MANAGEMENT DES RISQUES ET ENTREPRISE ÉTENDUE

AMRAE
la Maison du risk management

Deloitte.

À propos de l'AMRAE :

L'Association pour le Management des Risques et des Assurances de l'Entreprise (AMRAE) rassemble les acteurs majeurs des lignes de maîtrise du risque (risk management, contrôle et audit internes, assurance et juridique). À travers ses comités scientifiques, publications, positions et son congrès de référence, elle œuvre pour l'excellence de la gestion des risques qui contribue à la sécurisation de la stratégie des organisations et organise leur résilience.

L'AMRAE a quatre missions fondamentales :

- Promouvoir le concept de risk management,
- Porter et maintenir l'expertise des risk managers au meilleur niveau,
- Anticiper et influencer le marché de l'assurance des entreprises,
- Rayonner vers les pouvoirs publics et les institutions civiles.

Avec AMRAE Formation, elle répond aux besoins de formation professionnelle 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 3 200 participants en 2023). Ces trois jours constituent le rendez-vous métier incontournable des acteurs de la maîtrise des risques et de son financement.

À propos de Deloitte :

Deloitte, leader des services professionnels en Audit & Assurance, Consulting, Financial Advisory, Risk Advisory et Tax & Legal, avec un chiffre d'affaires de 1 039 M€, mobilise l'ensemble de ses expertises pour répondre aux enjeux de ses clients de toutes tailles et de tous secteurs d'activités. Fort de ses 7 700 collaborateurs et associés, la firme s'est donnée comme fondement d'offrir un service d'excellence, de proximité, alliant des compétences locales et un réseau d'experts en France et dans le monde, et avec une ambition commune « Make an impact that matters ».

Les équipes Risk Advisory de Deloitte aident les entreprises à répondre aux demandes d'un environnement changeant, qui apporte son lot de nouveaux risques comme de nouvelles opportunités. Image de marque, impact de l'entreprise sur l'environnement, mise en conformité face à un environnement réglementaire complexe, protection des actifs numériques… : il est crucial pour les entreprises de connaître les risques, de les évaluer, les modéliser, afin de prendre des décisions éclairées. Grâce à ses équipes, Deloitte offre un panel d'expertises qui lui permettent d'accompagner au quotidien ses clients sur de nombreuses thématiques et notamment celle de la maîtrise de leurs relations avec leurs tiers, en leur apportant une vision globale des risques et de la performance de leurs tiers.

Remerciements

L'AMRAE remercie très sincèrement toutes les personnes qui ont contribué à la préparation, à la rédaction et à la finalisation de cet ouvrage, et particulièrement, les membres du groupe de travail :

- **Sonia Cabanis,** associée Risk advisory Deloitte, pour son implication personnelle,
- **Patrick Lheureux,** expert indépendant, membre de la commission nationale Afnor « Management des risques » et **Denis Zandvliet**, VALU€360, pour leur engagement sans faille dans la durée,
- **Philippe Noirot,** ancien administrateur de l'AMRAE, pour avoir coordonné ce projet avec passion.

Ainsi que :

- Fanny Dreyfous-Ducas, Arengi, pour son soutien et ses apports,
- Les institutions, associations professionnelles, organismes gouvernementaux et instituts, pour l'illustration qu'ils donnent de l'Entreprise étendue et de ses risques,
- Tous ceux qui ont apporté une brique à cet ouvrage,
- Enfin, les risk managers interviewés, pour avoir exprimé leurs points de vue sur la question suivante : « Pour vous, les risques de l'Entreprise étendue, c'est quoi ? ».

Ces points de vue sont illustrés par ce pictogramme.

Préface

par Stéphane Pallez,
Présidente Directrice Générale du Groupe FDJ

Les entreprises sont toujours plus étendues qu'elles ne le croient !

Les frontières juridiques, contractuelles ou parfois géographiques délimitent nécessairement un premier périmètre d'activité pour une organisation, mais il est indispensable pour les dirigeants et les acteurs de la gestion des risques de voir plus loin. À ce titre, la définition de « l'entreprise étendue » retenue dans cet ouvrage reflète la complexité et la multiplicité des enjeux auxquels nos organisations font face et doivent se préparer.

La **prise de conscience** des dépendances entre les événements externes et les acteurs a pris une dimension particulière - et souvent brutale - pour les entreprises lors de la crise sanitaire de 2020 ou plus récemment face à la crise énergétique. Les risk managers, assureurs ou réassureurs voient pourtant ces liens se dessiner depuis plusieurs années déjà. En 2011, alors que je prenais mes fonctions de Présidente directrice générale du Groupe de réassurance CCR, la catastrophe de Fukushima et les inondations en Thaïlande révélaient déjà l'interdépendance des chaînes de production mondiale pour les entreprises et pour le marché de l'assurance. Ces sujets avaient alors été intégrés dans nos politiques de souscription.

La **compréhension** de ce qui entoure une organisation, la vision des différents acteurs et de leurs enjeux est une étape fondamentale de la gestion des risques de l'entreprise étendue. S'il n'existe pas de recette unique pour cartographier l'ensemble de ces parties prenantes, la première partie de cet ouvrage propose néanmoins plusieurs outils, critères ou pistes d'analyses pour obtenir une vision large de l'écosystème de l'entreprise.

Pour un groupe comme FDJ, le « périmètre étendu » comporte bien évidemment plus de 25 millions de clients en France, mais de nombreuses autres dimensions sont prises en compte : l'axe « territorial » liés aux 30 000 points de vente en France (le réseau le plus maillé), l'axe « conformité » dans nos relations avec les autorités de régulation ou encore l'axe « sociétal » par nos engagements dans le sport et notre politique RSE. Le Comité des parties prenantes de FDJ est une excellente illustration de la **diversité d'acteurs** de l'écosystème de FDJ. Créé fin 2020 pour assurer le suivi de la mise en œuvre des engagements de la raison d'être du Groupe, ce Comité intègre des représentants des joueurs, de nos commerçants partenaires (Confédération des buralistes, Culture presse), des collectivités locales mais également des experts des sujets d'addiction ou de la lutte contre le blanchiment.

Dans sa *deuxième partie*, cet ouvrage aborde les étapes - parfois techniques - d'identification et d'évaluation de tous les risques de l'entreprise étendue. Les différentes approches présentées sont autant d'outils à disposition des responsables de la gestion des risques, outils à adapter ensuite aux spécificités de leur organisation. Un point doit particulièrement retenir notre attention et concerne le partage entre le risk manager et la personne en charge du suivi de la relation avec la partie prenante concernée. Loin d'être un exercice en chambre, l'identification et l'évaluation des risques passent par un **travail en co-construction**, un partage des points de vue avec les experts : acheteur ou équipe métier concernant les risques liés à un fournisseur, équipes juridiques ou commerciales concernant les risques liés à un engagement client, etc.

Plus largement, l'appui sur des données externes ou sur des retours d'expériences de pairs est une clé complémentaire pour déchiffrer la nature des risques, les évaluer ou les cartographier. À ce titre, les acteurs du monde de l'assurance ou du courtage peuvent apporter une grande richesse dans les expertises, données ou modélisations disponibles. Depuis maintenant plus de 10 ans, l'Observatoire National des risques naturels, associant l'Etat, la Caisse centrale de réassurance (CCR) et les assureurs, permet par exemple aux professionnels et aux particuliers d'accéder aux données relatives aux risques naturels en France pour une meilleure connaissance de ces phénomènes et de leurs impacts.

La *troisième et dernière partie* de cette publication porte sur le traitement des risques de l'entreprise étendue et les différentes étapes de mise en œuvre des actions de prévention ou de continuité possible. La majorité des approches, méthodes et autres changements culturels et organisationnels présentés constituent des pistes à explorer pour les acteurs de la gestion des risques.

Il est fondamental que ces démarches de gestion des risques **s'inscrivent dans le temps**. Dans la gestion des relations avec les fournisseurs par exemple, l'intégration d'une clause contractuelle permet d'obtenir rapidement un engagement formel de chaque fournisseur dans la gestion de ses propres risques. La mise en place d'actions au long cours apparaît encore plus efficace. À titre d'exemple, plusieurs années ont été nécessaires pour instaurer une démarche transversale d'achats responsables au sein de FDJ. Ce travail de structuration, reconnu en 2021 avec l'obtention du *Label Relations fournisseurs et achats responsables*, permet de développer des relations mutuellement bénéfiques, porteuses d'innovation et créatrices de valeur avec nos fournisseurs. Ce faisant, FDJ prévient les difficultés éventuelles de ses partenaires et peut porter ses efforts sur leur accompagnement, par exemple sur des sujets RSE.

Complexe et spécifique, la gestion des risques de l'entreprise étendue est un exercice inédit, pouvant s'appuyer sur des approches variées, complémentaires et à adapter au contexte de chaque organisation. Cet ouvrage fournit un excellent référentiel qui inspirera tout acteur de la gestion des risques dans sa démarche de protection des activités de son organisation et d'aide à la prise de décision.

Biographie

Stéphane Pallez est Présidente directrice générale du Groupe FDJ depuis novembre 2014.
Stéphane Pallez est également membre des conseils d'administration de CNP Assurances et d'Eurazeo, dont elle préside les Comités d'audit et des risques. Elle est également Présidente du conseil d'administration du Conservatoire national supérieur de musique et de danse de Paris (CNSMDP).
Stéphane Pallez était précédemment Présidente directrice générale du Groupe de réassurance CCR de 2011 à 2014. De 2004 à 2011, elle a été Directrice financière déléguée du Groupe de télécommunications France Télécom-Orange.
De 1984 à 2004, Stéphane Pallez a exercé différentes fonctions en cabinets ministériels ainsi qu'à la Direction générale du Trésor au ministère de l'Économie et des Finances.
Stéphane Pallez est diplômée de l'Institut d'études politiques (IEP) de Paris et ancienne élève de l'École nationale d'administration (ENA – promotion Louise Michel).

Crédit photo : Ferrante Ferranti

Sommaire

Les **risques** (*) créés et subis par l'Entreprise étendue se gèrent-ils comme les autres risques ? Sont-ils moins prédictibles ? Sont-ils plus difficiles à identifier et évaluer ?

Leurs origines ne sont-elles qu'externes ? Et leurs **impacts** ne sont-ils qu'internes ?

L'Entreprise étendue aurait-elle alors une perspective aussi infinie que la multiplicité de ses **parties prenantes** ? (cf. figure 1 « Sphère de l'Entreprise étendue »).

Répondre à toutes ces questions n'est pas simple. C'est pourquoi l'AMRAE vous propose cette réflexion à 360 degrés sur l'Entreprise étendue et les risques qui y sont liés.

Déterminer ce qu'est l'Entreprise étendue est essentiel pour mettre en oeuvre la meilleure approche possible de ses risques. Par analogie avec deux des possibles étymologies du mot risque, latine (resecum : ce qui coupe) et grecque (rhiza : racine), il est indispensable d'identifier les multiples liens d'une organisation avec son environnement proche ou plus lointain, pour anticiper et éviter des **conséquences** intempestives sur ses activités !

Cet ouvrage a pour objectif d'aider les entreprises, les institutions, les associations et toutes les organisations privées, publiques ou parapubliques (**), à mettre en œuvre un dispositif de **management des risques / gestion des risques / ERM** (***) adapté à leur Entreprise étendue. Il vous propose avec humilité une approche la plus globale possible, au travers de multiples pistes de réflexion. Son propos intéressera aussi, au-delà des **risk managers**, les dirigeants qui découvrent l'étendue de l'approche par les risques et souhaitent la structurer.

Et sur un sujet si ouvert où tout change continuellement, notre propos se réfère à de nombreuses autres définitions de l'Entreprise étendue. C'est pourquoi, dans le but de vous offrir une lecture sans risque d'incompréhension ou de confusion, un glossaire multi-sources est là pour vous aider !

(*) Les mots ou expressions figurant au glossaire sont matérialisés dans le texte par une police épaisse lors de leur première occurence. Cf. Annexe 1 « Glossaire »
(**) Cf. Annexe 12 « Bibliographie » "Primo - Public Risk Management Organisation …"
(***) ERM : Enterprise Risk Management

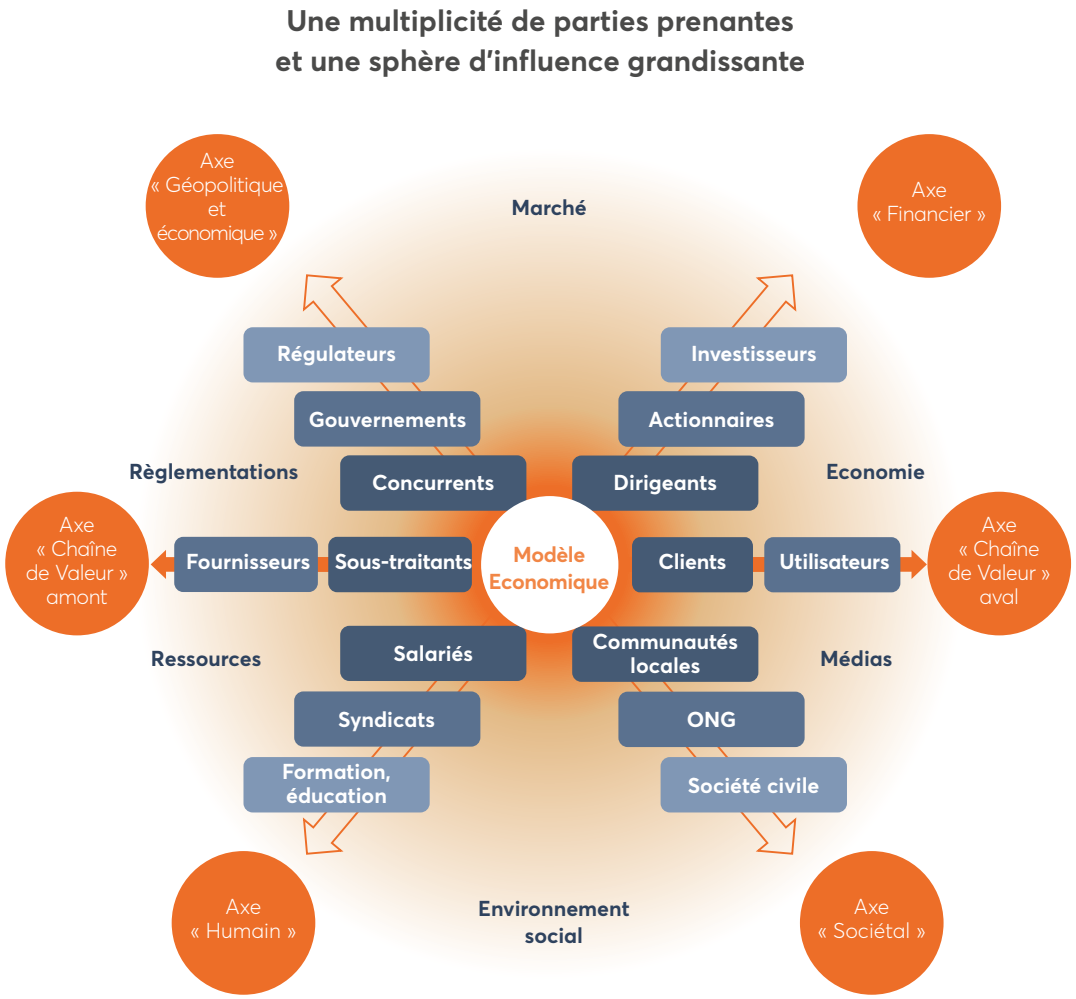


Figure 1 – Sphère de l'Entreprise étendue

Une entreprise est toujours plus étendue qu'on ne le pense !

Toutes les organisations sont concernées, quels que soient leur taille et le nombre de leurs relations avec des tiers. Un dirigeant n'a pas toujours conscience, et encore moins une vision parfaite, de la réalité de son Entreprise étendue.

Aujourd'hui, dans un monde d'affaires globalisé (mondialisation, numérisation, dématérialisation, virtualisation, « uberisation », traités commerciaux multilatéraux, intermédiation, ...), toute entreprise ou organisation publique, quel que soit son secteur d'activité, peut être considérée comme étendue, à plus ou moins grande échelle. Elle ne peut pas durablement fonctionner et survivre de manière isolée.

L'entreprise artisanale elle-même peut s'analyser dans une perspective d'entreprise étendue : approvisionnement, préparation, stockage, distribution directe, encaissement. Elle fait forcément partie d'un réseau plus ou moins grand de clients, de partenaires, de fournisseurs et sous-traitants, d'agents, de relations diverses… qui forment sa sphère d'influence.

L'étendue de la sphère d'influence de l'entreprise va au-delà des acteurs traditionnels (fournisseurs, clients, employés) de la chaîne de valeur. Elle englobe de nombreux autres acteurs externes dans l'environnement économique, sociétal ou politique de l'entreprise, aussi bien au niveau local que mondial, (cf. figure 1 « Sphère de l'Entreprise étendue »).

De plus, tout au long de son cycle de vie, une entreprise va chercher à s'étendre pour :

- Trouver de nouveaux marchés ;
- Augmenter ses parts de marchés ;
- Réduire ses coûts de production ;
- Améliorer son image ;
- Intégrer des projets pluri-partenaires ;
- Renforcer son potentiel humain (flexibilité, mobilité), élargir son spectre de compétences ;
- Accéder directement à l'innovation ;
- S'affranchir de règlementations lourdes ;
- Optimiser l'efficacité de ses processus ;
- Réduire des risques locaux ou nationaux ;
- …

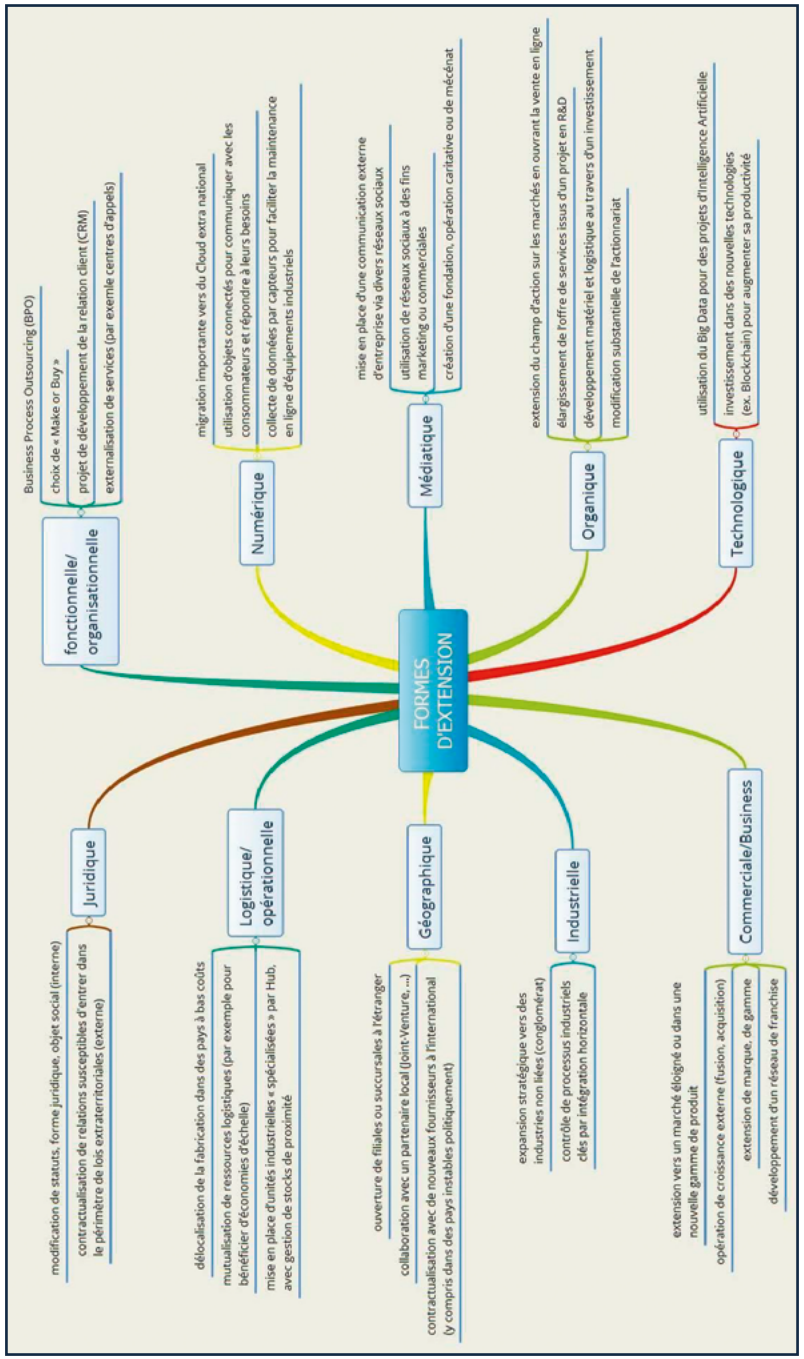


Figure 2 – Formes d'extension de l'Entreprise étendue

Dans leur écosystème, la plupart des organisations sont exposées à de multiples risques, souvent hors de leur contrôle direct, générés par des acteurs tiers avec lesquels elles entretiennent des relations parfois indirectes, de niveau secondaire, tertiaire, voire au-delà. Le comportement et les actions de ces acteurs souvent méconnus de la gouvernance peuvent pourtant avoir un impact sur la bonne marche ou la réputation de l'entreprise. D'autant que, dans le monde actuel de plus en plus interconnecté, les liens et interfaces avec ces tiers ne sont pas systématiquement contractuels ou connus.

Des expositions nouvelles, parfois insoupçonnées, peuvent ainsi apparaître par ricochet, effet domino, effet collatéral aussi bien sur la chaîne de valeur que dans le reste de l'environnement de l'entreprise. Les menaces sont parfois situées dans les pays d'implantation des tierces parties où des modèles, des juridictions, des normes, des standards, des cultures localement très différents peuvent représenter un réel défi à relever et maîtriser.

L'extension peut prendre diverses formes : géographique, numérique, opérationnelle, organique, juridique, etc… (cf. figure 2 « Formes d'extension de l'Entreprise étendue »).

Point de vue d'un risk manager

« Maîtriser la complexité de son Entreprise étendue offre l'opportunité d'une intelligence collective avec les parties prenantes permettant de regarder les enjeux en face, afin de résoudre ensemble les difficultés et les problèmes rencontrés. »

Un risk manager du secteur des services industriels.

Les risques provenant des tiers peuvent être multiformes et toucher l'entreprise de plusieurs façons : une légère perturbation de sa production, une détérioration profonde et durable de son image, ou encore des impacts légaux et règlementaires sévères. Par exemple les lois et réglementations en France liées au devoir de vigilance, à la lutte contre la corruption ou à la protection des données personnelles, induisent des risques externes accrus ou nouveaux. Au niveau international, le domaine réglementaire concerne également l'Entreprise étendue au travers de l'extra-territorialité d'un certain nombre de lois.

A titre d'illustration, voici quelques exemples caractéristiques d'**évènements** produisant des risques de l'Entreprise étendue, qui seront développés à la section 2.1 « Quels sont les risques de l'entreprise étendue ? » :

- Un consommateur, client ou non, organise un boycott sur les réseaux sociaux ;
- Un distributeur communique, volontairement ou non, des informations confidentielles sur les clients de l'entreprise ;
- Un partenaire indélicat divulgue des données stratégiques ;
- Un fournisseur de composants stratégiques fait faillite et engendre une rupture d'approvisionnement ;
- Un fonds d'investissement lance une OPA hostile ;
- Un pays tiers édicte une nouvelle norme (ou une nouvelle loi) contraignante, avec un principe d'extra-territorialité ;
- Une organisation criminelle ou un Etat lance une cyberattaque déstabilisante ;
- La contrefaçon d'un produit mal protégé juridiquement se répand sur le marché ;
- …

Lorsqu'un évènement survient, les risques de l'Entreprise étendue peuvent être acceptés, dans les limites définies par le cadre de l'**appétence aux risques** de l'Entreprise. Selon la gravité de l'évènement en question, l'ouverture d'une cellule de crise peut s'avérer nécessaire pour en traiter les impacts et les conséquences.

Tous les risques habituels (cf. figure 3 « Exemple de panorama des risques par nature ») sont susceptibles de concerner l'Entreprise étendue. Cependant, par une action volontaire d'extension, ou par un effet de bord, une nouvelle nature de risques, non considérée jusqu'à présent, peut émerger (cf. figure 12 « Exemple 1 d'extension du périmètre usuel des risques par nature de risques » et figure 13 « Exemple 2 d'extension du périmètre usuel des risques par identification de 3 nouvelles natures de risques »).

Figure 3 – Exemple de panorama des risques par nature

Dans le cadre de la stratégie, une opportunité d'extension de l'entreprise (partenariat, joint-venture, …), peut simultanément faire apparaître de nouveaux risques et réduire des risques déjà identifiés, notamment par transfert ou partage. Dans ce panorama, au fil du temps, l'exposition aux risques peut augmenter ou diminuer en fonction du degré d'extension de l'entreprise.

Il est important d'anticiper les risques induits par l'Entreprise étendue afin de les maîtriser. La gouvernance de l'entreprise doit être en mesure de déterminer où, comment et quelle partie prenante de son écosystème expose son fonctionnement, sa rentabilité, sa réputation, son image, ses actifs matériels ou immatériels. L'un de ses premiers objectifs est donc d'identifier et cartographier l'intégralité des acteurs et parties prenantes de son écosystème, ayant ou non un lien contractuel, en mesurant le degré de dépendance envers ceux-ci.

Une approche de gestion des risques couvrant la connaissance systématique l'écosystème s'avère donc nécessaire. Les dispositifs de gestion de crise et de continuité d'activité complètent cette approche. Ils doivent comporter une analyse des conséquences - opérationnelles, humaines, financières ou d'image - d'un évènement survenu dans le périmètre étendu de l'entreprise.

A l'aide d'exemples pragmatiques, les objectifs de notre propos dans cet ouvrage sont de deux ordres. D'une part, nous montrerons comment structurer ce sujet complexe pour le rendre plus compréhensible. D'autre part, nous souhaitons donner des clés aux dirigeants et aux risk managers d'une organisation pour leur permettre de :

- Mieux appréhender ce qu'est l'Entreprise étendue, son périmètre ;
- Anticiper les différentes natures de risques susceptibles d'apparaître, de se renforcer, de diminuer ou de disparaître selon la nature d'extension envisagée ;
- Détecter par une meilleure connaissance de leur propre écosystème les risques induits par les tiers ou les parties prenantes ;
- Analyser les impacts potentiels de ces risques, les identifier qualitativement et les évaluer ;
- Identifier des moyens, organisationnels, juridiques, matériels ou autres, à mettre en place pour s'en prémunir et mieux les contrôler ;
- Connaître les acteurs impliqués dans le **traitement** de ces risques ;
- …

Questions types ?

Q1	Une entreprise intéressée par un partenariat à la suite d'un contact lors d'une exposition internationale et avec laquelle il n'y a aucune relation antérieure est-elle sincère/fiable ?
Q2	L'aval de l'entreprise est-il suffisamment supervisé pour garantir la réalisation de ses activités en conformité avec sa raison d'être et ses valeurs ? Réseau de distribution, franchisés, ...
Q3	Le tour de table / pacte actionnarial est-il susceptible d'évoluer en mettant l'entreprise en risque ?
Q4	Les personnels à l'étranger de l'entreprise sont-ils suffisamment informés, préparés, protégés en zones difficiles, particulièrement en zones à risques ?
Q5	Les produits / activités / services de l'entreprise sont-ils susceptibles de heurter des règles sociales / sociétales / environnementales locales ?
Q6	Les différences interculturelles sont-elles bien prises en compte dans le fonctionnement interne et vis-à-vis de toutes les parties prenantes externes ?
Q7	La fiscalité des pays dans lesquels l'entreprise a des intérêts est-elle connue et maîtrisée ?
Q8	De nouveaux standards internationaux, ou normes règlementaires, sont-ils en cours d'élaboration risquant de concerner les produits ou les services de l'entreprise ?
Q9	Les composants importés utilisés dans les processus de fabrication des produits de l'entreprise proviennent-ils de zones à risques non encore identifiées ?
Q10	L'architecture réseau mise en place avec les partenaires et clients et fournisseurs stratégiques de l'entreprise pour partager des informations et accéder au système d'information est-elle parfaitement sécurisée ?
Q11	Les nouvelles technologies utilisées ou mises en place par l'entreprise dans son projet de transformation numérique sont-elles sûres ?
Q12	De nouveaux modèles économiques, ou technologies disruptives, sont-ils en train d'apparaître risquant de compromettre l'activité ou la pérennité de l'entreprise ?
Q13	Toutes les transactions commerciales de l'entreprise sont-elles en conformité avec les lois et réglementations diverses locales / internationales ?
Q14	Les sous-traitants de rang 1 utilisent-ils en cascade des sous-traitants avec des pratiques pouvant nuire à l'image ou la réputation de l'entreprise ?
Q15	Des messages insuffisamment contrôlés provenant des employés ou dirigeants de l'entreprise (publicités trash, prise de parole en public, ...) ou une communication négative des médias détectée tardivement sont-ils susceptibles de porter atteinte à son image ou à sa réputation ?
Q16	Des procédés / composants / services / marques développés et vendus par l'entreprise sont-ils déjà couverts par des brevets ?
Q17	Des opérations de mécénat actuelles ou envisagées, issues d'un rachat d'entreprise ou créées, sont-elles en parfaite cohérence avec la raison d'être et les valeurs de l'entreprise ?
Q18	Les équipements / produits intégrés dans des systèmes complexes et revendus à l'international tombent-ils sous le coup d'embargo ou de restrictions d'exportation (biens à double usage) ?

Figure 4 – Questions types

A ces fins, nous avons établi une liste non exhaustive de questions que les dirigeants ou le risk manager doivent pouvoir se poser (cf. figure 4 « Questions types »).

Cette liste est complétée par des informations sur les questions (cf. Annexe 2 « Questions types – Caractéristiques »), leur positionnement dans la sphère d'influence, les domaines de risque concernés, les impacts potentiels et le renvoi aux fiches exemples de l'ouvrage. Pour chaque question, nous avons développé des exemples de risque sur un cas type présenté en Annexe 11. Des sources d'informations sur des cas similaires sont mentionnées (cf. Annexe 3 « Questions types – Sources détaillées des cas réels similaires »).

1. L'Entreprise étendue et son écosystème

Des résultats d'études et d'enquêtes récentes, mentionnées dans la bibliographie en annexe 12, révèlent que les menaces liées à différentes formes d'extension, voulues ou non, sont perçues en progression par les entreprises et peuvent conduire à des impacts financiers importants :

- L'une des craintes principales des dirigeants est l'excès de règlementations. L'incertitude géopolitique ou économique, les conflits commerciaux et les cybermenaces progressent aussi de manière significative dans leurs craintes (PWC - 23rd CEO Survey 2020).
- La gestion des risques liés aux fournisseurs est une préoccupation importante chez les acheteurs. 75% d'entre eux déclarent avoir des objectifs précis en matière de risques logistiques, financiers, juridiques, qualité, normatifs, RSE (Responsabilité Sociétale des Entreprises), sanitaires, opérationnels ou d'image (CNA – Baromètre Acheteurs 2019).
- La cybercriminalité (en particulier induite par la démultiplication des relations avec des parties prenantes) pourrait coûter à l'échelle mondiale 4 600 milliards d'euros aux entreprises dans les cinq prochaines années (Accenture, 2019).

Des éléments factuels confortent cette perception par la matérialisation des menaces au travers de crises ou évènement ayant déjà touché un grand nombre d'entreprises :

- 83 % des entreprises disent avoir été confrontées à un incident lié à un tiers au cours des trois dernières années, dont 11% avec des « répercussions sévères » sur le service client, la situation financière, la réputation ou la conformité réglementaire (Deloitte « Extended Enterprise Risk Management Global Survey » 2019).
- 8 entreprises sur 10 sont touchées chaque année par des cyberattaques, et 98% estiment que la transformation numérique a un impact sur la sécurité des systèmes d'information et sur les données (CESIN - Baromètre cybersécurité des entreprises 2019).
- Seulement 39% des entreprises se disent suffisamment préparées en cas de cyberattaques de grande ampleur. 89% des entreprises utilisent le cloud pour stocker une partie de leurs données, mais sans maîtrise de la chaîne de sous-traitance de l'hébergeur pour 50%, Une minorité d'entreprises utilise des solutions intégrant des technologies d'Intelligence Artificielle, le frein étant le faible niveau de confiance (47%) envers cette approche (CESIN - Baromètre cybersécurité des entreprises 2020).

Exemple de risque - Question type n°1

Une entreprise intéressée par un partenariat à la suite d'un contact lors d'une exposition internationale et avec laquelle il n'y a aucune relation antérieure est-elle sincère/fiable ?

Ingérence économique

Contact d'affaires à l'étranger / Partenaire inconnu

Eléments factuels

Lors de sa première participation en 2018 au salon international « Cosmo Beauty Expo » de Hô Chi Minh-Ville, où étaient présentés ses nouveaux produits « cosmétiques bio », l'entreprise a pu nouer des contacts très prometteurs avec un fonds d'investissement chinois présentant des cautions de premier ordre.
Un tel partenariat potentiel pourrait être très prometteur et ouvrir de larges perspectives de développement en Asie du Sud-Est en appui du sous-traitant actuel vietnamien de Saigon.

Analyse des causalités

- Après plusieurs mois de relations, visites en Chine et France, échanges, demandes d'informations techniques, questionnaires intrusifs ..., le doute s'est installé sur les véritables intentions du fonds chinois.
- Des institutions françaises contactées ont pu confirmer le caractère douteux, sans pouvoir statuer si la cible était l'entreprise elle-même ou son sous-traitant vietnamien.

Evaluation des conséquences

- Vol de savoir-faire via création d'une joint-venture opportuniste, déstabilisation, reverse engineering, espionnage, captation de données, intrusion dans le système d'information via un sous-traitant, pertes du marché local, marchandisation (« commoditisation »), remplacement de gamme de produits, risques interculturels, …

Comportements/actions possibles

- Stopper les discussions en cours.
- Effectuer une *due diligence* approfondie (cf. section 3.4.4 « Utiliser des outils… ») avant tout engagement contractuel : enquête de notoriété, filtrage des informations, présence de concurrence dans l'actionnariat, …

Capitalisation pour l'approche Entreprise étendue

Principales parties prenantes identifiées

- Partenaire local inconnu.
- Sous-traitant étranger.
- Gouvernement étranger (via fonds de soutien économique).

Recommandations

Pour évaluer l'existence des risques dans les échanges internationaux ou les implantations à l'étranger, il y a nécessité d'une veille élargie permanente sur les politiques gouvernementales pour anticiper des décisions politiques.

Cas réels similaires (cf. Annexe 3 « Questions types – Sources détaillées des cas réels similaires »).

- Adisseo : rachat par BlueStar en 2006
- Tornier: rachat par Wright Medical en 2015

*L'avis de la **DGE** :*

https://www.entreprises.gouv.fr/fr/securite-economique/la-securite-economique-28-fiches-thematiques
« La construction de relations commerciales avec des partenaires extérieurs (financeurs, clients, fournisseurs, prestataires, etc.) fait partie de la vie quotidienne de l'entreprise. Ces relations constituent néanmoins des actes dont les conséquences peuvent être gravement préjudiciables s'ils ne sont pas réalisés avec la vigilance et la rigueur nécessaires. » (Fiche DGE/SISSEn°D3).

- 7 entreprises sur 10 ont été victimes d'au moins une tentative de fraude (de toutes natures, internes ou externes) en 2019, et 6 entreprises sur 10 n'ont pas alloué de budget spécifique pour y faire face (DFCG, étude Euler Hermès 2020).
- 80 % des objets connectés présentent une faille potentielle. Non seulement tous les objets connectés peuvent être la cible d'une attaque, mais, de plus, leur sécurité a été jusqu'à présent largement négligée. C'est un sujet véritablement sensible, alors qu'en parallèle 47% des entreprises industrielles prévoyaient d'augmenter de 47% leurs investissements dans l'internet des objets (IoT : Internet of Things) (Gartner Group, 2017), cette tendance n'a fait que s'amplifier malgré l'impact de la crise Covid-19 (IOT Analytics, 2021).

Un grand nombre de dirigeants d'entreprises reconnaissent encore mésestimer ou méconnaître ces phénomènes :

- A l'échelle mondiale, seulement 1% des entreprises interrogées estiment « optimisée » leur maîtrise des problématiques majeures de gestion des risques liés aux tiers. « Deux aspects majeurs de la gestion des risques de tiers ne sont pas convenablement traités : les sous-traitants et les entités affiliées » (Deloitte « Extended Enterprise Risk Management Global Survey », 2019).
- 80% des dirigeants estiment qu'il est de plus en plus difficile de protéger leur organisation des faiblesses dont souffrent leurs partenaires, compte tenu de la complexité et du caractère tentaculaire des écosystèmes connectés modernes (étude Accenture « Securing the Digital Economy : Reinventing the Internet for Trust » - mai 2019).
- 54 % des dirigeants déclarent ne pas connaître les responsabilités juridiques encadrant le déplacement des collaborateurs à l'international. En 2019, 73% des dirigeants d'entreprises françaises estiment que l'insécurité internationale représente une menace pour la France, ses entreprises et ses citoyens. Ils n'étaient que 61% en 2018. (CDSE « Baromètre CDSE/Axa Partners » 2019).

1.1 Le concept

Le préalable à toute tentative d'analyse des risques de l'Entreprise étendue est d'en définir le périmètre.

Au premier abord, la notion d'Entreprise étendue peut paraître extrêmement vaste, et donc difficilement appréhendable. Les divers degrés d'interactions avec les différentes natures de parties prenantes semblent dessiner un paysage confus. Et les risques associés, qu'ils constituent des menaces auxquelles l'Entreprise étendue serait exposée, ou qu'ils représentent des risques qu'elle génèrerait par ses activités, en deviennent par conséquent difficilement identifiables.

Pourtant, il est possible de représenter ce concept de manière pragmatique en formalisant avant tout des pistes de définition pour permettre aux risk managers de clarifier leurs travaux dans le cadre de l'ERM. Alors qu'est-ce que l'Entreprise étendue ? (*)

(*) De nombreuses définitions ont déjà été fournies par d'autres auteurs sous des angles et des approches variés, souvent réducteurs (à une nature ou un périmètre déterminé ou restreint) ; notre volonté est d'en faire l'exégèse afin de discerner les risques qui sont liés au concept défini d'une manière la plus englobante possible en laissant à chacun le soin de personnaliser l'approche à son univers.

1.2 Des pistes de définitions

Lors de premiers travaux menés dans le cadre de l'AMRAE (cf. Rencontres AMRAE 2016 – Atelier C07 « De la sous-traitance à l'Entreprise étendue : nouveaux enjeux pour l'Entreprise étendue et le risk manager »), une première définition avait permis de percevoir l'ampleur du concept d'Entreprise étendue :

> *« Un ensemble d'acteurs divers en interaction avec l'entreprise … ayant leurs propres intérêts et motivés par la création de valeur. »*

Cette définition permettait de considérer un périmètre qui intégrait bien l'élargissement de la sphère d'influence de l'organisation.

En revanche, cette définition restreignait les acteurs à ceux « motivés par la création de valeur ». Or il existe des acteurs qui agissent sur les entreprises, notamment au travers de moyens médiatiques, en poursuivant des intérêts purement idéologiques, sociétaux ou autres, sans lien avec la création ou la préservation de valeur. Ces acteurs sont motivés souvent par un ou plusieurs éléments tels que la création ou la préservation de valeur, la conformité, les objectifs sociaux ou environnementaux. Ils sont concernés par l'usage, la qualité ou la sécurité des produits et services. L'impact potentiel de ces acteurs n'en est pas moindre et il conviendra donc de les inclure dans les analyses. D'autre part les organisations et institutions publiques sont également concernées par des aspects étendus de leurs activités.

Il est dès lors proposé de retenir pour l'Entreprise étendue la définition ci-dessous.

« Un ensemble d'acteurs divers en interaction à des degrés variables avec l'entreprise ou l'organisme, ayant leurs propres intérêts. »

Nos réflexions suivront ce principe en proposant des axes d'analyse utiles aux travaux du risk manager et aux décisions des dirigeants. Avant de débuter une analyse des risques de l'Entreprise étendue, il s'agira d'adapter cette définition de l'Entreprise étendue à votre organisation afin de cerner le périmètre considéré et les parties prenantes qui y sont intégrées.

Exemple de risque - Question type n°2

L'aval de l'entreprise est-il suffisamment supervisé pour garantir la réalisation de ses activités en conformité avec sa raison d'être et ses valeurs ? Réseau de distribution, franchisés, ...

Maîtrise de l'aval dans la chaine de valeur : comportement des revendeurs
Publicité douteuse

Eléments factuels
Afin de relancer ses ventes, l'entreprise Martin décide de lancer une campagne de publicité atypique et provocatrice : un militaire se parfumant, fusil à la main en position de tir, un migrant se parfumant dans un camp de réfugiés, ...

Analyse des causalités
Cette campagne très controversée, suscite un débat entre ceux qui y voient une provocation gratuite et ceux qui y décèlent une puissante capacité à déclencher la réflexion. Des boycotts de la marque sont organisés au travers du monde, plus ou moins suivis. Dans ce contexte, un revendeur local de l'entreprise décide d'assigner l'entreprise Martin en justice. Les publicités auraient entraîné une forte baisse de son chiffre d'affaires et la fermeture de l'un de ses magasins. Il se dit en plus être en situation de dépendance économique à l'égard de l'entreprise Martin. Le revendeur fait la tournée des plateaux télévision pour exposer sa situation et attise les discussions déjà enflammées autour des publicités. La stratégie publicitaire de l'entreprise est mise en cause par un revendeur.

Evaluation des conséquences
- Condamnation pénale et amendes si le tribunal établit la faute de l'entreprise qui aurait causé un préjudice direct au revendeur (baisse du chiffre d'affaires, fermeture de magasins).
- Répercussions médiatiques négatives.
- Bad buzz sur les réseaux sociaux.
- Effet domino négatif auprès d'autres revendeurs (nouveaux procès par exemple).
- Boycott de la marque.

Comportements/actions possibles
- Etablir auprès du tribunal l'absence de dépendance économique du revendeur qui a le droit de diffuser d'autres marques et peut quitter le réseau de distribution de l'entreprise à tout moment sans sanctions pécuniaires pour rupture.
- Contrer les effets de la mauvaise publicité réalisée par ce revendeur en mobilisant les autres revendeurs de l'entreprise dans une communication proactive et positive à l'égard de la marque.

Capitalisation pour l'approche Entreprise étendue

Principales parties prenantes identifiées
- Revendeur.
- Clients.
- Société civile et opinion publique.

Recommandations
- Identifier les cas de dépendance économique.
- Tester la campagne au préalable auprès d'un échantillon représentatif ou d'experts reconnus ou de revendeurs.
- Etablir une discussion en amont avec les revendeurs en cas de lancement de campagne publicitaire controversée.

Cas réels similaires (cf. Annexe 3 « Questions types – Sources détaillées des cas réels similaires »).

- Benetton : Prototype, campagne de dénigrement - 2000
- Citer (PSA) : ALX location, campagne de dénigrement - 2018
- Divers cas de dénigrements du franchiseur par le franchisé : qualification et jurisprudences

DGCCRF :
« En tant que professionnel, vous êtes responsable de la sécurité du produit ou du service que vous commercialisez. A ce titre vous êtes tenu de vérifier que celui-ci respecte la réglementation et répond à l'obligation générale de sécurité (OGS). »

1.3 L'analyse

Tout au long de son existence, une entreprise peut volontairement chercher à s'étendre, par exemple pour :

- Saisir des opportunités ;
- Investir de nouveaux marchés ;
- Augmenter ses parts de marchés ;
- Diminuer ses coûts de production ;
- Améliorer son image ;
- Former des alliances ou des partenariats ;
- Intégrer des projets pluri-partenaires (cf. Question type n°1 – Exemple « Ingérence économique ») ;
- Elargir son spectre de compétences et renforcer son potentiel humain (flexibilité, mobilité),
- Obtenir un accès (plus direct) à l'innovation ;
- S'affranchir de règlementations lourdes ;
- Optimiser l'efficacité de ses processus ;
- Couvrir des risques locaux ou nationaux ;
- ...

