
- Former les collaborateurs et la Direction : media training, transferts d'expériences (in/out cœur de métier).
- Tester le dispositif avant la crise.

PENDANT LA CRISE :

Mettre en œuvre le bon scénario

- Connaître les faits, la vérité et globalité de l'information, dans un contexte d'urgence et de pression interne et externe.
- Choisir le scénario, définir le niveau de responsabilité associé (et gravité).
- Appliquer le scénario sur décision du PDG.
- Communiquer de manière appropriée…
- Organiser la coordination opérationnelle : lien avec la Préfecture et autres. interdépendances (informer son assureur au plus tôt) ; l'entreprise n'est pas seule.

APRÈS LA CRISE : DEBRIEFER

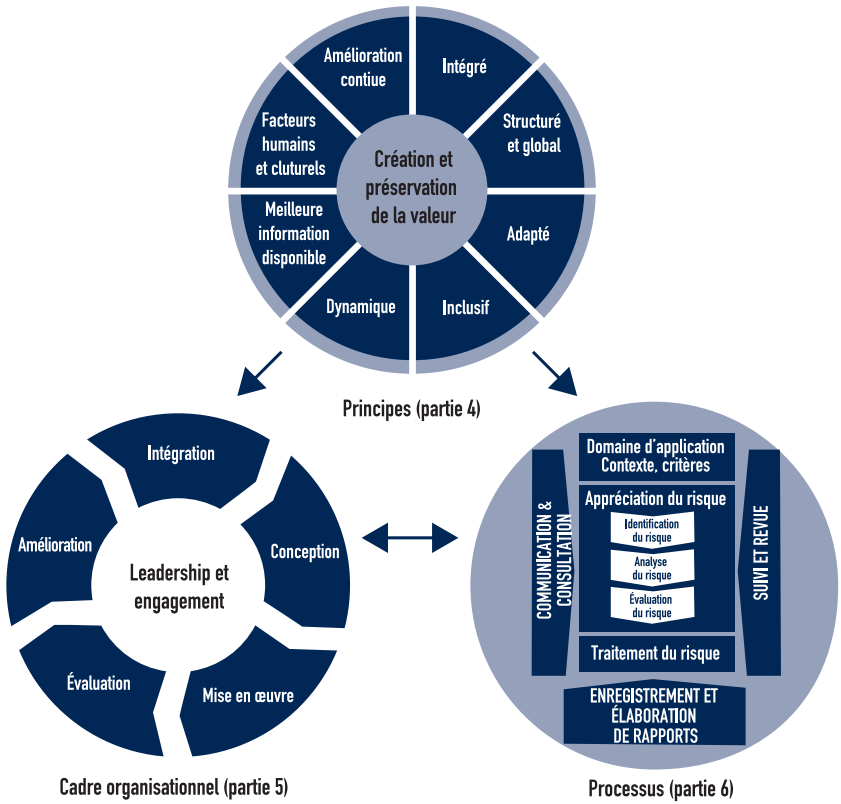
- Organiser le débriefing et les retours d'expérience : causes, conséquences, processus de A à Z, les acteurs, les moyens à disposition et les correctifs envisagés (y compris organisation , c'est le moment de se remettre en question) ;
- Décider de la poursuite ou non de la communication (média) ;
- Capitaliser selon le type et la durée de la crise.

Pour aller plus loin : AMRAE : « Le plan de Continuité d'Activité » - Auteurs : Sophie Huberson et Benoit Vraie - SNELAC. 2016

Annexe 4

Norme ISO 31000 – COSO ERM - AMF

ISO31000 : Norme qui fournit des principes, un cadre et des lignes directrices pour gérer toute forme de risque. Cette norme peut être utilisée par tout type d'organisme sans distinction de taille, d'activité ou de secteur. Elle n'a pas vocation à être certifiante.