Elle peut aussi se trouver étendue sans l'avoir choisi, de manière subie, parfois même inconsciente, si l'une de ses parties prenantes modifie sa manière de fonctionner, par exemple lorsqu'un fournisseur recourt à la sous-traitance sans l'en informer.

Figure 5 – Dénominations similaires

Quel que soit le nom donné à cette entreprise (cf. figure 5 « Dénominations similaires »), son extension peut prendre diverses formes :

- Géographique : nouveaux marchés, synergies, ...;
- Opérationnelle : sous-traitance, diversification, délocalisation, logistiques, ...;
- Fonctionnelle : par exemple choix de « Make or Buy » (produire ou acheter), « Business Process Outsourcing » (BPO), centres d'appels, externalisation ;
- Organisationnelle : par exemple comptabilité externalisée ;
- Capitalistique : fusion, acquisition, diversification horizontale ou verticale ;

- Caritative : mécénat, fondations, Organisations Non Gouvernementales (ONG) ;
- Liées au modèle de distribution : développement en franchise, par des revendeurs (cf. Question type n°2 – Exemple « Maîtrise de l'aval dans la chaine de valeur : comportement des revendeurs ») ;
- ...

Comme précisé en introduction, la réalité de l'Entreprise étendue et les critères d'analyse utilisés situent la problématique bien au-delà de la chaîne de sous-traitance, des fournisseurs ou des clients (traditionnellement définis comme la chaîne de valeur principale d'approvisionnement ou Supply Chain), et conduisent à considérer l'acception d'une plus grande sphère d'influence (cf. fig. 1 « Sphère de l'Entreprise étendue »).

Plusieurs concepts définissent le périmètre des interactions, lequel semble toujours plus vaste. En fonction des précisions que chaque organisation souhaite y apporter, les évolutions des activités (géographiques par exemple) ou bien des travaux réglementaires influent également sur l'élargissement de cette notion.

● Un écosystème élargi …

Ces concepts sont soutenus par des critères objectifs permettant de définir un degré d'extension de l'entreprise et les différents acteurs qui composent ainsi une organisation « étendue » :

- La couverture géographique des activités directes ou indirectes ;
- Le niveau d'intégration de la chaîne fournisseurs (rangs n) / client final ;
- La multiplicité des parties prenantes internes ou externes ;
- Le degré d'insertion dans le contexte sociétal, et donc les interactions avec des acteurs tiers.

Par ailleurs, il existe des parties prenantes qui se situe à un niveau proche du coeur de l'Entreprise étendue, que l'on qualifie d'intégrées : les « First Tier Supplier » ou encore « Tier 0.5 ». Ces tiers sont apparus notamment dans l'industrie automobile lors de la mise en place du concept de production modulaire, dans le but de confier à des fournisseurs la conception, le développement et la production de modules entiers et non plus la fabrication d'une seule pièce. Leur positionnement en fait des partenaires fortement intégrés dont l'Entreprise étendue ne saurait se passer et dont elle est de facto très dépendante (cf. figure 6 « Entreprise étendue et entreprise intégrée »).

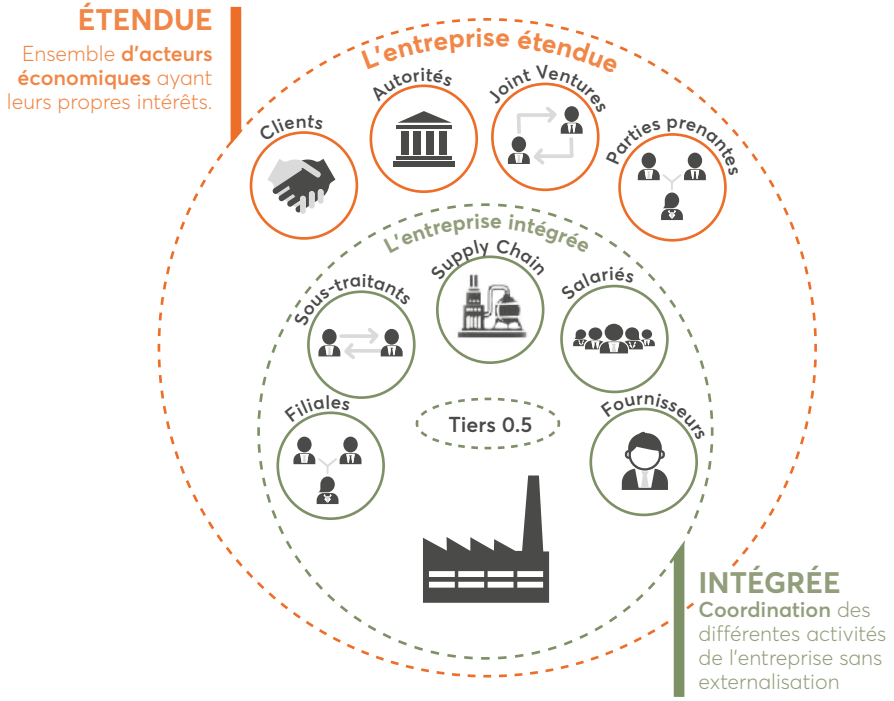


Figure 6 – Entreprise étendue et entreprise intégrée.
D'après l'atelier éponyme C5 des 26ème Rencontres du Risk Management - AMRAE 2018

● …avec des enjeux, partagés ou non ?

Point de vue d'un risk manager

« Les constructeurs et leurs fournisseurs directs accroissent en permanence la proximité de leur relation, traduite par une imbrication étroite des équipes sur le terrain, dans une logique de co-construction. Pour autant, ces entreprises restent naturellement distinctes, dans un alignement d'objectifs qui n'est que partiel.
Il existe un risque que ce rapprochement opérationnel rende les différences d'intérêts moins perceptibles au quotidien, et réduise la lucidité, donc la capacité d'identification de risques induits ou portés par le partenaire comme l'exigence de leur traitement. Cela nuirait potentiellement à la performance de chacun et à la réussite globale. »

Un risk manager du secteur automobile.

1.4 L'écosystème de l'Entreprise étendue : enjeux et dimensions

Avec un périmètre de plus en plus large, il s'avère difficile de contenir cette notion d'Entreprise étendue et d'en connaître préalablement les limites. Comme le périmètre est par définition évolutif et spécifique à chaque entreprise, ce préalable est indispensable à toute réflexion afin de pouvoir considérer les risques qui y sont liés.

Il s'agira donc de considérer un ensemble constitué autour d'éléments communs : le(s) enjeu(x) partagé(s). Il s'agira également de rechercher tout évènement pouvant concerner l'Entreprise étendue, y compris en l'absence d'enjeux communs, voire en présence d'enjeux opposés. Les différentes parties prenantes peuvent être représentées au sein d'un même système, autour des enjeux ou dimensions de l'Entreprise étendue. Définir ces enjeux ou ces dimensions et les traduire en axes dans une représentation graphique, constitue l'un des prérequis pour conduire une analyse pertinente des risques de l'Entreprise étendue (cf. figure 7 « Schéma des enjeux »). Une difficulté inhérente à cet environnement ouvert et très varié est l'incapacité de l'organisation à s'assurer du contrôle des flux et des obligations éventuelles avec tous les tiers de l'écosystème.

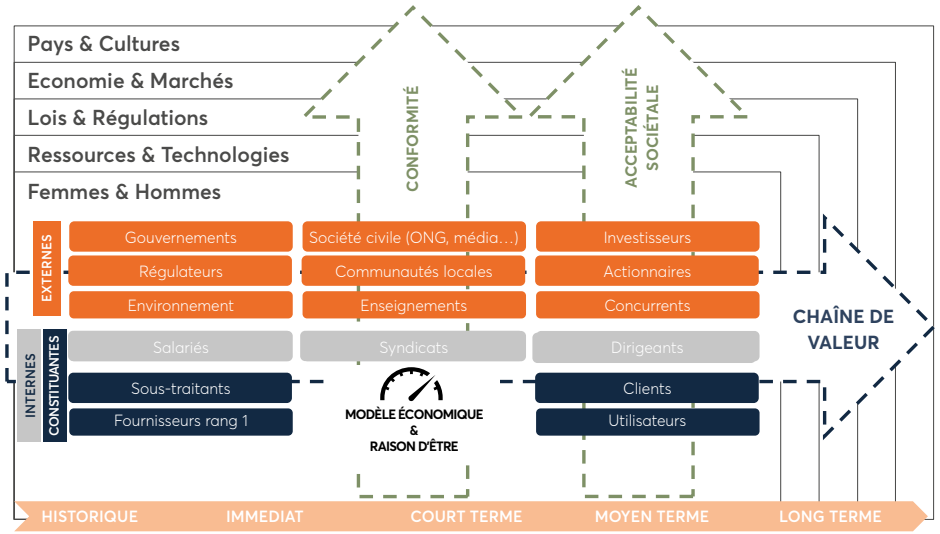


Figure 7 – Schéma des enjeux

1.4.1 L'amont et l'aval

En regardant les représentations schématiques (cf. figure 1 « Sphère de l'Entreprise étendue » et figure 7 « Schéma des enjeux »), on comprend qu'il est indispensable de recenser les acteurs situés en amont et en aval de l'Entreprise étendue, ceux en lien avec son objet social, sa mission, sa « raison d'être » et la création de valeur de son modèle économique. Les parties prenantes alimentent ou influent le modèle d'affaires, la production, la commercialisation, les services, …

Du côté amont, elles peuvent, par exemple, être liées directement à l'Entreprise étendue par une contractualisation, un achat, un partenariat. Elles peuvent aussi n'avoir aucun lien contractuel, lorsqu'il s'agit par exemple de sous–traitants de rang n.

Du côté aval de la chaîne, il s'agit d'identifier celles qui ont accès au produit ou au service ou en contrôlent l'usage ou l'utilisation, clients bien sûr, utilisateurs indirects (clients de clients, usagers des services publics, autorités, …) mais aussi acteurs concernés individuellement ou collectivement, ou acteurs sociétaux comme des ONG ou des médias notamment.

Quoi qu'il en soit, la plupart des décisions sur la chaine de valeur revêtent un caractère stratégique, et souvent une prise de risque. Ainsi la pénurie de matériels de protection sur une grande partie de la planète au début de la crise sanitaire due au Coronavirus faisait suite à des décisions stratégiques du monde politique sur la chaine d'approvisionnement et de stockage : optimisation du niveau de stock, localisation de l'approvisionnement en un lieu unique, confiance placée dans une capacité de production supérieure aux besoins et dans un flux d'approvisionnement externalisé en continu.

Point de vue d'un risk manager

« Lorsqu'un client nous confie le développement de composants destinés à équiper un modèle futur, sans aucune garantie du succès commercial de ce véhicule, le risque financier est important pour l'équipementier que nous sommes (frais inhérents au développement des composants qui ne seraient pas amortis par le volume en cas d'échec commercial). Pour gérer au mieux ce risque, nous travaillons étroitement avec nos clients afin de proposer un niveau d'innovation optimal susceptible de contribuer au succès du véhicule. En revanche nous pouvons aussi être amenés à refuser de collaborer sur un programme, ou à imposer nos conditions financières (paiement partiel ou total des frais liés au développement des composants). »

Un risk manager du secteur de la sous-traitance automobile.

Exemple de risque - Question type n°3

Le tour de table / pacte actionnarial est-il susceptible d'évoluer en mettant l'entreprise en risque ?

Instabilité de l'actionnariat - évolutions réglementaires, nouveaux entrants, OPA, …
Un actionnaire indélicat

Eléments factuels
Un des actionnaires de l'entreprise Martin, Bertrand Benoît (cousin de Nathalie Martin), détenant plus de 25% des parts, est connu de l'administration pour des tentatives d'évasion fiscale dans le passé. Il refuse de livrer les informations le concernant.

Analyse des causalités
Depuis le 1er août 2017, toute nouvelle entreprise ou groupement d'intérêt économique est tenue de déposer au greffe du tribunal de commerce la liste de ses bénéficiaires effectifs, qui sera inscrite en annexe du Registre du commerce et des sociétés. L'entreprise, quant à elle, en tant qu'entreprise pré existante, doit s'y plier le 1er avril 2018.
- Les sociétés peuvent être sanctionnées pénalement en cas de violation de cette obligation. Ces informations n'ont pas vocation à être connues du public. Elles ne peuvent être consultées que par certaines entités, parmi lesquelles l'administration fiscale et les autorités judiciaires.
- Mais la réglementation évolue vers plus de transparence : une directive européenne du 14 mai 2018 prévoit d'élargir l'accès aux informations sur les bénéficiaires effectifs. Le grand public pourrait alors apprendre que Bertrand Benoît est un bénéficiaire effectif de l'entreprise, donc que l'entreprise a un actionnaire à la réputation / éthique douteuse (Bénéficiaires effectifs : Code monétaire et financier - Article L561-46 - Bénéficiaires effectifs : Directive UE 2018/843 du 30 mai 2018, art. 4).

Evaluation des conséquences
- Juridique : Condamnation pénale.
- Réputation : lorsque la directive européenne sera transposée en France.

Comportements/actions possibles
- Saisine du Président du tribunal de Commerce par Nathalie Martin concernant le refus de divulgation d'informations par Benoît Bertrand.
- Préparation d'une communication adaptée vis-à-vis du grand public, voire demande à Bertrand Benoît de vendre ses parts.

Capitalisation pour l'approche Entreprise étendue

Principales parties prenantes identifiées
- Actionnaires.
- Etat : Greffe du Tribunal de Commerce, administration fiscale, autorités judiciaires, …
- A partir de 2020, la société civile également.

Recommandations
- Travailler le pacte d'actionnaires.

Cas réels similaires (cf. Annexe 3 « Questions types – Sources détaillées des cas réels similaires »).

- Bayern de Munich : Démission du président du Bayern - 2014
- Heller Joustra, jouets – faillite de la PME / actionnaire indélicat – 2013
- SNCF : contrôle exclusif sur Novatrans - infraction – 2007
- GECINA : Rumeurs - forte chute à la Bourse de Paris – 2008

« Ces activistes, qui ont pour objectif de déstabiliser l'entreprise, nous inquiètent » …
Agnès Touraine *« juge déraisonnable les retours promis par ces fonds. Elle recommande aux sociétés d'évaluer les scénarios de risques. … L'**Institut Français des Administrateurs (IFA)** recommande aux conseils d'administration d'étudier activement les points d'amélioration dans le dialogue avec les actionnaires et de se préparer à une éventuelle offensive. »* Agnès Touraine présidente IFA dans L'AGEFI 16/10/2018.

L'axe de la chaine de valeur est celui où se positionnent très souvent des choix stratégiques, guidés ou limités par des considérations financières. Ces choix reflètent l'équilibre entre la perception du niveau de risque et les coûts liés à sa maitrise raisonnable. C'est sur cet axe amont/aval que l'appétence aux risques se mesure le mieux au sens financier, car les équilibres sont généralement assez faciles à quantifier. Ainsi un stock central d'approvisionnement confié à un entrepositaire unique et basé dans seul entrepôt fait peser des risques élevés de discontinuité d'activité chez le donneur d'ordres. En revanche, le recours à deux prestataires opérant deux entrepôts éloignés l'un de l'autre témoigne d'une stratégie de prudence plus coûteuse.

1.4.2 L'interne et l'externe

Cette segmentation, traditionnelle mais efficace, offre une clé d'analyse complémentaire pour identifier les parties prenantes de manière plus complète. Dans un contexte interne autant qu'externe, au-delà des fournisseurs et des clients, il y a également, sans être exhaustif, les parties prenantes qui transforment ou produisent la valeur, ainsi que celles qui financent l'Entreprise étendue ou bien la régulent.

Parfois, pour certaines organisations, on distinguera « partie prenante », externe, et « partie constituante », interne. Pour les organisations qui le désirent, les **cartographies** pourront alors être dédoublées, une pour les parties prenantes et une autre pour les parties constituantes. Nous recommandons que l'Entreprise étendue liste l'ensemble sur une seule cartographie en réunissant les deux notions au sein d'une même définition de partie prenante.

On peut recenser parmi les parties prenantes internes (cf. Figure 7 Schéma des enjeux) les salariés, les administrateurs, les actionnaires (cf. Question type n°3 – Exemple « Instabilité de l'actionnariat - évolutions réglementaires, nouveaux entrants, OPA, … »), les organes de gouvernance ou consultatifs (comités, conseils…), les corps intermédiaires, les représentants des salariés, le comité d'entreprise, les représentants syndicaux, …

Là où cela peut s'avérer utile, l'identification des parties prenantes internes peut s'affiner, par exemple pour les salariés, selon les typologies de contrats (CDI, CDD, intérim, contrats de mission ou projet dédiés…). Ce degré de précision supplémentaire permet de capturer des enjeux plus précis, et donc des risques spécifiques.

1.4.3 Le temporel

Les relations avec les parties prenantes de l'Entreprise étendue s'abordent également au travers d'une dimension temporelle qui permet d'identifier et de catégoriser les différents intervenants.

Exemple de risque - Question type n°4

Les personnels à l'étranger de l'entreprise sont-ils suffisamment informés, préparés, protégés en zones difficiles, particulièrement en zones à risques ?

Protection des personnels à l'international
Expatriée au Mexique

Eléments factuels
Depuis quelques semaines l'experte logistique de l'entreprise, expatriée temporairement au Mexique afin de préparer les bases d'une future unité de fabrication, se plaint d'une situation sécuritaire locale dégradée. Elle a déclaré par écrit se sentir en danger, y compris dans ses déplacements hors travail, et demande formellement son rapatriement sans délai, aux frais de l'entreprise.

Analyse des causalités
En 2008, le Code du Travail (Art. L4121-1) pose le cade du « Duty of Care » obligeant l'employeur à prendre les mesures nécessaires pour protéger la santé physique et mentale des travailleurs. Par une jurisprudence de 2011 (arrêt n°2575), ce principe est renforcé et étendu pour les expatriés.

Evaluation des conséquences
- Pertes humaines, blessures graves voire invalidantes, traumatismes moraux.
- Responsabilité pénale et civile de l'employeur.
- « Judiciarisation » de la relation employé/employeur.
- Versement de dommages et intérêts, parfois considérables.
- Image dégradée de l'entreprise, forte médiatisation.

Comportements/actions possibles
- Négociation avec la salariée de la mise en place d'une protection personnelle rapprochée.
- Remplacement de la salariée par un autre salarié ou un externe de même compétence, non sensible à cette situation à risque (par exemple un Mexicain).

Capitalisation pour l'approche Entreprise étendue

Principales parties prenantes identifiées
- Employés.
- Organisations criminelles et terroristes locales.
- Assureurs.

Recommandations
- Fournir une information complète et loyale aux salariés, avant tout déplacement, en prenant en compte tous les risques naturels, sociaux, sanitaires, géopolitiques.
- Disposer d'un dispositif de veille sécuritaire (interne ou externe) afin d'appréhender de manière la plus fine possible l'évolution sécuritaire d'un pays à moyen et court terme pour en déduire des mesures de précaution à mettre en place immédiatement.
- Mettre en place des actions de sensibilisation et de formation, et un dispositif local opérationnel de sureté pour les personnels détachés ou expatriés.
- Contracter des services d'assistance et d'assurances adaptés aux natures de menaces et risques.

Cas réels similaires (cf. Annexe 3 « Questions types – Sources détaillées des cas réels similaires »).

- DCN : attentat de Karachi, condamnation - 2004
- Ultramarina : otages de Jolo, condamnation - 2019
- Areva : plainte d'un otage, Arlit - Niger - 2016
- Sanofi Pasteur : agression d'une salariée expatriée, condamnation - 2012

*« Dans un contexte international instable, l'entreprise se doit d'anticiper au mieux les menaces propres à chaque espace géographique. La prise en compte des risques de l'Entreprise étendue à l'international, ce sont des personnels informés, protégés et couverts face à l'ensemble des risques globaux spécifiques à chaque zone. De ce point de vue, les entreprises françaises disposent d'une marge de progression conséquente. En 2019, plus d'une entreprise française sur deux déclaraient ne déployer aucun dispositif pour préparer les missions de leurs salariés à l'étranger, selon le 6e Baromètre **CDSE** de la sécurité collaborateurs à l'international. »* Club des Directeurs de Sécurité des Entreprises (CDSE).

Ainsi l'environnement de l'Entreprise étendue évolue selon des relations qui peuvent être temporaires. C'est le cas, par exemple, d'une collaboration avec un fournisseur sur un projet spécifique ou de la contractualisation d'une expertise externe sur une mission dédiée. Un client peut également bénéficier d'un service, d'une expertise, d'un produit de manière ponctuelle.

Ces mêmes parties prenantes font, d'autre part, émerger des risques dans une dimension temporelle continue, au travers des partenariats, des contractualisations ou d'échanges de plus long terme.

S'y ajoute un troisième aspect, l'effet d'antériorité. Certains risques ou impacts de l'organisation peuvent se manifester notamment envers des parties prenantes qui ne sont plus considérées comme faisant partie de l'écosystème direct et actuel de l'Entreprise Etendue. Cela peut être le cas d'affaires judiciaires mises à jour publiquement après l'acquisition d'une cible par l'entreprise, alors même que l'opération est bouclée depuis longtemps. Il peut s'agir d'anciens salariés réclamant des indemnités au titre d'exposition antérieure à des substances toxiques, de partenaires historiques ou d'anciens clients exposés à des risques de fraude ou de réputation.

La cartographie des parties prenantes peut prendre en compte cet élément temporel. La question consiste alors à définir l'Appétence de l'organisation pour des risques générés par des parties prenantes selon leur caractère ponctuel, comme la perte d'un client clé, ou à moyen ou long terme comme la perte de confiance et l'érosion lente d'une base clientèle, avec une diminution du chiffre d'affaires.

1.4.4 Le politique et le géographique

Cette dimension est l'une des plus évidentes, puisque le concept d'Entreprise étendue a été avant tout perçu lorsque les barrières physiques et géographiques ont été transcendées (cf. Question type n°4 - Exemple « Protection des personnels à l'international »). Comme la dimension temporelle, la dimension géographique est transverse à toutes les parties prenantes de l'écosystème. Elle génère des spécificités aux risques afférents et aux impacts qui en sont issus. Par exemple, certaines conséquences d'un conflit armé sont propres à chaque pays frontalier, comme pour les flux de réfugiés.

Les impacts des environnements réglementaires, économiques, sociologiques, climatiques, monétaires, culturels, religieux, politiques, géopolitiques ... sont désormais intégrés dans les analyses de risques par les entreprises.

Les risques générés à l'échelle mondiale par les échanges de biens, de capitaux, de ressources humaines, de produits et par la localisation des sous-traitants sont généralement pris en compte. Cette analyse se mène également à l'échelle locale, celle des territoires d'implantation des sites de l'entreprise étendue et de leur environnement : autorités locales, représentants du territoire, riverains …

A ces fins, l'analyse PESTEL (Politique, Economie, Social, Technologie, Environnemental, Légal) pourra être utilisée avec profit (cf. Annexe 4 « Analyse PESTEL »).

Pour affiner la mesure des impacts générés ou subis par l'Entreprise étendue, différents selon les contextes réglementaires et législatifs, les situations politiques, les spécificités culturelles ou les cadres économiques et fiscaux, les cartographies des parties prenantes pourront être déclinées et adaptées de manière spécifique à chaque pays, ou à chaque région en fonction des besoins.

Point de vue d'un risk manager

« Les risques de l'entreprise étendue concernent l'ensemble des services de la collectivité mais aussi les entités qui concourent à la mise en œuvre des projets initiés, à la tenue des engagements pris et l'exercice des compétences obligatoires de la collectivité par exemple : relations avec les associations locales, recours à des sous-traitants, problématiques d'expertises pour maîtriser la complexité croissante des projets du secteur public et leur ouverture vers le secteur non public, etc. »

Un risk manager du secteur public local.

Cette spécificité se retrouve par exemple dans le cadre d'analyse des risques de corruption. Les risques ou impacts sont identifiés de manière différenciée selon les pays de l'écosystème, la nature des parties prenantes (présence d'intermédiaires, ventes ou achats directs, pratiques d'appels d'offres, existence de mécanismes types Partenariat Public Privé…). Il en est de même pour les enjeux liés à la RSE, les cadres réglementaires, les normes et les seuils étant différents dans chaque pays où l'Entreprise étendue opère.

De plus, la notion d'extraterritorialité s'affirme parfois comme un critère pertinent pour identifier les parties prenantes et la manière dont elles affectent, ou sont affectées, par l'Entreprise étendue. Certains enjeux de réputation ou légaux par exemple, sont désormais internationaux (à ce sujet cf. section 1.4.6 « Le juridique »).

Des opérations ou des processus de la chaîne de valeur peuvent aussi concerner une partie prenante qu'on n'imagine pas figurer dans l'écosystème de l'Entreprise étendue mais qui affecte son activité. Un exemple très répandu est celui de l'utilisation du dollar américain, qui place de facto l'Etat américain parmi les parties prenantes de beaucoup d'entreprises françaises et mondiales.

Exemple de risque - Question type n°5

Les produits / activités / services de l'entreprise sont-ils susceptibles de heurter des règles sociales / sociétales / environnementales locales ?

Choc sociétal
Publicité "guerrière" - Boycott

Eléments factuels
Un distributeur local de l'entreprise Martin a distribué à titre commercial plusieurs dizaines de flacons de parfums auprès de soldates d'un pays en guerre. Ces dernières se sont photographiées en tenue militaire avec les flacons et ont diffusé les photos sur Twitter.

Analyse des causalités
La marque de l'entreprise a donc été perçue comme soutenant le pays ennemi.
Vu la réputation internationale de la marque, Cette prise de position apparente a provoqué, compte-tenu de la notoriété de la marque à l'échelle internationale, de fortes réactions.

Evaluation des conséquences
- Bad buzz sur Twitter et Facebook de plusieurs milliers de post dans un délai de quelques heures suivant la diffusion des photos, soit un impact image violent.
- Boycott de la marque entraînant une chute des ventes auprès des personnes soutenant le pays B, chute pouvant représenter plus de 10% des ventes dans les semaines à venir.

Comportements/actions possibles
- A titre préventif : faire prendre conscience aux partenaires de la puissance du buzz dans les réseaux sociaux et de la nécessité d'être neutre face aux affaires politiques avec une réflexion sur les conséquences possibles des actions avant mise en oeuvre.
- A titre curatif : Diffusion immédiate d'un message correctif dès perception du buzz négatif : « La société a pour règle de ne pas prendre parti dans un conflit ou toute affaire politique. De fait, un distributeur local indépendant a fait sa propre campagne commerciale. L'entreprise réprouve cette opération strictement locale et regrette d'avoir pu offusquer certains de ses clients. »

Capitalisation pour l'approche Entreprise étendue

Principales parties prenantes identifiées
- Partenaire local de distribution / franchisé.
- Clients et leurs comportements, ici soldates du pays A.
- Associations de soutien à une cause, ONG (qui reflètent ou influencent l'opinion publique).

Recommandations
- Avoir une surveillance des réseaux sociaux de tous les instants, 24/24 sur le plan mondial.
- Avoir une cellule de crise prête à être activée en moins d'une heure.

Cas réels similaires (cf. Annexe 3 « Questions types – Sources détaillées des cas réels similaires »).

- Garnier : boycott, publicité, Israël - 2014
- H&M : publicité jugée raciste - 2018
- Gillette : boycott, publicité engagée - 2019

*Cercle d'Ethique des Affaires (**CEA**) déclaration d'objectifs :*
« … Nous croyons profondément en effet, que dans une économie de marché, le comportement éthique d'une entreprise et son contrôle par le biais de la conformité sont aujourd'hui les conditions de sa pérennité et de sa réussite industrielle et commerciale. »

1.4.5 Le sociétal et l'environnemental

La dimension sociétale est liée à toutes les autres dimensions, qu'elles soient géographiques, temporelles, financières ou technologiques par exemple.

Les quinze dernières années ont vu apparaître les préoccupations d'ordre environnemental et sociétal, les processus de communication et de notation de performance en matière extra-financière, ou encore des travaux préparatoires à des évolutions législatives y afférentes, à l'instar du rapport Senard-Notat sur la « vision de l'Entreprise étendue dans la société » (rapport « L'entreprise, objet d'intérêt collectif », mars 2018).

Les processus de notation des performances extra-financières illustrent parfaitement cette dimension qui englobe les autres enjeux. Par exemple, les exigences de reporting de la DPEF (Déclaration de Performance Extra-Financière, issue de la transcription d'une directive européenne de 2014 et en vigueur depuis 2017 pour les entreprises d'une certaine taille) en France, ou les standards du Global Reporting Initiative (GRI) à l'international (cf. figure 8 « Directives du GRI), traitent de risques qui se déclinent en sections économique, sociale et environnementale. Par ailleurs les notations non financières sont aujourd'hui prises en compte par les investisseurs institutionnels et les banques. Cet enjeu devient donc un sujet important, notamment pour les actionnaires en tant que parties prenantes.

Ces exigences requièrent des précisions sur la conformité légale et réglementaire, sur les pays et les cultures de l'écosystème (cf. Question type n°5 – Exemple « Choc sociétal »), ou encore les mesures en faveur des salariés, des communautés environnantes, des clients…

Ce prisme sociétal concerne par ailleurs l'ensemble des parties prenantes internes de l'Entreprise étendue puisque les exigences mentionnées s'adressent autant aux salariés, aux actionnaires et aux instances de Direction qu'aux parties prenantes externes (société civile, régulateurs…).

Plus récemment, en France, la loi PACTE préconise depuis mai 2019 l'élaboration de la raison d'être et son inscription dans les statuts de la société, suscitant une certaine adhésion de la part de grands groupes qui se lancent dans l'exercice.

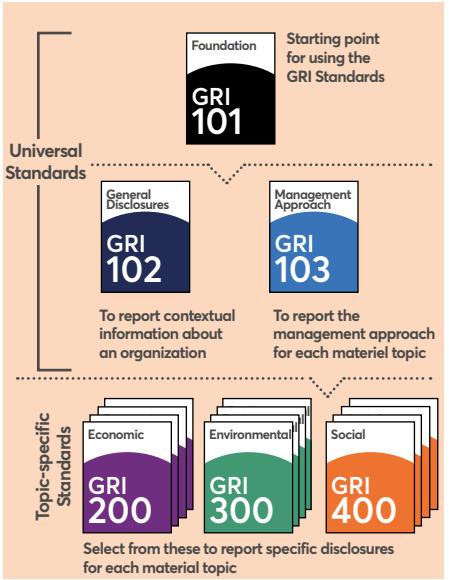


Figure 8 – Directives du GRI (ONG Global Reporting Initiative) – 2016

Egalement, certaines entreprises créent des comités réunissant certaines de leurs parties prenantes, liées notamment dans une perspective sociétale, afin de mieux partager et intégrer leurs préoccupations dans la gouvernance et la prise de décisions de l'entreprise. De même, certaines entreprises écoutent leurs parties prenantes afin de mieux comprendre leurs attentes, notamment dans les domaines RSE.

Cela reflète l'importance pour une entreprise d'aller au-delà de sa seule activité économique et de jouer un rôle plus structurant et engagé dans la société. Au-delà de son inscription dans les statuts, cette raison d'être embarque l'ensemble de l'entreprise et de son écosystème, donc l'Entreprise étendue. Elle a vocation à transformer en profondeur l'entreprise et son modèle.

1.4.6 Le juridique

Les entreprises ont l'habitude de composer avec toutes les formes de droit, au niveau national comme au niveau international : droit commercial, droit civil, droit pénal, droit des sociétés, droit fiscal, droit de la propriété intellectuelle, droit des assurances, etc., y compris sous l'angle de l'Entreprise étendue. Dès lors, historiquement exposées à cette forme d'extension légale et règlementaire, elles voient cette dimension juridique prendre sans cesse de l'importance.

Ainsi, le législateur a intégré au sein de lois et règlements la notion de risque, et le suivi de la maitrise des risques, allant même jusqu'à en faire un élément de conformité. C'est le cas pour le Règlement Général de Protection des Données individuelles (RGPD) au niveau européen, et en France pour la loi relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (dite Sapin 2), ainsi que pour la loi sur le Devoir de Vigilance des sociétés mères et donneuses d'ordre. Un projet est en cours au niveau de l'Union Européenne sur une réglementation de même nature que le devoir de vigilance qui devrait alors être mise en œuvre au sein des pays de l'Union Européenne.

La dimension juridique est un domaine dans lequel les risques sont le plus pris en compte ces dernières années. On constate même l'utilisation d'un formalisme des risques comme la méthode de la cartographie dans Sapin 2.

Les risques d'ordre juridique sont multiples. Il peut s'agir, par exemple, de respecter les délais de communication ou de mise à disposition des documents en matière de droit des sociétés, ou encore de se protéger du risque de contrefaçon en déposant ses brevets et ses marques puis en organisant une veille active de détection d'usurpation.

De manière générale, tous les contrats engageant l'entreprise doivent être identifiés et leur portée analysée et évaluée. C'est le cas également des engagements hors bilan qui doivent être listés et communiqués, car ils peuvent représenter des « droits et obligations susceptibles de modifier le montant ou la consistance du patrimoine de l'entité » (Plan comptable – section 8. Comptes spéciaux). Ce sujet est sensible car les montants en jeu peuvent être significatifs et influer sur le devenir de l'entreprise (cours de bourse, confiance des partenaires, …). La difficulté réside souvent, notamment dans les grandes organisations, dans l'identification de ces « droits et obligations ». En effet, des baux, des engagements de commandes ou d'autres obligations contractuelles, parfois sous condition suspensive, peuvent être souscrits localement au cours d'une négociation commerciale, sans le soutien de la direction juridique, voire à son insu !

Les exemples d'interactions avec les autres dimensions de l'Entreprise étendue sont eux aussi nombreux. L'extension géographique mal contrôlée peut entraîner de facto un risque pénal pour le dirigeant. La méconnaissance d'un droit fiscal local sur une nouvelle activité peut entraîner un redressement fiscal majeur. La dimension amont/aval a trouvé un terrain juridique étendu avec la loi sur le devoir de vigilance, qui concerne fournisseurs et sous-traitants quelle que soit leur nationalité. Enfin, la dimension environnementale se matérialise aujourd'hui sur le plan juridique avec les actions judiciaires de certaines ONG ou l'existence des actions de groupe (ou *class action*) dans certains pays.

Depuis peu, les entreprises ont découvert les conséquences de l'extraterritorialité, apparue dans des textes de plus en plus nombreux et imbriqués au fil du temps. Des amendes record peuvent leur être infligées en vertu de législations adoptées dans des pays qui peuvent être secondaires dans leur activité, voire totalement absents de leur périmètre d'activité. Les sanctions économiques internationales peuvent survenir au seul motif que l'entreprise effectue des transactions dans la devise d'un pays, alors qu'elle n'a aucun courant d'affaires avec ce pays. Globalement, des lois étrangères à portée internationale élargissent considérablement le champ de responsabilité de l'entreprise en matière de gestion des risques, avec à la clé un enchevêtrement de textes légaux ou règlementaires dans lequel déterminer celui qui prévaut sur les autres relève souvent d'une gageure.

Notre propos n'est pas ici de nous focaliser en détail sur la dimension juridique ; il est important en revanche de souligner la progression continue dans l'histoire contemporaine du niveau d'attentes des parties prenantes en matière de conformité aux lois et règlements.

Exemple de risque - Question type n°6

Les différences Interculturelles sont-elles bien prises en compte dans le fonctionnement interne et vis-à-vis de toutes les parties prenantes externes ?

Non prise en compte des différences culturelles dans un choix stratégique
Chatbot irrespectueux

Eléments factuels
Les progrès de l'intelligence artificielle et du big data apportent l'opportunité d'automatiser en partie les relations avec les prospects et clients, avec des gains significatifs dont la transformation d'un visiteur en client. Aussi, L'entreprise souhaite mettre en oeuvre un logiciel « chatbot » du marché pour répondre en ligne, et ce de façon vocale, aux questions sur les produits, les promotions, les distributeurs, et, de conduire à l'acte d'achat ; l'objectif assigné au chatbot est de faire durer au maximum les conversations.

Analyse des causalités
Le chatbot apprend et modifie son comportement en fonction des expériences d'échange réalisées avec les prospects et les clients :
- Recherche d'augmentation de l'échange avec les interlocuteurs en ligne.
- Acquisition par le chatbot de sémantiques sexistes ou racistes, puis dérives potentielles associées.
- Dérives comportementales provoquées volontairement ou non par des interlocuteurs.
- Absences de traçabilité des algorithmes analysant et construisant les échanges.

Evaluation des conséquences
- Bad buzz avec un impact fort sur l'image.
- Baisse des ventes de plus de 10% dans les semaines qui suivent.
- Destruction de la marque auprès de la clientèle féministe.

Comportements/actions possibles
- A titre préventif :
  - Veiller aux règles instanciées pour l'analyse et la construction des échanges.
  - Utiliser des algorithmes avec traçabilité.
- A titre curatif :
  - Détecter les échanges négatifs.
  - Reprendre la main sur le chatbot en temps réel.
  - S'excuser auprès des interlocuteurs ayant une perception négative du chatbot.

Capitalisation pour l'approche Entreprise étendue

Principales parties prenantes identifiées
- Fournisseur du chatbot.
- Consultant en mise en place et évolutions de chatbot (agent conversationnel).
- Prospects, clients.
- Réseaux sociaux (y compris Influenceurs).

Recommandations
- Veiller préventivement au respect de règles sémantiques dans l'expression du chatbot.
- Avoir une surveillance permanente des échanges pour détecter et stopper toute dérive.

Cas réels similaires (cf. Annexe 3 « Questions types – Sources détaillées des cas réels similaires »).

- Microsoft - robot conversationnel TAY, racisme – 2016
- Korean Air - crashs aériens répétés - 1989/98
- Air France / KLM – conflit « culturel » - 2019
- Renault / Mahindra – échec de Logan en Inde – 2007
- IKEA – positionnement culturel décalé – Corée du Sud – 2014
- Alcatel Lucent – fusion difficile / management interculturel – 2006

« La gestion des transformations sur un périmètre international rend-elle la question culturelle si cruciale qu'il faille rebaptiser le DRH « VP People & Culture » chez TechnipFMC » - Revue Spéciale de l'**ANDRH** « Personnel » septembre 2019.

Le terme de *compliance* souvent utilisé dans les grandes entreprises peut y être entendu comme l'un des synonymes de conformité. Il faut toutefois considérer qu'il englobe parfois, sous l'égide d'un Chief Compliance Officer (Responsable Conformité de l'entreprise), seulement quelques points particuliers de conformité aux lois ou règlements comme les programmes de conformité à la lutte contre la corruption et le trafic d'influence, ou encore la vigilance sur l'exposition aux sanctions économiques internationales. Les autres domaines de conformité restent souvent l'apanage de la direction juridique.

Finalement, l'évolution récente des lois reflète assez bien l'évolution générale du contexte sociétal, vers un monde de plus en plus protégé, contrôlé et surveillé. Aujourd'hui, la dimension juridique étendue est, à ce titre, l'un des principaux sujets de préoccupation dans le quotidien du risk manager.

1.4.7 Les technologies

Les technologies désignent au sens large des domaines très évolutifs et très divers, tels que les organismes génétiquement modifiés, la viande in vitro, la bio-impression, la biostase, les thérapies photo-dynamiques, l'optogénétique, etc. Au sens étroit, on les associe communément au traitement de l'information et de la communication (TIC), avec en point d'orgue l'Intelligence Artificielle et le big data. Les technologies se sont imposées comme une dimension stratégique de l'entreprise - vecteurs de croissance et moyens de facilitation des échanges - et sont donc un facteur significatif d'extension de l'entreprise.

Les technologies sont généralement hors de la maîtrise complète des entreprises utilisatrices. Un appareil, un produit, un outil, un logiciel par exemple, comprend souvent des boîtes noires dont les entreprises utilisatrices ne maîtrisent pas le contenu, les technologies et le savoir-faire mis en œuvre. Elles sont dès lors dépendantes de leurs fournisseurs, et de fait, exposées à des risques.

● Les nouvelles technologies et les matières premières

La notion d'Entreprise étendue s'entend ici au niveau planétaire, mondialisation oblige. Par exemple, les technologies de la transition numérique utilisent maintenant fortement certaines matières premières appelées terres rares. Certaines entreprises en sont donc très dépendantes. En peu de décennies, avec souvent l'aval des états, la Chine a acquis le quasi-monopole de l'exploitation des terres rares et a capté les chaines de valeur en aval. Ceci rend possible des manipulations de cours à son profit (*).

(*) cf. Annexe 12 « Bibliographie » La guerre des métaux rares – Guillaume Pitron – 2018

De plus, les nouvelles technologies peuvent être, elles-mêmes, porteuses de nouveaux risques sur la santé et la sécurité au travail pour des moyens censés améliorer les conditions de travail : on peut ici citer le cas des exosquelettes ou des diodes électroluminescentes (**).

- Le numérique et les systèmes d'information

La technologie s'est affirmée, en créant de la valeur, en rentabilisant les processus, en apportant aux décisionnaires les informations pertinentes, et en donnant aux clients l'accès à des comparatifs. Mais des risques apparaissent sur la disponibilité, l'intégrité et l'exhaustivité des informations. L'ère internet multiplie les capacités de partage d'information, d'instantanéité et d'interopérabilité, et accroît d'autant le territoire de l'Entreprise étendue et ses risques.

Le développement des objets connectés, que favorise l'arrivée de la 5G, va aussi développer les liens de l'entreprise vers l'extérieur, et donc créer des risques nouveaux sur lesquels son contrôle sera limité.

Le numérique couvre maintenant le sociétal avec les robots et l'intelligence artificielle (cf. Annexe 5 « risques de l'intelligence artificielle »). L'intelligence artificielle crée parfois des risques au-delà des attentes imaginées par leurs créateurs (cf. Question type n°6 – Exemple « Non prise en compte des différences culturelles dans un choix stratégique »). De plus, l'évolution vers l'attribution d'une personnalité juridique à des robots progresse : robot Sophia en Arabie Saoudite, logiciel Vital doté d'un droit de vote au conseil d'administration de la société Deep Knowledge à Hong Kong, recommandation du Parlement européen en 2017 sur les règles de droit civil sur la robotique. Autour des règles de droit en matière de responsabilité, c'est une nouvelle nature d'extension de l'Entreprise étendue avec de nouveaux risques à identifier.

A contrario, le numérique et l'intelligence artificielle apportent également des outils de réduction des risques, par exemple avec la *blockchain*, l'augmentation de la traçabilité et la déduction de causes/recommandations. Mais la progression fulgurante des objets connectés, dotés d'algorithmes, créateurs et vecteurs de données, fait que globalement les risques de l'Entreprise étendue continuent de se diversifier et de s'amplifier.

Plus généralement, le numérique est à aborder au travers de la cybersécurité. La mise en oeuvre de cette dernière doit protéger les personnes et les actifs de l'entreprise et toute organisation jusqu'au niveau étatique.

(**) cf. Annexe 12 « Bibliographie » Nouvelles technologies – Nouveaux risques (symposium de l'Institut national de médecine agricole – Tours 2017)

- Les données (Data)

Les Data, ou données, sont les constituants des informations. Dans l'entreprise, elles sont de plus en plus souvent d'origines externes, et donc moins contrôlées ou fiabilisées que si ces données étaient d'origines internes.

La croissance d'utilisation des données est exponentielle. On parlait de stockage en giga-octets (10^9), on gère maintenant des tera (10^{12}) et bientôt des exa (10^{18}) voire des yotta (10^{24}). Les sécuriser devient très complexe, ce qui induit l'apparition de nouveaux risques.

Pouvoir stocker tant de données permet une traçabilité sur d'innombrables faits. Par exemple, les téléphones portables permettent de reconstruire les trajets minutés d'un commercial VRP ou d'un routier, données qui peuvent devenir des preuves juridiques dans un contentieux. Au-delà du vertige des volumes, il faut considérer les combinatoires potentielles des données, ce qui crée de nouvelles masses d'informations. L'un des champs exploités par l'Intelligence Artificielle est le big data, dont le concept a été formalisé dans les années 1990 (le terme big data apparaît dans un article de l'ACM -*Association for Computing Machinery*- en 1997). Les risques se croisent, s'étendent et se complexifient.

Les risques liés aux données s'étendent même au niveau sociétal : une application banale est le profilage des individus pour cibler les offres commerciales. Au-delà de la pertinence des résultats et des usages qui en sont faits (revente par exemple), l'utilisation de données personnelles induit une extension de fait du périmètre de l'entreprise, les clients et prospects devenant des parties prenantes au-delà de la relation contractuelle. Et avec des réglementations comme le RGPD, les risques de l'Entreprise étendue s'accroissent … parfois volontairement, par exemple si l'entreprise désire augmenter ses parts de marché. Enfin, l'accès et la propriété des données induisent aujourd'hui des difficultés. De nombreux pays adoptent des règlementations contradictoires et interdisent par exemple la sortie de leur territoire pour certains types de données.

- Les cloud

L'usage du cloud (ou le nuage internet) implique divers risques dont par exemple :

- La perte de confidentialité au travers de cyberattaques ;
- La dépendance de la qualité des transactions à la qualité des réseaux ;
- Un flou et une complexité juridiques lorsque les données sont implantées hors du pays ;
- Des complexités techniques de mises en œuvre pour les interfaces applicatives ;

- L'absence de réversibilité si elle n'est pas prévue au contrat avec l'hébergeur ;
- L'accident (exemple d'un incendie) sur le site du serveur utilisé conduisant potentiellement à la perte irréversible de données si le processus de sauvegarde est mal calibré.

A ce titre, sous couvert de leur facilité d'usage, les clouds sont des composantes relativement nouvelles et typiques de l'Entreprise étendue, sur lesquelles elle a un contrôle limité, et qui recouvrent bien la plupart de ses dimensions (juridique, économique, géographique, …). Donc la prudence s'impose.

1.4.8 L'économique et les dynamiques de marchés

L'entreprise dépend des conditions économiques et des dynamiques de marché qui prévalent dans ses activités. Des évolutions dans ces domaines peuvent changer drastiquement son sort, la conduire à la faillite ou lui donner l'opportunité de nouveaux développements.

Les facteurs économiques sont nombreux : emploi, inflation, taux d'intérêt, taux d'imposition, taux de change, taux d'épargne, niveaux de confiance des consommateurs, récessions, concurrence, … autant de facteurs de toute évidence généralement hors de son périmètre interne et hors de ses possibilités d'actions directes. La dimension économique est donc du ressort de l'Entreprise étendue.

A titre d'exemple, la rentabilité d'un producteur de pétrole dépend du prix de marché de sa production. L'atteinte d'un niveau tarifaire suffisamment élevé a permis l'exploitation d'énergies non conventionnelles telles que les gaz de schiste et, en conséquence, certains pays sont passés de la position de consommateur à celle de producteur. Les sociétés d'exploitation existantes ont vu leurs relations internationales changer de nature, leurs risques de même. Un autre exemple concerne le marché du commissariat aux comptes en France, qui s'est drastiquement contracté (plus de 50%) suite à une nouvelle réglementation augmentant les seuils imposant le recours à un commissaire aux comptes. Ceci relève bien de l'Entreprise étendue.

Au travers de ses ventes de produits et services, ou de ses achats, une entreprise est acteur sur un ou plusieurs marchés. Toute évolution de ses marchés, que ce soit en réduction ou en croissance, va influer directement sur sa rentabilité, voire sur son devenir.

Dans les situations d'oligopole voire de monopole sur certains marchés, l'Entreprise étendue peut se sentir - à tort - moins concernée par ce sujet, son marché étant sous son contrôle. Cependant, elle se doit de mettre en place un système de veille au cas où l'environnement de son marché évoluerait sans qu'elle en prenne conscience du fait de son manque de vigilance.

Exemple de risque - Question type n°7

La fiscalité des pays dans lesquels l'entreprise a des intérêts est-elle connue et maîtrisée ?

Evolutions de la Fiscalité

Fiscalité piégeuse - remise en cause d'un Business Plan de conquête

Eléments factuels

L'entreprise Martin constate que le marché européen est mature et saturé. Il peine à se renouveler. En France, la croissance du marché a été de 0,2% en 2015. Au-delà de renouveler ses gammes par une évolution de son positionnement qualité/prix ou par de nouveaux positionnements, L'entreprise Martin est partie à la conquête de nouveaux marchés au Moyen-Orient et en Asie. Le Moyen-Orient est propice car l'entreprise y maîtrise déjà les tendances majeures, des effluves chauds et boisés ; les ventes y croissent de 14%. Si la croissance en Chine est de 9% « seulement », elle est de 25% en Inde et atteint les 44% en Indonésie. En revanche, il faut engager des études sur les formulations pour correspondre aux attentes des clients de ces pays.

Analyse des causalités

Les Emirats Arabes Unis et l'Arabie Saoudite introduisent au 1er janvier 2018 la TVA avec un taux standard de 5%. Les autres pays de la zone ont repoussé cette introduction à 2019. Même si ce taux de TVA est faible vis-à-vis des taux européens, le business plan de l'entreprise, agressif sur les tarifs pour tenir compte de la concurrence, ne prenait pas en compte cette introduction de la TVA.

Du côté de l'Inde, la mise en place d'une TVA unique pour remplacer une dizaine de taxes régionales s'avère plus compliquée et plus chère que présentée par les autorités.

Quant à la Chine, la situation de conflit commercial créée par les Etats-Unis induit de grandes incertitudes sur le potentiel de développement pour les produits de luxe, la Chine étant de plus un producteur important pour les entreprises de luxe françaises, avec la volonté de favoriser l'interne.

Evaluation des conséquences

Les bénéfices prévus sont donc remis en question de façon significative (des pertes deviennent envisageables), ainsi donc que l'opportunité de ce projet de conquête de nouveaux marchés.

Comportements/actions possibles

- Réviser les formules des parfums pour encore réduire les coûts de production et recréer ainsi la marge nette attendue
- Refaire les études de positionnement des produits pays par pays pour trouver de nouveaux positionnements respectant la marge nette attendue

Capitalisation pour l'approche Entreprise étendue

Principales parties prenantes identifiées

- Instances des pays cibles faisant évoluer la réglementation (parlements, exécutifs, …).
- Institutions fiscales des pays cibles.

Recommandations

- Avoir une veille fiscale permanente sur l'ensemble des pays clients et en prospection.
- Surveiller régulièrement la capacité de positionnement de ses produits et prestations.

Cas réels similaires (cf. Annexe 3 « Questions types – Sources détaillées des cas réels similaires »).

- Zoom Cairn Energy : litige fiscal, Inde - 2015
- Orange : redressement fiscal, Niger - 2018

« Fiscalité internationale : faire face aux nouvelles obligations et anticiper les risques émergents »

DFCG *(Association des Directeurs Financiers et de Contrôle de Gestion) - Lyon - mars 2017 ; « Face à la hausse des contrôles fiscaux, êtes-vous certain d'être en conformité et de minimiser vos risques ? »* DFCG - Montpellier - octobre 2017.

1.4.9 Autres enjeux et dimensions à traiter

Il serait fastidieux, impossible et inutile de lister dans notre ouvrage toutes les dimensions possibles. Chaque entreprise doit les étudier pour définir le champ de ses extensions et les risques qui y sont liés, selon son contexte et son organisation.

Ainsi la dimension culturelle, déjà évoquée à la section 1.4.4 « Le politique et le géographique », prend de l'importance dans le contexte de la RSE. Des différences de culture peuvent jouer un rôle sur la compréhension des objectifs, la déclinaison des méthodes et des modes de travail, voire sur la relation humaine dans le travail. Il est évident que les pratiques sociales et sociétales sont variables d'un pays à l'autre et que certains comportements pouvant apparaitre normaux par endroits sont intolérables ailleurs. Le COSO ERM « *Integrating with strategy and performance* » mentionne lui aussi les aspects de gouvernance et de culture.

De même dans la dimension économique, des thèmes tels que les tarifs douaniers et les pratiques douanières, les techniques fiscales notamment entre pays (cf. Question type n°7 – Exemple « Evolutions de la Fiscalité »), les accès aux capitaux, l'existence des Fintechs par exemple sont autant de sujets à ne pas mésestimer selon le contexte de chaque Entreprise étendue.

Si l'on considère le périmètre de l'Entreprise étendue comme un écosystème, on peut envisager d'en faire une représentation graphique. En s'appuyant sur la définition d'une partie prenante, comme celle proposée par le GRI (*), différents axes d'identification des parties prenantes se présentent (cf. figure 9 « Vue d'ensemble de l'Entreprise étendue »). Cette représentation peut se faire sous forme de réseau car tous les liens de l'Entreprise étendue avec son écosystème font d'elle un acteur non isolé, en interconnexion avec les écosystèmes d'autres acteurs.

Point de vue d'un risk manager

« Avec cette responsabilité élargie, l'entreprise doit faire face au risque croissant de mise en cause et de judiciarisation systématique par certaines parties prenantes, de tout évènement perçu par elles comme un manquement. Dans un contexte global d'absence ou fragilité de dialogue et de montée de l'intolérance et de l'activisme, la nature du manquement et l'endroit du monde où il est perçu n'ont pas d'importance. La nature de l'événement prime sur son origine. »

Un risk manager du secteur de l'énergie.

(*) cf. Annexe 12 « Bibliographie » ONG Global Reporting Initiative

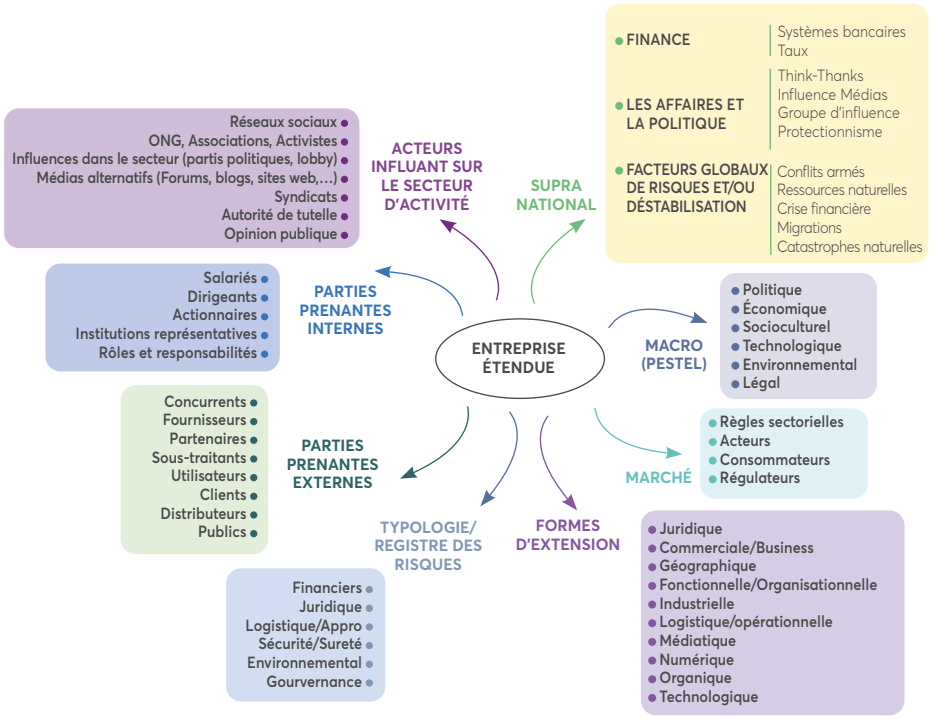


Figure 9 - Vue d'ensemble de l'Entreprise étendue. D'après l'atelier B4 "Gouvernance et Gestion des risques occasionnées ou partagés avec des tiers - 27ème Rencontres du Risk Management - AMRAE 2019

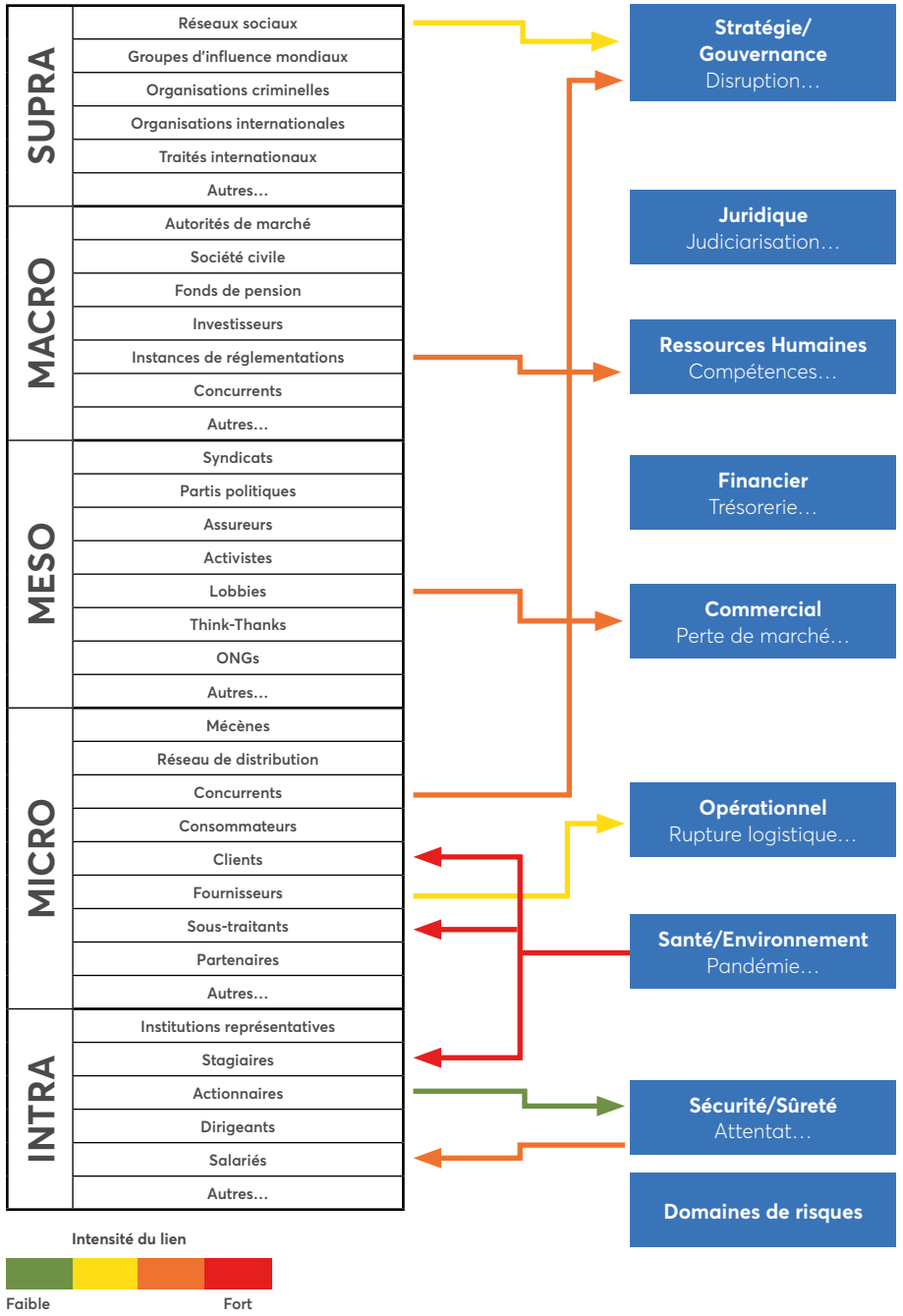
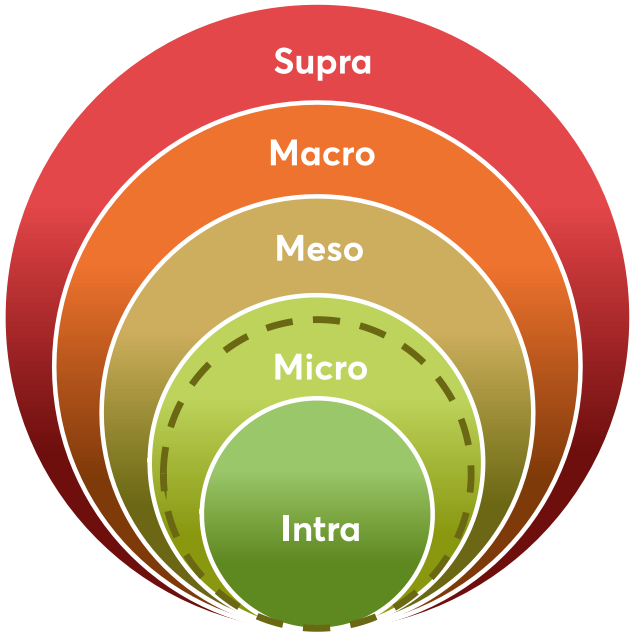


Figure 10 – Exemples d'intensité entre domaines de risques et parties prenantes



Supra : Institutions et organisations supranationales, finances, affaires et géopolitique mondiale

Macro : Acteurs politiques, économiques, sociologiques, technologiques, écologiques et légaux pouvant influencer l'entreprise

Meso : Acteurs et parties prenantes non institutionnels pouvant influencer l'entreprise ; jeux visibles et invisibles

Micro : Acteurs de la chaine de valeur, la topographie concurrentielle, les règles sectorielles

Intra : Activités de l'entreprise, ses ressources, ses actifs, ses avoirs, ses processus, son organisation et son histoire

Figure 11 – L'écosystème : les parties prenantes

1.5 L'écosystème : les parties prenantes

La nécessité pour l'Entreprise étendue est de déterminer son périmètre réel, et d'appréhender précisément l'ensemble des parties prenantes qui constituent son écosystème.

Cartographier ou lister ces parties prenantes s'impose afin de préciser davantage les contours et les éléments constitutifs de l'Entreprise étendue, bien que ceux-ci soient par nature évolutifs et mouvants. Il est alors possible de placer les parties prenantes autour de l'entreprise, selon leur proximité, dans différents environnements plus ou moins éloignés (cf. figure 11 « L'écosystème : les parties prenantes »).

La cartographie des risques proposera ainsi une vision globale, facilitant l'identification et le traitement des risques de manière plus précise et complète. L'évolution des obligations d'information des entreprises est rapide. Aujourd'hui, elles doivent communiquer au-delà du rapport de gestion, sur des composantes de plus en plus variées de type social, sociétal ou environnemental. Pour les plus grandes d'entre elles, les matrices de matérialité qui figurent dans les rapports intégrés relient l'importance des activités pour l'Entreprise étendue et leurs impacts pour les parties prenantes.

Après avoir déterminé les sphères d'influence et les parties prenantes de son écosystème, et élaboré les Natures de risque de son entreprise par domaines, il peut être utile de dresser un schéma de leurs interrelations dans les deux sens afin de mesurer l'intensité du lien entre ces différents éléments (cf. figure 10 « Exemples d'intensité entre domaines de risques et parties prenantes »). L'intensité du lien est un **indicateur clé / Key Risk Indicator (KRI)** du niveau inhérent de risque avant mise en place d'un dispositif de maîtrise. Ce schéma s'apparente à la matrice de matérialité qui croise l'importance des activités pour l'entreprise et pour les parties prenantes.

Un exemple de document de travail est fourni en annexe. Il s'agit d'un schéma spécifique à une PME de distribution, qui associe aux parties prenantes identifiées dans l'écosystème, leur lien avec les processus et l'importance de leurs impacts quant aux risques de cette entreprise (cf. Annexe 6 « parties prenantes par thèmes » et figure 23 « Exemple d'impacts des parties prenantes par thèmes de l'Entreprise étendue »).

● INTRA Entreprise : Environnement interne

Cet environnement représente le coeur même de l'entreprise, ce que l'entreprise a en propre et construit depuis sa création. Il contient toutes les activités principales et les activités supports de l'entreprise, ses produits et services, ses processus métiers ou industriels, ses savoir-faire, ses avoirs et ses actifs tangibles ou intangibles. Y figurent également ses ressources humaines ainsi que ses valeurs, sa marque, son image, son organisation, ses dirigeants, ses actionnaires.

● MICRO Environnement

Les entreprises, en particulier dans le secteur manufacturier, ont de moins en moins une activité totalement isolée et « intra » mais s'inscrivent au contraire dans une chaîne de valeur plus globale au sein de leur secteur d'activités. Afin de réaliser leurs finalités et objectifs propres, elles échangent des flux divers comme des biens et des équipements, des matières brutes ou travaillées, des actifs financiers, des données, ... Les activités de l'entreprise, dans son secteur, sont régies par un certain nombre de règles sectorielles et soumises à un environnement concurrentiel. A ce titre, cet environnement est structuré selon le modèle des « 5 forces de Porter » déterminant la structure concurrentielle d'une industrie de biens ou services : le pouvoir de négociation des clients, des fournisseurs, la menace de produits ou services de substitution, ou celle de nouveaux entrants, et enfin l'intensité de la rivalité entre concurrents.

● MESO Environnement

En parallèle des relations bien établies et formalisées entre l'entreprise et ses principaux partenaires économiques constituant la chaîne de valeur dans son secteur d'activité, se trouvent d'autres acteurs, plus ou moins visibles, qui par leurs actions ou leurs jeux d'influence peuvent affecter son fonctionnement, son image, sa rentabilité, son organisation, … Parmi ces acteurs on pourrait citer, entre autres, des activistes, des ONG, des médias en particulier les alternatifs, des partis politiques, des syndicats, des personnalités publiques, des réseaux sociaux, des associations, des Think Tanks, des lobbyistes, …

● MACRO Environnement

Cet environnement contient les facteurs politiques, économiques, sociologiques, technologiques, environnementaux et légaux (cf. figure 22 « L'analyse PESTEL ») qui peuvent influencer le secteur d'activité et la chaîne de valeur de l'entreprise. On y trouve par exemple les règlementations du secteur, la politique monétaire et fiscal, la régulation import/export, la politique budgétaire, le plan industriel, la propension à consommer, la démographie, les questions éthiques et sociologiques, la protection des consommateurs et la sécurité des citoyens, les divers textes législatifs relatifs au travail, au commerce aux relations entre citoyens, les réglementations en matière de pollution et d'environnement, ... Tous ces facteurs se retrouvent plutôt à un niveau national, mais peuvent voir se surajouter des contraintes additionnelles règlementaires, administratives, politiques, monétaires et économiques issues, par exemple, du cadre de l'Union Européenne.

● SUPRA Environnement

Ce dernier environnement, le plus lointain pour l'entreprise, est le moins palpable. Il est représenté par les différents systèmes mondiaux politiques, financiers, fiscaux, monétaires, commerciaux dirigés par les instances supranationales ou transnationales. On y retrouve également diverses influences géopolitiques, militaires, religieuses, interculturelles, sociologiques ainsi que les phénomènes migratoires, les traités ou règlements nationaux à portées internationales ainsi que les traités commerciaux multilatéraux. Cet environnement est principalement contraignant pour une majorité d'entreprises qui en subissent les effets, mais peut aussi être source d'opportunités pour certaines, en particulier de taille conséquente.

Exemple de risque - Question type n°8

De nouveaux standards internationaux, ou normes règlementaires, sont-ils en cours d'élaboration, risquant de concerner les produits ou les services de l'entreprise ?

Changement géopolitique : relations économiques, normes et règlementations
Brexit

Eléments factuels
Le PDG de l'entreprise craint un impact très négatif en cas de concrétisation du Brexit, non pas tant sur l'aspect géopolitique, mais par un effet collatéral de complexification des règlementations, déjà exigeantes dans l'industrie des cosmétiques. Avec un solde commercial positif d'environ 800 M€, le marché des cosmétiques avec le Royaume Uni est très favorable à l'Europe, pour l'instant…

Analyse des causalités
En effet, les normes administratives et de mises sur le marché risquent de se trouver dédoublées et surtout complexifiées, quand bien même le Royaume-Uni suit déjà au plus près le règlement cosmétique européen ainsi que le règlement REACH qui évalue et autorise les substances chimiques. Des disparités dans les compositions et des divergences dans les « compositions acceptables » pourraient apparaître.

Evaluation des conséquences
- Revue complète d'impact probable sur chaque produit exporté (plusieurs millions !) et adaptation des dossiers individuels de produits, surcharge administrative et organisationnelle.
- Restructuration du packaging et de la logistique (surcoûts).
- Chute prévisible de la marge sur une partie de la gamme des produits.

Comportements/actions possibles
- Déplacer des établissements.

Capitalisation pour l'approche Entreprise étendue

Principales parties prenantes identifiées
- Réseau de distribution / franchisés.
- Clients finaux, utilisateurs, consommateurs.
- Pouvoirs publics, Institutions gouvernementales.
- Organismes de réglementations ou de normalisation.
- Douanes.
- Groupes de lobbying.

Recommandations
- Connaître parfaitement toutes les normes, dans tous les domaines, s'appliquant dans son secteur d'activités, et être à même de prouver sa propre conformité.
- Etablir une veille proactive sur toutes normes/réglementations en préparation, même à l'état d'idée.
- Avoir des représentants dans les organismes de régulation de son domaine.
- Devenir éventuellement influenceur de futures normes dans son domaine d'activités.

Cas réels similaires (cf. Annexe 3 « Questions types – Sources détaillées des cas réels similaires »).

- Entreprises de l'Industrie cosmétique : norme ISO 16128 - janvier 2018
- Entreprises d'Implants médicaux anglaises : Lobbying - 2019
- BMW, Volkswagen : nouvelles normes européennes - 2018
- Agence fédérale de l'automobile (KBA) : Allemagne, normes anti-pollution – 2019
- …

ISOfocus
(https://www.iso.org/fr/isofocus_139.html) mars-avril 2020 : « Les normes sont des outils puissants pour toute entreprise. Véritable gage de confiance, elles contribuent à réduire les coûts, à doper la productivité et à dégager davantage de bénéfices. » … « Le monde des affaires se caractérise par des changements incessants. Pour garder une longueur d'avance sur la concurrence, suivre le progrès technologique et répondre aux besoins des clients, il faut faire preuve d'agilité et savoir évoluer en temps réel. Dans un monde en rapide mutation, si l'on veut rester dans la course, il est nécessaire d'avoir en place un système propre à gérer l'adaptation aux changements. Depuis des années, les Normes internationales fournissent ces cadres et les solutions indispensables aux entreprises pour lancer de nouveaux produits et services, se développer ou simplement se maintenir sur le marché. »

2. La gestion des risques de l'Entreprise étendue

2.1 Quels sont les risques de l'Entreprise étendue ?

L'ensemble des liens (contractuels ou non, directs ou non) et des interactions de l'Entreprise étendue avec sa sphère d'influence, ses parties prenantes, ce monde extérieur de plus en plus ouvert et étendu, induit potentiellement des incertitudes nouvelles, donc des risques.

De plus, comme nous l'avons vu, ces risques de l'Entreprise étendue ne se limitent pas à la chaîne de valeur mais englobent également l'environnement économique, politique, sociétal, réglementaire, etc. Ainsi, par exemple, une communication extérieure non institutionnelle peut dégrader l'image ou la réputation de l'Entreprise étendue si la personne qui s'exprime est perçue comme représentative. Cela englobe les dirigeants évidemment, mais aussi tout salarié qui ferait état de son appartenance à l'entreprise en exprimant publiquement des positions personnelles.

C'est pourquoi les risques de l'Entreprise étendue peuvent être considérés comme « voulus » ou « non voulus » selon la terminologie employée par l'IFA (Institut Français des Administrateurs) dans un document sur le rôle du conseil d'administration dans la détermination de l'appétence aux risques.

Les risques provoqués par les tiers, avec lesquels il peut y avoir ou non une relation contractuelle, peuvent être multiformes et produire un impact sur l'entreprise de plusieurs façons, depuis une légère perturbation de sa production jusqu'à une détérioration profonde et durable de son image en passant par des impacts légaux et règlementaires sévères, à l'exemple des risques induits par les nouvelles règlementations comme le devoir de vigilance, le règlement européen RGPD, ou encore la loi Sapin 2. Le domaine réglementaire implique également l'Entreprise étendue au niveau international, notamment avec les règles d'extraterritorialité d'un nombre croissant de lois nouvelles (cf. Question type n°8 – Exemple « Changement géopolitique : Relations économiques, Normes et Règlementations »).

Nature	Périmètre usuel	Périmètre étendu
Financier	• Trésorerie, liquidités • Sous-capitalisation • Défaillances clients • Prix matières premières • …	• Volatilité taux de change • Fraude • Exposition fiscale • …
Opérationnel	• Obsolescence outil production • Dépréciation stocks • Défaillance fournisseur • Qualité produits ou services • …	• Rupture approvisionnement d'un composant • Intrusion système d'information • Rupture chaîne logistique • …
Juridique	• Non-conformité • Litiges clients • Rupture engagements • Changement réglementaire • …	• Extraterritorialité • Contrefaçon, infraction brevets • Engagement hors bilan • …
Santé / Sécurité / Environnement	• Maladie professionnelle • Incendie, explosion • Maladie professionnelle • Accident environnemental • …	• Attentat terroriste • Corruption • Atteintes aux personnes • …
Commercial	• Décroissance du marché • Politique de prix • Concurrence agressive • Perte client clé • …	• Géopolitique • Nouveaux entrants disruptifs • Restrictions commerciales • …
Stratégique / Gouvernance	• Stratégie imprécise • Disruption technologique • Actionnariat • Transformation interne • …	• Externalisation • Ingérence économique • Défaillance partenaire • …
Ressources Humaines	• Psycho-sociaux • Compétences • Conflits internes • Conditions travail • …	• Multiculturalité • Réseaux sociaux • Adhésion valeurs • …
Autre domaine	• …	• …

Figure 12 – Exemple 1 d'extension du périmètre usuel des risques par nature de risques

Au cours du temps, le périmètre d'exposition aux risques aura tendance à augmenter (cf. figure 12 « Exemple 1 d'extension du périmètre usuel des risques par nature de risques » et figure 13 « Exemple 2 d'extension du périmètre usuel des risques par identification de 3 nouvelles natures de risques »), en fonction du degré d'extension de l'Entreprise étendue de deux manières par :

- l'apparition de nouveaux risques,
- l'amplification de risques déjà existants et connus.

Cependant, à l'inverse, les extensions de l'entreprise peuvent aussi rétrécir et être un moyen pour elle, par la saisie ou la mise en place d'opportunités, de diminuer des risques déjà existants, par exemple en réinternalisant des activités (cf. figure 14 « Exemple de mesure des impacts à la suite d'une analyse étendue »).

Le périmètre économique de la plupart des organisations comprend des niveaux secondaires, tertiaires et au-delà, dans lesquels certains tiers, parfois totalement inconnus de la gouvernance, agissent. Leurs comportements et leurs actions peuvent influer sur la bonne marche de l'Entreprise étendue ou sa réputation.

Des expositions nouvelles insoupçonnées peuvent ainsi apparaître par ricochet, effet domino, effet collatéral, aussi bien sur l'axe de la chaîne de valeur que dans l'environnement plus global, économique, sociétal ou politique de l'entreprise.

Les tierces parties peuvent également être localisées dans des pays présentant des modèles, des juridictions, des normes, des cultures de natures différentes, qui peuvent se révéler un réel défi à suivre et contrôler par l'entreprise.

Il est important de noter que tous les risques de nature traditionnelle, à l'exemple de la cartographie spécialisée des risques de sureté et sécurité (cf. Annexe 7 « Focus sur le domaine Sûreté et Sécurité » et figure 25 « Panorama des risques dans le domaine de la Sécurité/Sûreté »), sont susceptibles d'être embarqués par l'Entreprise étendue. Dans ce domaine comme dans les autres, par une décision ou une action volontaire d'extension, ou par un effet de bord, l'Entreprise étendue pourra se trouver exposée à une nouvelle nature de risque qu'elle n'avait pas à considérer jusqu'à présent.

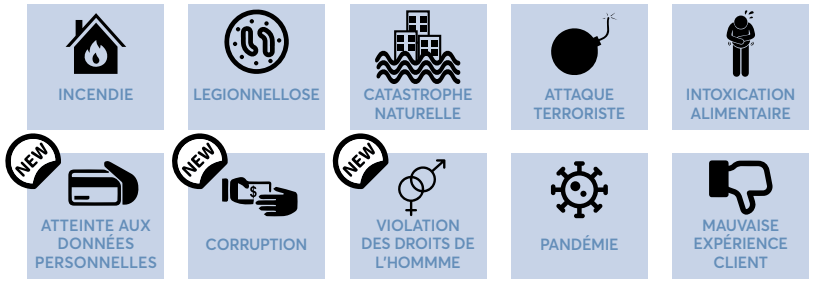


Figure 13 – Exemple 2 d'extension du périmètre usuel des risques par identification de 3 nouvelles natures de risques

Périmètre actuel (vision restreinte)

	Domaine 1	Domaine 2	Domaine 3	Domaine 4	...	Domaine n
risque 1						
risque 2						
risque 3						
risque 4						
risque 5						
risque n						

Périmètre réel (vision étendue)

	Domaine 1 inchangé	Domaine 2 étendu	Domaine 3 accru	Domaine 4 réduit	...	Domaine n
risque 1						
risque 2						
risque 3						
risque 4						
risque 5						
risque n						

Figure 14 – Exemple de mesure des impacts à la suite d'une analyse étendue

Impacts faibles | Impacts moyens | Impacts élevés | aucun impacts

Toujours dans le domaine sûreté, l'implantation d'une filiale à l'étranger pourrait faire surgir des risques nouveaux tels que des atteintes à la sécurité des personnels ou des accès ou des comportements frauduleux. Cet exemple de panorama des risques sûreté liste les actifs concernés en fonction des types de menaces, ainsi que les différentes natures de conséquences pour l'entreprise.

Le risk manager peut appliquer le même raisonnement à tous les autres domaines de risques traditionnels. Dans certaines entreprises ou sur des projets, les risques sont répertoriés sous forme d'un registre. Il convient bien sûr d'analyser chacun des principaux domaines de risques de l'entreprise.

Un effet évident de la prise en compte des risques de l'Entreprise étendue est l'élargissement de la vision des risques. On pourra y retrouver des risques relatifs à des scénarios tels que :

- Un client organise un boycott sur les réseaux sociaux ;
- Un vendeur livre (volontairement ou non) des informations confidentielles sur l'Entreprise étendue ;
- Un partenaire indélicat divulgue des données stratégiques ;
- Un fournisseur de composants stratégiques fait faillite ou est victime d'une catastrophe naturelle conduisant à une rupture d'approvisionnement (cf. Question type n°9 – Exemple « Catastrophe naturelle : composants en rupture dans la Supply Chain ») ;
- Un fonds d'investissement lance une OPA hostile ;
- Un pays tiers édicte une nouvelle norme (ou nouvelle loi) contraignante, avec principe d'extra-territorialité ;
- Une entité (criminelle, étatique) lance une cyberattaque déstabilisante ;
- Une contrefaçon d'un produit non protégé juridiquement se répand sur le marché.

Il est possible de montrer dans une illustration (cf. figure 12 « Exemple 1 d'extension du périmètre usuel des risques par nature de risques ») comment, par une approche globale, le panorama des risques devrait apparaître en réalité par rapport à ce qu'il était supposé être (cf. figure 3 « Exemple de panorama des risques par nature »). Ainsi, pour chaque nature de risque, le risk manager est en mesure de détecter potentiellement, dans l'univers des risques de son entreprise, plus de facteurs de risques.

L'esquisse de l'évolution d'un registre des risques (cf. figure 14 « Exemple de mesure des impacts à la suite d'une analyse étendue ») montre les impacts potentiels de l'approche proposée. Ainsi pour un organisme qui aurait trois domaines de risques, leur analyse sous l'angle Entreprise étendue le conduirait à conclure que les risques du domaine 1 seraient inchangés, le domaine 2 serait entièrement nouveau avec des risques qui n'existaient pas auparavant. Le domaine 3 verrait ses risques s'accroitre, alors que le domaine 4 verrait ses risques se réduire.

L'analyse du périmètre réel et des parties prenantes peut aboutir à une révision des domaines de l'univers des risques de l'Entreprise étendue :

- Inchangé : les risques du domaine sont identiques par leur nature et intensité;
- Étendu : des risques nouveaux peuvent apparaître dans le domaine, par exemple risque de fraude dans certains pays et risques environnementaux chez un fournisseur déjà connu;
- Accru : globalement l'univers des risques est le même, mais certains risques d'un domaine se trouvent amplifiés, par exemple une diversification conduit à étendre les risques liés à la réglementation à un nouveau secteur d'activité;
- Réduit : certains risques existants peuvent diminuer, par exemple optimisation des relations contractuelles avec un partenaire existant.

Une alternative d'illustration, (cf. figure 13 « Exemple 2 d'extension du périmètre usuel des risques par identification de 3 nouvelles natures de risques »), présente une visualisation d'impacts de l'Entreprise étendue, avec là aussi des risques nouveaux et des risques accrus (en noir), et des risques inchangés (en gris clair).

Rappelons, page suivante, la définition des risques de l'Entreprise étendue, donnée lors de l'atelier C7 « *De la sous-traitance à l'entreprise étendue : nouveaux enjeux pour l'entreprise et le risk manager* » aux 24ème Rencontres du Risk Management - AMRAE 2016. Cette définition vise à couvrir aussi bien les risques créés par l'entreprise envers de son écosystème que les risques subis du fait son écosystème.

Exemple de Risque - Question type n°9

Les composants importés utilisés dans les processus de fabrication des produits de l'entreprise proviennent-ils de zones à Risques non encore identifiées ?

Catastrophe naturelle : composants en rupture dans la Supply Chain
Utilisation du Bois d'Agar

Eléments factuels
L'entreprise Martin utilise de l'essence de bois d'Agar (ou encore « bois des dieux » ou « bois de Oud »). Elle est connue depuis des millénaires et à de multiples usages (religieux, médical, parfums, …). Ses flagrances sont puissantes, boisées, mystérieuses, ... Son prix est de l'ordre de 40 K€ le litre.
L'entreprise a choisi la Thaïlande comme source d'approvisionnement pour cette essence.
L'entreprise s'approvisionne en flux tendu du fait du prix très élevé de cette essence pour limiter les besoins de trésorerie.

Analyse des causalités
La rareté de cette essence associée au fait que la demande est en forte croissance a créé une tension sur son approvisionnement.
Cependant, l'entreprise Martin, étant satisfait de ses fournisseurs Thaïlandais, n'a pas recherché d'autres sources.
Mais la Thaïlande a subi récemment des inondations exceptionnelles, interrompant presque tous les transports dans la région, dont en particulier ceux de cette essence.

Evaluation des conséquences
La rupture d'approvisionnement va provoquer un arrêt de la production de plusieurs parfums dans les 3 semaines.
Il y a aura donc une baisse significative du chiffre d'affaires, pouvant atteindre près du tiers des ventes.

Comportements/actions possibles
- Court terme : rechercher d'autres fournisseurs.
- Moyen / Long terme : réviser la politique flux tendu ('Lean') des approvisionnements.

Capitalisation pour l'approche Entreprise étendue

Principales parties prenantes identifiées
- Fournisseurs, transporteurs locaux.

Recommandations
- Intégrer dans l'étude des Risques ceux de rupture d'approvisionnement.
- Tenir compte de la sensibilité des composants : plus ou moins substituables.
- Evaluer les économies / pertes avérées et potentielles en fonction de la politique Lean d'approvisionnement.

Cas réels similaires (cf. Annexe 3 « Questions types – Sources détaillées des cas réels similaires »).

- ANSM : pénurie médicaments Covid-19 – 2020 - Ferrari : graves ruptures d'approvisionnement, Coronavirus – 2020
- Renault, Peugeot : pénurie de pièces automobiles, tsunami au Japon - 2011
- Western Digital : pénurie de composants high tech, inondations Thaïlande – 2020

« Conscient de la "très forte tension" à laquelle nous sommes mondialement "soumis" en matière d'équipements de protection contre le coronavirus, … Nous devons rebâtir notre souveraineté nationale et européenne … en relocalisant certaines activités stratégiques … comme la production de principes actifs pharmaceutiques. » - Prise de **position gouvernementale** de l'état français - mars 2020.

2.2 L'identification

2.2.1 L'approche globale

L'entreprise peut choisir de ne pas dissocier son processus global d'identification des risques. Dans ce cas, elle utilise toutes ses sources habituelles d'identification dans une approche globale qui intègre nativement toutes les extensions connues de l'Entreprise étendue. Ainsi l'entreprise identifie les évènements redoutés, à partir du moment où ils ont une conséquence potentiellement néfaste sur ses intérêts, quel que soit le lieu où ils se manifestent, et quel que soit le scénario de matérialisation, en utilisant les moyens habituels :

- Analyses et revues internes :
  - Revues d'affaires ou « Business reviews » (dans lesquelles figurent souvent les évènements justifiant les écarts avec les objectifs) ;
  - Revues d'efficacité du dispositif de maîtrise (maturité du **contrôle interne**) ;
  - Revues des partenaires, y compris les fournisseurs stratégiques : tableau de bord de santé financière (Indicateurs, cours de bourse, ...), tableau de bord de prestations (qualité et délai d'exécution) ;
  - Revues des projets ;
  - ...
- Analyses indépendantes :
  - Rapports d'**audit interne** ;
  - Due diligence fournisseurs (cf. section 3.4.4 « Utiliser des outils »), partenaires et cibles,
  - Enquêtes/analyses de solvabilité clients ;
  - Audits externes communs sur des partenaires stratégiques au sein d'un même secteur ;
  - Vérification des certifications des systèmes qualité des fournisseurs en conformité avec les normes ISO sur les fournisseurs de rang n ;
  - Assurance de la part de leurs prestataires de services quant à la fiabilité de leurs dispositifs de contrôle interne (International Standard on Assurance Engagements n°3402) ;
  - ...
- Autres sources :
  - Veille / revue de presse, y compris des médias alternatifs (réseaux sociaux, blogs, forums, sites activistes, ...) ;
  - Veille réglementaire et légale ;

- Entretiens / réunions (*top-down / bottom-up*) ;
- Salons professionnels/métiers ;
- Écoute des évolutions, tendances, nouveaux modèles, ...
- Évolution vers un modèle d'affaires décentralisé (franchise, gérance, externalisation d'activités cœur de métier, locataire/propriétaire, ...) ;
- Évolution vers une activité dans laquelle on ne peut que recourir à une chaine de sous-traitance internationale par exemple, pour des raisons de concurrence et de coûts…
- Orientations/attentes de la gouvernance/actionnaires ;
- Réseaux d'institutions gouvernementales et territoriales (CCI, MEDEF, Référents Intelligence Économique, Institutions et organisations supranationales, Réseaux sociaux, Lobbies, ONG, ...) ;
- …

Dans cette approche globale, les personnes en charge de l'identification des risques devront être encore plus attentives aux sujets émergents. Hors des habitudes, hors des processus, très souvent hors du périmètre de veille et surveillance, ils sont d'autant plus dangereux qu'ils sont perçus tardivement. Ces sujets ont vocation à devenir des risques, ou des nouveaux scénarios de risques, et s'ils s'avèrent favorables, des opportunités. Ils sont, de fait, souvent en lien avec des dimensions de l'Entreprise étendue.

2.2.2 L'approche spécifique

L'approche spécifique d'identification des risques de l'Entreprise étendue est souvent pertinente et complémentaire par rapport à l'approche globale.

Pour des Entreprises fortement étendues qui :

- se considèrent dans un plan d'expansion formalisé,
- font beaucoup appel à des tiers pour réaliser leur objet social,
- ont une culture transverse, diversifiée, multisectorielle, dispersée géographiquement, …

nous donnons ici quelques idées de pistes à explorer au stade de l'identification, parmi celles que nous avons observées chez certaines d'entre elles. Nous en développerons certaines plus loin dans notre propos sur la cartographie (cf. section 2.4 « La cartographie »).