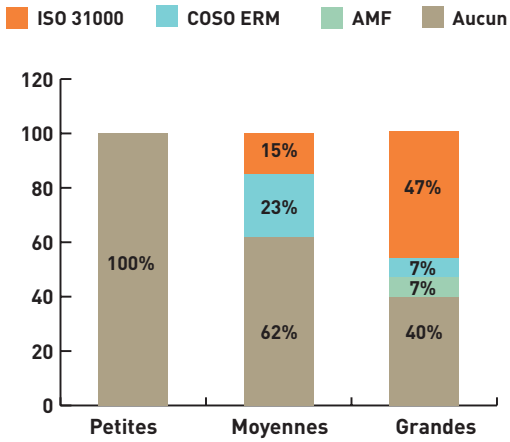


ISO 31000:2018 - Management du risque - Lignes directrices

COSO ERM : Référentiel qui permet aux entreprises de mieux comprendre l'impact concret de la culture sur la gouvernance des risques et l'appréciation des risques dans la sélection et l'exécution de la stratégie.

CADRE AMF : Sur le sujet de l'utilisation de ces référentiels, l'Amrae a présenté, lors d'un atelier-conférence, aux Rencontres du Risk Management Amrae 2018, une « Comparaison des référentiels utilisés par les sociétés non cotées » : *Source DELOITTE Décembre 2017.*

Les résultats présentés se fondaient sur la base de 20 organisations françaises non cotées en bourse : 2 petites, 13 moyennes et 5 grandes. Les « Petites organisations » ont un effectif inférieur à 250 personnes. Les organisations de taille « Moyenne » ont un effectif inférieur à 5000 personnes. Les « Grandes organisations » ont un effectif supérieur à 5001 personnes.



Annexe 5

Les principaux indicateurs financiers pour construire son tableau de bord

Chaque chef d'entreprise suit, bien évidemment, son activité et la situation financière de son entreprise. La mise en place d'un tableau de bord « formalisé » reprenant les indicateurs clés est donc un outil de pilotage et de réduction des risques financiers. Leur suivi à des échéances très régulières est indispensable.

Neuf indicateurs sont détaillés ici pour compléter les vôtres. C'est notamment sur la base de ces indicateurs que vos partenaires financiers réalisent leurs analyses et la cotation de votre entreprise.

- **Chiffre d'affaires dégagé sur la période :** cet indicateur peut être ventilé par produits ou famille de produits ; on s'attardera davantage sur son évolution que sur le chiffre lui-même.
- **Affaire moyenne traitée (ou panier moyen) :** là aussi l'évolution sera surtout prise en compte. Sachant qu'en général le coût unitaire pour un client est le même quel que soit le montant des achats, on sera attentif à une baisse de cet indicateur.
- **Taux de nouveaux clients :** c'est le nombre de nouveaux clients rapporté au nombre de clients fidèles. Cela permet de mesurer le dynamisme commercial de l'entreprise.
- **Taux de marge brute par opération :** exprimé en pourcentage, c'est la différence entre le prix de vente et le prix de revient (coût d'acquisition pour les entreprises uniquement commerciales) divisé par le prix de vente. Une érosion du taux montre des difficultés à vendre au prix catalogue, soit sous l'effet d'une concurrence accrue, soit d'un marché atone.
- **Solde de trésorerie d'exploitation :** différence entre les encaissements et les décaissements d'exploitation. Cela indique si l'exploitation dégage du cash de façon récurrente.
- **Solde global de la trésorerie :** A suivre particulièrement. Une baisse continue du solde de trésorerie indique des difficultés de rentabilité de l'entreprise.

- **Evolution des comptes clients :** une forte augmentation de ceux-ci peut être bien entendu liée à une progression du chiffre d'affaires. Mais elle est souvent le résultat d'un laisser-aller au niveau des relances clients.
- **Montant du carnet de commandes :** cela donne une visibilité à plusieurs semaines, voire plusieurs mois. Une baisse continue présage de difficultés futures.
- **Estimation du chiffre d'affaire prévisionnel pour les 3 prochains mois :** tout comme le montant du carnet de commandes, il nous donne une visibilité et donc laisse la possibilité d'une action commerciale rectificative au cours des prochains mois.

Notes

Notes