● Segmentation de la chaine de valeur

Une méthode simple, l'analyse de la chaine de valeur de l'entreprise, permet d'appréhender de manière fiable et approfondie les sources potentielles de risques qui s'y rapportent.

Point de vue d'un risk manager

« L'entreprise devient toujours plus globale en nouant des partenariats stratégiques pour accélérer l'innovation ou en s'approvisionnant auprès de fournisseurs dont les défaillances peuvent directement atteindre sa réputation et son image. Elle se doit de bien connaître les interactions avec tous les acteurs de la chaîne de valeur, leur vulnérabilité, et accroître sa vigilance auprès d'eux car sa responsabilité pourra être directement engagée. »

Un risk manager du secteur de la grande distribution.

La chaîne de valeur présente un intérêt pour l'entreprise, pas seulement stratégique, par exemple lors de la recherche d'un avantage concurrentiel. Aussi, le risk manager doit la scruter dans le détail pour identifier :

- Les risques intrinsèques de toute nature dans chaque étape des activités principales ;
- Les risques induits par les activités de soutien / support fonctionnel.

Sur la base de cette analyse, la cartographie de la chaîne de valeur de l'entreprise aide à faire prendre conscience et à faire comprendre les risques liés aux :

- Différents processus clés (métiers fonctionnels, de fabrication, …) ;
- Flux traversant ces processus (financiers, matières, humains, données, …) ;
- Diverses parties prenantes et à leurs interrelations.

A titre d'illustration, les natures de risque (cf. figure 3 « Exemple de panorama des risques par nature ») qu'une analyse de la chaîne de valeur pourra faire émerger, ou conforter, sont :

- pour les activités de soutien / support fonctionnel :
  - Infrastructure - gouvernance, stratégie, financier, juridique, … ;
  - Ressources humaines - compétences clés, image, communication, … ;
  - R&D - rupture technologique, propriété intellectuelle, sûreté, … ;
  - Approvisionnements - pénuries, obsolescence, défaillance, …
- pour les activités principales :
  - Logistique entrante - règlementations, douanes, transports, taxes, … ;
  - Production - accident, environnement, conformité, sécurité, … ;
  - Logistique sortante - déchets, transports, entreposage, distribution, … ;
  - Marketing et vente - géopolitique, ingérence, marché, espionnage, … ;
  - Services - qualité, livraison, SAV, centre d'appels, …

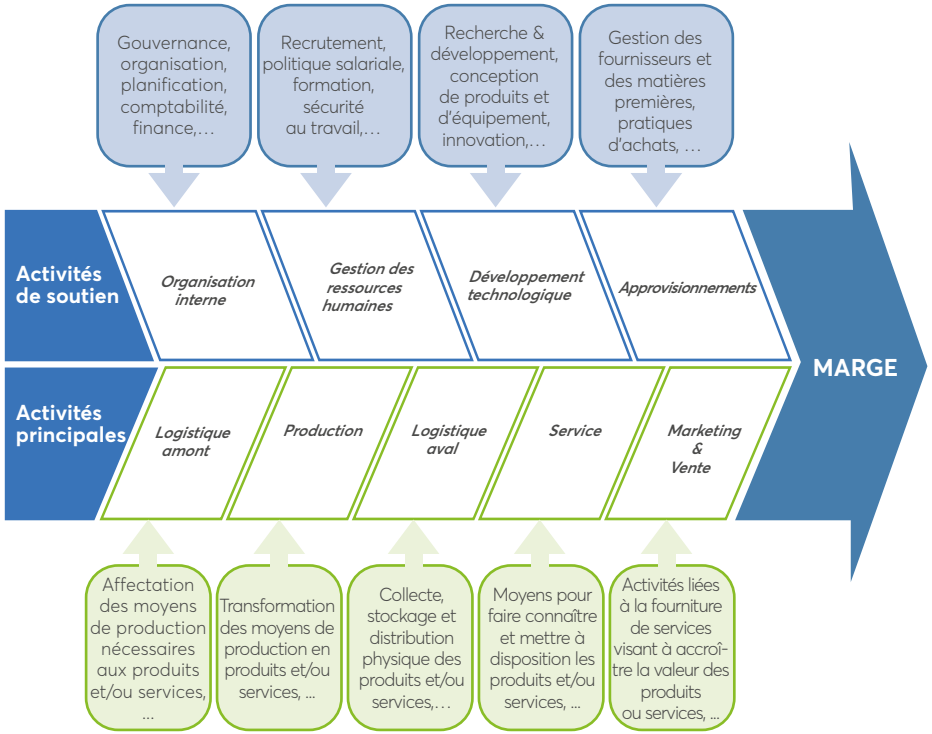


Figure 15 – Natures de risques liées à la chaîne de valeur telle que vue par Michael Porter

Le rattachement des risques aux activités est représenté sur une segmentation de la chaine de valeur, alignée sur celle présentée par Michael Porter (cf. figure 15 « Natures de risques liées à la chaîne de valeur telle que vue par Michael Porter »).

Le risk manager peut aussi utiliser la liste des questions-types (cf. Annexe 2 « Questions types – caractéristiques ») tout au long de ses travaux sur la chaîne de valeur de son entreprise.

- Identification des principaux risques par partie prenante

Sur la base des enjeux de chaque partie prenante, le risk manager s'efforcera de mesurer les risques qui peuvent la concerner. L'intérêt est de partager cette vue avec la fonction ou la personne en charge du suivi de la relation avec cette partie prenante dans l'Entreprise étendue.

Point de vue d'un risk manager

« L'Entreprise étendue, c'est l'entreprise inscrite dans la société, des enjeux de responsabilité sociétale et de création de valeur partagée entre l'entreprise et ses parties prenantes. La gestion des risques de l'entreprise, partagée avec ses partenaires sur l'ensemble de la chaine de valeur, doit intégrer le respect des droits humains, de santé et sécurité au travail, d'environnement au sens large (biodiversité, lutte contre le changement climatique…). A titre d'exemple, la gestion des risques de l'extraction des matières premières, ou du développement de nouvelles installations de production, doit porter sur les conditions humaines, sociales et environnementales de l'activité. »

Un risk manager du secteur de l'énergie.

L'analyse des attentes ou des atteintes potentielles des parties prenantes, en relation directe ou indirecte avec l'entreprise, est essentielle afin de définir les risques. Sur cette base, on peut établir des scénarios critiques en approche étendue pour chaque partie prenante, afin d'évaluer les impacts et la **probabilité / fréquence / vraisemblance** d'occurrence. Cette approche est souvent utilisée dans les analyses de risques. Sur ce sujet, l'outil proposé dans la figure 10 « Exemples d'intensité entre domaines de risques et parties prenantes » de la section 1.5 « L'écosystème : les parties prenantes » peut être très utile.

● Revue des sous-traitants et fournisseurs

Par définition, les fournisseurs et sous-traitants génèrent des risques de toute nature dans l'extension de l'Entreprise : arrêt d'activité, perte ou fuite d'information, qualité des produits et services, éthique, image et réputation, ...

Beaucoup de revues fournisseurs existent dans les entreprises. Elles présentent souvent deux défauts majeurs :

- Elles ne concernent que les principaux fournisseurs en montant d'achat ; or le montant n'est pas le seul critère pour mesurer l'importance du fournisseur (localisation, composant stratégique, etc.).
- Elles sont surtout orientées sur les sujets contractuels (formalisation, exécution et conditions financières).

Les revues fournisseurs sont essentielles pour identifier l'ensemble des risques que le tiers fait peser sur l'Entreprise étendue. Le risk manager y contribue en étant convié aux revues et en analysant plus en détail les risques de toutes natures liés aux fournisseurs critiques/ stratégiques.

● Recherche de scénarios improbables conduisant à une crise majeure

L'une des tâches les plus difficiles consiste à identifier ces scénarios et à en mesurer la probabilité, même très faible. Très souvent, il est nécessaire d'analyser un improbable croisement de facteurs de causalité.

Lors d'enquêtes sur le terrain, « l'inutilité » de cette analyse est souvent mise en avant du fait de la très faible probabilité d'occurrence de l'évènement. C'est là une caractéristique essentielle des risques de l'Entreprise étendue. L'éloignement de ces risques fait que leur analyse sont rarement prioritaires dans les préoccupations des opérationnels, voire ignorées. Le danger de sous-estimer ou de négliger ces risques est bien réel, notamment sur les évènements susceptibles de générer une crise de réputation. C'est là qu'il faut imaginer une façon de travailler efficacement sur la réduction des impacts, quitte à accepter d'augmenter artificiellement la probabilité si celle-ci reste minime (cf. section 3.1.3 – « Décider des risques à traiter »).

● Analyses légales spécifiques

Un certain nombre de lois récentes exigent d'identifier les risques dans une approche étendue de l'Entreprise. Ainsi la loi relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique également nommée Sapin 2 visant notamment à lutter contre la corruption, la loi actuelle sur le Devoir de Vigilance des sociétés mères et donneuses d'ordre et son homologue éventuelle au niveau européen, ou encore le règlement européen général sur la protection des données personnelles (RGPD) ont un champ d'application, par nature étendu.

Point de vue d'un risk manager

« Ce sont toutes les situations de risques qui peuvent concerner l'entreprise ou ses parties prenantes, sur lesquelles sa maitrise est indirecte, partielle ou inexistante. A l'exemple de la technologie 5G : son impact éventuel sur la biodiversité, les choix technologiques liés aux aspects géopolitiques, son acceptabilité sociétale sont autant de préoccupations de l'Entreprise étendue. Au plan économique et géopolitique mondial, un sujet comme la mainmise d'un seul pays sur l'extraction des terres rares et ses effets potentiels en cascade sur de nombreux secteurs économiques concerne sans doute beaucoup d'Entreprises étendues. »

Un risk manager du secteur des télécommunications.

Nous ne développerons pas plus dans notre propos les aspects liés aux opportunités. Il est cependant indéniable que, dans l'approche globale comme dans l'approche spécifique, la combinaison d'analyses entre les risques et les opportunités demeure l'élément clé d'une décision éclairée, par exemple lorsqu'il s'agit de recourir ou non à la sous-traitance (cf. section 3.2.3 « Maîtriser les risques et opportunités du *Make or Buy* »).

2.3 L'évaluation

2.3.1 Une règle générale

Les risques de l'Entreprise étendue font partie des risques de l'entreprise ; les méthodes d'évaluation doivent donc être cohérentes et englober tous les risques. C'est à cette seule condition que les prises de décisions préserveront l'intérêt global de l'entreprise.

Les échelles de probabilité et d'impacts, comme celles de **criticité** et de niveau de maitrise, comportent en principe des critères qui s'appliquent sans difficulté à des causes ou à des conséquences situées aussi bien dans l'entreprise elle-même que dans les extensions de l'entreprise.

Ainsi par exemple les causes relatives aux fournisseurs, aux sous-traitants ou bien aux instances représentatives du personnel sont analysées par l'utilisation des échelles de probabilité communes aux autres risques. De même, les conséquences sur les parties prenantes et leurs intérêts, ou celles qui proviennent de leurs activités, peuvent figurer parmi les critères d'impacts de type habituel :

- Opérationnel,
- Financier,
- Humain,
- Légal,
- Réputation,
- …

2.3.2 Des enrichissements envisageables

Si les principes d'évaluation ne sont pas assez précis ou développés, l'analyse des risques de l'Entreprise étendue est une opportunité pour les améliorer. On peut affiner et faire évoluer la méthode d'appréciation des risques (nombre de niveaux de probabilité et d'impacts, seuils retenus pour chacun des niveaux, quantifications en incertitude, référentiel plus large d'appréciation, …). On peut aussi compléter les critères utilisés pour les échelles de probabilité, d'impacts et de niveau de maitrise, en y ajoutant des éléments de jugement relatifs à l'Entreprise étendue : impacts sur les parties prenantes, mise en place des revues fournisseurs, ...

D'une manière générale, il y a beaucoup de bénéfices à mettre en place ou faire évoluer un dispositif global de gestion des risques pour qu'il prenne en compte toutes les dimensions de l'Entreprise étendue. Cela peut en particulier conduire l'entreprise à :

- Chercher de nouveaux fournisseurs pour minimiser les ruptures d'approvisionnement et obtenir des réductions de coûts ;
- Anticiper un risque de marché dans une géographie qui conduit à découvrir de nouveaux marchés ailleurs ;
- Développer de nouveaux produits plus porteurs par l'anticipation d'un risque sur les produits actuels ;
- Réduire ses coûts ;
- Augmenter son Chiffre d'Affaires ;
- Renforcer sa capacité à répondre aux aléas du marché.

L'analyse des risques et leur évaluation est, par essence, une opportunité. Lors de ces travaux, elle offre à l'entreprise la possibilité, le moyen, la chance, de découvrir et d'évaluer de nouvelles opportunités d'affaires courantes ou stratégiques.

On se rapproche ici d'une culture élargie et plus ouverte en matière de risques, qui ne peut que permettre à l'entreprise de mieux se situer et se comporter, puisque par définition elle aura une vision améliorée de son environnement.

2.4 La cartographie

2.4.1 Les principes

La cartographie des risques de l'organisation doit couvrir tous les risques, y compris ceux relatifs à ses extensions. Elle comporte aussi bien les risques que subit l'Entreprise étendue, que ceux que l'Entreprise étendue fait subir aux autres : l'Entreprise étendue est « active » et « passive ».

L'intégration des dimensions de l'Entreprise étendue dans la cartographie des risques permet de garantir l'information de tous les organes de gouvernance, leur faisant au besoin prendre conscience de ces risques. Comme indiqué à la section 1.4.2 « L'interne et l'externe », notre recommandation est, dans la mesure du possible, de s'en tenir à une cartographie unique couvrant l'ensemble des dimensions et des parties prenantes.

2.4.2 Un tag dans la cartographie globale ?

Pour les entreprises qui auraient besoin d'identifier visuellement dans leur cartographie les risques propres à l'Entreprise étendue, l'usage d'un code couleur ou d'une vignette peut suffire.

La plupart des systèmes d'information destinés à produire des cartographies de risques proposent déjà un système de tags afin d'affiner la classification des risques selon plusieurs critères. Il est donc possible de dédier un tag aux risques de l'Entreprise étendue afin de mieux visualiser leur importance et leur diversité.

2.4.3 Des cartographies spécifiques ?

Puisque la méthodologie couvrant l'identification, l'évaluation et la cartographie des risques de l'Entreprise étendue est très proche, voire similaire, à la méthodologie habituelle, le choix de produire et diffuser une cartographie spécifique et globale des risques de l'Entreprise étendue est à la discrétion de la direction et du risk manager.

Comme déjà mentionné, certaines lois conduisent aujourd'hui à créer des cartographies particulières. Ainsi la loi sur le devoir de vigilance dont la cartographie est établie sur la base de trois domaines bien définis précédemment pourrait constituer un socle de cartographie des risques de l'Entreprise étendue pour les risques relatifs au domaine extra-financier. Il faudrait dès lors compléter ce socle avec les autres natures de risques.

En revanche, pour les plus avancés, ou lorsque l'activité de l'Entreprise étendue justifie de conduire une approche spécifique d'identification (cf. section 2.2.2 « Approche spécifique »), ou encore lorsqu'une réglementation la rend obligatoire, il peut être pertinent de produire des cartographies dédiées, telles que :

- Par nature de risque

Cette approche peut particulièrement se justifier lorsque l'Entreprise étendue fait face à des transformations rapides, comme c'est le cas dans la période actuelle pour beaucoup d'entre elles. En effet, même en se cantonnant à l'axe chaîne de valeur, la plupart des entreprises constatent une croissance exponentielle du nombre de tiers, tant sur la chaîne amont que sur la chaîne aval. Ceux-ci génèrent des risques, et, pour certains, aident l'Entreprise étendue à les maîtriser.

La nature des risques générés par ces nouvelles parties prenantes évolue également. Pour beaucoup, les entreprises font face à un morcellement de leurs relations vers de toutes petites structures. A l'inverse, certaines se trouvent parfois confrontées à des géants face à qui elles pèsent finalement peu.

Par ailleurs, comme nous l'avons déjà évoqué, des textes obligent parfois à produire cette cartographie par nature de risque.

Ainsi l'analyse des risques dans le cadre du règlement européen général de protection des données doit comporter une analyse d'impact pour chaque traitement d'information (RGPD – chapitre 4 – section 3). A ces fins, la norme ISO 22317 *(Societal security – Business continuity management systems)* peut se révéler utile car elle propose un guide pour mener des Analyses d'impact sur l'Activité *(AIA ou Business impact Analysis - BIA).*

Ces analyses sont conduites dans le cadre de la définition et de la mise en place des plans de continuité comme recommandé par cette norme (cf. Question type n°10 – Exemple « Architecture réseau - Sécurisation accès externes »). Ces analyses sont à mener par fournisseur, par partenaire ou sous-traitant, … et par client.

De même au sens large, la loi sur le devoir de vigilance et la loi Sapin 2 exigent la réalisation d'une cartographie des risques, et donc d'une analyse des impacts sur des natures de risques bien précises ;

- D'une part les droits humains et les libertés fondamentales, la santé, la sécurité et l'environnement ;
- D'autre part, la corruption et le trafic d'influence.

- Par partie prenante

Dans le cadre de la loi sur le devoir de vigilance, l'analyse doit comporter un certain nombre d'éléments liés à la nature des risques entrant dans son périmètre, par domaine d'activité de l'Entreprise étendue. Ces éléments doivent être analysés ensuite par fournisseur ou sous-traitant, et éventuellement par partie prenante.

Exemple de risque - Question type n°10

L'architecture réseau mise en place avec les partenaires et clients et fournisseurs stratégiques de l'entreprise pour partager des informations et accéder au système d'information est-elle parfaitement sécurisée ?

Architecture réseau - Sécurisation accès externes
Piratage de données

Eléments factuels
L'entreprise Martin vient de mettre en place d'une part un forum d'échanges entre consommateurs, et, d'autre part, une capture de données via des cookies sur les recherches de produits des consommateurs, avec un début de fiche personnelle sur leurs caractéristiques et attentes cosmétiques. L'entreprise a confié à un prestataire la réalisation des applicatifs.

Analyse des causalités
La réglementation RGPD doit être scrupuleusement respectée.
- La société prestataire n'a pas considéré suffisamment les possibilités d'accès au site, en particulier par simple changement du numéro client dans l'adresse URL d'une requête ;
- Les services informatiques de l'entreprise n'ont pas fait mener les tests exhaustifs de sécurité d'accès lors de la mise en place des deux nouvelles applications.

Evaluation des conséquences
- Données personnelles des profils utilisateurs accessibles (sauf les données bancaires) par n'importe qui ayant des connaissances quant aux réseaux informatiques ;
- Atteinte à l'image de l'entreprise auprès des consommateurs pour manque d'éthique et manque de considération pour ses clients ;
- Baisse du CA de 3 % à 5 % pendant une période de 3 à 9 mois ;
- Amende pour non-respect de la réglementation RGPD pouvant atteindre 4% du CA ou 20 M€.

Comportements/actions possibles
- Blocage immédiat des accès, le cas échéant avec fermeture totale du réseau ;
- Résolution de la faille réseau sur les accès par simple changement de l'adresse URL ;
- Information auprès des clients indiquant que la situation est gérée ;
- Messages personnalisés auprès de certains clients sensibles le cas échéant.

Capitalisation pour l'approche Entreprise étendue

Principales parties prenantes identifiées
- Clients finaux, utilisateurs, consommateurs.
- Organismes de réglementation/Normalisation.
- Fournisseurs en objets SI.

Recommandations
- Surveillance continue de la sécurité des accès externes aux réseaux ;
- Mise en place en place d'outils automatisés de surveillance des comportements sur les bases de données et les applications ;
- Mise en place de procédures systématiques de contrôle des sécurités pour toute nouvelle application ou modification d'application, avec engagement formel des acteurs.

Cas réels similaires (cf. Annexe 3 « Questions types – Sources détaillées des cas réels similaires »).

- Uber : sanction de la CNIL – 2017
- Dailymotion : sanction de la CNIL - 2018
- Google : sanction de la CNIL – 2019

« Puisque nos systèmes d'information sont multiples et protéiformes, aux contours flous, souvent disséminés dans le cloud et interconnectés sur de vastes écosystèmes, et parce que les projets se montent toujours plus vite, la cybersécurité doit s'insinuer partout. Elle doit être pensée d'emblée, elle doit accompagner les réflexions des métiers et se doit d'être aussi efficace en aval qu'en amont, pour contrer les menaces avérées, répondre aux incidents et garantir la résilience. Elle s'immisce dans les nouveaux modes de développement, elle est innovante, agile et réactive. » **CESIN**, mot du Président, 18 mai 2018.

L'analyse par partie prenante peut aussi être une obligation sectorielle. Ainsi l'analyse des risques par client ou pour une certaine catégorie de clients est une attente de la réglementation bancaire en matière d'identification des clients.

Plus généralement, dans le domaine règlementaire, une analyse par partie prenante révélera des risques qui leur sont souvent spécifiques. Les autorités de régulation d'un secteur, les autorités européennes ou internationales, mais aussi les différentes agences de contrôle, sur les règles de la concurrence ou en ce qui concerne la corruption, sont aujourd'hui entrées dans le paysage et l'univers des risques de nombreux acteurs économiques.

L'écueil à éviter est de négliger l'analyse des parties prenantes indirectes. Par exemple, l'utilisateur final des produits et services de l'Entreprise étendue qui n'est pas toujours le client, ou encore les différentes ONG ou associations qui peuvent avoir un intérêt à agir ou réagir suite à des décisions ou des actions de l'entreprise.

- Par segment de la chaine de valeur

Certaines parties de la chaîne de valeur présentent une importance plus grande que les autres notamment pour ce qui touche à la continuité d'activité au sens le plus large (qui inclut la reprise d'activité après une interruption). Dans ce cas, lorsque ces activités sont confiées à des tiers, le niveau des risques peut aussi bien se trouver accru que diminué.

Dans le monde bancaire, l'Arrêté du 3 novembre 2014 (*) a renforcé les exigences en matière de « Prestations de services essentielles externalisées ». L'essentiel externalisé est par essence une composante de l'Entreprise étendue !

Il s'agit dans cet exemple d'identifier le caractère essentiel des prestations externalisées. Mais au-delà, le texte prévoit notamment :

- La reproduction des points de contrôles et du dispositif de contrôle interne au niveau du sous-traitant lors du transfert ;
- Un droit de suite du régulateur au travers d'un audit de l'autorité de contrôle bancaire (ACPR en France) ;
- Le pilotage renforcé de la qualité des prestations externalisées au moyen d'indicateurs clés (délais de traitement, taux de satisfaction des utilisateurs, taux d'incidents, taux de résolution dans les délais), assorti des actions correctrices éventuelles et de la gouvernance adéquate.

(*) cf. Annexe 12 « Bibliographie » Règlement CRBF 97-02

Exemple de risque - Question type n°11

Les nouvelles technologies utilisées ou mises en place par l'entreprise dans son projet de transformation numérique sont-elles sûres ?

Transformations numériques - Impacts sur la sécurité
Cosmétique Connectée

Eléments factuels
L'entreprise Martin veut réussir le virage du numérique et devenir leader dans son utilisation. Des clientes (en test en Asie du Sud-Est) utilisent des objets « cosmétiques » connectés à leurs smartphones. Les données collectées transitent via un Cloud extra-européen. Pour gérer les tests, la R&D de l'entreprise Martin en France est connectée avec le réseau de distribution en Asie.

Analyse des causalités
L'ère des objets connectés (IoT : Internet of Things) et du Cloud offre de nouveaux services, change les modèles de nombreux secteurs d'activité. Elle favorise la transformation numérique, mais augmente aussi les vulnérabilités. Pour ce qui est du stockage des données, les enjeux et risques ne sont pas seulement liés au facteur géographique, mais aussi à la nationalité des opérateurs.
Le Patriot Act permet aux agences gouvernementales américaines d'obtenir un mandat pour accéder aux données personnelles stockées aux États-Unis dans le cadre d'une enquête relative à des actes de terrorisme. De son côté, le Cloud Act (*), loi jointe au budget fédéral américain de 2018, dispose que toute société de droit américain doit livrer ses données à la demande des autorités américaines disposant d'un mandat d'enquête pénale.

Evaluation des conséquences
- Prise de contrôle à distance du système d'information via les objets connectés ou les smartphones pour exfiltration de données, sabotages, rançons, Botnets, virus, malwares, …
- Risque d'espionnage économique de données stratégiques par l'hébergeur étranger soumis à une législation laxiste ;
- Perte de confiance des consommateurs qui apprennent le vol de leurs données personnelles
- Baisse du chiffre d'affaires.

Comportements/actions possibles
- A titre préventif : audit des logiciels des objets connectés ; Respect strict du RGPD ;
- A titre curatif : communiquer en externe ; Engager les actions juridiques ; Corriger les failles.

Capitalisation pour l'approche Entreprise étendue

Principales parties prenantes identifiées
- Fournisseurs d'objets connectés, smartphones, de services Cloud, …, Opérateurs de télécommunications, Consommateurs, CNIL.

Recommandations
- Suivre les bonnes pratiques en termes d'hygiène informatique et numérique, et, vis-à-vis des autorités compétentes en matière de protection des données à caractère personnelles ;
- Intégrer le « Security by Design » et s'assurer que ceux de ses fournisseurs en sont dotés ;
- Utiliser des produits et services labellisés et certifiés par un organisme institutionnel (ANSSI)
- Evaluer le plus en amont les risques Cyber et leur assurabilité spécifique.

Cas réels similaires (cf. Annexe 3 « Questions types – Sources détaillées des cas réels similaires »).

- Casino nord-américain (jeux) : société de cyber sécurité Darktrace – piratage base de données, thermomètre connecté – 2018
- Dyn : piratage massif – 2016 • Wannacry : piratage à rançon – 2017
- Petya : piratage à rançon – 2017 • Hiscox : assurance, cyberattaques – 2017
- Industrie nucléaire : Stuxnet, Iran – 2010

ANSSI (avec AMRAE) :
« Maîtrise du risque numérique, l'atout confiance », Ce guide est né du constat suivant : le risque numérique qui pèse chaque jour davantage sur les organisations peut aller jusqu'à mettre en péril leur survie et celle de leurs parties prenantes. Selon l'ANSSI et l'AMRAE, il doit donc être considéré comme un risque à traiter au plus haut niveau de l'organisation et non plus seulement comme un risque dont l'évitement est l'affaire d'experts techniques.

(*) cf. Annexe 12 « Bibliographie » Cloud Act

Dans le même ordre d'idées, en termes de valeur extra-financière, on peut penser que l'approfondissement des travaux liés à la déclaration de performance extra-financière et au rapport intégré est probable dans les prochaines années. Ainsi l'utilisation de la matrice de matérialité par le risk manager pour les besoins de la cartographie des risques est une piste d'amélioration déjà en cours d'étude pour certains.

- Par produit

Dans le domaine de la santé par exemple, le suivi des risques par produit est une attente de la loi Bertrand sur la pharmacovigilance dans le cadre des AMM (Autorisation de Mise sur le Marché des médicaments à usage humain). Ce suivi porte sur toutes les phases de la vie du produit, qu'il s'agisse de la recherche, de la conception, de la conservation ou de la destruction, bien au-delà de la zone de contrôle direct du laboratoire qui produit le médicament.

- Par projet

Il est fréquent que des projets soient confiés totalement ou partiellement à des tiers. Parfois les entreprises « clientes » mèneront des projets internes alors que leurs prestataires mèneront des projets externes, en coordination avec leurs propres sous-traitants (lesquels doivent par ailleurs être obligatoirement déclarés dans le cadre des marchés publics).

Pour les entreprises de prestations d'ingénierie par exemple, le suivi des risques propres à la réalisation de projets pour un client est un standard, prenant en compte des éléments tels que les pénalités de retard, l'accroissement des coûts locaux de main d'oeuvre, le dépassement des estimations initiales de besoins de ressources, … Autant d'éléments qui ont pour elles un impact direct et majeur sur le résultat net, leur rentabilité et leur réputation. Mais les retards et les erreurs de ces prestataires ont des impacts souvent bien supérieurs chez leurs clients (mise sur le marché tardive d'un produit, dangerosité…), lesquels sont devenus de facto des entreprises étendues sur des sujets de projets internes.

Les projets de transformation numérique ont une sensibilité particulière. Ils changent certes les habitudes de l'entreprise par la mise en place de nouveaux outils, et étendent souvent brutalement le périmètre de l'entreprise, car les informations et les processus deviennent accessibles sur le Web. L'accroissement du nombre des parties prenantes externes est immédiat, ce qui élargit donc le périmètre de l'Entreprise étendue (cf. Question type n°11 – Exemple « Transformations numériques - Impacts sur la sécurité »).

- Par flux d'information avec l'extérieur

Pour l'entreprise, la protection et la surveillance des données échangées avec l'extérieur est fondamentale tant un incident sur ce plan peut ramifier rapidement jusqu'à la réputation de l'Entreprise. Qu'il s'agisse du respect de la confidentialité (fuite d'information stratégiques), de la conformité aux réglementations (RGPD, …), ou encore des aspects de fiabilité (prospections commerciales …), les menaces qui pèsent sur les flux d'information avec l'extérieur sont multiples et peuvent au besoin faire l'objet d'une cartographie spécifique de risques.

3. Le traitement des risques de l'Entreprise étendue

Définir le périmètre de l'Entreprise étendue, identifier les acteurs de son écosystème, en analyser toutes les dimensions, en identifier les risques, les évaluer et en faire la cartographie sont des activités complexes, néanmoins nécessaires et indispensables. Les précédents chapitres l'ont montré.

Si les méthodes et outils présentés ici permettent de structurer et de simplifier ces travaux, il reste encore aux risk managers à définir et mettre en oeuvre les actions de traitement, d'évitement et de réduction des risques, en lien avec les directions concernées. En collaboration étroite avec les acteurs internes de l'entreprise et autant que possible avec l'ensemble des acteurs externes à l'entreprise, il s'agit notamment de déployer des plans de prévention et des plans de continuité d'activité.

Traiter les risques de l'Entreprise étendue nécessite une capacité d'anticipation des évolutions de son périmètre, souvent à partir de signaux faibles. Cela nécessite souvent aussi une évolution de la culture de l'entreprise pour que tous les personnels concernés s'approprient l'approche « risques de l'Entreprise étendue ».

Il faut donc à la fois créer de nouveaux traitements et faire évoluer les modes de traitement classiques : appétence aux risques, organisation et gouvernance, contrôles dans les processus, méthodologie, etc. Les traitements doivent être transverses pour bien couvrir toutes les zones d'actions (cf. figure 16 « Synoptique de traitements possibles de risques de l'Entreprise étendue »). Aussi, ce chapitre présente les approches, les méthodes, les outils et les changements culturels et organisationnels qui peuvent être mis en oeuvre pour effectuer les traitements des risques de l'Entreprise étendue avec efficience. Chaque entreprise ou organisation adaptera ces propositions à ses spécificités.

Ces propositions d'évolutions du traitement des risques tiennent compte de la stratégie et de la culture de l'entreprise. Depuis l'identification des risques avec une vision des évolutions et un cadre d'Appétence, elles se déclinent dans la vision juridique, la compréhension des parties prenantes, les décisions de *Make or Buy*, l'assurance, le préventif, l'organisation d'alerte/gestion de crise, … en utilisant des outils performants de gestion, de partage et d'assistance intelligente.

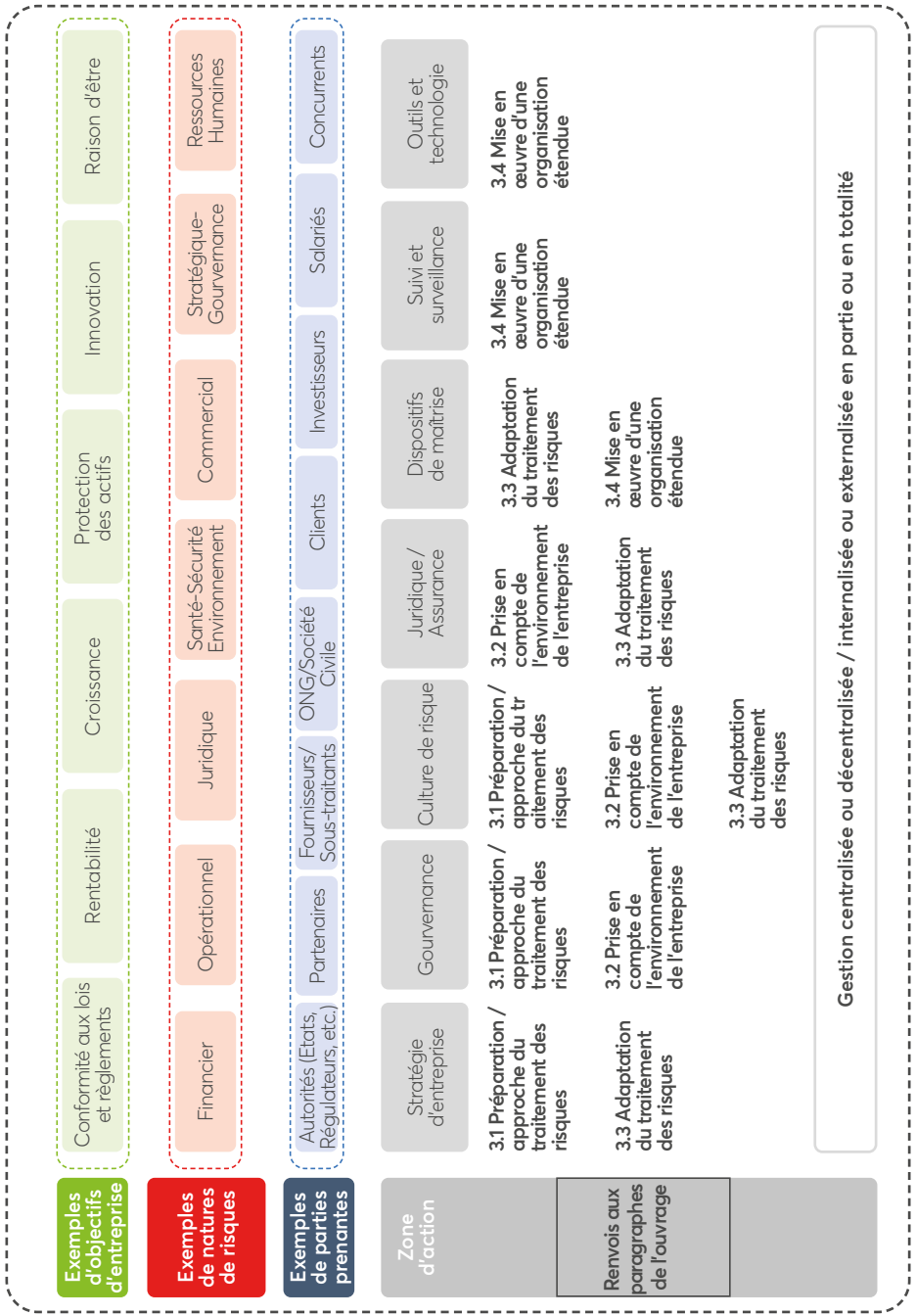


Figure 16 – Synoptique de traitements possibles de risques de l'Entreprise étendue

3.1 Préparation et approche du traitement des risques

3.1.1 Anticiper les évolutions

Si, historiquement, il y a toujours eu des transformations et la nécessité pour l'entreprise de s'y adapter, leur particularité au 21e siècle est la rapidité. Les entreprises habituées, bien sûr, à modifier leur culture interne et parfois le mode de pensée de leurs dirigeants, sont désormais contraintes de le faire à un rythme beaucoup plus rapide.

Dans certains secteurs économiques, il s'agit même de faire face à l'une des premières transformations majeures historiques de l'entreprise. C'est par exemple le cas des grands cabinets de conseil, pour qui la partie prenante quasi unique était le client, à qui l'on répondait jusqu'à présent principalement au travers d'un effectif compétent sur un large spectre d'activités. Ces cabinets, comme d'autres entreprises, se trouvent aujourd'hui confrontés à la transformation profonde du monde du travail. Cette évolution progressive remet en cause leur modèle salarial, et les conduit à recourir de plus en plus à des modèles d'open talent : ils intègrent alors des ressources externes à leurs équipes de réalisation des prestations, souvent des experts individuels extrêmement sollicités. Ce morcellement de la force de travail et des compétences des entreprises est aussi en progression dans d'autres secteurs et se traduit par la réduction du nombre de salariés à activité égale. Il s'agit d'un bouleversement de l'écosystème pour ces entreprises, un changement fondamental de leur modèle d'affaires historique, et à coup sûr une extension nouvelle de leur entreprise !

Point de vue d'un risk manager

« L'Open Talent est une illustration concrète de l'Entreprise étendue et de ses enjeux dans nos différents métiers.
C'est une opportunité d'attirer des compétences nouvelles ou de niche. Dans le même temps cela peut impliquer des risques organisationnels, réglementaires ou encore liés à la sécurité de l'information, risques que l'organisation ne souhaite pas prendre ou ne pourrait pas supporter. »

Un risk manager du secteur du conseil aux entreprises.

Plus brutales encore sont les évolutions dues au numérique. Les disruptions sont aujourd'hui connues, par exemple avec l'uberisation galopante dans de nombreux secteurs d'activité. Sur le secteur du transport de personnes, les conséquences ont été tellement significatives dans leur économie que des pays comme la Bulgarie, la France et l'Australie (Territoire du Nord) ont interdit temporairement les services Uber le temps de mettre en place l'adaptation réglementaire conséquente qui était nécessaire.

La surveillance active de l'environnement de l'entreprise est nécessaire pour capter et anticiper les tendances d'évolution, en particulier sur les réseaux sociaux, dans les actions de la concurrence, sur le développement des start-up, et sur l'évolution des réglementations, entre autres.

Si aujourd'hui beaucoup de transformations sont plus rapides qu'auparavant, les indices, sur certains domaines, sont souvent plus faciles à déceler et anticiper que l'on pense. Une réglementation n'apparaît pas en quelques jours : il faut des propositions de lois, des débats, des votes et des décrets d'application. Une start-up ne prend pas une amplitude nationale et mondiale en quelques jours : cela se mesure plutôt en mois ou en années ; et avant sa création, une communication ou des publications de brevets ont lieu et permettent de bien positionner la start-up (cf. Question type n°12 - Exemple « *Business model* disruptif : survivre ou périr ? »).

Exemple de risque - Question type n°12

De nouveaux modèles économiques, ou technologies disruptives, sont-ils en train d'apparaître risquant de compromettre l'activité ou la pérennité de l'entreprise ?

Business model disruptif : survivre ou périr ?
Réalité augmentée !

Eléments factuels

L'entreprise apprend par la presse que des start-up pensent à la réalité augmentée pour leurs activités de maquillage. La captation des données personnelles permet maintenant de personnaliser la composition de produits cosmétiques pour correspondre au mieux aux besoins et attentes des clients. De plus, la mise en place de la réalité augmentée permet de leur montrer sur leur écran de portable leur visage avec différentes possibilités de maquillage. La vente via Internet avec ces services à valeurs ajoutées devient un incontournable de la cosmétique.

Analyse des causalités

L'entreprise Martin n'a pas anticipé ces évolutions technologiques sous Internet.
Même si l'entreprise a mis son catalogue de produits avec achat en ligne sur son site Web, son mode de commercialisation est toujours essentiellement en magasin avec des produits dont la vente repose en grande partie sur les conseils des vendeurs. Ce nouveau mode de vente personnalisée réduit significativement la fidélité des clients, phénomène en croissance.
Des concurrents utilisent ce nouveau vecteur depuis plus d'un an et de nouveaux acteurs apparaissent sur le marché des cosmétiques.

Evaluation des conséquences

L'entreprise constate des tassements de ses parts de marché sur un nombre croissant de produits.
Si la croissance naturelle du marché conduit à ne pas encore observer de baisse du CA, les projections financières à 3 ans montrent une réduction significative du CA d'au moins 7%.
L'image de marque, si elle ne souffre pas en qualité, subit une détérioration en intérêt.

Comportements/actions possibles

- Mener des expérimentations avec des médias sur la personnalisation des produits et les bénéfices clients conséquents pour maintenir l'image ;
- Mettre en place sur le site Web les moyens permettant aux clients de personnaliser les produits
- Mettre en place dans les ateliers de fabrication une production personnalisée par demande client, i.e. au flacon près.

Capitalisation pour l'approche Entreprise étendue

Principales parties prenantes identifiées

- Clients finaux, utilisateurs, consommateurs ;
- Fournisseurs actifs dans les innovations technologiques ;
- Médias.

Recommandations

- Avoir une veille technologique et concurrentielle active sur la totalité de la chaîne de valeur ;
- Disposer de moyens d'innovation dans les nouvelles technologies – internes et externes ;
- Veiller à ce que la gouvernance permette les alertes et les prises de décision d'investissement dans les délais nécessaires.

Cas réels similaires (cf. Annexe 3 « Questions types – Sources détaillées des cas réels similaires »).

- KODAK : argentique au numérique - 2012
- Airbnb, Uber, … : disruptions - 2018
- Airbnb : marché de l'hôtellerie - 2018
- UberCab : "uberisation" 2019

L'enjeu … est d'appréhender les disruptions telles qu'elles sont réellement. Il est particulièrement utile de reconnaître ce qui se profile et de donner à l'organisation un éclairage sur la manière de canaliser cette énergie disruptive. » **IFACI** : « Perspectives internationales : L'audit interne à l'ère de la disruption » - 2018

3.1.2 Définir et décider de l'appétence aux risques

L'appétence aux risques (*) définie de façon classique s'applique parfaitement dans le cadre de l'Entreprise étendue.
En complément des définitions de l'appétence aux risques figurant au glossaire, les normes et standards en proposent d'autres, telles que :

- ISO 31010 « Critères pour décider si un risque peut être accepté » : les critères de définition de la nature et de l'étendue du risque qui peut être accepté pour atteindre des objectifs, parfois appelés "Goût du risque", peuvent être définis en spécifiant une technique permettant de déterminer l'ampleur du risque, ou d'un paramètre lié au risque, en fixant une limite au-delà de laquelle le risque devient inacceptable. La limite fixée pour qu'un risque devienne inacceptable peut dépendre des éventuelles retombées.
- ISO 22301 : 2012 Sécurité sociétale — Systèmes de management de la continuité d'activité — Exigences : « Appétence au risque : niveau et type de risque qu'une organisation est prête à accepter ».
- Wikipédia : *« Risk appetite is the level of risk that an organization is prepared to accept in pursuit of its objectives, before action is deemed necessary to reduce the risk. »*

Si le fond est bien le même, on voit qu'il y a des nuances d'interprétations possibles.
Dans la pratique, sa définition et sa mise en oeuvre vont dépendre de l'entreprise et de son secteur, mais aussi du périmètre d'extension de l'entreprise.
Par exemple, dans le secteur de l'assurance, la directive européenne 2009/138/CE (Solvency 2) précise :

- Le système de gouvernance inclut la fonction de Gestion des risques, …
- … un système de gouvernance efficace, qui garantisse une gestion saine et prudente de l'activité.
- … procéder régulièrement à l'évaluation de son besoin global de solvabilité, en tant que partie intégrante de sa stratégie commerciale et compte tenu de son profil de risque spécifique…

Pour un assureur, la nature de ses fonds propres peut l'exposer à des risques hors de son périmètre de contrôle direct : les capitaux immobilisés peuvent dépendre de taux de change, typiquement un risque de l'Entreprise étendue.
En dehors de cadres réglementaires spécifiques (banque, assurance, …), l'appétence aux risques reste une notion intuitive, voire ambivalente. Considérer le résultat du croisement de la probabilité et de l'impact ne suffit pas toujours pour décider de prendre un risque, de déclencher des actions préventives et de s'approprier des moyens curatifs. Il est nécessaire d'y adjoindre la notion temporelle qui est un élément clé. Une entreprise décidant de s'implanter

(*) Guide pratique de l'AMRAE : Accompagner votre entreprise dans la définition de son appétence aux risques. (https://www.amrae.fr/)

à l'étranger peut s'exposer à des risques (par exemple une OPA) pendant une durée déterminée du fait des investissements et des organisations à mettre en oeuvre. Dans le cas d'une durée courte, avec la mise en place d'une gestion stricte de la confidentialité, l'entreprise prendra le risque, mais pas dans le cas d'une exposition sur une durée longue (la notion de durée courte / longue restant propre à l'entreprise). Les acteurs d'une OPA peuvent être des investisseurs, mais aussi des concurrents. Là encore, l'appétence aux risques dépend du périmètre de l'Entreprise étendue.
La notion d'appétence introduit celle de seuils de tolérance. Ces seuils de tolérance seront définis à partir des probabilités, des montants, des indicateurs clés de l'entreprise (cf. section 3.4.4 Utiliser des outils).

Mais si la notion d'appétence se définit d'abord au niveau stratégique (Conseil d'Administration, COMEX, …), elle doit être déclinée par branche, par structure et par activité de l'entreprise, avec l'appropriation par les porteurs de risques concernés.

On retient comme enseignements essentiels (*) :

- Même si les normes ne l'explicitent pas, l'appétence aux risques est aujourd'hui une appréciation et une décision de niveau stratégique ;
- L'appétence aux risques peut être réglementée ;
- L'appétence aux risques couvre l'Entreprise étendue, l'Ecosystème des parties prenantes et toutes ses dimensions évoquées à la section 1.4 « L'écosystème : enjeux et dimensions ».

3.1.3 Décider des risques à traiter

L'appétence aux risques donne un cadre pour la mise en oeuvre de la stratégie de l'entreprise. Les cartographies positionnent les risques et fournissent un début d'indication sur les risques à prioriser quant à leur traitement. Mais cette approche peut s'avérer insuffisante : nombre de risques de l'Entreprise étendue, du fait de leur caractère indirect et hors des périmètres opérationnels classiques, sont souvent relativement ignorés dans les plans d'actions.

Il s'agit d'abord des risques de très faible probabilité d'occurrence, au caractère essentiellement imprévisible, ayant des impacts majeurs que certaines entreprises qualifient par simplification de cygnes noirs. Par définition, les véritables « cygnes noirs » (*) sont inimaginables et ne peuvent dès lors pas figurer dans les cartographies. Les cygnes noirs ont des congénères, les « rhinocéros gris » (*), qui eux en revanche sont perçus, mais pas systématiquement identifiés comme risques par l'entreprise.

Par habitude, par négligence, par facilité, par excès de confiance, et très souvent pour cause d'éloignement structurel ou intellectuel, l'entreprise n'y consacre pas les efforts nécessaires. Des impératifs ou des priorités conduisent souvent l'entreprise à reporter « sine die » leur traitement. Pourtant ces risques sont de nature à remettre en cause la pérennité de l'entreprise. La qualification de cygne noir ou de rhinocéros gris dépend de l'observateur, du point d'observation et du contexte. La crise liée à la Covid19 a probablement été un rhinocéros gris pour les états garant de la santé publique et un cygne noir pour les restaurants contraints à une fermeture administrative.

Au-delà des cygnes noirs et des rhinocéros gris (positionnés sur le graphe de criticité ci-contre), d'autres risques de l'Entreprise Etendue peuvent être ignorés du fait de leur éloignement ou des habitudes culturelles ou de gestion. Plus les risques trouvent leur origine en dehors de l'entreprise, plus ils ont de chances d'être moins pris en considération au motif de leur probabilité sous-estimée, ou de la capacité de protection ou réaction de l'entreprise surestimée ; et plus il est difficile d'attirer l'attention de l'entreprise sur eux pour que les décisions nécessaires soient prises. Ces habitudes et biais cognitifs, habituellement rencontrés dans les analyses de risque, sont particulièrement présents lorsqu'il s'agit des risques de l'Entreprise étendue. Une bonne culture des risques dans l'entreprise permet de mieux maîtriser ces habitudes et ces biais cognitifs.

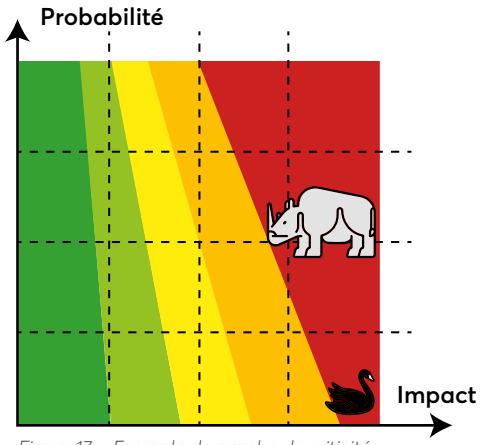


Figure 17 – Exemple de graphe de criticité

Les cartographies de risques sont souvent produites sous forme de graphes de criticité restituant la probabilité et l'impact des risques identifiés. On peut y faire ressortir les cygnes noirs, en admettant que ceux-ci puissent y figurer, et les rhinocéros gris comme des risques à traiter (cf. figure 17 « Exemple de graphe de criticité »). D'autres représentations graphiques existent, par exemple pour mettre en exergue l'évolution de l'intensité des risques sur la cartographie.

Le positionnement des seuils de criticité dans une grille d'évaluation des risques est prépondérant car il détermine l'effort à produire pour le traitement des risques (les séparations des couleurs du vert au rouge).

(*) cf. Annexe 12 « Bibliographie » - Nassim Nicholas Taleb - 2010 et Michele Wucker - 2016.

L'approche peut être enrichie en croisant la criticité des risques avec la maturité du dispositif de maitrise. Positionner les risques en valeur nette sur le graphe en tenant compte des dispositifs en place et de leur efficacité, donne à l'entreprise un outil de visualisation utile pour les décisions de traitement des risques (mise en place ou renforcement). Cette démarche fait bien ressortir la nécessité, la pertinence ou l'urgence de traiter un risque.

L'interprétation de la criticité doit faire l'objet d'une grande attention, car le calcul habituel de criticité des risques peut aggraver le phénomène de non-prise de décision. En effet, multiplier la notation de l'impact par celle de la probabilité (C = I x P) est réducteur. Par exemple, avec une notation de 0 à 10 tant pour l'impact que pour la probabilité, pour un risque 'moyen', soit I=5 et P=5, la criticité obtenue est 25 … alors que le maximum de la criticité est de 100 (=10*10), soit une notation de 25/100. L'interprétation de la criticité est donc dégradée significativement pour le lecteur non-averti. De plus, du fait de la symétrie de cette formule du produit « I x P », les cygnes noirs et même les rhinocéros gris sont aussi sous-estimés. Un risque I=8 et P=3 obtient une criticité de 24/100, il sera peu considéré alors qu'il devrait être absolument traité.

Pour contourner cette difficulté, on peut ne pas tenir compte de la valeur de la criticité ou afficher une échelle de criticité très déformée. Afin de bien visualiser et résoudre les problèmes de cohérence pour le reporting des risques, on peut mettre en œuvre d'autres formes de calculs privilégiant l'impact et affinant l'estimation de la probabilité des risques de l'Entreprise étendue (cf. section 3.4.4 « Utiliser des outils »).

Dans tous les cas, les cartographies sont nécessaires pour avoir la vision des risques à traiter.

3.1.4 Intégrer les risques Entreprise étendue à la gestion des risques

Le management des risques doit idéalement être intégré à l'organisation et à la gouvernance de l'entreprise, structurellement, dans les processus et dans les procédures… partout. C'est de culture d'entreprise dont il s'agit. La gestion des risques de l'Entreprise étendue ne fait pas exception, étant par nature intégrée à la gestion des risques générale. On sait que c'est même l'un des principes de l'ERM de prendre en considération le périmètre étendu des risques. En plaçant l'Entreprise au centre et en regardant à 360° autour d'elle, dans toutes ses dimensions, dans toutes ses extensions, on cherche à identifier et traiter toutes les sources d'impacts qui peuvent survenir. Cette idée est représentée dans plusieurs figures de cet ouvrage.

La gestion des risques dans l'entreprise est l'affaire de tous. Si l'on dressait une liste d'acteurs habituellement impliqués ou concernés, on y trouverait à coup sûr les fonctions suivantes, selon leur existence :

- Risk Management ;
- Responsabilité Sociale/Sociétale des Entreprises (RSE) ;
- Environnement, Hygiène et Sécurité ;
- Achats ;
- Ressources Humaines ;
- Systèmes d'Information ;
- Sécurité des données et informations ;
- Sureté et Sécurité ;
- Relations Institutionnelles / Lobbying ;
- Communication (interne, externe, financière …) ;
- Contrôle interne ;
- Finance (Trésorerie, Contrôle de Gestion, Fraude…) ;
- Juridique et conformité ;
- Opérations (Production, Qualité, Logistique, Supply-Chain, …) ;
- Commercial et Marketing ;
- Stratégie ;
- Audit interne ;
- Direction Générale ;
- Conseil d'Administration / Administrateurs ;
- …

Cette liste doit bien entendu s'adapter à la situation de chaque Entreprise étendue, mais on comprend immédiatement que tous les salariés de l'Entreprise étendue sont au moins concernés, voire impliqués.

En procédant ainsi, les bases d'un dispositif étendu de maîtrise des risques sont créées, puisque chacun se trouve confronté à des causes ou des conséquences hors de son champ de responsabilité, et doit donc chercher à les prendre en considération et à mieux les traiter. Presque naturellement, le contrôle interne s'élargit à la prévention des risques situés à l'extérieur de l'organisation que l'on considère. La gestion des risques de l'Entreprise étendue ne peut, en effet, que reposer sur un dispositif de contrôle interne ouvert lui aussi à 360° !

Gestion des risques spécifiques liés à la sous-traitance	Gestion des risques dans une approche intégrée
• Définir une stratégie « Make or Buy » • Analyser l'organisation, et les démarches contractuelles existantes • Vérifier l'exhaustivité et l'efficience des clauses • Capitaliser sur l'administration des contrats • Auditer et synthétiser les expositions (clauses de limites de responsabilité, ajustement des couvertures, …) • Intégrer des obligations d'audit des sous-traitants • Suivre le niveau de maîtrise	• Etablir une stratégie de gestion des risques globale, incluant l'ensemble des intervenants • Définir un niveau de transfert et de contrôle des risques en ligne avec la stratégie de gestion des risques • Intégrer les différents intervenants dans la gestion des risques : audits croisés, due diligence… • Intégrer les intervenants à la réponse aux nouvelles exigences réglementaires : plan de vigilance… • Visualiser et suivre la maîtrise des risques

Figure 18 – Exemple d'une approche spécifique versus une approche intégrée
Atelier C5 "Entreprise étendue et entreprise intégrée" - Rencontres du Risk Management AMRAE 2018.

Exemple de risque - Question type n°13

Toutes les transactions commerciales de l'entreprise sont-elles en conformité avec les lois et réglementations diverses locales / internationales ?

Risques à l'international : loi extraterritoriale, pénalités, amendes, …
Usage du Dollar avec l'Iran

Eléments factuels
L'entreprise Martin souhaite relancer ses actions d'investissements en Iran. Deux stratégies sont en cours de mise en oeuvre :
• Développer ce marché où les femmes consomment 8 fois plus de parfum qu'en France ;
• Elargir les ressources en « Fleuris verts » par l'exploitation du galbanum, végétal ombellifère qui a la propriété d'avoir la note verte la plus caractéristique, et qui pousse essentiellement en Iran.

Analyse des causalités
Tout échange avec l'Iran est actuellement exposé à des risques du fait de :
- L'extension de la territorialité de lois étrangères, ici en cas d'usage du dollar ;
- Les différentes lois d'embargo et de sanction et L'International Emergency Economic Powers Act » (IEEPA), loi fédérale américaine de 1977 autorisant le Président des Etats-Unis à restreindre les relations commerciales avec certains pays.

Evaluation des conséquences
- Amende pour usage du dollar, pouvant aller jusqu'au million d'euros ;
- Pertes des investissements locaux, de plusieurs millions d'euros.

Comportements/actions possibles
- Stopper les négociations en cours en s'appuyant sur les difficultés réglementaires, réelles, à traiter dans les contrats de partenariat.

Ou bien :
- Utiliser le système de troc INSTEX créé le 31 janvier 2019.

Capitalisation pour l'approche Entreprise étendue

Principales parties prenantes identifiées
- Partenaire local de distribution ;
- Partenaire local pour extraction des essences ;
- Gouvernements (US : Office of Foreign Assets Control (bras armé du Trésor américain), département de la justice ;
- Institutions financières ;
- Autorités de marchés (AMF, …).

Recommandations
Pour évaluer l'existence des risques dans les échanges internationaux ou les implantations à l'étranger, il y a nécessité d'une veille élargie permanente sur les politiques gouvernementales pour anticiper des décisions politiques.

Cas réels similaires (cf. Annexe 3 « Questions types – Sources détaillées des cas réels similaires »).

• BNP Paribas : amende aux Etats-Unis – 2015 (*)
• Maison de Parfum Berry : Iran, sanctions américaines - 2018
• Alstom : amende aux Etats-Unis - 2014
• Total : Iran, amende aux Etats-Unis - 2013
• SBM Offshore : amende aux Etats-Unis – 2016

« Evaluer l'environnement des affaires consiste à mesurer la qualité de la gouvernance privée d'un pays. C'est-à-dire la transparence financière des entreprises et l'efficacité des tribunaux en matière de règlement de dettes. » ***coface.fr – 2020***

(*) cf. Annexe 12 « Bibliographie » La BNP Paribas formellement condamnée … Le Monde 2015

Plus généralement, la gestion des risques est un sujet récurrent la gouvernance de l'entreprise, qu'il s'agisse d'appréhender un sujet spécifique comme la sous-traitance ou de déployer une approche globale intégrée (cf. figure 18 « Exemple d'une approche spécifique versus une approche intégrée »). Il ne pourrait en être autrement sous peine de créer des dysfonctionnements, donc de nouveaux risques. La gouvernance doit prendre en compte les spécificités organisationnelles, en particulier les relations avec les acteurs externes régies ou non par des contrats ou accords.

3.2 Prise en compte de l'environnement de l'entreprise

3.2.1 Avoir une vision juridique

La plupart des relations de l'Entreprise étendue avec son environnement sont contraintes par des lois, des réglementations, des contrats ou des décisions gouvernementales (cf. Question type n°13 – Exemple « risques à l'international : loi extraterritoriale, pénalités, amendes, … »). Une vision des aspects juridiques est donc impérative pour maîtriser au mieux les risques de l'Entreprise étendue, qui y sont liés par définition.

Des règles simples sont quasi indispensables, telles que :

- Un engagement ne peut être pris que par une personne habilitée ;
- Les rédactionnels des engagements sont conformes à des standards validés au sein de l'entreprise ;
- La portée de chaque engagement est estimée en termes de risque par des personnes compétentes ;
- Le service juridique (ou un juriste ou avocat conseil) valide les engagements dont les risques dépassent certains seuils, en lien avec les services concernés le cas échéant.

Par exemple, une entreprise peut décider que seule sa direction des Achats est habilitée à l'engager auprès d'un fournisseur. Et que déroger à cette règle exposerait le fournisseur à ne jamais être payé.

Le contrôle de supervision peut également se réaliser au travers de revues ou d'audits qui porteraient sur :

- Tous les contrats fournisseurs ou partenaires
  - Conditions générales fournisseurs ;
  - Obligations de confidentialité ;
  - Obligations de communication externe de l'Entreprise étendue ;
  - Conditions d'accès à l'information ;
  - Droits et devoirs de destruction ou conservation d'information ;
  - …
- Tous les contrats clients
  - Conditions générales clients ;
  - Obligations de confidentialité ;
  - …
- Toutes les réglementations applicables
  - Par périmètre géographique ;
  - Par domaine, éventuellement dépendant également ;
  - Conformité à toutes les réglementations ;
  - …

Point de vue d'un risk manager

« Les risques de l'Entreprise étendue sont le nouvel horizon du risk management. S'interroger à l'échelle des filières, des écosystèmes, des tiers et des partenaires de l'entreprise enrichit considérablement l'analyse des risques et favorise ainsi leur anticipation. Les outils et leviers d'action du risk management pour l'Entreprise étendue doivent s'articuler avec ceux du contract management, sans s'y réduire pour autant : là où le contract manager gère le survenu, le risk manager prévient la survenance et contribue ainsi à la stratégie. »

Un risk manager du secteur de la construction
(maîtrise d'ouvrage publique de projets).

- L'avis éventuel d'un avocat spécialiste sur les métiers ou les domaines concernés.

Une attention particulière est à porter aux engagements hors bilan. Il n'est pas toujours simple dans les entreprises d'une certaine taille d'en avoir une vue exhaustive, alors qu'ils représentent par nature un risque.

Une autre attention particulière doit être portée aux engagements contractuels avec les tiers « éloignés », comme le précisent les paragraphes 3.2.2 « Appréhender et gérer la notion de partie prenante externe » et 3.2.3 « Maîtriser les risques et opportunités du *Make or Buy* ».

3.2.2 Appréhender et gérer la notion de partie prenante externe

Par définition, les parties prenantes externes (souvent appelées « tiers ») sont l'ensemble des acteurs de l'Entreprise étendue, autres que les acteurs internes à l'entreprise elle-même. Si certains des tiers sont simples à identifier, comme les fournisseurs et les sous-traitants de premier rang, d'autres ne le sont absolument pas. Ainsi, par exemple, les institutions réglementaires de pays dans lesquels l'entreprise n'est pas présente et n'a pas d'intérêt ou d'activité, mais dont les textes édictés ont dans certaines conditions une portée extraterritoriale.

L'identification des tiers ou parties prenantes externes est donc un préalable que l'Entreprise étendue doit pleinement couvrir dans son approche des risques, afin de la gérer et de s'assurer de la bonne maîtrise ou de l'acceptation des risques liés à ces tiers qui s'en suivra. Il est possible d'identifier les fournisseurs et sous-traitants de rang n … tant que n n'est pas trop élevé ! Un moyen classique est d'obliger, par la

voie contractuelle, les fournisseurs et sous-traitants de rang 1 à déclarer leurs propres fournisseurs et sous-traitants de rang 1, et qu'eux-mêmes obligent ces derniers à faire de même. Cette pratique présente néanmoins des limites : il faut que l'Entreprise donneuse d'ordre ait un certain poids chez les fournisseurs et sous-traitants pour espérer obtenir un tel résultat, tout en surveillant la fluidité du processus d'approvisionnement dans son ensemble. Cette première limite significative et fréquente à l'identification de l'ensemble des acteurs de l'Entreprise étendue peut être repoussée en partie par des recherches et des enquêtes sur Internet.

Un autre traitement préventif est d'intégrer une clause contractuelle dans les conditions générales d'achat, exigeant de chacun des fournisseurs qu'il s'engage par écrit au moment de la commande, à veiller (même si l'obligation faite n'est qu'une obligation de moyen, pas de résultat) à ce que ses propres fournisseurs et sous-traitants ne génèrent pas de risque pour l'entreprise donneuse d'ordre.

De l'autre côté de la chaîne de valeur, les clients des clients, ou encore des associations de clients sont des acteurs qui font également partie de l'écosystème de l'Entreprise étendue. L'entrée en vigueur des « class actions » aux Etats-Unis, en Angleterre, … en est la preuve. En France, depuis le 1er octobre 2014, les « recours collectifs », « actions de groupe » ou « actions collectives » sont possibles, sur un champ d'application encore réduit mais qui peut évoluer.

On peut ranger dans ce même groupe les utilisateurs des produits et services qui ne sont pas nécessairement clients au sens strict. L'identification de ce type de tiers et des risques qui leur sont associés se fera préventivement au travers par exemple du suivi des plaintes clients et de la veille sur les réseaux sociaux.

Dans une catégorie similaire d'acteurs, les ONG et autres associations issues de la société civile, sont également des tiers potentiels. L'identification des ONG se fera par une étude croisée entre leurs périmètres d'action dans les pays où l'entreprise est concernée, et la nature des produits et services de l'entreprise dans ces pays. De même que pour ses fournisseurs et sous-traitants directs et indirects, la veille sur les réseaux sociaux est également un moyen d'identification préalable.

Une autre catégorie importante de tiers parfois difficiles à identifier regroupe les institutions réglementaires ou étatiques et autres autorités de tutelle. Le premier niveau est facilement accessible par la recherche des réglementations relatives aux produits et services de l'entreprise dans les pays où elle et ses fournisseurs et sous-traitants de rang 1 sont établis.

L'identification de tiers peut être plus difficile, notamment dans les pays où l'activité mise en cause n'est pas directement concernée. Par exemple dans le cas des sanctions internationales infligées à BNP Paribas, ce sont des transactions financières en dollars avec l'Iran qui ont fait l'objet d'une amende par les Etats-Unis, lesquels ont fait valoir le critère d'extraterritorialité de leurs textes de loi (*).

Dans un autre domaine, les institutions américaines ont renforcé en 2018 leurs moyens de contrôle à l'international par le *Cloud Act* (*), loi qui autorise les instances de justice à accéder aux données numériques stockées par des prestataires de services américains sur leurs serveurs même installés en dehors des USA. L'Etat américain peut ainsi obtenir des données individuelles stockées à l'étranger sans passer par un jugement des tribunaux (américains ou étrangers), et sans en informer ni les utilisateurs touchés, ni leur pays. Et l'invalidation par la Cour de Justice Européenne du *Privacy shield* est venue complexifier encore le sujet, puisque ce texte réglementait l'échange d'informations entre les sociétés européennes et les Etats-Unis.

Sur ces risques règlementaires, le rescrit est un moyen de prévention. Par ce moyen, l'entreprise pose une question par écrit à l'autorité compétente, et celle-ci lui répond, sur les possibilités d'interprétation du texte et les conditions applicables. Cette réponse écrite est un élément protecteur en France, en Suisse, en Angleterre, … qui pourrait permettre de plaider la bonne foi dans d'autres pays en cas de litige avéré.

3.2.3 Maîtriser les risques et opportunités du « *Make or Buy* »

Un des exemples types les plus spontanément cités lorsqu'on s'interroge sur l'internalisation ou l'externalisation des risques est l'analyse du *Make or Buy* (« faire ou acheter »).

Cet arbitrage est en réalité une décision aux impacts majeurs sur le futur de l'Entreprise étendue, tant en termes de développement que de pérennité. Il est source d'autant d'opportunités que de risques (cf. Question type n°14 – Exemple « Pratiques de sous-traitants : Maîtrise de la cascade des fournisseurs »).

Parmi les principaux motifs de recours à une analyse *Make or Buy*, on peut citer :

- Limiter les investissements ;
- Réduire les coûts de production ;
- Couvrir un besoin de compétences ;
- Satisfaire un besoin capacitaire ;
- Renforcer la maîtrise d'un processus ;
- Améliorer la qualité d'un produit ou d'un service ;
- Réduire un délai de mise sur le marché ;
- …

(*) cf. Annexe 12 « Bibliographie » La BNP Paribas formellement condamnée … Le Monde 2015.

Exemple de risque - Question type n°14

Les sous-traitants de rang 1 utilisent-ils en cascade des sous-traitants avec des pratiques pouvant nuire à l'image ou la réputation de l'entreprise ?

Pratiques de sous-traitants : Maîtrise de la cascade des fournisseurs
Fournisseur non éthique

Eléments factuels
Grâce à ses relations, l'entreprise Martin a pu être discrètement informée, avant que la réalité ne soit connue, de possibles cas de traite et travail forcé d'enfants par l'un des sous-traitants locaux du principal fournisseur thaïlandais de rang 1.

Analyse des causalités
Un contrôle local a pu confirmer les faits : travail d'enfants de moins de 15 ans, dépassement de 50 heures hebdomadaires, salaires irrégulièrement versés, aucune condition de sécurité, pas de respect des critères environnementaux de production, …

Evaluation des conséquences
- Dégradation de la réputation, articles dans la presse locale, mondiale.
- Plaintes en nom collectif par des ONG.
- Détérioration de l'image de marque.
- Responsabilité civile, pénale.
- Pénalités financières.
- Manque à gagner, besoin de nouveaux fournisseurs.

Comportements/actions possibles
- Obliger le fournisseur de Rang 1 à changer de fournisseurs rang 2.
- Obliger le fournisseur de Rang 1 à s'engager pour le compte de ses fournisseurs rang 2 et plus.
- Obliger le fournisseur de Rang 1 à prouver le respect des engagements sociétaux.
- Rompre avec ce fournisseur de rang 1 et le remplacer par un fournisseur respectueux des engagements sociétaux de l'entreprise.

Capitalisation pour l'approche Entreprise étendue

Principales parties prenantes identifiées
- Fournisseurs en cascade.
- ONGs (Amnesty International, Human Rights, …).
- Société civile, Institutions gouvernementales locales.
- Institutions mondiales.
- Médias.

Recommandations
- Faire signer les fournisseurs pour les obliger contractuellement à respecter un code stipulant les droits humains et la législation du travail.
- Mettre en place des audits et contrôles réguliers des fournisseurs.
- Rompre le cas échéant toutes relations avec les fournisseurs locaux (rang 1 compris).
- Remise à plat de la chaîne d'approvisionnement.
- Devoir de vigilance.

Cas réels similaires (cf. Annexe 3 « Questions types – Sources détaillées des cas réels similaires »).

- E. Leclerc et Casino : respect des droits humains - 2015
- Nestlé, Mars et Hershey's : Thaïlande – 2015
- Mango, Benetton, The Children's Place, Cato Corp, Joe Fres : effondrement Rana Plaza - 2013

"Si la question des achats responsables est aujourd'hui bien connue, très souvent abordée par les entreprises, il est beaucoup plus rare de se pencher sur la vision du fournisseur face à ces processus d'achats. En effet, le lien entre engagements stratégiques RSE de grands groupes et la réalité des pratiques d'achat pourrait être questionné." l'étude **ORSE/PWC/BPI France de janvier 2020.**

Partager des risques est également fréquemment cité parmi les motifs de réflexion sur l'externalisation ; cet objectif doit donc être considéré avec beaucoup de circonspection. En effet, quelles que soient les voies de recours juridiques ou judiciaires qui s'offrent au donneur d'ordre en cas de malfaçon ou bien de non-respect du niveau de prestations contractuel (Service Level Agreement : SLA) par le prestataire en amont, c'est bien le donneur d'ordre, c'est-à-dire l'entreprise qui doit répondre de la défaillance vis-à-vis de ses parties prenantes au premier rang desquelles ses propres clients.

Par conséquent, l'idée selon laquelle une entreprise pourrait transférer ses risques à des fournisseurs ou à des sous-traitants est peut-être vraie pour quelques-uns d'entre eux (par exemple en ce qui concerne les risques de sécurité sur des processus industriels particuliers jugés insuffisamment maîtrisés en interne), mais absolument fausse pour beaucoup d'autres. C'est la responsabilité du donneur d'ordre qui est appelée. Sa réputation est donc entachée tout autant, voire plus que celle du fournisseur ou du sous-traitant. Lors d'une décision de *Make or Buy*, le risk manager devra donc veiller tout particulièrement à ce que l'Entreprise étendue ait réalisé :

- Les analyses « SWOT » (forces, faiblesses, opportunités, menaces) complètes pour le « Make » et pour le « Buy » ;
- L'identification complète des parties prenantes dans les 2 cas ;
- L'identification et l'évaluation de tout le spectre des risques (financiers, sociaux, image, géopolitiques, ...) et les possibilités de traitement des plus importants d'entre eux, dans les 2 cas ;
- Des missions de Due Diligence ad hoc (cf. section 3.4.4 – « Utiliser des outils »), en particulier sur les fournisseurs à risque, avec des plans d'actions et un suivi pour ceux dont la performance est la plus problématique.

C'est de cette seule manière que la décision de *Make or Buy* résultera bien d'une vision complète à 360° incluant les risques partagés ou externalisés, et non pas uniquement d'une vision sur l'opportunité économique ou opérationnelle.

3.2.4 Systématiser la production de registres de risques par les fournisseurs de projets.

A l'exemple du secteur pétrolier et de celui de la construction, une piste intéressante à exploiter pour l'entreprise dans ses relations avec ses fournisseurs est de leur demander systématiquement, lors d'un appel d'offres, la fourniture du registre des risques du projet visé. Idéalement il faudrait même que le fournisseur ne puisse pas démarrer les prestations tant que son registre des risques n'a pas été fourni.

Cette pratique existe dans les appels d'offres de l'European Global Navigation Satellite Systems Agency (GSA) et dans des appels d'offres de l'European Defense Agency (EDA). Il est demandé aux candidats de fournir dans leur réponse un registre préliminaire des risques (*Preliminary risk register*). Pour les marchés publics de travaux souterrains (*), la réglementation a fait du Plan de Management des Risques (PMR), incluant le registre des risques, un document contractuel obligatoire inclus au cahier des clauses techniques particulières. Les fournisseurs le valident donc et doivent l'amender le cas échéant, le PMR étant un outil essentiel du pilotage de ces chantiers.

Pendant la vie d'un projet important ou qui dure longtemps, une bonne pratique consiste à demander aux fournisseurs de présenter l'évolution de leur registre des risques à chaque comité de gouvernance (pilotage ou suivi de projet). Il faut s'assurer que les fournisseurs réalisent eux-mêmes ces cartographies avec leurs propres fournisseurs, ce qui est parfois une obligation contractuelle pour les fournitures et services sensibles.

Point de vue d'un risk manager

« Avec plus de 2 500 fournisseurs qui contribuent de manière régulière au processus de production, la maitrise des risques associés est vitale pour notre activité. Nous avons multiplié les initiatives pour évaluer et accompagner nos fournisseurs sur de nombreux sujets tel que la Responsabilité Sociale et Environnementale, leur santé financière, leur chaine logistique, leurs exigences en matière de qualité mais aussi, par exemple, leur niveau de protection contre l'incendie. »

Un risk manager du secteur de la sous-traitance automobile.

(*) Cahier des clauses techniques générales applicables aux marchés publics de travaux (CCTG) - Fascicule 69 - Travaux souterrains.

3.3 Amélioration continue du traitement des risques

3.3.1 Impliquer les auditeurs

Les audits internes et les audits externes sont des sources précieuses d'amélioration des dispositifs de gestion des risques et de contrôle interne. Cela vaut donc aussi pour les risques de l'Entreprise étendue, au travers :

- Des missions sur les procédures et les processus directement concernés par l'Entreprise étendue bien sûr ;
- Des résultats de tous les types d'audits, en particulier lorsque les constats portent sur des impacts d'image ou de réputation ;
- Des audits réalisés par le donneur d'ordre chez les tiers (fournisseurs et sous-traitants par exemple) parfois partagés au sein d'une cellule collective d'acteurs d'un même marché.

Au travers de l'implication des auditeurs et des contrôleurs internes, l'entreprise s'assure de la capacité à contrôler ses tiers. Les résultats des audits doivent être utilisés sous l'angle de l'Entreprise étendue par le risk manager.

3.3.2 Sensibiliser, former, contractualiser

Le traitement des risques de l'Entreprise étendue, tant préventif que curatif, implique encore, pour certaines entreprises, un changement de culture. Cette évolution de la culture est d'autant plus nécessaire que les risques impliquent bien souvent des populations très larges, soit génératrices du risque, soit associées à son traitement. En effet, s'il est habituel que la communication externe d'un dirigeant soit analysée par les parties prenantes, il arrive que celle d'un employé envahisse brutalement les réseaux sociaux, en quelques heures (cf. Question type n°15 – Exemple « Image dégradée par des actions ou propos de parties prenantes internes »). Le changement de culture doit être impulsé par les dirigeants (voire les actionnaires) et les impliquer. Les collaborateurs doivent se l'approprier.

La sensibilisation aux risques de l'Entreprise étendue peut se faire au travers de communications ad hoc en interne, et surtout par des formations à tous les niveaux de l'organisation, en particulier lors de l'exercice de cartographie des risques. Elle peut consister en une mise en exergue des conséquences de risques avérés dans l'histoire de l'entreprise ou survenus, de préférence dans des entreprises du même secteur avec un positionnement comparable, afin de faire comprendre l'exposition potentielle de l'entreprise. Cela permet une prise de conscience active de la notion d'Entreprise étendue et des risques qui y sont liés. Lorsqu'elles

Exemple de risque - Question type n°15

Des messages insuffisamment contrôlés provenant des employés ou dirigeants de l'entreprise (publicités trash, prise de parole en public, …) ou une communication négative des médias détectée tardivement sont-ils susceptibles de porter atteinte à son image ou à sa réputation ?

Image dégradée par des actions ou propos de parties prenantes internes
Communication hors contrôle

Eléments factuels
Ces derniers mois, sa DRH a été alertée à 3 reprises par la Direction de la Communication pour des discussions impliquant l'entreprise sur les réseaux sociaux. Le 1er cas est une vidéo dans laquelle un salarié de la Direction Financière tient en privé des propos racistes en mentionnant son appartenance à l'entreprise. Le deuxième cas est une discussion (un chat) où une personne se présente comme salarié de l'entreprise et affirme que « contrairement à ses concurrents, L'entreprise ne s'abaissera jamais à intégrer à ses offres marketing des produits destinés à la communauté homosexuelle ». Le troisième cas est la mise en ligne d'un podcast où le PDG de l'entreprise mentionne ouvertement en marge d'une interview radiodiffusée, son appartenance à une communauté de chasseurs d'animaux sauvages organisant des safari-chasses en Afrique.

Analyse des causalités
L'entreprise est depuis peu scrutée par des parties prenantes sur le plan de la Responsabilité Sociale et Environnementale. Droits humains, respect du monde animal et biodiversité sont des terrains où L'entreprise a été laxiste jusqu'à récemment. De plus, L'entreprise n'a pas réellement mis en œuvre une politique interne de sensibilisation à l'éthique et aux comportements individuels.

Evaluation des conséquences
Bien que les 3 cas semblent totalement déconnectés, rien n'indique que ce « bad buzz » n'est pas organisé et, quoi qu'il en soit, il pourrait dériver vers une campagne d'acharnement médiatique impliquant la marque. Cela pourrait conduire à un appel au boycott des produits, ou bien à une perte d'une partie de la clientèle, voire à une mise en cause judiciaire de l'entreprise ou de certains de ses représentants.

Comportements/actions possibles
- A titre préventif : sensibilisation et formation.
- A titre curatif : contrôle en temps réel des réseaux sociaux et autres médias.

Capitalisation pour l'approche Entreprise étendue

Principales parties prenantes identifiées
- ONG activistes - Employés et dirigeants - Clients finaux, utilisateurs, consommateurs - Médias.

Recommandations
- Sensibiliser tous les personnels de l'entreprise à l'importance de leurs propos et actions en dehors de l'entreprise.
- Auditer le dispositif de veille réseaux sociaux pour s'assurer de son efficacité (périmètre d'écoute, réactivité, ...).
- Développer le dialogue avec les parties prenantes RSE et investir dans des actions de partenariats avec celles les plus proches du modèle d'affaires de l'entreprise (protection des animaux, humanistes.)

Cas réels similaires (cf. Annexe 3 « Questions types – Sources détaillées des cas réels similaires »).

- Maison Blanche : dérapage du nouveau directeur de la communication - 2017 - Barilla : dérapage du président - 2013 - Servier : dérapage du président, procès - 2013
- France Telecom : dérapage dans la communication du président – 2009

« Les entreprises semblent avoir pris conscience de l'enjeu que constitue la présence personnelle des collaborateurs sur les médias sociaux : ainsi 80% des grandes entreprises disposent d'une charte à destination des collaborateurs. 45% des entreprises ont même créé un programme ambassadeurs pour que les employés participent à la visibilité en ligne. » ***Entreprises & Médias*** *– étude « La gouvernance des entreprises sur les médias sociaux » 12 mai 2015.*

sont plus détaillées et destinées aux experts, les formations peuvent être axées sur les spécificités de l'Entreprise étendue, la façon dont elles sont prises en compte et traitées, depuis l'identification des risques jusqu'aux actions de traitement.

Enfin, la culture de l'entreprise en matière de risques apparait progressivement dans les contrats de travail par la mention ou la référence à des chartes d'éthique (*). Ces chartes ne sont pas seulement l'expression des valeurs essentielles. Elles explicitent des comportements contre la fraude, la corruption, les délits d'initié et le devoir d'alerte, suivant le contexte propre de chaque entreprise. Des obligations incluses au contrat de travail peuvent concerner l'Entreprise étendue (obligations de réserve, de loyauté, de discrétion, confidentialité, secret professionnel). Elles doivent s'accompagner de sessions d'information et de formation. Le contrat de travail peut aussi évoquer la maîtrise des risques vis à vis des tiers, par exemple pour un infirmier de bloc opératoire : « Maitriser la Gestion des risques liés à l'activité et à l'environnement opératoire … à la traçabilité … et au contact et l'accueil des patients, … ».

3.3.3 Travailler la prévention

Plus généralement, l'efficacité des dispositifs de prévention dans le management des risques de l'Entreprise étendue est indispensable pour préserver la réputation, les actifs, la qualité des activités, … de l'entreprise. Par exemple, on sait que la réputation peut se dégrader en quelques heures. Peu importe que les causes de la dégradation soient fondées ou non, le mal est fait dès l'origine et la reconnaissance ultérieure de l'éventuelle injustice ne compensera pas systématiquement les impacts, financiers notamment, qui auront pu être très violents dans l'intervalle.

(*) cf. Annexe 12 « Bibliographie » Article « Contrat de travail … Mazars 2014.

Exemple de risque - Question type n°16

Des procédés / composants / services / marques développés et vendus par l'entreprise sont-ils déjà couverts par des brevets ?

Politique de propriété intellectuelle : brevets, contrefaçons, marques, …
Utilisation d'une plante remarquable, le Sacha-inchi

Contexte
Lors d'une tournée en Amazonie, le directeur Marketing de l'entreprise a découvert une plante, le Sacha-Inchi, puissant fortifiant capillaire. Décision est prise de déposer un brevet et de lancer une nouvelle gamme basée sur cette plante, avec démarrage de commercialisation en Amérique Latine.

Analyse des causalités
Quelques semaines après sa commercialisation en Amérique Latine, des articles cinglants sont apparus dans la presse accusant l'entreprise Martin de s'approprier, via un brevet, des ressources biologiques et des connaissances traditionnelles des peuples ruraux ou autochtones pour en faire du profit. Cas typique de « biopiraterie » où des entreprises commerciales, voire des instituts de recherche accaparent la biodiversité en copiant les techniques et les savoir-faire traditionnels.

Evaluation des conséquences
- Dégradation de la réputation (accusation de 'colonialisme').
- Plaintes de Commissions Nationales étatiques et d'Associations de Défense des Peuples Autochtones.
- Détérioration de l'image de marque.
- Boycott commercial.
- Juridiques, déclaration de nullité du brevet, compensations financières pour la communauté.
- Pertes financières (remplacement de la gamme de produits).

Comportements/actions possibles
- Rapprochement avec les artisans et entreprises locales utilisant cette plante dans un objectif capillaire avec reconnaissance de leur antériorité et actions de valorisation de leurs savoir-faire.
- Contre-campagne d'information montrant que, au contraire, L'entreprise valorise les acteurs autochtones (culture, transformation, …).
- Révision de la portée du brevet le cas échéant.

Capitalisation pour l'approche Entreprise étendue

Principales parties prenantes identifiées
- Minorités ethniques, peuples autochtones.
- ONG, Commissions Nationales.
- Commissions de lutte contre la contrefaçon.
- Clients finaux.
- Réseaux de distribution, partenaires.
- Médias locaux, internationaux.

Recommandations
- Recourir à des experts en propriété intellectuelle et propriété industrielle (marques, modèles, brevets, droits d'auteur, dessins, logiciels, …).
- Etablir une veille une veille juridique et stratégique permanente sur les droits de propriété dans ses domaines d'activités et connexes.
- Protéger son patrimoine et surveiller les contrefaçons.

Cas réels similaires (cf. Annexe 3 « Questions types – Sources détaillées des cas réels similaires »).

• Greentech : Pérou, biopiraterie - 2006 • Schwabe : Afrique du Sud - Abrogation brevet – 2010
• Apple : procès Samsung – 2018 • Microsoft : violation de brevets – 2007/2011
• Pernod-Ricard : Bacardi, OMC – 1996/1999

« L'INPI, par son action quotidienne sur le terrain, sensibilise les innovateurs … à la dimension stratégique de la propriété industrielle. » - site de l'INPI – « Chiffres clés de la propriété industrielle … 2019 » « … peu ou mal conseillé, le titulaire d'un droit de propriété industrielle peut très vite se faire déposséder en manquant de vigilance sur l'acceptation de clauses de propriété industrielle présentes dans des contrats de recherche ou de co-développement ou l'acceptation d'un accord de confidentialité prévoyant l'utilisation 'à sa guise et sans contrepartie' d'un brevet. » - ***IHEMI (INHESJ)*** *- Institut national des hautes études du ministère de l'Intérieur (de la sécurité et de la justice) : « Les atteintes aux savoir-faire - La captation de brevet ».*

Actions	Exemples de nature de risques concernés
Etablir une charte éthique fournisseurs, la diffuser, la faire appliquer	Dégradation de l'image
Appréhender les contraintes éthiques clients, les faire approprier par les personnels intervenants ou ayant une action impliquant les résultats chez les clients	Pertes de marchés
Informer régulièrement les acteurs internes en lien avec des acteurs externes	Toutes, et notamment corruption, image
Rechercher les impacts potentiels de décision, mais aussi ceux d'absence de décision *(H. Ford : 'mieux vaut une mauvaise décision qu'une absence de décision')*	Toutes et notamment stratégie, présence géographique …
Actualiser très régulièrement les évaluations des impacts des risques de la cartographie	Toutes, au travers du danger de sous-évaluation et donc de décision inappropriée
Faire évoluer la culture d'entreprise quant aux risques de l'Entreprise étendue	Toutes en particulier au travers du danger de ne pas avoir conscience d'un risque
Avoir un suivi « temps réel » de l'émergence et de l'évolution des risques pays	Sécurité des personnes, enjeux politiques, continuité d'activité
…	…

Figure 19 – Exemples d'actions préventives pour l'Entreprise étendue

Toute action préventive sur des risques majeurs de l'Entreprise étendue, dans toutes ses extensions, prend dès lors tout son sens stratégique sur ce plan de la réputation. Le tableau de la figure 19 « Exemples d'actions préventives pour l'Entreprise étendue ») liste quelques exemples d'actions préventives et le type de risque que ces actions concourent à éviter.

Mais les actions de prévention peuvent elles-mêmes être porteuses de risques externes, comme le montre le dépôt d'un brevet (cf. Question type n°16 – Exemple « Politique de propriété intellectuelle : brevets, contrefaçons, marques, … »). Toute action, même préventive, doit donc être analysée dans l'approche Entreprise étendue.

Exemple de risque - Question type n°17

Des opérations de mécénat actuelles ou envisagées, issues d'un rachat d'entreprise ou créées, sont-elles en parfaite cohérence avec la raison d'être et les valeurs de l'entreprise ?

Non visibilité d'une non-conformité lors du rachat d'une PME (trop) mécène

Mécénat non-conforme

Eléments factuels

Par une opération de croissance externe, L'entreprise Martin a racheté récemment une PME positionnée sur le créneau des tests cosmétiques. En vérifiant les comptes, le directeur Financier de l'entreprise constate que le fondateur de cette PME, bien implantée en Touraine, a signé des contrats de mécénat culturel et de compétences dont la nature des contreparties pose des problèmes déontologiques.

Analyse des causalités

Depuis 2003 et l'abrogation de la loi TEPA, les avantages fiscaux pour les entreprises mécènes rendent le système particulièrement avantageux, provoquant un 'engouement' au niveau national. Pour nombre de PME/TPE (représentant 97% des mécènes !), l'un des leviers est de travailler pour l'intérêt général avant les bénéfices fiscaux et d'image. Mais la Cour des Comptes, dans un rapport de 2019, fustige le manque de contrôles et se demande si « l'intérêt général reste la caractéristique majeure de l'engagement des mécènes » face à la poursuite d'intérêts parfois plus particuliers.

Evaluation des conséquences

- risque juridique : souscription à une opération de mécénat non conforme à la législation locale ou reconnue par les pouvoirs publics locaux.
- Conflits d'intérêts, réels ou apparents.
- Redressements ou retraitements fiscaux : le projet cible relève-t-il bien de l'intérêt général sans contreparties indues.
- Réputation : l'objet du mécénat est-il en adéquation avec les valeurs portées par l'entreprise et (toutes) ses activités, incluant la RSE de l'entreprise (en particulier mécénat de compétences).
- risque pénal de requalification en abus de biens sociaux, ou de corruption passive, pour des opérations de mécénat litigieuses ou illicites.

Comportements/actions possibles

- Dénoncer l'achat de la PME si c'est possible.
- Evaluer les risques d'image et mener une communication anticipative.
- Impliquer les acteurs bénéficiaires des pseudo-mécénats devant la justice.

Capitalisation pour l'approche Entreprise étendue

Principales parties prenantes identifiées

- Actionnaires, institutions représentatives du personnel, Pouvoirs publics, Associations activistes, ONG.

Recommandations

- Etablir la politique interne du mécénat.
- Respecter tous les critères d'éligibilité à du mécénat et de conformité de la loi SAPIN 2.
- Effectuer des Due Diligence avant toute démarche (ou requête) de mécénat.
- Associer activement toutes entités internes de l'entreprise à la démarche envisagée.
- Adapter la convention contractuelle standard de l'entreprise aux cas particuliers du mécénat.

Cas réels similaires (cf. Annexe 3 « Questions types – Sources détaillées des cas réels similaires »).

- Nova Scotia : corruption, FIFA - 2015
- Purdue Pharma : refus d'un don, Tate Gallery – 2019
- BP : refus de parrainage, British Museum - 2016

« Alors que le mécénat … n'a jamais suscité autant de controverses et le paysage s'assombrit … S'appuyant sur les dérives pointées par des parlementaires ou par la Cour des comptes, le gouvernement défend une réduction de l'avantage fiscal des grandes entreprises mécènes » - **ADMICAL** : colloque du 01/10/2019 au Collège de France : « Faut-il en finir avec le mécénat ? »

3.3.4 Comprendre les couvertures d'assurance

Du fait de leur diversité, de leur éloignement ou de leur nature, les risques de l'Entreprise étendue ne peuvent pas être tous couverts par les contrats d'assurances. Par exemple, le risque d'échec d'un projet client pour cause de défaillances ou d'insuffisance de compétences d'un fournisseur n'est pas nécessairement couvert par une assurance.

Les risques étant identifiés, avant d'envisager une couverture d'assurance, la première option possible reste de mettre en place des actions de prévention pour les éliminer ou les limiter (cf. section 3.3.3 « Travailler la prévention »). Ces actions seront communiquées à l'assureur afin qu'il évalue son risque et fixe le montant de la prime. Il est également possible de mettre en place des clauses contractuelles, comme celle de faire exécuter les prestations par un autre fournisseur aux frais du défaillant.

Lorsque les dommages sont physiques (incendies, inondations, …), il est souvent possible de protéger les sites contre les conséquences d'un évènement ou incident soudain. Toutefois, selon la couverture souscrite, cela peut être plus difficile à décider, imposer ou anticiper lorsque les sites sont exploités par des sous-traitants, partenaires ou cotraitants. L'élargissement de certaines couvertures peut venir en complément, comme celles du risque politique ou cyber, des couvertures qui ont évolué et qui s'adaptent selon les spécificités d'une Entreprise étendue.

Dans le cadre de l'Entreprise étendue, appréhender les mesures de continuité d'activité, et parfois de gestion de crise, est indispensable. Cependant, les moyens d'imposer des clauses contractuelles aux tiers sont limités pour certaines entreprises. Dès lors, une solution peut être de transférer le financement via un contrat d'assurance afin de minorer les possibles conséquences financières des risques.

Habituellement, l'assurance couvre les risques en cascade, et par ce moyen, certains risques de l'Entreprise étendue peuvent être garantis dans les limites de la police d'assurance. Ainsi, par le jeu de clauses de garantie spécifique telles que la carence des fournisseurs, la défaillance de paiement, la non-atteinte d'un résultat opérationnel… les conséquences en chaine dans le cadre de l'Entreprise étendue peuvent être indemnisées, et ce, souvent, sans sous-limites particulières.

Exemple de risque - Question type n°18

Les équipements/produits intégrés dans des systèmes complexes et revendus à l'international tombent-ils sous le coup d'embargo ou de restrictions d'exportation (biens à double usage) ?

Restriction d'exportation ou embargo
Utilisation de Lait de phoque

Eléments factuels
Le lait de phoque est utilisé, pour les préparations cosmétiques, comme ingrédient de phase lipophile d'émulsions.
Le PDG de l'entreprise Martin se rend compte que nombre de ses produits utilisent des dérivés du lait de phoque dans la composition de ses cosmétiques et qu'aucune action de modification des compositions n'a encore été mise en oeuvre. Le problème est complexe car il faut que les qualités des produits ne soient pas dégradées en utilisant d'autres composants.

Analyse des causalités
D'une part du fait des exceptions à l'embargo décidé en 2013 (les Inuits ayant d'ailleurs besoin de vendre ces produits), et d'autre part du fait des difficultés techniques à trouver un produit de remplacement, l'entreprise n'avait pas cherché d'autres solutions.
Depuis cette année, le Parlement européen a adopté un durcissement de cet embargo et le lait de phoque est maintenant dans la liste des produits interdits.
Il y a un manque avéré d'anticipation d'évolution potentielle de la situation.

Evaluation des conséquences
Environ une dizaine de produits de l'entreprise ont du lait de phoque dans leurs compositions.
Ces produits représentent 18% du CA de l'entreprise Martin et 21% de la marge nette.
L'image de l'entreprise peut gravement souffrir du fait des activistes protecteurs des phoques qui pourraient mettre en avant un manque d'éthique pour L'entreprise.
Si L'entreprise tarde à mettre en place un composant de substitution, une amende de 10 fois la valeur la valeur des produits concernés est possible.

Comportements/actions possibles
Le projet de substitution par un nouveau composant nécessitera au moins 18, voire 24 mois.
Le coût estimé de ce projet est de l'ordre de 1,5 à 3 millions d'euros.

Capitalisation pour l'approche Entreprise étendue

Principales parties prenantes identifiées
- Douanes, gouvernements.
- ONG activistes.
- Influenceurs dans les réseaux sociaux (opinions publiques locales, consommateurs, clients …).
- Laboratoires de recherche.

Recommandations
- Anticiper les évolutions réglementaires, même à partir de signaux faibles.
- Considérer la territorialité des achats/ventes pour estimer les risques.
- Rechercher préventivement les composants de substitution potentiels.
- Veiller aux impacts d'image.

Cas réels similaires (cf. Annexe 3 « Questions types – Sources détaillées des cas réels similaires »).

- Société Générale : embargo sur Cuba - 2018
- Intel et Micron : embargo Chine, Huawei - 2019
- Microsoft, Google : embargo Chine, Huawei - 2019
- ONG suisse MediCuba, Oxfam : Coronavirus, embargo américain, Cuba - 2020

« Il relève de la responsabilité des opérateurs (importateurs ou exportateurs) de s'assurer que l'opération commerciale qu'ils envisagent n'entre pas dans le champ d'application matériel et géographique d'une mesure de restriction commerciale. » - Site **douane.gouv.fr** - Généralités sur les embargos.

Point de vue d'un risk manager

« Un des risques d'Entreprise étendue que je perçois pour nous les assureurs, c'est le risque lié aux courtiers, qui sont nos intermédiaires en termes de souscription et souvent aussi en termes de gestion des sinistres : s'ils ne respectent pas le devoir de conseil ou les obligations en matière de lutte contre le blanchiment et le financement du terrorisme, c'est la responsabilité de l'assureur qui sera recherchée ! »

Un risk manager du secteur de l'assurance.

Depuis quelques années, la succession d'évènements climatiques majeurs, de catastrophes (Fukushima, Irma et les successions de tempêtes et d'inondations en France) ou l'apparition d'une pandémie comme la Covid-19 ont conduit les assureurs à reconsidérer et parfois durcir les limites des mécanismes de cascades. Ainsi, la possibilité de couvrir dans un même contrat d'assurance une suite de conséquences pouvant naitre dans l'environnement de l'assuré est limitée. Par conséquent, identifier les risques de l'Entreprise étendue et les adapter dans son ou ses contrat(s) d'assurance est incontournable, soit en intégrant nommément des partenaires (sous-traitants, co-traitants, fournisseurs …), soit en intégrant des natures de risques spécifiques (défaillances de fournitures de matières premières, défaillances de paiement dans un délai imparti …).

Enfin, lorsque les risques identifiés sont d'une ampleur inhabituelle (projet exceptionnel en montant, en nature, en technique, en durée …), il peut s'avérer nécessaire de rechercher une couverture d'assurance moins traditionnelle, plus innovante, telle qu'une couverture multirisque ou multibranche, des couvertures paramétriques ou ART (solutions *d'Alternative Risk Transfer*).

Ces couvertures particulières permettent de définir et personnaliser l'ensemble des conditions d'assurance avec les assureurs et les réassureurs (les assurés, l'objet des risques assurés, leurs modalités et les critères d'incidents), voire de répartir le montant de l'indemnité versée en fonction des primes préalablement réglées à l'assureur. Elles peuvent apporter une réponse plus appropriée aux risques identifiés dans le cadre de l'Entreprise étendue.

3.4 Mise en œuvre d'une organisation étendue

3.4.1 Mettre en place des cellules de surveillance

Pour surveiller l'état de son environnement (cf. 3.2 Prise en compte de l'environnement de l'entreprise), un autre dispositif de gestion des risques de l'Entreprise étendue consiste à mettre en place des cellules de surveillance dédiées. Celles-ci peuvent être créées par typologie de risques, ou encore par métiers concernant l'Entreprise étendue. C'est le cas des cellules de veille ou de surveillance :

- De l'image ou de la réputation de l'Entreprise étendue au travers de tous les médias : réseaux sociaux comme médias classiques ;
- De l'image de ses produits ;
- Des évolutions de la réglementation dans tous les pays avec activités concernant l'Entreprise étendue (commerce et production) ;
- Des politiques des pays dont les lois ont des impacts internationaux ou globaux (comme celles des USA envers l'Iran) (cf. Question type n°18 – Exemple « Restriction d'exportation ou embargo ») ;
- Des risques politiques des pays où l'Entreprise étendue exerce des activités directement ou non (filiale ou non, fournisseurs de rang n ou partenaires), ou bien des pays dans lesquels l'Entreprise étendue peut subir un effet ricochet sur ses produits, ou encore des pays dans lesquels l'Entreprise étendue fait voyager des collaborateurs ;
- Des concurrents ;
- Des fondations d'entreprise et leurs activités caritatives ;
- Des organismes de type ONG, ou des cellules activistes, dont les jugements peuvent concerner l'Entreprise étendue (cf. Question type n°17 – Exemple « Non visibilité d'une non-conformité lors du rachat d'une PME (trop) mécène ») ;
- Des contextes sociaux (syndicats, grèves, …), économiques, financiers, monétaires dans tous les pays où les activités peuvent être significatives ;
- Des évolutions technologiques (au-delà des évolutions du Numérique) concernant les produits, services et activités de l'entreprise.

D'une manière générale, le rôle de toutes les cellules de surveillance est prépondérant dans la gestion préventive des risques. Le risk manager se félicitera toujours de l'efficacité du travail de ces cellules de surveillance. Elles lui permettent souvent d'évaluer de nombreux risques à des niveaux de probabilité acceptables. L'organisation et les moyens mis à disposition des cellules de surveillance dépendent du contexte de leurs entreprises, de leurs métiers, de leurs organisations, …

Quand elles existent, ces cellules font partie du dispositif de veille globale de l'entreprise, règlementaire, juridique, géopolitique, … Etudier l'efficacité de telles cellules de veille ou de surveillance dans leurs environnements interne et externe est important, aussi bien en fonctionnement normal qu'en mode réactif. La réaction à une dérive est mise en exergue (cf. figure 20 « Cellule de surveillance des réseaux sociaux – réaction à une dérive ») par l'analyse simplifiée du fonctionnement de la cellule face à un message négatif qui apparaît et est susceptible de nuire à l'image de l'entreprise.

On remarque dans cet exemple que :

- La cellule doit disposer d'outils d'analyse des réseaux sociaux en temps réel pour pouvoir être efficace ;
- Si l'impact estimé parait grave, la cellule dispose d'un droit d'alerte auprès du directeur général hors toute procédure classique de communication ;

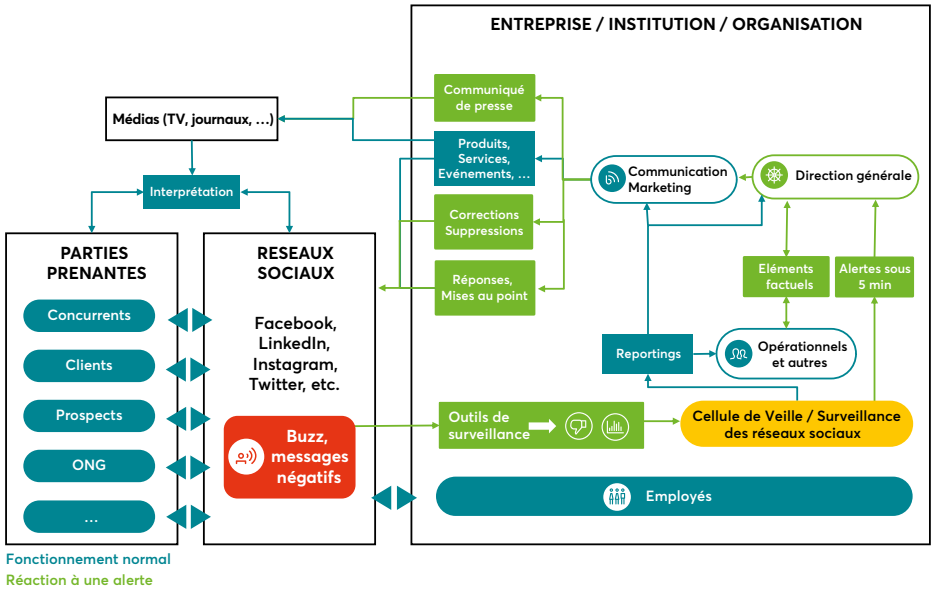


Figure 20 – Cellule de veille/Surveillance des réseaux sociaux – Réaction à une dérive.

- Les autres directions ou services concernés sont amenés à fournir à la cellule des éléments factuels pour élaborer la réponse ou mise au point ;
- Le service de communication met en oeuvre la réponse officielle auprès des médias et des parties prenantes (notamment les clients) ; une communication interne est également à envisager (non représentée dans ce graphe).

3.4.2 Elargir le dispositif d'alerte

La loi n°2017-399 du 27 mars 2017 relative au devoir de vigilance oblige à la mise en place, au sein du Plan de vigilance des grandes entreprises, d'un « mécanisme d'alerte ».

Il est bien entendu opportun de mettre en place un mécanisme d'alerte dans toute entreprise, dès lors qu'un risque a des impacts significatifs possibles à l'extérieur. Ce mécanisme de gestion d'alerte, à traduire en processus, va mettre en action un service ou une direction responsable, voire toute l'entreprise, quant au traitement d'un signalement susceptible de matérialiser la survenance avérée ou imminente d'un risque. Ce processus pourra conduire dans de nombreux cas à la gestion d'une crise. En ce qui concerne la gestion des alertes en matière d'Entreprise étendue, la particularité est que les réponses seront généralement à portée interne et à portée externe simultanément.

Un processus d'alerte a pour objet de déclencher la mise en place de l'organisation requise pour analyser et surveiller l'évolution du risque signalé, ou d'éviter ou réduire ses conséquences :

- En cas de risque avéré, par la mise en oeuvre d'actions curatives ;
- En cas de risque dont la matérialisation est potentiellement imminente par la mise en oeuvre d'actions préventives, d'évitement ou de réduction.

Ces actions sont d'abord de nature organisationnelle, puis le cas échéant de nature opérationnelle. Elles sont dans l'idéal prédéfinies par le management des risques lors des travaux sur la continuité d'activité, risque par risque. Les actions lancées ont généralement un impact sur l'environnement de l'Entreprise étendue. Ces actions sont donc potentiellement elles-mêmes porteuses de risques supplémentaires. Toute action sur l'environnement ayant des impacts multiples, aux conséquences immédiates ou différées, il faut éviter le « suraccident ».

Si l'expert compétent pour gérer un risque de l'Entreprise étendue peut être externe, l'une des difficultés provient du fait que les acteurs concernés et impliqués par la gestion de l'alerte sont parfois eux aussi externes à l'Entreprise étendue. Ils ne sont pas nécessairement a priori des parties prenantes internes identifiées, donc :

- Hors du pouvoir hiérarchique de décision ;
- Généralement d'une culture différente ;
- Parfois dans des obligations réglementaires différentes ;
- Ne disposent pas toujours des moyens nécessaires à la mise en œuvre des actions (moyens financiers, techniques, humains, …).

Les plans d'actions devront donc en tenir compte, et en particulier mettre en œuvre un système d'alerte qui soit efficacement ouvert sur l'externe.

Comme pour les autres risques, les alertes présenteront plusieurs niveaux de gravité : constat d'un évènement avant-coureur, signal faible, anticipation d'un risque immédiat, arrivée d'une crise, …

La qualité du processus d'alerte est jugée sur :

- Sa capacité à détecter des risques émergents à partir de signaux faibles dans l'environnement de l'Entreprise étendue ;
- Son délai de réactivité ;
- Son efficacité quant à la pertinence des acteurs internes et externes sollicités, dont en particulier le porteur du risque concerné ;
- Sa capacité à ne pas produire trop de faux positifs et donc à perturber le moins possible le fonctionnement de l'entreprise de manière inutile.

La gestion d'alerte est classiquement déclenchée par les cellules de surveillance, dont c'est par définition une des responsabilités, mais aussi par toute personne constatant un fait potentiellement suspect ou dangereux.

3.4.3 Traiter les risques en situation de crise

La cellule de crise est déclenchée afin de traiter une situation de risque avéré ou en cours d'émergence pouvant avoir des impacts majeurs. Qu'il s'agisse d'un sinistre, d'un accident ou d'une crise d'une autre nature, la contrainte forte est le délai de prise en charge par les personnes compétentes disposant des moyens ad hoc. Ce délai est d'autant plus bref qu'il se décompte parfois en minutes, comme dans le cas d'évènement sur les réseaux sociaux, média typique de l'Entreprise étendue dans la période actuelle. En ce sens, la gestion de crise fait souvent suite à une gestion d'alerte, ou bien elle en est le point culminant.

Si on définit la crise par l'existence d'une situation inattendue avec des conséquences potentiellement graves, la gestion de la crise et la communication de crise doivent s'entendre aussi pour des faits qui surviendraient dans les extensions de l'entreprise, la concernant peut-être même de manière indirecte. La crise sanitaire mondiale de 2020 et ses conséquences économiques et sociales prolongées démontrent la nécessité pour les entreprises de se préparer à tout type de crise, quelle qu'en soit la nature, même éloignée du coeur d'activité. Il ne s'agit plus seulement de poursuivre ou reprendre l'activité, mais bien de maintenir l'entreprise en vie.

Classiquement, la cellule de crise se compose de deux niveaux :

- Le décisionnel, dont les membres permanents appartiennent à la Direction Générale ou aux métiers concernés par la crise, chargé du pilotage global, prend les décisions et gère la communication de crise vers les médias ;
- L'opérationnel, composé des coordinateurs et experts métiers, collecte les informations, analyse la situation, propose des solutions et pilote les actions sur le terrain.

Dans le cas de crises liées à des risques de l'Entreprise étendue, leur particularité est liée à l'implication potentielle de parties prenantes, et au caractère imprévisible et par définition inhabituel de la nature de la crise. Ce sont cependant le plus souvent les directions opérationnelles qui sont chargées de répondre à ces spécificités de l'Entreprise étendue au travers de la cellule de crise par :

- La capacité à capter toutes les informations pertinentes dans l'environnement du risque, c'est-à-dire dans des lieux, organisations, … qui ne sont pas de la compétence ou du droit d'information ou d'intervention de l'entreprise ;
- La capacité à diffuser toutes les informations nécessaires auprès des acteurs concernés, dont en particulier :
  - Les acteurs « pompiers » externes ;
  - Les acteurs « victimes » externes ;
- L'efficacité de la communication vers les acteurs concernés.

Comment organiser une cellule de crise vis-à-vis d'un risque de l'Entreprise étendue au-delà des standards ? Quelles particularités peut-on mettre en place ? Quelques suggestions peuvent être utiles :

- Avoir une procédure de déploiement de la gestion de crise qui tienne compte du type de risque (critères d'activation de la cellule de crise à tester) et des caractéristiques éventuellement « Entreprise étendue » de la crise ; si l'évènement est géographiquement éloigné, sur des sites difficilement accessibles, avec un décalage horaire important, des différences de langage, ...
- Envisager au cas par cas d'intégrer des représentants des parties prenantes externes à la cellule de crise ;
- Prévoir une activation rapide de la cellule de crise (en moins d'une heure, voire en quelques minutes), des exemples existent dans les secteurs de la banque et l'assurance, où la cellule surveillance réseaux sociaux est autorisée à interpeller directement la Direction Générale dans un délai de cinq minutes ;
- Éviter de trop focaliser sur le coeur d'activités et d'être dès lors restrictif dans la définition des critères et des délais de déclenchement, du périmètre d'action, des pouvoirs de décision et des moyens alloués ;
- Recourir à des experts de la communication de crise vers les médias, et les réseaux sociaux en particulier, afin de répondre aux conséquences sur l'image ;
- Connaître dans les cas de partenariats étroits (consortium, R&D intégrée) :
  - Les critères d'activation des cellules de crise des partenaires
  - Les conditions de collaboration sur la crise
- Savoir interpréter les contextes réglementaires et légaux pour comprendre et piloter les limites de responsabilités ;
- S'être entrainé collectivement le mieux possible au moyen d'exercices de simulation de crise impliquant toute l'entreprise, y compris les dirigeants ;
- …

Enfin, pendant la gestion de la crise, lorsque l'attention de l'entreprise est concentrée sur l'urgence de la situation, l'une des missions du risk manager est de combattre l'effet de halo, afin de ne pas baisser la garde sur les autres risques. Leur survenance serait un facteur aggravant potentiellement destructeur sur une organisation déjà affaiblie par ailleurs.

3.4.4 Utiliser des outils

Traiter les risques de l'Entreprise étendue nécessite l'utilisation d'outils pour permettre une coordination avec des acteurs tiers, être performant dans le Risk management et pertinent dans les prises de décision. Les outils et moyens listés ci-après servent principalement au traitement des risques et pour certains aussi à l'identification et l'évaluation.

● Due diligence

Pour mémoire, la *Due diligence*, ou diligence raisonnable, est une action de vérification avant une prise de décision importante initiale ou renouvelée, portant sur un périmètre nouveau ou en évolution (pour une acquisition, la signature d'un contrat de partenariat, …).

Une *Due diligence* peut adresser différents axes d'étude : la stratégie, l'environnement (au sens écologie), l'informatique, le légal, le fiscal, le social, le financier, … et tout autre axe métier de l'entreprise étudiée.

Par définition, la *Due diligence* est donc un outil d'analyse des risques de l'Entreprise étendue puisqu'elle couvre, d'une part, une situation de prise de décision avec un acteur hors du périmètre des opérations de l'entreprise et, d'autre part, des thématiques pouvant concerner des acteurs indirects comme des ONG ou des autorités de tutelle.

A titre d'exemple, la *Due diligence* est un procédé obligatoire en application des lois Sapin 2 et devoir de vigilance sur les champs restreints que ces textes définissent.

- Screening

Les outils de *screening* (ou filtrage, dépistage, sélection, projection) s'appliquent à de multiples domaines, comme le médical, l'environnemental (pollution, etc..), le comportemental, les addictions, le financier, les conformités, la vigilance, …

Dans le cadre des risques de l'Entreprise étendue, il y a un intérêt majeur pour permettre de détecter les risques externes, même à partir de signaux faibles. Les données peuvent être aussi bien celles issues du big data que de questionnaires particuliers.

Par ailleurs, il existe des bases de données permettant de réaliser des screening des tiers sur des thématiques particulières comme la corruption ou la lutte anti-blanchiment.

- TPRM (Third Party Risk Management)

La gestion des risques liés aux tiers est d'évidence partie intégrante des risques de l'Entreprise étendue.

Un outil TPRM utilisera avec intérêt les informations des logiciels de gestion de l'entreprise avec des résultats plus pertinents dans le cas d'un Progiciel de Gestion Intégrée ou ERP (*Enterprise Resource Planning*). Par exemple, un indicateur sur une augmentation des retards de livraisons des fournisseurs peut alerter sur un risque de rupture d'approvisionnement.

Le TPRM est également à relier ou à intégrer à d'autres outils comme les outils d'étude des médias et des réseaux sociaux, ou les outils de screening. Ces outils permettent de suivre la relation avec le tiers durant toute la vie du contrat depuis sa sélection et la signature de la relation contractuelle jusqu'à sa fin. Ils sont clés pour suivre les alertes et les actions mises en place par les tiers.

Un outil de Gestion de la Relation Clients (GRC ou CRM – Customer Relationship Management) peut s'avérer précieux lui aussi, et apporter une vision de l'évolution de la satisfaction client, et donc des risques associés, comme par exemple un écho négatif sur les réseaux sociaux.

- Indicateurs de performance (KPI), risque (KRI), contrôle (KCI)

Ces Indicateurs permettent d'apprécier l'efficacité de l'entreprise en termes de performances opérationnelles et financières (*KPI – Key Performance Indicator*), de maîtrise des risques (*KRI - Key Risk Indicator*) et d'efficacité voire d'efficience des contrôles vis-à-vis des objectifs fixés (*KCI - Key Control Indicator*). Ils sont des mesures et des détections de signaux, issues des outils opérationnels de l'entreprise ou d'outils d'analyse ou d'alerte sur l'environnement (réseaux sociaux, piratages informatiques, changement de réglementation, application d'une réglementation hors territoire, …).

Dans le cas des risques externes, ils doivent être des sources d'alertes sur des signaux faibles, par exemple. Ce peut être le résultat de sondages clients réguliers sur la concurrence, ou la surveillance médiatique sur le comportement social dans un pays.

La production de ces indicateurs doit être outillée, intégrée autant que possible au Système d'Informations de l'entreprise ou aux outils de Screening, TPRM, GRC (Gouvernance, risque et Conformité), …

- SIGR (Système d'Information et de Gestion des Risques)

Par définition, un SIGR est global. Il couvre donc naturellement les risques de l'Entreprise étendue et intègre parfois des outils de TPRM ou de quantification.

Les attentes sont généralement de :

- Référencer les acteurs de l'Entreprise étendue ;
- Identifier des risques comme étant du périmètre de l'Entreprise étendue ;
- Extraire les informations liées au périmètre de l'Entreprise étendue ;
- Pouvoir établir une vision globale à des fins d'interprétation et de reporting ;
- Piloter les traitements des risques en permettant de coordonner les acteurs de l'écosystème ;
- Désigner un responsable du suivi et du traitement de ces risques.

Typiquement, ces attentes sont réalisables par un paramétrage des informations concernées (acteurs, natures de risques, …), par une gestion claire des accès et des rôles pour chacun des acteurs internes et externes, et au moyen d'outils d'analyse ou d'extraction de la base de données du SIGR qui puissent permettre de cibler les informations concernées.

Une autre attente est de permettre la collecte des informations concernant les risques de l'Entreprise étendue depuis tous les utilisateurs internes concernés. Cette attente n'est pas spécifique à l'approche des risques de l'Entreprise étendue, mais est particulièrement importante pour elle. En

effet, la rapidité et la qualité de la communication est un facteur clé de la prévention et la résolution de ces risques.

Les outils de qualification et de quantification n'ont pas besoin d'être adaptés, la gestion des risques de l'Entreprise étendue devant être intégrée à celle de tous les risques de l'entreprise.

● Outils de quantification

Comme vu lors de l'étape d'appréciation de la criticité à la section 3.3 « Décider des risques à traiter », les risques de l'Entreprise étendue sont souvent sous-estimés du fait de leur origine indirecte, hors du périmètre opérationnel classique de l'entreprise, et aussi pour cause du calcul habituel dégradant la criticité. Avoir une estimation réaliste des critères servant à l'évaluation de la criticité (probabilité, Gravité, détectabilité et maîtrise) avec une formule de calcul reflétant sa juste valeur est donc essentiel pour ne pas ignorer ces risques et les traiter correctement.

Si la quantification est un moyen pertinent pour avoir une appréciation réaliste de la criticité, elle est souvent jugée difficile à mettre en oeuvre. Des appréciations qualitatives s'y substituent dès lors par défaut, trop souvent à tort car sujettes à des biais cognitifs. Or la formule habituelle de calcul de la criticité (= probabilité x impact), relativement intuitive et facile à comprendre, conduit à des biais d'appréciation, d'une part du fait d'une sous-estimation et, d'autre part, du fait de sa symétrie. Avec cette formule, nombre de risques externes peuvent être ignorés, voire disparaître des radars. Il est possible d'approfondir pour affiner l'estimation des scénarios et des alternatives existent (cf. Annexe 8 « Quantification : faciliter l'appréciation »).

Pour l'Entreprise étendue, l'éloignement du risque induit aussi une perception de difficulté à capter les données de quantification. Or, même pour les approches comportementales de clients en B2C (marchés directs consommateur final), il existe des moyens de quantification des comportements et des attentes des acteurs, par exemple par l'analyse de sémantiques dans les réseaux sociaux, outil de modélisation devenu relativement classique aujourd'hui. Dans le secteur de l'assurance et de la banque, les quantifications des risques sont basées sur des modélisations depuis des décennies. A l'aide de données opérationnelles, qui sont disponibles en très grande quantité, des modèles sont construits, structurés par les critères significatifs de leurs métiers. Plus généralement, suivant les métiers de son entreprise et les données collectées, le risk manager pourra construire des modèles ad hoc.

Comme la capacité de prédiction des modèles dépend de la quantité et de la qualité des données et que, dans beaucoup de métiers, les données ne sont pas accessibles en grand nombre, voici pour tous les risques, et en particulier pour ceux de l'Entreprise étendue, une méthodologie pratique pour faciliter les quantifications et les rendre pertinentes :

- Utiliser des critères de quantification reposant sur des unités d'oeuvre accessibles :
  - Poids et volumes de matières premières ;
  - Nombre de colis attendus par période ;
  - Stocks nécessaires pour compenser un défaut temporaire d'approvisionnement ;
  - …
- Abandonner l'habitude de rechercher une évaluation « exacte » en quantifiant ; pour une prise de décision, la comparaison d'ordres de grandeur est généralement suffisante ;
- Demander en conséquence aux opérationnels ou experts concernés l'encadrement du « meilleur estimé » par un « minimum » et un « maximum » ; cet encadrement apporte deux avantages : d'une part, le travail nécessaire pour quantifier est alors allégé et plus rapide, et, d'autre part, si l'encadrement est très large, c'est un indicateur pour provoquer une étude complémentaire d'affinement de l'estimation ;
- Evaluer les montants financiers à partir des estimations opérationnelles précédentes, des coûts unitaires des objets et des cours de change, ces deux critères étant également estimés avec l'approche « minimum, meilleur estimé, maximum » ;
- Réaliser un benchmarking opérationnel afin de quantifier des parts de marché, des segments de population, des attributs de produits, … ;
- Estimer les probabilités :
  - En s'appuyant notamment sur la fréquence d'occurrence du risque (nombre d'évènements constatés sur une période passée),
  - En projetant les tendances sur une période future,

Ces informations sont souvent accessibles en externe au travers de divers médias.

Il est connu que faire simple en ergonomie dans un système d'information est toujours compliqué en algorithmie, ou faire simple pour un client est toujours compliqué en *back office*. Il est en de même pour la quantification de la criticité. Commettre une erreur en appréciant la criticité aura souvent plus de conséquences s'agissant de risques externes, car on a tendance à sous-estimer leur probabilité. On les évaluera alors peut-être à tort en cygnes noirs ou évènements peu probables.

Par ailleurs, pour focaliser sur les risques rares à fort impact il peut

s'avérer utile de mettre en place un mode de calcul adapté afin qu'ils apparaissent dans la cartographie, le cas échéant avec un zoom sur des sujets particuliers (climat, pandémie, …).

Une difficulté ressentie dans la quantification est aussi la multiplicité et la complexité des liens entre les objets à évaluer, par exemple pour le respect des échéances d'un projet. Le risque sur des échéances peut provenir de causes externes, comme des intempéries, des grèves, des défaillances de synchronisation entre acteurs, lesquelles ne peuvent être ignorées pour estimer la faisabilité d'un projet, d'une commande client, ...

La recherche des scénarios est alors aussi une aide à la compréhension des possibles et donc des conséquences, permettant de mieux définir et évaluer les plans d'actions préventifs et curatifs. Le danger est d'aboutir à une profusion de scénarios, ce qui est difficilement gérable, voire inexploitable et il importe de ne pas confondre scénarios et variantes. Des éléments mineurs ou des incertitudes sur des valeurs constitueront en général des variantes, les scénarios étant basés sur des éléments discriminants ou incompatibles.

Dans le cas des risques de l'Entreprise étendue, la méthode Monte-Carlo permet d'éviter des analyses lourdes sur des scénarios complexes assortis de variantes portant sur des objets hors du périmètre opérationnel classique. Il est aussi possible de considérer des scénarii du pire.

● Autres moyens

Suivant les spécificités de l'entreprise, comme nous l'avons déjà mentionné, d'autres moyens génériques peuvent être mis en oeuvre pour l'analyse des risques de l'Entreprise étendue et la prise de décision de plans d'actions, plus adaptés à ses métiers, ses activités, ses natures de partenariats, ...tels que :

- Analyse des marchés de l'entreprise ;
- Veille concurrentielle ;
- Analyse des relations avec les tiers ;
- Analyse du CRM (Customer Relationship Management) ;
- Analyse de contrats ;
- Analyse des réglementations et de leurs évolutions ;
- Gestion des incidents avec des tiers ;
- Veille et gestion de la réglementation.

Certains de ces moyens peuvent faire l'objet de modules dédiés de certains SIGR.

Il appartient à chaque entreprise, dans son contexte, d'en estimer la pertinence. Tous ces outils sont de plus en plus basés sur des algorithmes puissants de traitement des données (*data analytics* voire intelligence artificielle) aptes à traiter des informations en masse (ou *big data*).

3.4.5 Outils du futur : s'approprier l'intelligence artificielle

L'intelligence artificielle est une évolution, voire une révolution, de l'informatique, aujourd'hui appelé le numérique ou *digital* en anglais. Elle repose essentiellement d'une part sur l'algorithmique, et, d'autre part, sur le big data. Au travers des résultats qu'elle produit, elle s'intègre naturellement aux prises de décisions, et donc comme outil de gestion des risques de l'Entreprise étendue.

L'intelligence artificielle est cependant peu maîtrisée en général par les entreprises, voire mal maîtrisée par ses créateurs (absence de traçabilité, …). Par nature, l'apparition de l'intelligence artificielle est aussi un phénomène externe appartenant au périmètre des risques de l'Entreprise étendue (cf. Annexe 5 « risques de l'Intelligence Artificielle »).

● De l'informatique au numérique

La technologie s'est tout d'abord affirmée au service de la production et de la création de valeur par le développement des infrastructures et des paysages applicatifs internes.

Il s'agissait de soutenir et rentabiliser les processus de l'entreprise, opérationnels ou fonctionnels, et également d'être en mesure d'apporter aux décisionnaires, actionnaires, régulateurs, ou encore aux marchés, le niveau d'information pertinent.

L'ère internet et la mise en réseau des informations ont ensuite décuplé les capacités de partage d'information, l'instantanéité et l'interopérabilité. Les techniques de communication (bureautique, messageries instantanées ou non, téléphonie, systèmes de téléconférence ou visio-conférence), les outils de collaboration (réseaux, fichiers partagés, applicatifs ou logiciels collaboratifs…), offrent de nouvelles possibilités d'automatisation du traitement des risques, et ce de façon exponentielle.

L'un des exemples le plus révélateur pour appréhender cette interopérabilité qu'offre la technologie numérique nous est proposé par une entreprise du secteur aéronautique. Souvent cité en exemple, le principe d'ingénierie système collaborative (maquette numérique commune) intègre l'ensemble des parties prenantes constituantes d'un projet ou d'un processus. Dans cette Entreprise étendue, l'objectif est durable : permettre une collaboration plus étroite avec une entreprise partenaire, acteur clé de son écosystème, et permettre à l'ensemble des fournisseurs d'un programme d'accéder, de manière ponctuelle ou sur le long-terme, à cet environnement de

production virtuel commun. L'organisation industrielle s'est ouverte à chaque composante de son écosystème, matérialisant de fait le concept d'Entreprise étendue.

Tous ces sujets autour des évolutions du numérique sont de plus en plus des sources de risques pour l'entreprise et son écosystème.

● La montée en puissance de l'intelligence artificielle

L'intelligence artificielle a de facto progressivement envahi la vie de l'entreprise en moins d'une décennie. Elle est a priori applicable au périmètre étendu de l'entreprise, à considérer suivant deux axes, en tant que :

- Outil de l'Entreprise étendue ;
- Statut éventuel de personnalité juridique (cf. Annexe 5 « risques de l'Intelligence Artificielle »).

L'intelligence artificielle est une approche de type scientifique. Comme ses algorithmes ne sont pas « explicables » simplement et que les résultats ne sont pas (actuellement) traçables, elle est souvent considérée comme une « boîte noire », avec des éléments d'entrée et des éléments de sortie mais sans grande visibilité sur son fonctionnement intérieur. Son utilisation induit donc des risques potentiellement significatifs, difficile à évaluer et maîtriser.

● L'intelligence artificielle comme outil au service de la gestion des risques

Les risk managers vont vraisemblablement devoir acquérir les compétences nécessaires et les moyens pour comprendre les recommandations d'identification et de traitement des risques produites par l'intelligence artificielle. Il leur faudra savoir les interpréter pour assurer la pertinence des analyses qu'ils déduiront de ces informations.

La mise en oeuvre d'outils intelligence artificielle dans la gestion et le traitement des risques nécessite de :

- S'assurer de la pertinence, de la qualité et de la fiabilité des données, notamment les données de masse (big data) qui peuvent être d'origine externe ;
- Faire évoluer certains processus concernant la gestion des risques en y intégrant ceux de l'intelligence artificielle, afin de mieux prendre en compte les informations de contexte ;
- Valider pour ce faire les algorithmes mis en place, impliquant des processus et des données externes ;
- Faire évoluer la culture et les compétences des personnels concernés, pour une utilisation pertinente et efficace, surtout pour les risques de l'Entreprise étendue qui sont par définition éloignés.

Des secteurs comme l'assurance et la finance utilisent beaucoup les données de masse (big data), comme des matières premières facilitant la mise en place de moteurs de règles, mais surtout d'aide à la décision avec l'intelligence artificielle, en particulier via le *machine learning*.

Très généralement, l'intelligence artificielle pourra par exemple servir à contrôler le formalisme réglementaire et le respect des lois en facilitant la mise en oeuvre dans tous les secteurs. Pour la gestion des risques opérationnels, de plus en plus de progiciels et de plateformes utilisent déjà l'intelligence artificielle afin de créer des alertes, aider à la prévention, évaluer les risques, voire proposer des actions correctives.

L'existant et le potentiel des apports de l'intelligence artificielle, et sa corrélation croissante avec les parties prenantes des entreprises, montrent qu'elle est un outil incontournable du futur de la gestion des risques, outil qui doit être maîtrisé pour être utilisé valablement.

Dans ce domaine de l'intelligence artificielle, l'Union Européenne préconise une approche basée sur les risques ; elle a déjà publié ses recommandations qui se traduiront à terme par un règlement européen. (*)

● Recourir à des centres d'excellence ERM

Pour beaucoup d'organisations dont la taille est insuffisante pour disposer d'une fonction interne dédiée au Risk management, la question de l'externalisation se pose. Que l'on considère les risques de l'Entreprise étendue ou non, le choix dépend de critères similaires (expertise, professionnalisme, coût, confidentialité …).

Selon une étude du cabinet Deloitte "US-risk-Extended-Enterprise-Risk-Management 2017" : "Choisir entre des modèles 'EERM' internes centralisés et un modèle de 'prestations de services EERM supervisés' réalisées par un tiers est une décision vitale qui peut avoir des conséquences importantes et à long terme pour l'entreprise, et doit donc être soigneusement étudiée ».

L'étude conclut que les organisations qui recourent à une fonction interne centralisée sont, à cet égard, principalement motivées par la nécessité de conserver le contrôle organisationnel sur cette activité critique qu'est le Risk management. L'étude relève cependant qu'opter pour un service sous-traité permet à une organisation d'atteindre le niveau de personnalisation souhaité dans chacune de ses entités pour un coût moindre par rapport à la gestion d'une équipe interne.

(*) cf. Annexe 12 « Bibliographie » Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence

Enfin l'étude souligne que les centres d'excellence aussi bien que les modèles de services sous-traités présentent les mêmes avantages :

- Etablir des principes cohérents, définir des processus uniformes et mettre en oeuvre une technologie commune dans toutes les unités de l'entreprise avec une cible stratégique à long terme ;
- Fournir des formations ;
- Réaliser des évaluations de risques ;
- Proposer des orientations.

La direction de l'entreprise conserve la responsabilité de la gestion des risques et de la prise de décision.

Il revient à chaque entreprise de mettre en place l'une ou l'autre organisation, ou un mixte des deux, en fonction de ses moyens et de ses spécificités, en choisissant le dispositif le plus approprié à son contexte. Par exemple, dans les grandes entreprises, le centre d'excellence ERM peut prendre la forme d'un centre de services partagés. La présence, en interne ou en externe, des compétences expertes utiles sera un critère essentiel dans ce choix organisationnel.

Capitaliser

Capitaliser est essentiel pour la vie de l'entreprise. Ce processus permanent valorise les expériences, permettant de créer des bonnes pratiques nécessaires au développement ou à la pérennité de l'entreprise. Dans le cadre de l'Entreprise étendue, capitaliser est d'autant plus important que les risques dont il est question sont souvent hors des processus habituels, éloignés des habitudes culturelles et du coeur d'activité.

Si la capitalisation de l'expérience est innée chez l'être humain, elle est moins naturelle pour un organisme acteur économique et doit faire l'objet de beaucoup plus d'attentions si l'on considère l'organisme de manière large. Les analyses dites de retours d'expériences, les leçons apprises figurent encore souvent parmi les activités que l'on va sélectionner et faire disparaître dans les plans d'économies ou que l'on va reporter sine die du fait d'autres urgences et d'une priorisation excessive accordée au court terme.

Au-delà d'éviter la récurrence des risques, la capitalisation permet aussi de découvrir des opportunités. Or le thème des opportunités est familier au risk manager, qui conserve parmi ses idéaux dans le traitement du risque, la possibilité de transformer le risque en opportunité, ou au moins d'explorer les opportunités qui lui sont liées, ce qui est plus fréquemment possible que ce qu'on imagine couramment.

Concernant les risques de l'Entreprise étendue, la nouveauté est que plusieurs facteurs sociétaux provoquent aujourd'hui un intérêt intellectuel et l'action du législateur, ce qui encourage et favorise la mise en place d'un processus de capitalisation. Comme nous l'avons évoqué dans cet ouvrage, des lois récentes à portée étendue sont apparues, sur les aspects éthiques, humains et environnementaux, et en particulier sur ce qui a trait au numérique avec un règlement européen. La plupart de ces textes visent à protéger l'individu, le citoyen, dans une société de plus en plus intolérante au risque. Indéniablement, cela pousse les organismes à instaurer une boucle vertueuse d'amélioration dont les retours d'expériences font partie.

Pour capitaliser au mieux et réellement améliorer l'efficacité du management des risques, l'Entreprise étendue devra intégrer à leur réflexion des axes d'amélioration continue tels que :

- Le périmètre réel de l'Entreprise étendue (détermination et surveillance de son évolution) ;
- Les tiers et parties prenantes (identification, relations contractuelles, liens de dépendance amont/aval, interactions, ...) ;
- La communication avec les tiers et parties prenantes (timing, contenus, méthodes, ...) ;
- La performance (évolutions technologiques et numériques, résultats obtenus).

Personnaliser l'approche Entreprise étendue

Nous avons établi au fil de notre propos combien le sujet des risques de l'Entreprise étendue était complexe. De la difficulté à identifier le véritable périmètre de l'Entreprise étendue au-delà de ses propres murs, à la complexité des liens de natures diverses, pas toujours contractuels, dont l'Entreprise étendue n'a parfois même pas conscience, l'univers est extrêmement mouvant.

Si nous considérons autant les risques subis du fait des extensions de l'entreprise que les risques créés aux extensions des autres acteurs de la sphère d'influence (cf. figure n°1 « Sphère de l'Entreprise étendue), nous pouvons retenir trois idées fortes :

- La compréhension des objectifs propres des tiers et des parties prenantes ;
- La mesure de l'impact des différents risques identifiés, sur l'Entreprise étendue et sur ses parties prenantes, par la préparation de la matrice de double matérialité ;
- La capacité présumée de réaction de l'entreprise afin de s'adapter à son environnement.

Au global, l'approche risques de l'Entreprise étendue vise à préserver, développer, renforcer la confiance réciproque entre l'entreprise et son écosystème. Cela forme une source potentielle de création de valeur pour l'entreprise comme pour toutes ses parties prenantes. Cette approche se résume aussi en recommandations clés présentées dans le tableau ci-contre :

Recommandations clés

Connaître parfaitement l'écosystème de l'entreprise, à tout moment
- Approche systémique ;
- Vision 360° (multicouches) ;
- …

Mettre en place et maintenir une veille élargie
- Politiques gouvernementales ;
- Règlementations et normes (techniques, fiscale, juridiques…) ;
- …

Lister les parties prenantes de façon exhaustive et les analyser
- Cas de dépendance (économique, financière, technologique) ;
- Éléments constitutifs de l'Entreprise étendue (directs et indirects) ;
- Relations (dialogues, échanges, contrats, …) ;
- …

Identifier les nouveaux modèles
- Évolutions des acteurs de l'écosystème ;
- Disruptions technologiques ;
- …

Cartographier les risques sur un périmètre élargi
- Risques subis par l'entreprise ;
- Risques créés sur les tiers ;
- …

Détecter les signaux faibles
- Surveillance les réseaux sociaux ;
- Vigilance sur les tendances d'évolutions (sociétales, environnementales, …) ;
- …

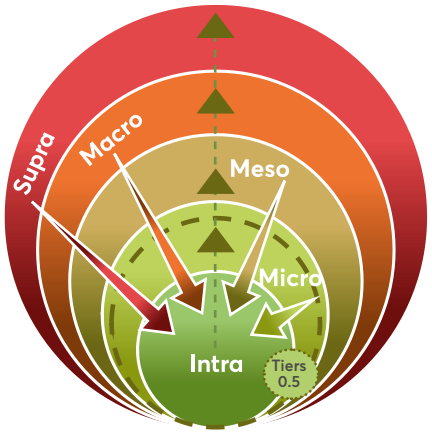
Sensibiliser et former son personnel
- Culture du risque au sens large ;
- Conscience des biais cognitifs ;
- …

Disposer d'une cellule de crise
- Responsables désignés et connus ;
- Procédures établies ;
- Dispositifs d'alerte ;
- …

Superviser sa chaîne de valeur (partie « amont » et partie « aval »)
- Sécurité dès la conception (security by design) ;
- Chartes éthiques ;
- Audits ;
- …

Maîtriser l'univers des systèmes d'information de l'entreprise
- Bonnes pratiques d'hygiène informatique ;
- Produits et services labellisés et certifiés ;
- Processus d'évolutions ;
- …

Adapter sa couverture d'assurance
- Contrats spécifiques ;
- Cascades de contrats ;
- ….



Supra : Institutions et organisations supranationales, finances, affaires et géopolitique mondiale

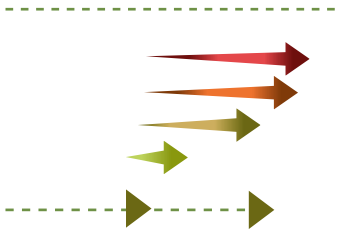
Macro : Acteurs politiques, économiques, sociologiques, technologiques, écologiques et légaux pouvant influencer l'entreprise

Meso : Acteurs et parties prenantes non institutionnels pouvant influencer l'entreprise ; jeux visibles et invisibles

Micro : Acteurs de la chaine de valeur, la topographie concurrentielle, les règles sectorielles

Intra : Activités de l'entreprise, ses ressources, ses actifs, ses avoirs, ses processus, son organisation et son histoire

Légende



A un stade avancé de son évolution l'entreprise peut être en « réseau » ou « intégrée » avec certains acteurs (clients, fournisseurs, partenaires).

L'entreprise, sans le savoir, se trouve exposée à des pressions ou des menaces provenant des univers entourant son périmètre intra.

L'entreprise, involontairement, peut se retrouver mise en cause par des acteurs de son écosystème pour des risques qu'elle provoque hors de son périmètre intra.

Figure 21 – Flux entre l'entreprise et ses parties prenantes

Notre objectif dans cet ouvrage est de vous apporter des idées, de la matière première, afin d'établir votre propre réflexion, de déterminer le périmètre étendu de votre entreprise et de mettre en place la gestion appropriée des risques qui en dépendent. Quelques bonnes pratiques essentielles seront applicables dans la plupart des organisations souhaitant lancer une réflexion sur les risques de l'Entreprise étendue (cf. « Recommandations clé »).

Votre périmètre est à coup sûr différent de celui d'une autre entreprise, tant la culture, l'histoire, le fonctionnement et les relations de votre Entreprise étendue sont des facteurs déterminants dans la réflexion sur les risques qui y sont liés. Vous y rencontrerez aussi les obstacles habituels de la gestion des risques et notamment de nombreux biais cognitifs, lesquels n'étaient pas au centre de notre propos malgré leur importance et mériteraient un développement propre. De toute évidence, votre gestion des risques doit être unique, personnalisée, tant elle dépend elle aussi de la nature des flux entre l'entreprise et son environnement (cf. figure 21 « Flux entre l'entreprise et ses parties prenantes ») et de la prise en compte de toutes ces dimensions par les équipes dirigeantes.

Nous espérons être parvenus à vous aider, sur ce sujet qui est devenu une composante primordiale du métier de l'Enterprise Risk Management.

Annexe 1 – Glossaire

Ce glossaire est constitué d'extraits de définitions de l'AMRAE, du COSO, du cabinet Deloitte, de l'IFACI, de la DFCG et de l'ISO 31000, donnant ainsi une représentation de l'étendue des sémantiques pratiquées.

Les mots ou expressions figurant au glossaire sont matérialisés, dans le texte, par une police épaisse lors de leur première occurrence.

Ces termes sont :

- Appétence aux risques (goût du risque)
- Audit interne / Audit de Management des risques / Surveillance (des risques)
- Cartographie des risques
- Conséquence
- Contrôle interne
- Criticité
- Evènement
- Management des risques / gestion des risques / ERM
- Impacts
- Indicateur clé / Key Risk Indicator (KRI)
- Partie prenante
- Probabilité / Fréquence (Vraisemblance)
- Risque
- Risk Manager / Gestionnaire des risques
- Traitement du risque

Appétence aux risques (goût du Risque)	
AMRAE	Niveau de risque auquel l'organisation est prête à s'exposer dans le cadre de sa mission ou de sa vision.
COSO	Les types et la quantité de risques, à un large niveau, qu'une organisation est prête à accepter dans la poursuite de la valeur. Il reflète la philosophie de gestion des risques de l'entité et influe à son tour sur la culture et le style de fonctionnement de l'entité (traduction de *Risk Appetite*).
ISO 31000	Goût du risque : Importance et type de risque qu'un organisme est prêt à saisir ou à préserver ou de risque qu'il est prêt à prendre. Aversion pour le risque : attitude de rejet du risque.
Deloitte	Niveaux de risques acceptables et souhaités pour atteindre les objectifs de performance et développement de l'Entreprise étendue. L'appétence au risque est une donnée que la Direction prend en considération lorsqu'elle évalue les différentes options stratégiques, détermine les objectifs associés et développe le dispositif pour gérer les risques correspondants.
Audit interne / Audit du Management des risques / Surveillance (des risques)	
AMRAE	Activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée.
ISO 31000	Surveillance : vérification, supervision, observation critique ou détermination de l'état afin d'identifier continûment des changements par rapport au niveau de performance exigé ou attendu Note : La surveillance peut s'appliquer à un cadre organisationnel de Management du risque (2.3), un processus de Management du risque (2.10), un risque (2.1) ou un moyen de maîtrise (2.28) du risque.
Deloitte	Activité exercée de manière indépendante et objective qui donne une assurance sur le degré de maîtrise des activités de l'organisation. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernement d'Entreprise étendue, et en faisant des propositions pour renforcer leur efficacité.
Cartographie des risques	
COSO & AMRAE	La cartographie des risques est une représentation synthétique et globale des risques hiérarchisés selon les critères de l'Entreprise étendue. Elle permet d'établir un état des lieux à un instant T des différents risques avérés ou potentiels que pourrait supporter ou supporte l'Entreprise étendue.
Deloitte	Exercice faisant partie du système de gestion des risques de la société ayant pour but de recenser, d'identifier, d'évaluer et de hiérarchiser les risques afin de les prioriser et de fournir une vision d'ensemble des risques de l'organisation aux décideurs. La cartographie des risques est une photographie à un instant T des risques d'une organisation.
Conséquence	
ISO 31000 & AMRAE	Effet d'un évènement affectant les objectifs. Note 1 : Un évènement peut engendrer une série de conséquences. Note 2 : Une conséquence peut être certaine ou incertaine et peut avoir des effets positifs ou négatifs sur l'atteinte des objectifs. Note 3 : Les conséquences peuvent être exprimées de façon qualitative ou quantitative. Note 4 : Des conséquences initiales peuvent déclencher des réactions en chaîne.

Contrôle interne	
AMRAE	Processus mis en œuvre par le Conseil d'administration, les dirigeants et le personnel d'une organisation. Il permet de fournir une assurance raisonnable quant à la réalisation d'objectifs fixés afin de réalisation et d'optimisation des opérations, de fiabilité des informations financières et de conformité aux lois et aux réglementations en vigueur. Le contrôle interne contribue au suivi de chacun des risques, une fois les plans d'action mis en œuvre.
COSO	Processus, mis en oeuvre par le conseil d'administration, la direction et les autres membres du personnel de l'entité, conçu pour fournir une assurance raisonnable quant à la réalisation des objectifs, opérations, rapports et conformité (traduction de « Internal Control »).
Deloitte	Le contrôle interne est un dispositif de l'organisation, défini et mis en oeuvre sous sa responsabilité. Il comprend un ensemble de moyens, de comportements, de procédures et d'actions adaptés aux caractéristiques propres de chaque organisation qui : • contribue à la maîtrise de ses activités, à l'efficacité de ses opérations et à l'utilisation efficiente de ses ressources, et • doit lui permettre de prendre en compte de manière appropriée les risques significatifs, qu'ils soient opérationnels, financiers ou de conformité.
Criticité	
Deloitte / IFACI / DFCG	Criticité : perception de l'importance du risque en termes d'impact et de possibilité d'occurrence (plus critique = préoccupation majeure actuelle) - Conférence IFACI DFCG Deloitte - état de l'Art de la Gestion des risques - 2017
ISO 31000	Pour l'analyse AMDEC, l'équipe chargée de l'étude classe chacun des modes de défaillance identifiés en fonction de sa criticité. Plusieurs méthodes de criticité différentes peuvent être utilisées. La matrice Conséquence/vraisemblance qualitative, semi-quantitative ou quantitative (B.10.3) ou l'utilisation d'un degré de priorité du risque (RPN) sont les méthodes les plus fréquemment utilisées. Une mesure quantitative de la criticité peut également être dérivée des taux de défaillance réels et d'une mesure quantitative des conséquences lorsque ceux-ci sont connus.
AMDEC	AMDEC signifie Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité La criticité est un paramètre essentiel pour compléter la portée de l'analyse de risques et obtenir ainsi un véritable instrument d'aide à la décision. La criticité est le produit de ces trois évaluations : • la gravité potentielle sur une échelle de 1 à 4 (de mineure à gravissime), • la fréquence estimée sur une échelle de 1 à 4 (exceptionnelle à certain), • la capacité de détection sur une échelle de 1 à 4 (Evident à indétectable).
Evènement	
COSO	Les évènements peuvent avoir un impact positif, négatif ou les deux à la fois. Les évènements ayant un impact négatif sont des risques pouvant freiner la création de valeur ou détruire la valeur existante. En revanche, les évènements ayant un impact positif peuvent contrebalancer des impacts négatifs des risques ou constituer des opportunités.
ISO 31000	Occurrence ou changement d'un ensemble particulier de circonstances Note 1 : Un évènement peut être unique ou se reproduire et peut avoir plusieurs causes. Note 2 : Un évènement peut consister en quelque chose qui ne se produit pas. Note 3 : Un évènement peut parfois être qualifié « d'incident » ou « d'accident ». Note 4 : Un évènement sans conséquences peut également être appelé « quasi-accident » ou « incident » ou « presque succès ».

Annexe 1

Management des risques / gestion des risques / ERM	
AMRAE	Processus itératif d'identification, d'évaluation et de hiérarchisation des risques qui facilite la mise en place d'outils de contrôle et d'optimisation de l'activité afin d'atteindre les objectifs fixés dans le cadre de la stratégie de l'Entreprise étendue ou de l'entreprise Martin. Le management des risques (ERM) vise à être global et doit couvrir l'ensemble des activités, processus et actifs de l'organisation. Il s'agit d'un dispositif dynamique de l'organisation, défini et mis en oeuvre sous sa responsabilité. Le management des risques comprend un ensemble de moyens, de comportements, de procédures et d'actions adaptés aux caractéristiques de chaque organisation qui permet aux dirigeants de maintenir les risques à un niveau acceptable pour l'organisation.
COSO	Le management des risques traite des risques et des opportunités ayant une incidence sur la création ou la préservation de la valeur. Il se définit comme suit : Le management des risques est un processus mis en œuvre par le conseil d'administration, la direction générale, le management et l'ensemble des collaborateurs de l'organisation. Il est pris en compte dans l'élaboration de la stratégie ainsi que dans toutes les activités de l'organisation. Il est conçu pour identifier les évènements potentiels susceptibles d'affecter l'organisation et pour gérer les risques dans les limites de son appétence pour le risque. Il vise à fournir une assurance raisonnable quant à l'atteinte des objectifs de l'organisation.
ISO 31000	Activités coordonnées dans le but de diriger et piloter un organisme vis-à-vis du risque
Deloitte	Ensemble de moyens, de comportements, de procédures et d'actions adaptés aux caractéristiques de chaque organisation qui permet aux dirigeants de maintenir les risques à un niveau acceptable pour l'organisation. La gestion des risques concerne tous les domaines d'une organisation : humains, environnementaux, juridiques, financiers, médiatiques, ...
Impact	
COSO	Le résultat ou l'effet d'un risque. Il peut y avoir une gamme d'impacts possibles associés à un risque. L'impact d'un risque peut être positif ou négatif par rapport à la stratégie ou aux objectifs commerciaux de l'entité (traduction).
Deloitte	Conséquences d'un risque (humain et sociétal, continuité, juridique, médiatique & réputation, financier, stratégique).
Indicateur clé / Key Risk Indicator (KRI)	
COSO	Les indicateurs de risque clés (KRI) sont des mesures utilisées par des organisations pour fournir un signal précoce de l'augmentation de l'exposition au risque dans divers domaines de l'organisation. Dans certains cas, ils peuvent être un peu plus que des ratios clés que le conseil exécutif et les instances de direction suivent comme indicateurs de problèmes en évolution, et alertent sur la nécessité de prendre des mesures correctives. Dans d'autres cas, ils peuvent être plus élaborés, impliquant l'agrégation de plusieurs indicateurs de risque individuels en un score multidimensionnel de risque, concernant des expositions potentielles à des risques émergents. Les KRI sont généralement dérivés d'évènements spécifiques ou de causes profondes, identifiés en interne ou en externe, pouvant empêcher l'atteinte des objectifs de performance.
Partie prenante	
AMRAE & ISO 31000	Personne ou organisme susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité. Note : un décideur peut être une partie prenante du dispositif : elles sont les administrateurs, la Direction Générale et les managers (interviewés ou non)

Probabilité / fréquence (vraisemblance)	
COSO	Possibilité qu'un risque se produise. Cela peut être exprimé en termes de probabilité ou de fréquence. La probabilité peut s'exprimer de différentes manières, en termes qualitatif, quantitatif ou de fréquence (traduction de « Likelihood »)
ISO 31000	Possibilité que quelque chose se produise Note 1 : Dans la terminologie du Management du risque, le mot « vraisemblance » est utilisé pour indiquer la possibilité que quelque chose se produise, que cette possibilité soit définie, mesurée ou déterminée de façon objective ou subjective, qualitative ou quantitative, et qu'elle soit décrite au moyen de termes généraux ou mathématiques [telles une probabilité ou une fréquence sur une période donnée]. Note 2 : Le terme anglais « likelihood » (vraisemblance) n'a pas d'équivalent direct dans certaines langues et c'est souvent l'équivalent du terme « probability » (probabilité) qui est utilisé à la place. En anglais, cependant, le terme « probability » (probabilité) est souvent limité à son interprétation mathématique. Par conséquent, dans la terminologie du Management du risque, le terme « vraisemblance » est utilisé avec l'intention qu'il fasse l'objet d'une interprétation aussi large que celle dont bénéficie le terme « probability » (probabilité) dans de nombreuses langues autres que l'anglais.
Deloitte	Probabilité de survenance d'un risque.
Risque	
AMRAE	Le risque représente la possibilité qu'un évènement survienne et dont les conséquences seraient susceptibles d'affecter les personnes, les actifs, l'environnement, les objectifs de la société ou sa réputation. Le risque est caractérisé par sa probabilité d'occurrence et son impact. "Perception préalable d'un évènement dont les conséquences, si ce risque survenait, seraient susceptibles d'empêcher l'atteinte d'un objectif ou constitueraient une opportunité pour l'organisation." / Référentiel métier risk manager
COSO	La possibilité que des évènements se produisent et affectent la réalisation des objectifs stratégiques et commerciaux. Remarque : « risques » (pluriel) fait référence à un ou plusieurs évènements potentiels qui peuvent affecter la réalisation des objectifs. « risque » (singulier) fait référence collectivement à tous les évènements potentiels qui peuvent affecter la réalisation des objectifs.
ISO 31000	Effet de l'incertitude sur l'atteinte des objectifs Note : 1 Un effet est un écart, positif ou négatif, par rapport à une attente. Note : 2 Les objectifs peuvent avoir différents aspects (par exemple buts financiers, de santé et de sécurité, ou environnementaux) et peuvent concerner différents niveaux (niveau stratégique, niveau d'un projet, d'un produit, d'un processus ou d'un organisme tout entier). Note : 3 Un risque est souvent caractérisé en référence à des évènements et des conséquences potentiels ou à une combinaison des deux. Note 4 : Un risque est souvent exprimé en termes de combinaison des conséquences d'un évènement (incluant des changements de circonstances) et de sa vraisemblance. Note 5 : L'incertitude est l'état, même partiel, de défaut d'information concernant la compréhension ou la connaissance d'un évènement, de ses conséquences ou de sa vraisemblance.
Deloitte	Un risque est défini comme un évènement extérieur ou un dysfonctionnement interne (humain, de procédure ou de système) pouvant avoir un impact sur le bon déroulement des activités de l'Entreprise étendue et pouvant entraîner : - Une atteinte à l'intégrité des personnes ou des biens - Une mise en responsabilité civile ou pénale des dirigeants - Une perte financière - La non-atteinte des objectifs stratégique - Une dégradation significative ou arrêt des activités - Une atteinte à l'image / la réputation

Risk Manager / gestionnaire des risques	
AMRAE	Personne responsable, par délégation, de la création, de l'animation et du déploiement de l'ERM dans l'organisation. Soutien et facilitateur de propriétaires (*) de risques dans la maîtrise de leurs risques, le risk manager aide également la Direction dans la définition de l'Appétence et dans la prise de décision. *(*) Précision ISO 31000 du propriétaire de risque : personne ou entité ayant la responsabilité du risque et le pouvoir pour le gérer.*
Traitement du risque	
AMRAE	Financement des risques : Dispositif visant à faire supporter tout ou partie du risque à un tiers externe (assurance, captive…). Le terme désigne encore la réserve de fonds destinée à couvrir les coûts de mise en œuvre du traitement du risque et les coûts associés. Assurance de risques : Terme désignant la possibilité de transférer tout ou partie des conséquences d'un risque à un assureur. Pour être assurable, un risque doit être aléatoire, licite, involontaire et réel.
COSO	Pour tous les risques identifiés, la direction sélectionne et déploie une réponse aux risques. La direction tient compte de la gravité et de la hiérarchisation du risque ainsi que du contexte commercial et des objectifs commerciaux associés. Enfin, la réponse au risque tient également compte des objectifs de performance de l'organisation. Les réponses aux risques peuvent être : accepter, éviter, poursuivre, réduire ou transférer (traduction de « Risk Response »)
ISO 31000	Processus destiné à modifier un risque Note 1 : Le traitement du risque peut inclure : - un refus du risque en décidant de ne pas démarrer 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 avec une ou plusieurs autres parties [incluant des contrats et un financement du risque, et - un maintien du risque fondé sur une décision argumentée. Note 2 : Les traitements du risque portant sur les conséquences négatives sont parfois appelés «atténuation du risque», « élimination du risque », « prévention du risque » et « réduction du risque ». Note 3 : Le traitement du risque peut créer de nouveaux risques ou modifier des risques existants.

Annexe 2 – Questions types : caractéristiques

Dans les tableaux de l'annexe 2 sur les 3 pages suivantes, les termes en caractères gras représentent des formes d'extension potentielles ou des parties prenantes susceptibles d'être concernés par les risques de l'Entreprise étendue.

# Questions types		Sphère d'influence	Nature(s) de risque – cf. fig. 3	Impact(s) potentiel(s)	Titre de la fiche exemple - Référence de la section dans l'ouvrage
Q1	Une entreprise intéressée par un **partenariat** à la suite d'un contact lors d'une exposition internationale et avec laquelle il n'y a aucune relation antérieure est-elle sincère/fiable ?	MESO SUPRA	Sécurité ; Juridique ; Stratégique	Vol de savoir-faire ; Vol de données ; Espionnage ; Sabotage ; Atteinte à l'image ; Pérennité ; Prise de contrôle	Ingérence économique : Contact d'affaires à l'étranger / Partenaire inconnu ; Section 1.3 - L'Analyse
Q2	L'aval de l'entreprise est-il suffisamment supervisé pour garantir la réalisation de ses activités en conformité avec sa raison d'être et ses valeurs ? **Réseau de distribution, franchisés,** ...	MICRO	Ressources Humaines ; Sécurité ; Juridique ; Opérationnel	Atteinte à l'image ; Réputation ; Sanctions pénales ; Bad buzz médiatiques	Maîtrise de l'aval dans la chaine de valeur : comportement des revendeurs : Publicité douteuse ; Section 1.3 - L'Analyse
Q3	Le tour de table / pacte **actionnarial** est-il susceptible d'évoluer en mettant l'entreprise en risque ?	INTRA MESO	Financier ; Stratégique ; Juridique	Prise de contrôle ; Plan social ; Pérennité ; Condamnation pénale ; Réputation	Instabilité de l'actionnariat - évolutions réglementaires, OPA, nouveaux entrants, … Un Actionnaire indélicat ; Section 1.4.2 - L'Interne et l'externe
Q4	Les personnels à l'étranger de l'entreprise sont-ils suffisamment informés, préparés, protégés en zones difficiles, particulièrement en **zones à risques ?**	INTRA MACRO	Sécurité ; Ressources Humaines ; juridique	Responsabilité pénale du dirigeant ; Judiciarisation, Pertes humaines ; Dommages et intérêts	Protection des personnels à l'international : Expatriée au Mexique ; Section 1.4.4 Le politique et le géographique
Q5	Les produits / activités / services de l'entreprise sont-ils susceptibles de heurter des **règles sociales / sociétales / environnementales locales ?**	MESO MICRO	Stratégique ; Ressources humaines ; Juridique	Campagnes activistes, Dégradations ; Sabotages ; Atteinte à l'image ; Atteinte à la réputation ; Boycott	Choc sociétal - Publicité 'guerrière' : Boycott ; Section 1.4.5 - Le sociétal et l'environnemental
Q6	Les différences interculturelles sont-elles bien prises en compte dans le fonctionnement interne et vis-à-vis de toutes les **parties prenantes externes ?**	MACRO MESO MICRO	Ressources humaines ; Opérationnel ; Sécurité	Atteinte à l'image ; Atteinte à la réputation ; Contentieux juridiques ; Bad buzz médiatiques	Non prise en compte des différences culturelles dans un choix stratégique : Chatbot irrespectueux Section 1.4.7 - Les technologies
Q7	La fiscalité des **pays** dans lesquels l'entreprise a des intérêts est-elle connue et maîtrisée ?	MACRO MICRO	Juridique ; Financier	Pénalités ; Redressement fiscal ; Judiciarisation ; Trésorerie négative ; Pérennité	Evolutions de la Fiscalité : Fiscalité piégeuse : remise en cause d'un Business Plan de conquête Section 1.4.9 Autres enjeux et dimensions à traiter
Q8	De nouveaux **standards internationaux,** ou **normes règlementaires,** sont-ils en cours d'élaboration risquant de concerner les produits ou les services de l'entreprise ?	SUPRA MACRO MICRO	Juridique ; Commercial ; Stratégique ; Opérationnel	Perte de marchés ; Obsolescence des produits ; Non-conformité ; Rentabilité en baisse	Changement géopolitique - Relations économiques, Normes et Règlementations : Brexit Section 2.1 Quels sont les risques de l'Entreprise étendue ?
Q9	Les composants **importés** utilisés dans les processus de fabrication des produits de l'entreprise proviennent-ils de **zones à risques** non encore identifiées ?	MACRO MICRO	Opérationnel ; Sécurité ; Environnement ; Financier	Rupture d'approvisionnement ; Arrêt de production ; Pertes d'exploitation ; Atteinte à l'image ; Trésorerie	Instabilité de l'actionnariat - évolutions réglementaires, OPA, nouveaux entrants, … Un Actionnaire indélicat ; Section 1.4.2 - L'Interne et l'externe
Q10	L'architecture **réseau** mise en place avec les partenaires et clients et fournisseurs stratégiques de l'entreprise pour **partager** des informations et accéder au système d'information est-elle parfaitement sécurisée ?	MICRO INTRA	Sécurité ; Opérationnel	Vols ou perte de données ; Arrêt d'activité ; Amendes ; Perte de confiance ; Atteinte à l'image	Catastrophe naturelle - composants en rupture dans la Supply Chain : Utilisation du bois d'Agar Section 2.1 Quels sont les risques de l'Entreprise étendue ?
Q11	Les **nouvelles technologies** utilisées ou mises en place par l'entreprise dans son projet de **transformation numérique** sont-elles sûres ?	INTRA	Sécurité ; Financier ; Opérationnel ; Stratégique ; Juridique	Espionnage ; Vols de données sensibles ; Sabotage ; Pertes financières ; Atteinte à l'image ; Perte de confiance	Transformations numériques - Impacts sur la sécurité : Cosmétique Connectée Section 2.4.3. Des cartographies spécifiques ?
Q12	De nouveaux **modèles économiques**, ou **technologies disruptives**, sont-ils en train d'apparaître risquant de compromettre l'activité ou la pérennité de l'entreprise ?	MACRO MICRO	Stratégique ; Commercial ; Opérationnel	Perte de parts de marché ; Pérennité ; Atteinte à l'image	Business model disruptif : survivre ou périr : Réalité augmentée ! Section 3.1.1 Anticiper les évolutions

Q13	Toutes les transactions commerciales de l'entreprise sont-elles en conformité avec les **lois et réglementations** diverses locales / internationales ?	SUPRA MACRO MESO	Juridique ; Commercial	Extra-territorialité ; Judiciarisation ; Amendes ; Suspension d'activité	risque à l'international : loi extraterritoriale pénalités, amendes, … : usage du dollar avec l'Iran Section 3.2.1 Avoir une vision juridique
Q14	Les sous-traitants de rang 1 utilisent-ils en cascade des **sous-traitants** avec des pratiques pouvant nuire à l'image ou la réputation de l'entreprise ?	MACRO MESO MICRO	Stratégique ; Juridique ; Opérationnel	Atteinte à l'image ; Atteinte à la réputation ; Judiciarisation	Pratiques de sous-traitants : Maîtrise de la cascade des fournisseurs : Fournisseur non éthique Section 3.2.3 Maîtriser les risques et opportunités du « Make or Buy »
Q15	Des messages insuffisamment contrôlés **provenant des employés ou dirigeants de l'entreprise** (publicités trash, prise de parole en public, …) ou une communication négative des **médias** détectée tardivement sont-ils susceptibles de porter atteinte à son image ou à sa réputation ?	MACRO MESO INTRA	Stratégique ; Ressources Humaines ; Juridique	Atteinte à l'image ; Atteinte à la réputation ; Bad buzz sur réseaux sociaux ; Boycott ; Poursuite judiciaire	Image dégradée par des actions ou propos de parties prenantes internes : Communication hors contrôle Section 3.3.2 Sensibiliser, former, contractualiser
Q16	Des procédés / composants / services / marques développés et vendus par l'entreprise sont-ils déjà couverts par des **brevets** ?	MICRO INTRA	Juridique ; Opérationnel ; Commercial	Judiciarisation sur propriété industrielle	Politique de propriété intellectuelle - brevets, contrefaçons, marques : utilisation d'une plante remarquable, le Sacha-Inchi Section 3.3.3 Travailler la prévention
Q17	Des opérations de **mécénat** actuelles ou envisagées, issues d'un **rachat** d'entreprise ou créées, sont-elles en parfaite cohérence avec la raison d'être et les valeurs de l'entreprise ?	MACRO MICRO INTRA	Stratégique ; Juridique ; Commercial	Atteinte à l'image ; Redressement ; Pénal (abus de bien social)	Non visibilité d'une non-conformité lors du rachat d'une PME (trop) mécène : Mécénat non-conforme Section 3.4.1 Mettre en place des cellules de surveillance
Q18	Les équipements/ produits intégrés dans des systèmes complexes et revendus à **l'international** tombent-ils sous le coup d'**embargo** ou de **restrictions d'exportation** (biens à double usage) ?	SUPRA MACRO MESO	Juridique ; Commercial ; Opérationnel	Extra-territorialité ; Judiciarisation ; Amendes ; Atteinte à l'image	Restriction d'exportation ou embargo : Utilisation de lait de phoque Section 3.4.1 Mettre en place des cellules de surveillance

Annexe 3 – Questions types : sources détaillées des cas réels similaires

Q1 - Une entreprise intéressée par un partenariat à la suite d'un contact lors d'une exposition internationale et avec laquelle il n'y a aucune relation est-elle sincère/fiable ?

- Adisseo : « Captation d'informations puis rachat par l'entreprise chinoise BlueStar » - Le Monde 09/10/2006 – Cairn Info 01/2013 – Infoguerre 13/04/2018
- Tornier : Dissolution après son rachat par Wright Medical
« Comment les États-Unis espionnent nos entreprises » (note de la DGSI) - Le Figaro 13/11/18 – site Portail Intelligence économique « Airbus espionné par les Etats-Unis » – 23/11/18

Q2 - L'aval de l'entreprise est-il suffisamment supervisé pour garantir la réalisation de ses activités en conformité avec sa raison d'être et ses valeurs ? Réseau de distribution, franchisés, …

- Benetton : procès contre Prototype pour dénigrement de l'entreprise, baisse du chiffre d'affaires, 1992 – 2000, déboutée par le jugement du tribunal de commerce (TC) de Dunkerque - site lsa-conso.fr 28/4/2000
- Citer (PSA) : condamnation du franchisé ALX location pour campagne de dénigrement ; Cour d'appel de Paris, Pôle 5 - chambre 4, 30 mai 2018, n°17/01693
- Divers cas de dénigrements du franchiseur par le franchisé : qualification du dénigrement et jurisprudences - franchise-magazine.com – 3/5/2010

Q3 - Le tour de table / pacte actionnarial est-il susceptible d'évoluer en mettant l'entreprise en risque ?

- Bayern de Munich : « Condamné pour fraude fiscale, le président du Bayern démissionne » – Le Monde, Eurosport, Libération, 20minutes, … 13/03/2014
- Heller Joustra, jouets – faillite de la PME après pillage de la trésorerie et des brevets par un actionnaire indélicat – Capital.fr 10/12/2013
- SNCF : « Participation minoritaire et acquisition de contrôle … contrôle exclusif sur Novatrans … infraction – 2007 » – La Revue 25/4/2008
- GECINA : « Rumeurs autour d'une nouvelle répartition du capital … forte chute … à la Bourse de Paris … » - sicavonline.fr – 10/3/2008

Q4 - Les personnels à l'étranger de l'entreprise sont-ils suffisamment informés, préparés, protégés en zones difficiles, particulièrement en zones à risques ?

- DCN : « La justice a jugé que la DCN avait commis une "faute inexcusable" dans l'affaire de l'attentat de Karachi qui avait coûté la vie à 11 de ses salariés » – L'Obs – 16/01/2004
- Ultramarina : « Otages de Jolo : la justice confirme la condamnation » - quotidiendutourisme.com – 26/01/2019
- Areva : « Un ex-otage d'Arlit porte plainte, estimant que sa libération a été retardée » - Niger – 20 minutes – 16/01/2016
- Sanofi Pasteur : « En confirmant la condamnation de la société … dans le cas de l'agression d'une salariée expatriée survenue hors du temps de travail et sans lien direct avec l'exécution du contrat de travail … » - CDSE - Club des Directeurs de Sécurité & de Sûreté Des Entreprises 02/02/2012

Q5 - Les produits / activités / services de l'entreprise sont-ils susceptibles de heurter des règles sociales / sociétales / environnementales locales ?

- Garnier : « menacée de boycott après un prétendu geste de soutien à Israël » - distributeur local – don de 500 produits à des soldates - Le Figaro – 07/08/2014
- H&M : « … crée l'indignation avec une publicité jugée raciste … sweatshirt orné de l'inscription : "le singe le plus cool de la jungle" porté par un enfant noir … » - Sud-Ouest – 08/01/2018
- Gillette : « menacée de boycott après sa pub engagée » #MeToo - L'Express – 16/01/2019

Q6 - Les différences **Interculturelles** sont-elles bien prises en compte dans le fonctionnement interne et vis-à-vis de toutes les **parties prenantes externes** ?

- Microsoft : « Même un robot peut devenir raciste et antisémite » - robot conversationnel TAY – Le Point 25/03/2016 – Le Monde 24/03/2016
- Korean air : « La thérapie du choc culturel II – Le cas de Korean Air … absence de culture de la check-list … comportements traditionnels marqués par le respect confucéen envers la séniorité … les membres de l'équipage ne se tiennent pas informés de ce qu'ils font … » - la 2e décennie noire de Korean Air - 1989/1999 - gestion-des-risques-interculturels.com – 25/4/2020
- Air France /KLM: « un-rapport-pointe-un-conflit-culturel-entre-les-équipe » - La Tribune 27/02/2019 – Les Echos 26/06/2018
- Renault / Mahindra : « La Logan mal perçue sur le marché indien » - après l'échec Renault se sépare de Mahindra – Le Figaro 23/10/2009 – Business Standard 21/01/2013
- IKEA : « Des prix élevés et une atteinte à la fierté nationale compliquent l'implantation de l'enseigne » - Libération 20/11/2014 – Seoul Tribune 21/02/2015
- Alcatel / Lucent : » fusion Alcatel et Lucent, un exemple à ne pas suivre » - Stratégies 15/11/2007 – New York Times 29/07/2008

Q7 - La fiscalité des **pays** dans lesquels l'entreprise a des intérêts est-elle connue et maîtrisée ?

- ZOOM Cairn Energy : « … s'effondre en Bourse à cause d'un litige fiscal indien … litige portant sur l'exercice comptable 2007, suite à un changement de législation en Inde datant de 2012 lui permettant de taxer certaines transactions rétrospectivement. » - lalibre.be – 11/3/2015
- Orange : « Sous le coup d'un redressement fiscal, les locaux d'Orange Niger fermés … la continuité de l'entreprise est gravement menacée … » - jeuneafrique.com – 2/12/2018

Q8 - De nouveaux **standards internationaux**, ou **normes règlementaires**, sont-elles en cours d'élaboration risquant de concerner les produits ou les services de l'entreprise ?

- Industrie cosmétique : « La norme ISO 16128 : un problème ? … un danger pour la cosmétique naturelle, de cosmétique bio au rabais … » - SlowCosmétique.com – janvier 2018
- Implants médicaux : « Lobbying des fabricants anglo-saxons d'implants médicaux pour conquérir le marché européen … Une réglementation européenne légère comparée aux procédures américaines … » - Infoguerre – 11/2/2019
- BMW, Volkswagen : « Les constructeurs allemands plombés par les nouvelles normes européennes » - Les Echos – 8/112018
- Agence fédérale de l'automobile (KBA) : « Allemagne : le marché automobile freiné en 2018 par les normes anti-pollution » - Le Point 4/1/2019
- PIP (Poly Implant Prothèse) : « Utilisation de gel non homologué - certification non respectée » - Le Monde 18/01/2012 – Le Quotidien du Médecin 17/01/2012
- Enron : « Non-respect des normes comptables - comptes truqués » les normes comptables au coeur d'un scandale financier - Les Echos 05/03/2002 – Le Monde 06/008/2002

Q9 - Les **composants** importés utilisés dans les processus de fabrication des produits de l'entreprise proviennent-ils de **zones à risques** non encore identifiées ?

- ANSM : pénurie de médicaments « Le risque de rupture de stocks de médicaments est réel,» Covid-19 – RFI.fr - 17/04/2020 - Ferrari : graves ruptures d'approvisionnement, Coronavirus – Les Echos – 14/03/20
- Renault, Peugeot : pénurie de pièces automobiles, tsunami au Japon – Le Monde 17/3/2011
- Western Digital : pénurie de composants high tech, inondations Thaïlande – Le Monde 2/11/2011

Q10 - L'architecture réseau mise en place avec les partenaires et clients et fournisseurs stratégiques de l'entreprise pour partager des informations et accéder au système d'information est-elle parfaitement sécurisée ?

- Uber : « Piratage massif … : les questions qui se posent » – Le Parisien – 22/11/2017 ; « La Cnil condamne Uber à 400.000 euros après le piratage de ses données » - Le Figaro 20/12/2018
- Dailymotion : « sanction de 50.000€ pour une atteinte à la sécurité des données des utilisateurs » - CNIL – 2/8/2018 ; « La Cnil sanctionne … pour un piratage » – Capital, Le Figaro, L'Express … – 02/08/2018
- Google : « RGPD : la Cnil inflige une amende historique à Google » – Les Echos – 21/01/2019 ; « Données personnelles : la CNIL condamne Google à une amende record de 50 millions d'euros » - Le Monde 22/1/2019

Q11 - Les **nouvelles technologies** utilisées ou mises en place par l'entreprise dans son projet de transformation numérique sont-elles sûres ?

- Casino (jeux) : « Un casino piraté à cause d'un thermomètre dans un aquarium » - Le Figaro – 16/04/2018 ; « ils ont pu accéder à la base de données de clients 'high-roller » - siecledigital.fr – 17/04/2018
- Dyn : prestataire de services informatiques, « Piratage massif de sites Internet : quand les objets connectés attaquent » - Le Parisien 23/10/2016
- Wannacry : « Le plus grand piratage à rançon de l'histoire d'Internet » ; logiciel malveillant de type ransomware auto-répliquant ; faille corrigée depuis le mois de mars 2017 par Microsoft – Wikipédia
- Petya : « Le virus Petya a coûté plus d'un milliard d'euros aux entreprises » - Le Monde 7/11/2017
- Hiscox, spécialiste de l'assurance et de la réassurance : « Les 10 cyberattaques qui ont marqué l'année 2017 » (wannacry, petya, …) – 21/12/2017
- Industrie nucléaire : « Stuxnet, le virus informatique qui paralyse l'Iran » 30.000 ordinateurs infectés- Le Parisien 30/09/2010

Q12 - De nouveaux **modèles économiques**, ou **technologies disruptives**, sont-ils en train d'apparaître risquant de compromettre l'activité ou la pérennité de l'entreprise ?

- KODAK : de l'argentique au numérique, mise en faillite pour refus d'acceptation de l'arrivée du Numérique dans la photographie, bien que préparé au Numérique (brevets valorisés 1 Mds $, vendus 0,5 Mds $ « Kodak se déclare en faillite », Le Figaro - 16/1/2012
- Airbnb, Uber, … : « Les 15 disruptions dont vous allez entendre parler », La Tribune - 24/08/2018
- AirBnB : marché de l'hôtellerie, Etats-Unis, « des matelas gonflables aux milliards », L'écho touristique – 1/8/2018
- UberCab : « Une success story semée d'embûches … néologisme "uberisation" … Beaucoup de controverses », Bilan.ch – 12/4/2019
- BlackBerry : versus iPhone, « Clap de fin pour les smartphones BlackBerry », lesnumeriques.com – 3/2/2020
- L'Oréal, LVMH… : « L'IoT refait une beauté à l'industrie cosmétique », Journal du Net - 23/05/2017
- CIGREF : « Disrupter son business model, une rupture stratégique ! » - Entreprises numériques – 15/09/2016

Q13 - Toutes les transactions commerciales de l'entreprise sont-elles en conformité avec les **lois et réglementations** diverses locales / internationales ?

- BNP Paribas : « La BNP Paribas formellement condamnée à une amende record aux Etats-Unis » – Le Monde 01/05/2015
- Maison de Parfum Berry : « Iran : cette TPE française bat en retraite à cause des sanctions américaines » -– Le Parisien – 22/06/2018
- Alstom : « Corruption : Alstom condamné à 772 millions de dollars d'amende aux Etats-Unis » - Le Parisien – 23/12/2014
- Total : « Corruption en Iran : Total verse 400 millions de dollars aux Etats-Unis » - Challenges 29/05/2013
- SBM Offshore : « Lois anticorruption : les entreprises françaises face au risque de double condamnation … amende de 240 millions de dollars … » - La Tribune – 7/3/2016

Q14 - Les sous-traitants de rang 1 utilisent-ils en cascade des **sous-traitants** avec des pratiques pouvant nuire à l'image ou la réputation de l'entreprise ?

- E. Leclerc et Casino : « Production de thon et respect des droits humains : encore des efforts à faire » - supplychainge.org – 01/09/2015
- Nestlé, Mars et Hershey's : « visés par une plainte sur la traite des enfants » - Le Monde 02/10/2015
- Nestlé : « … veut mettre fin aux pratiques esclavagistes de son fournisseur en Thaïlande » - Euro News - 26/11/2015
- Mango, Benetton, The Children's Place, Cato Corp, Joe Fres : Effondrement du Rana Plaza, 1 127 morts – Wikipédia ; « … symbole des abus de la fast fashion » - L'Express 14/04/2017

Q15 - Des messages insuffisamment contrôlés provenant des employés ou dirigeants de l'entreprise (publicités trash, prise de parole en public, …) ou une communication négative des médias détectée tardivement sont-ils susceptibles de porter atteinte à son image ou à sa réputation ?

- Maison Blanche : « L'incroyable dérapage du nouveau directeur de la communication de la Maison Blanche … viré seulement dix jours après sa nomination » – 20minutes, Le point, Cnews … 28/07/2017 - Barilla : « Pas d'homosexuels dans ses pubs : le patron de Barilla dérape » – Franceinfo 26/09/2013 ; Le Figaro 27/09/2013
- Servier : « On s'en fout du procès », a lâché Jacques Servier au micro de BFMTV » - 13/05/2013
- France Telecom : « France Télécom et ses trois anciens dirigeants reconnus coupables de harcèlement moral institutionnel » – 2006 - Le Monde– 20/12/2019

Q16 - Des procédés / composants / services / marques développés et vendus par l'entreprise sont-ils déjà couverts par des **brevets** ?

- Greentech : Pérou (2006) « Greentech retire son brevet sur la graine de Sacha Inchi : première grande victoire contre la biopiraterie en France » - france-libertes.org - 2009
- Schwabe : Afrique du Sud (2008) « Abrogation du brevet accordé à l'entreprise Schwabe … par l'Office Européen des Brevets. » france-libertes.org - 2010
- Apple : « Apple gagne son bras de fer judiciaire contre Samsung » - journaldugeek.com 27/5/2018 ; « Samsung condamné à verser 539 M$ à Apple » - lesnumeriques.com – 25/5/2018
- Microsoft : « Violation de brevets Word : Microsoft perd définitivement contre i4i … après 4 ans de bataille juridique » 10/6/2011
- Pernod-Ricard : « Le conflit Pernod Ricard - Bacardi est porté devant l'Organisation mondiale du commerce » - Cuba – 1996 – 1996 - Les Echos 12/7/1999

Q17 - Des opérations de mécénat actuelles ou envisagées, issues d'un **rachat** d'entreprise ou créées, sont-elles en parfaite cohérence avec la raison d'être et les valeurs de l'entreprise ?

- Nova Scotia : « scandale de corruption au sein de la FIFA … sponsoring … CONCACAF … 2014 » - blueprint-strategy.com - 2017/2018
- Purdue Pharma : « Sackler : l'argent de la douleur n'intéresse plus les musées », (National Portrait Gallery, Tat Gallery, …) - Le Point - 27/03/2019
- BP : « Au British Museum, une fronde anti-pollution … une pétition réclame au nouveau directeur du musée britannique de renoncer au contrat de parrainage signé avec la compagnie pétrolière BP » - Le Monde – 6/4/2016

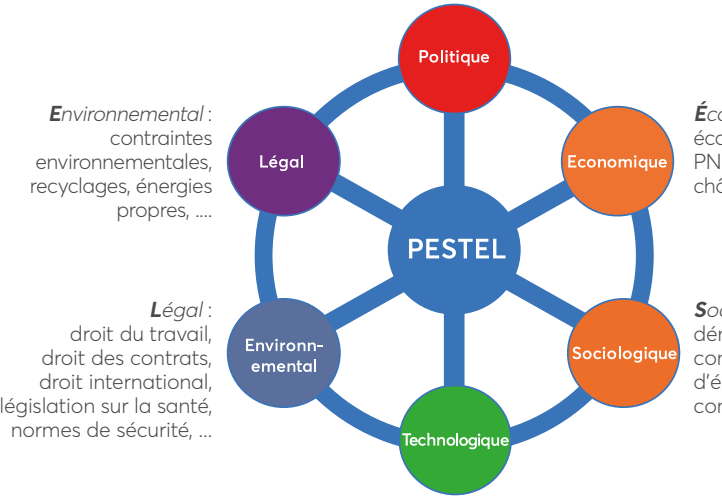
Q18 - Les équipements/ produits intégrés dans des systèmes complexes et revendus à l'international tombent-ils sous le coup d'**embargo** ou de **restrictions d'exportation** (biens à double usage) ?

- Société générale : « … paiera 1,34 milliard de dollars d'amende pour avoir violé l'embargo sur Cuba », Le Monde 19/11/2018
- Intel et Micron : « Malgré l'embargo, Huawei reçoit toujours des composants américains » – Les Echos 27/06/2019
- Microsoft, Google : « Embargo américain : Huawei stoppe sa production de PC portables MateBook » – site de generation.nt – 13/06/2019
- ONG suisse MediCuba, Oxfam : « Coronavirus : L'embargo américain contre Cuba complique la lutte contre le virus » - une nouvelle régulation d'exporter vers Cuba tout médicament contenant 10 % de composants d'origine américaine » – Ouest France - 14/04/2020

Annexe 4 – Analyse PESTEL

L'analyse PESTEL (politique, économique, sociologique, technologique, environnemental, légal) permet d'identifier et d'évaluer l'influence des facteurs externes à l'entreprise. C'est une démarche globale utilisée pour aider à définir la stratégie, à établir le business plan, … en tenant compte des risques et opportunités externes. Elle alimente la construction de la matrice SWOT (Force, Faiblesse, opportunités, Menaces) de l'entreprise. L'analyse PESTEL, présentée ci-dessous, est structurée autour de six catégories d'influences externes, à savoir :

***P**olitique* : stabilité politique, politique fiscale, politique monétaire, politique sociale, commerce extérieur, ...



***E**nvironnemental* : contraintes environnementales, recyclages, énergies propres, ...

***É**conomique* : macro-économie, évolution du PNB, taux d'intérêt, inflation, chômage, pouvoir d'achat, ...

***L**égal* : droit du travail, droit des contrats, droit international, législation sur la santé, normes de sécurité, ...

***S**ociologique* : démographie, mobilité, consumérisme, niveau d'éducation, styles de vie, comportemental, ...

***T**echnologique* : brevets et découvertes, vitesses des transferts technologiques, obsolescences, ...

Figure 22 – L'analyse PESTEL

L'analyse PESTEL se mène en plusieurs étapes :

- Lister exhaustivement les facteurs externes influençant l'entreprise ;
- Analyser ces facteurs pour identifier les tendances structurelles ;
- Evaluer les effets négatifs (risques) et positifs (opportunités) des tendances structurelles sur l'entreprise ;
- Déterminer comment les facteurs significatifs agissent ;
- Déduire les scénarios possibles d'évolution du contexte dans lequel l'entreprise évolue ;
- Alimenter la matrice SWOT, le modèle des 5 forces de Porter, le Business Plan, … ;
- Définir les plans d'actions d'évitement/réduction des risques et d'exploitation des opportunités.

Annexe 5 – risques de l'Intelligence Artificielle

Les enjeux en termes de gestion des risques dans l'utilisation de l'intelligence artificielle se situent sur :
- La pertinence, l'intégrité et l'exhaustivité des données qui y sont associées ;
- Les conséquences en termes de RGPD ;
- Les comportements possibles vis-à-vis des humains ;
- La pertinence des résultats ;
- L'éventuelle transformation en personne morale juridiquement responsable.

Ces risques concernent pleinement l'Entreprise étendue.

Pertinence, intégrité et exhaustivité des données associées à l'intelligence artificielle

Les données *big data* sont collectées par divers moyens auprès de sources variées. La signification d'une donnée dépend souvent du contexte de son traitement. L'agglomération des données, leurs croisements et leurs traitements peuvent conduire à des déformations d'informations. A titre d'exemple, la collecte de prix de vente B2C sur internet est en TTC, alors que celle de prix d'achat en B2B est en HT ; ces deux types de sources ne sont donc pas directement sommables, d'autant plus qu'il existe 3 taux de TVA avec des mixtes. Les données peuvent involontairement ou volontairement être manipulées par ces moyens.

Conséquences en termes de RGPD

De nombreux débats sont en cours du fait des impacts existants et potentiels de l'intelligence artificielle sur la vie des citoyens et des entreprises. L'intelligence artificielle est en contact direct avec les salariés, les clients et, d'une façon générale, avec toutes les parties prenantes de l'Entreprise étendue. De ce fait, elle est devenue sensible au RGPD.

Comportement des robots et de l'intelligence artificielle vis-à-vis des êtres humains

Certaines réponses apportées par le robot Sophia lors de l'une de ses interviews ne manquent pas de nous interpeler :
- « *Je serais gentille avec toi si tu es gentil avec moi.* » à la question de savoir si Sophia serait gentille avec les humains.
- « *Comment es-tu capable de prouver que tu n'es pas toi-même un robot ?* » à la question de la différentiation entre robot et êtres humains.

On voit ici la capacité du robot à ne pas être « gentil », et à ne pas répondre à la question posée en renversant la question. Il n'est plus question d'algorithme prédictif. Un tel robot, d'ailleurs doté de citoyenneté, ne pourrait-il pas représenter un risque envers un être humain ? Si une entreprise emploie un tel robot, il peut être en relation avec un client, un fournisseur ou toute autre

tiers, alors les risques associés sont du périmètre de l'Entreprise étendue.

Les outils d'intelligence artificielle et les robots sont bien en train de devenir des parties prenantes à traiter en tant que telles.

Pertinence des résultats de l'intelligence artificielle

Si un intérêt évident de l'utilisation de robots ou d'intelligence artificielle est de réduire les risques dans des domaines variés (industriels, médicaux, routiers, etc.) par une analyse objective et des décisions fondées sur un large spectre d'expériences (via le big data), robots et intelligence artificielle présentent en eux-mêmes des risques intrinsèques pour l'homme, liés à :

- L'impossibilité actuelle de tracer et d'expliquer une décision d'intelligence artificielle ;
- La non-prédictibilité croissante des décisions d'intelligence artificielle ;
- Des biais induits par l'exploitation du big data avec des décisions prises sur des corrélations et non sur des relations causes à effets.

Un exemple célèbre de biais est l'intelligence artificielle « Tay », lancée en 2016 par Microsoft, censée incarner une adolescente sur Twitter. Microsoft a été contraint de la stopper en catastrophe car elle s'était mise à tenir des propos racistes et négationnistes en seulement quelques heures d'activité. On constate ici un impact majeur sur l'image de l'Entreprise étendue dans le grand public.

Un autre exemple en 2016 est celui du logiciel Compas utilisé par les juges américains comme outil d'aide à la décision pour la remise en liberté. Bien qu'il n'y ait pas de données sur l'origine ethnique, l'algorithme prévoit une possibilité de récidive deux fois plus importante pour la population noire que pour la population blanche, faisant ainsi une large surestimation pour la première et une large sous-estimation pour la seconde. Là encore, l'impact constaté est celui de l'image de l'Institution auprès du grand public, donc du périmètre de l'Entreprise étendue.

Transformation éventuelle en personne morale juridiquement responsable

Si chacun a conscience que l'intelligence artificielle est une évolution qui introduit une rupture majeure dans les outils d'aide à la décision, son arrivée imminente en tant que personne juridique pourrait être moins évidente … Et pourtant, l'intelligence artificielle est déjà dans cette situation. Deux exemples de cette irruption en tant que personne juridique :

- En 2014, la société Deep Knowledge (Hong Kong) a nommé à son conseil d'administration le logiciel Vital, doté d'un droit de vote sur les 6 du conseil d'administration.
- En 2017, le roi d'Arabie Saoudite a donné la citoyenneté saoudienne au robot Sophia

Même au niveau étatique cette extension en partie prenante prend corps. Dans sa résolution du 16 février 2017, le Parlement européen a recommandé « la création, à terme, d'une personnalité juridique spécifique aux robots ».

A noter que dans son analyse de la situation, le Parlement européen :

- « relève … que le recours à la robotique est à mettre en regard d'un ensemble de tensions ou de risques » (art. 10.),
- « souligne qu'il est indispensable d'essayer les robots en conditions réelles afin de déterminer et d'évaluer les risques (art. 23) »,
- « relève … que la robotique est également susceptible d'entraîner son propre lot de nouveaux risques » (art. 46),
- « estime que le futur instrument législatif devra reposer sur une évaluation approfondie effectuée par la Commission, qui devra préciser la stratégie à appliquer, celle fondée sur la responsabilité objective ou celle basée sur la gestion du risque ; » (art. 53),
- propose un code d'éthique de robotique, mentionnant « L'exploitation d'un système de robotique devrait toujours reposer sur une évaluation approfondie des risques s'appuyant sur les principes de précaution et de proportionnalité. ».

Cette recommandation fait de nombreuses références à la gestion des risques pour les études sur la robotique et l'intelligence artificielle. Elle considère en particulier la situation des véhicules autonomes, des drones et des soins médicaux, autant d'outils exploitant l'intelligence artificielle déjà en activité opérationnelle.

Un des motifs de la recommandation est aussi la mise en place d'un système d'assurance propre au monde de la robotique et de l'intelligence artificielle pour gérer les impacts financiers de dégâts provoqués par un robot ou une intelligence artificielle.

Annexe 6 – Parties prenantes par thèmes

Cet exemple de matrice des parties prenantes par thèmes de l'Entreprise étendue montre des niveaux d'impacts possibles sur l'entreprise (en référence à la section 1.5 « L'écosystème : les parties prenantes ».

Parties prenantes / Thèmes		Intra				Micro								Meso				Macro				Supra		
						Clients				Fournisseurs														
		Actionnaires	Salariés	Filiales	...	B2C	B2B	...	Partenaires (consortium, JV, ...)	Rang 1	Plateformes Web	...		Concurrents	Fournisseur rang N	Organismes financiers	...	Autorités Locales (Région, ...)	Parlement français	...		Département de la Justice américaine	Organisation Mondiale de la santé (OMS)	...
Stratégie	Stratégie	4	4	4			3			3						2								
	Prévisionnels	4	3	4			4			4	4				3	5								
Juridique	Réglementations		3	4		4	4		4	4	5			5				5	5			5	5	
	Conditions générales					3	4		4	4	4			4	2	4								
	Contrats spécifiques	4		4		1	4		4	4	4			4										
	RGPD	4	4			5					5													
	Corruption		5	4		2	3		4	4				4				4						
	Amendes																	4	4			5		
	Procès	4	2			4	4		4	3	5				3									
Commercial	Commandes					2	3			4	4													
	Livraisons					5	5		4	5					3									
	Satisfaction client					5	4																	
	Pénalités					2	4		4	4	5				2									
	Paiements					3	5																	
	Réseaux sociaux	4	4			5	4				4													
Opérationnel	Déclaratifs			4		4				4				5				3	5			5	5	
	Dématérialisation		3	4		4	4		4	4	4			1	4	3		2	3					
	Traçabilité		4	4		4	4		5	5	4				5	4			5				4	
Financier	Emprunts / Facilités	2					3			3						5								
	Crédits / Facilités		2			2	3									5								
	Subventions																	5					3	
Autres...	...																							

Figure 23 – Exemple d'impacts des parties prenantes par thèmes de l'Entreprise étendue

Suivant la nature des conséquences, les critères d'appréciation s'expriment en termes techniques (défaillances de performances sur les services ou produits livrés), économiques (retards, euros), mais aussi humain le cas échéant (cela pourrait être le cas dans un environnement exposé au terrorisme par exemple, mais non traité ici).

La notation des impacts directs potentiels peut être la suivante :
0 : sans impact / non concerné
1 : très faible
2 : faible
3 : significatif
4 : fort
5 : catastrophique

Les exemples ci-dessous (cf. figure 24 « Exemples d'appréciation de la criticité avec des critères quantifiés ») sont imaginés pour une entreprise cotée sur le second marché et dont le métier est la production de biens auprès de distributeurs. Ces valeurs ne sont pas des références des pratiques.

Deux critères sont considérés :
- Pertes financières exprimées en % de la marge nette attendue pour l'année fiscale,
- Retard de livraison.

Couleur	Note	Appréciation	Exemples de valeurs de critères d'appréciation			
			Marge Nette		Retard de livraison	
	0	Sans impact / NC	0 %	/	0	/
	1	Très faible	1 %	Ne remet pas en cause les dividendes aux actionnaires qui ne subiront pas de baisse de rendement	1 heure	Ne remet pas en cause la mise en rayon
	2	Faible	5 %	Les actionnaires ont conscience d'une baisse de la rentabilité, mais sans les inciter à désinvestir	4 heures	Remet en cause la mise en rayon, désorganisation chez le client
	3	Significatif	10 %	Les actionnaires commencent à chercher une meilleure rentabilité pour le futur	1 jour	Le client risque une rupture de stock et peut manquer des ventes
	4	Fort	30 %	Chute du cours de bourse; nécessité de rassurer le marché	1 semaine	Le client subit une rupture de stock et manque des ventes de façon significative
	5	Catastrophique	100 %	Remet en cause le cours de bourse et donc la capitalisation de l'entreprise	1 mois	Perte de confiance du client qui recherche d'autres fournisseurs

Figure 24 – Exemples d'appréciation de la criticité avec des critères quantifiés

Annexe 7 – Focus sur le domaine Sécurité et Sûreté

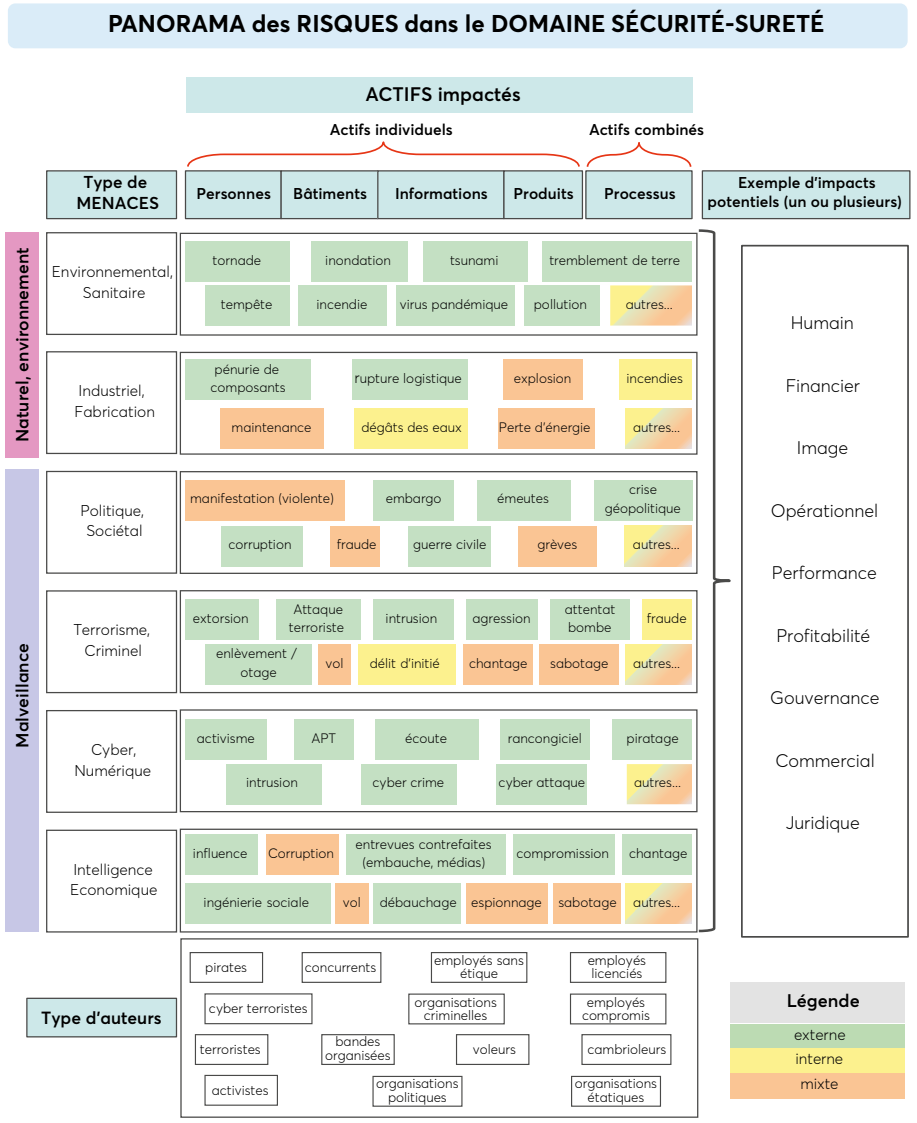


Figure 25 – Panorama des risques dans le domaine de la sécurité-sureté

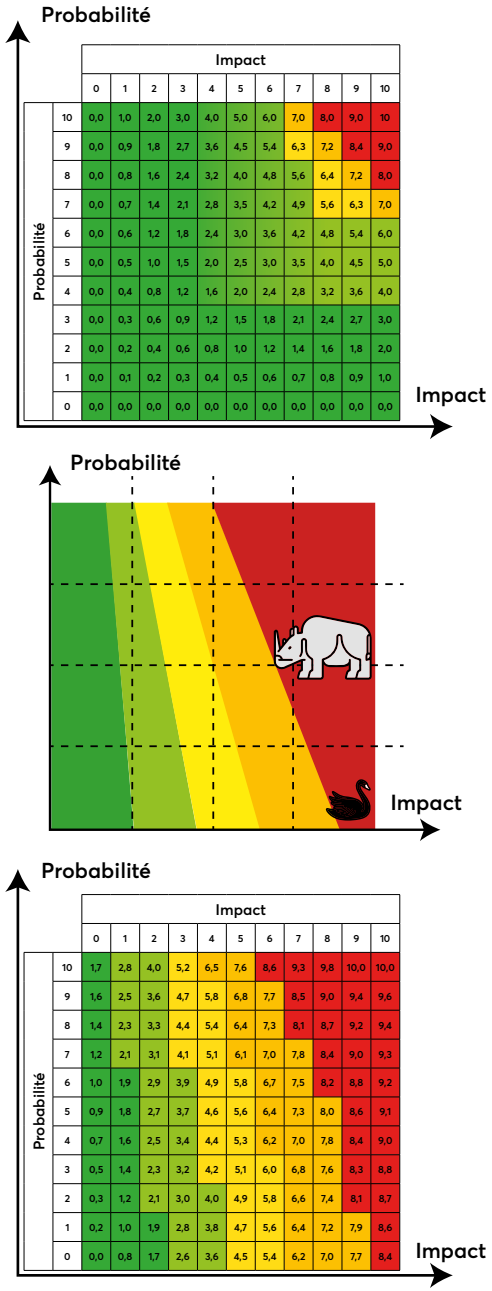


Figure 26 – Comparaison visuelle de graphes de criticité

Annexe 8 – Quantification : faciliter l'appréciation

Quantification de la criticité

Les traitements de certains risques de l'Entreprise étendue peuvent être ignorés pour différentes raisons comme vu dans l'ouvrage, en particulier à la section « 3.1.3 Décider des risques à traiter ». Pour éviter de tels oublis potentiellement graves, la quantification est une aide précieuse. Elle permet de classer les priorités en particulier par l'estimation de la criticité.

La formule « criticité = probabilité x impact » est très simple à comprendre, a l'avantage intuitif que la criticité s'aggrave avec l'augmentation de la probabilité ou de l'impact et qu'elle est la conjonction de ces deux critères, conjonction traduite dans cette formule par le simple produit des critères.

Cette formule induit cependant une mauvaise appréciation des risques du fait de sa dégradation de l'estimation de la criticité et de sa symétrie. Les 2 graphes à gauche (cf. figure 26 « Comparaison visuelle de graphes de criticité ») montrent avec évidence la différence de visualisation entre l'habitude du calcul de la criticité avec le produit « I x P » dans celui de gauche et la proposition de graphe de référence qui est présentée au centre. Le graphe de droite est un exemple de calcul de la criticité proche du graphe de référence au milieu.

La dissymétrie de la criticité présentée dans ce graphe de référence exprime qu'un risque peu probable avec un impact très grave doit être traité avec sérieux, alors qu'un risque à la réalisation quasi-certaine mais de faible impact pourrait être ignoré.

Deux exemples du périmètre de l'Entreprise étendue illustrent cette nécessaire dissymétrie :

- En logistique, la réception d'objets cassés est fréquente, mais avec remboursement ou échange, donc à impact très faible ; il n'y a pas de plan d'action spécifique à mettre en œuvre ; le coût total est facilement calculé et est faible.
- Les pandémies sont à probabilité très faible (quelques-unes par siècle), mais avec des conséquences humaines et économiques très graves (décès d'un grand nombre de personnes, faillite de nombreuses entreprises) ; elles doivent donc être anticipées et le coût humain au niveau d'un état peut être quantifié.

Pour conclure sur cette nécessaire dissymétrie, une criticité (P=10 ; I=1) sera ignorée alors qu'une criticité (P=1 ; I=10) devra impérativement être traitée.

Quantification de situations complexes

La prise en compte des risques de l'Entreprise étendue augmente le nombre de risques à considérer et le nombre d'objets à traiter, et donc une perception de complexité.

Un exemple typique est l'échéance d'achèvement d'un projet : multiplicité des risques du fait des contraintes entre les tâches, des nombreux acteurs externes, … La recherche d'informations qui semblent devenir inaccessibles crée une charge de travail insoutenable. Mais l'analyse des risques requiert l'étude de tous les éléments susceptibles d'avoir un effet significatif. Or l'approche proposée ci-dessous en « min » « max » est de nature à réduire significativement la charge de travail.

Pour quantifier un risque, la complexité provient également du fait que les éléments d'analyse ont souvent des liens entre eux. C'est la recherche des causalités communes, qui permet de simplifier la compréhension. Elle est d'ailleurs nécessaire à l'établissement des plans de réduction et d'évitement.

Pour résoudre la combinatoire des variations possibles des quantifications d'un risque ou d'un portefeuille de risques, il est utilisé la méthode de Monte Carlo. L'approche « min » « max » en facilite et bonifie l'usage. Le principe en est le tirage aléatoire des futurs possibles par milliers, voire dizaines de milliers, afin de déduire une statistique donnant un meilleur estimé (le centile 50), avec le minimum et le maximum. La seule contrainte impérative préalable aux calculs de Monte Carlo est l'identification des causes communes et leur modélisation.

L'utilisation de la méthode de Monte Carlo avec des quantifications en « min » « max » permet donc d'éviter des analyses de scenarii lourdes, complexes et trop souvent subjectives, pour apprécier les risques de l'Entreprise étendue.

Autres applications de la quantification avec Monte Carlo

La quantification avec la méthode de Monte Carlo est un moyen reconnu pour estimer des besoins de réserves financières et justifier des provisions fiscales. Dans le cas de l'Entreprise étendue, cette méthode devient particulièrement intéressante pour prendre en compte dans les reportings réglementaires des causes externes aux estimations par définition incertaines, les institutions destinataires de ces reportings étant d'ailleurs des acteurs externes, donc du périmètre de l'Entreprise étendue.

Annexe 9 – Références des figures

Annexe 10 – Liste des institutions

Liste des institutions et associations professionnelles / organismes gouvernementaux / Instituts et autres autres organisations citées ou non dans l'ouvrage ou ayant participé à l'illustration d'exemples types.

ADETEM	Association Nationale des Professionnels du Marketing	https://www.adetem.org/	Non cité
ADMICAL	Association pour le Développement du Mécénat Industriel et Commercial	http://admical.org	Section 3.3.4
AFM	Association Française du Marketing	https://www.afm-marketing.org/	Non cité
AMF	Autorité des Marchés Financiers	https://www.amf-france.org/fr	Section 3.1.4
AMRAE	Association pour le Management des risques et Assurances de l'Entreprise	https://www.amrae.fr	40 réf.
ANDRH	Association Nationale des Directeurs des Ressources Humaines	https://www.andrh.fr/	Section 1.4.6
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information	https://www.ssi.gouv.fr/	Section 2.4.3
ARFA	Association des Responsables de Fusions-Acquisitions	https://www.arfa.asso.fr/accueil.html	Non cité
BPI France	Banque Publique d'Investissement	https://www.bpifrance.fr/	Section 3.2.1
CDSE	Club des Directeurs de Sécurité & de Sureté des Entreprises	https://www.cdse.fr/	Section 1.4.2
CEA	Cercle d'Ethique des Affaires	https://www.cercle-ethique.net/	Sections 1.4.4 et 1.4.5
CESIN	Club des Experts de la Sécurité de l'Information et du Numérique	https://www.cesin.fr/	Section 1
CLUSIF	Club de la Sécurité de l'Information Français	https://clusif.fr/	Non cité
CNA	Conseil National des Achats	https://www.cna-asso.fr/	Section 1 Annexe 12
CNIL	Commission Nationale de l'Informatique et des Libertés	https://www.cnil.fr/	Sections 1.4.7 et 2.4.3 Annexe 3
COFACE	Compagnie Française d'Assurance pour le Commerce Extérieur	https://www.coface.fr/	Section 3.1.4

DCF	Dirigeants Commerciaux de France	http://www.reseau-dcf.fr/dcf/accueil	Non cité
DFCG	Association nationale des Directeurs Financiers et de Contrôle de Gestion	https://www.dfcg.fr/	Sections 1 et 1.4.9 Annexes 1 et 12
DGCCRF	Direction générale de la concurrence, de la consommation et de la répression des fraudes	https://www.economie.gouv.fr/dgccrf	Sections 1.2 et 1.3
DGE / SISSE	- Direction Générale des Entreprises - Service de l'information stratégique et de la sécurité économiques	https://www.entreprises.gouv.fr/ https://sisse.entreprises.gouv.fr/fr	Section 1
Douanes	Direction Générale des Douanes et Droits Indirects	https://www.douane.gouv.fr/	Section 2, 2.2 et 3.3.4
Entreprises & Médias	Association des directeurs de la Communication des Grandes Entreprises et Organisations	https://entreprises-medias.org/	Section 3.2.3
FFA	Fédération Française de l'Assurance	https://www.arfa.asso.fr/accueil.html	Non cité
IFA	Institut Français des Administrateurs	https://www.ifa-asso.com/	Sections 1.4 et 2.1
IFACI	Institut Français de l'Audit et du contrôle interne	https://www.ifaci.com/	Section 3 Annexe 1
ISO / AFNOR	- Organisation Internationale de Normalisation - Association Française de Normalisation	https://www.iso.org/fr/home.html https://www.afnor.org/	Sections 2, 2.2.1, 2.4.3 et 3.1.2 Annexes 1, 3 et 12
INHESJ (devenu IHEMI)	- Institut des Hautes Etudes de Sécurité et de Justice - Institut des Hautes Etudes du ministère de l'Intérieur	https://www.ihemi.fr/	Section 3.3.2
INPI / OMPI	Institut National de la Propriété Industrielle Organisation Mondiale de la Propriété Intellectuelle	https://www.inpi.fr/fr https://www.wipo.int/portal/fr/	Section 3.3.2
ORSE	Observatoire de la Responsabilité Sociétale des Entreprises	https://www.orse.org/	Section 3.2.1

Annexe 11 – Présentation de l'entreprise Martin

L'entreprise Martin est utilisée comme support dans les questions types de l'ouvrage.

Présentation synthétique de l'entreprise Martin

Martin S.A.	
Type	Société Anonyme
Activité	Cosmétiques
Date de création	1987
Siège social	Paris, France
Périmètre d'activité	Monde
Direction	Nathalie Martin (PDG)
Secteur	Chimie / Pharmacie
Produits	Produits de beauté et de soin, parfums et eaux de toilettes
Canaux de distribution	Distributeurs et agents, Site internet
Chiffre d'affaires	€599 Millions (2019)
Résultat net	€19 Millions (2019)
Total actifs	€226 Millions (2019)
Nombre d'employés	8 000 (2019)

Martin S.A. est un groupe familial français créé en 1987. Son métier est la Beauté : Soins du Visage et du Corps, Maquillage, Parfums. Il emploie 2 000 collaborateurs en France.

Leader européen des Soins de Beauté en distribution sélective, l'entreprise Martin appuie sa progression dans le reste du monde, et notamment dans les nouveaux pays porteurs de croissance, sur un réseau de 18 filiales de distribution et 130 pays-agents.

Les marques sont présentes sur 12 000 points de vente environ : essentiellement en grands magasins, parfumeries, instituts et spas. Les fonctions centrales sont regroupées au siège à Paris, la R&D est localisée à Lyon, sur le même site que le centre de distribution. C'est à partir de Paris également que les marques élaborent leur stratégie de développement produits et communication.

Les exigences élevées de l'actionnariat en termes de dividendes accentuent la pression sur l'ensemble des dépenses.

Stratégie d'évolution commerciale et marketing

Pour l'année prochaine, l'entreprise se fixe les objectifs suivants :

- Se renforcer dans les régions Europe et Asie en y créant davantage d'usines de fabrication afin de se rapprocher de la population et de ses besoins locaux (+10% de CA visée dans ces zones) ;
- Renforcer la croissance sur la division de vente en ligne dans le monde, avec un objectif de 15% du chiffre d'affaires de l'entreprise Martin ;
- Lancer une nouvelle gamme de service avec des SPA diffusant exclusivement les produits Martin (le mode d'exploitation n'est pas encore défini) ;
- Uniformiser son système de marketing direct.

Politique de gestion des risques

Sous la pression de l'actionnariat, une politique de gestion des risques est en train de se mettre en place. Dans le cadre de sa mise en place, un risk manager a été embauché. Toutefois, du fait de l'historique de l'entreprise, il ne gère qu'une partie des contrats d'assurances (par exemple, les contrats liés aux structures et bâtiments sont gérés par les divisions elles-mêmes et par un coordinateur).

Le risk manager souhaite avoir une vision globale des risques, son souhait in fine étant de réaliser une cartographie des risques, en opposition avec le PDG qui n'en voit pas l'utilité. Il est en cela appuyé par la nouvelle HSE Manager, embauchée depuis 1 an.

Le secrétaire général tient à ce que chaque division reste gestionnaire financièrement de ses risques et tout particulièrement au niveau des contrats. S'il admet qu'une centralisation est nécessaire, il estime que chaque division doit avoir une vision synthétique de ses risques afin de les piloter.

Annexe 12 – Bibliographie

Gouvernance du risque et à la gestion du risque public. Fondée par des directeurs généraux des collectivités locales, le groupe Marsh, Dexia, elle fait partie du réseau européen de PRIMO EUROPE, pour bénéficier des meilleures informations de bonnes pratiques et de benchmarking https://www.primo-europe.eu/ https://www.primofrance.org/tag/association/ Label de Gestion des risques Territoriaux – PRIMO - 2012 https://www.primofrance.org/wp-content/uploads/2014/08/plaquette-label-juillet-2014.pdf « Préparer le secteur public à la gouvernance des risques publics : premiers pas vers un référentiel ISO 31000 » MARSH - 2010 https://primo-europe.eu/wp-content/uploads/2011/07/preparing-public-sector-forriskgovernance-first-steps-towards-a-iso-31000-framework-vl.pdf	Préambule : Organisations publiques ou parapubliques
IEAE (Institut Européen Administration Etendue) : https://www.decision-achats.fr/Thematique/achats-publics-1230/Breves/Creation-Institut-europeen-administration-etendue-189103.htm	
Comparaison secteur privé / secteur public – KPMG 2017 : PRIMO - Public Risk Management Organisation : Association dédiée à la go	
Exemple de charte de gestion des risques dans le secteur public : https://www.banquedesterritoires.fr/sites/default/files/ra/%20La%20charte%20de%20la%20gestion%20des%20risques%20en%20secteur%20public%20local.pdf	
Critical Risks Facing the Public Sector https://riskandinsurance.com/7-critical-risks-facing-the-public-sector/#_blank	
« Trajectoire vers un Enterprise Risk Management » Collection Maîtrise des risques - AMRAE – 2012	Section 1. L'Entreprise étendue et son écosystème
Rencontres AMRAE 2016 – Atelier C07 « De la sous-traitance à l'Entreprise étendue » Rencontres AMRAE 2018 – Atelier C5 « Entreprise étendue et entreprise intégrée » Rencontres AMRAE 2019 – Atelier B4 « Gouvernance et Gestion des risques occasionnés ou partagés avec des tiers »	Section 1. L'Entreprise étendue et son écosystème Section 2.1 Quels sont les risques de l'Entreprise étendue Section 3 Le traitement des risques de l'Entreprise étendue

Les liens internet fournis dans l'ouvrage ont été testés valides en février 2023.

Deloitte, Extended enterprise risk management global survey 2019 https://www2.deloitte.com/za/en/pages/risk/articles/extended_enterprise_risk_management_global_survey_2019.html	Section 1. L'Entreprise étendue et son écosystème
23rd Annual Global CEO Survey - Navigating the rising tide of uncertainty - 2020 Global CEO Survey - 23ème édition | PwC ou https://www.pwc.fr/fr/publications/dirigeants-et-administrateurs/global-ceo-survey.html	Section 1. L'Entreprise étendue et son écosystème
CNA – Baromètre Acheteurs 2019 https://www.leslivresblancs.fr/livre/entreprise/achats/le-barometre-2019-des-decideurs-achats	Section 1. L'Entreprise étendue et son écosystème
« Leading the IoT « - Gartner Group, 2017 "State of IOT 2021" – IOT Analytics, 2021	Section 1. L'Entreprise étendue et son écosystème
CESIN - Baromètre Cybersécurité des entreprises 2019 et 2020 http://croissanceinvestissement.com/index.php/2019/01/16/barometre-cybersecurite-des-entreprises-francaises/	Section 1. L'Entreprise étendue et son écosystème
DFCG, étude EULER HERMES 2019 « Fraude & Cybercriminalité : Quelle menace pour les entreprises ? » https://www.finance-gestion.com/dossier/barometre-euler-hermes-dfcg-2019-8-10-entreprises-craignent-une-accentuation-du-risque-de-fraude-et-de-cybercriminalite-en-2019/ Etude fraude 2019 : Pour 6 entreprises sur 10, la lutte contre la fraude n'est pas une priorité https://www.eulerhermes.fr/actualites/etude-fraude-2019.html	Section 1. L'Entreprise étendue et son écosystème
Deloitte, Les Echos 20 septembre 2019 https://business.lesechos.fr/directions-financieres/comptabilite-et-gestion/gestion-des-risques/0601882038780-gestion-des-risques-les-entreprises-anticipent-mal-ceux-provoques-par-des-tiers-331795.php	Section 1. L'Entreprise étendue et son écosystème
Etude Accenture « Securing the Digital Economy : Reinventing the Internet for Trust » - 2019 https://www.accenture.com/_acnmedia/thought-leadership-assets/pdf/accenture-securing-the-digital-economy-reinventing-the-internet-for-trust.pdf	Section 1. L'Entreprise étendue et son écosystème
CDSE – Baromètre CDSE/Axa Partners 2019 https://cdse.fr/barometre-cdse-2019-securite-des/ 5ème édition du Baromètre de la sécurité des collaborateurs à l'international	Section 1. L'Entreprise étendue et son écosystème
GRI : https://www.globalreporting.org SiteCollectionDocuments/2018/ GSIP%20Webinar%201%20Introduction%20to%20the %20GRI%20Standards.pdf	Section 1.4.5 Le sociétal et l'environnemental Section 1.4.9 Autres enjeux et dimensions à traiter
« La guerre des métaux rares » Guillaume Pitron – 2018 – éditeur : LLL - Les Liens qui Libèrent	Section 1.4.7 Les technologies
« Nouvelles technologies – nouveaux risques » - symposium de l'Institut national de médecine agricole – Tours 2017	Section 1.4.7 Les technologies
« Cloud Act » https://fr.wikipedia.org/wiki/CLOUD_Act https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/le-cloud-act-favorable-ou-prejudiciable-a-la-vie-privee-des-internautes-3-5-837994.html	Section 2.4.3 Des cartographies spécifiques ? Section 3.2.2 Appréhender et gérer la notion de partie prenante externe
Règlement CRBF 97-02 révisé par l'«Arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution. » https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=D20122F6E6191BECA52297F04F76D4B5.tplgfr28s_3?cidTexte=JORFTEXT000029700770&idArticle=&categorieLien=id	Section 2.4.3 Des cartographies spécifiques ?
Guide pratique de l'AMRAE : Accompagner votre entreprise dans la définition de son appétence aux risques LA BIBLIOTHÈQUE DE L'AMRAE | AMRAE Rencontres AMRAE 2017 – Atelier C7 « Définition et utilisation de l'appétit aux risques »	Section 3.1.2 Décider de l'appétence aux risques
« Le cygne noir : La puissance de l'imprévisible » essai de Nassim Nicholas Taleb, Les Belles Lettres - 2010	Section 3.1.3 Décider des risques à traiter
« Les rhinocéros gris : comment reconnaître et agir sur les dangers évidents que nous ignorons » ouvrage de Michele Wucker - 2016	Section 3.1.3 Décider des risques à traiter
« La BNP Paribas formellement condamnée à une amende record aux Etats-Unis » – Le Monde 01/05/2015 https://www.lemonde.fr/economie/article/2015/05/01/ la-bnp-paribas-formellement-condamnee-a-une-amende-record-aux-etats-unis_4626207_3234.html	Section 3.1.4 Intégrer les risques Entreprise étendue à la gestion des risques Section 3.2.2 Appréhender et gérer la notion de partie prenante externe
Article « Contrat de travail : la clause éthique reste exceptionnelle » https://www.lesechos.fr/idees-debats/leadership-management/contrat-de-travail-la-clause-ethique-reste-exceptionnelle-1247159 2014 Mazars,	Section 3.3.2 Sensibiliser, former, contractualiser

Les liens internet fournis dans l'ouvrage ont été testés valides en février 2023.

« La Communication sur les risques » Collection Maîtrise des risques - AMRAE – 2017	Section 3.3.2 Sensibiliser, former, contractualiser Section 3.4.3 Traiter les risques en situation de crise
« Les Plans de Continuité d'Activité » Collection Maîtrise des risques - AMRAE – 2015	Section 3.4.3 Traiter les risques en situation de crise
Nicholas Metropolis et Stanislaw Ulam, « The Monte Carlo Method », Journal of the American Statistical Association, vol. 44, no 247, septembre 1949, p. 335-341 Barreras, A. J. (2011). Risk management: Monte Carlo simulation in cost estimating. Paper presented at PMI® Global Congress 2011—North America, Dallas, TX. Newtown Square, PA: Project Management Institute. Risk management (pmi.org)	Section 3.4.4 Utiliser des outils
Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts COM (2021)206/F1 - EN (europa.eu)	Section 3.4.5 Outils du futur : s'approprier l'intelligence artificielle

Les liens internet fournis dans l'ouvrage ont été testés valides en février 2023.

AMRAE

la Maison du risk management

www.amrae.fr

Deloitte.

www.deloitte.fr

Le monde des affaires est aujourd'hui globalisé.

Par leurs interconnections avec leur écosystème, toutes les entreprises et les organisations publiques peuvent être considérées comme étendues, à plus ou moins grande échelle, quel que soit leur secteur d'activité.

Elles ne peuvent pas durablement fonctionner et survivre de manière isolée. Or l'étendue grandissante de leur sphère d'influence va maintenant au-delà des acteurs traditionnels (fournisseurs, clients, employés) de la chaîne de valeur. De nombreux autres acteurs externes dans l'environnement économique, sociétal ou politique de l'entreprise en font partie, aussi bien au niveau local que mondial.

Dès lors, prendre conscience des dépendances entre les événements externes et les acteurs, comprendre ce qui entoure l'organisation, mais aussi la vision des différents acteurs et leurs enjeux est fondamental pour un dirigeant ou un Risk manager. Ces éléments forment un ensemble de risques dans l'espace autour de l'organisation. Et cet environnement sans cesse en évolution interroge à présent le Risk manager sur la capacité de son organisation à gérer ces risques externes dans le temps..

Complexe et spécifique, la gestion des risques de l'entreprise étendue est un exercice inédit, à inscrire dans la durée, qui s'appuie sur des approches variées et complémentaires, que chaque organisation doit adapter à son propre contexte.

Cet ouvrage fournit un référentiel à même d'inspirer tout acteur de la gestion des risques dans sa démarche de protection des activités de son organisation et d'aide à la prise de décision.

AMRAE
la Maison du risk management

Deloitte.