

Méthodologie d'identification et d'analyse des risques

L'identification rationnelle et objective des risques de sinistralité est basée sur la réponse à quatre types d'interrogations :

- Quels sont les outils permettant une identification objective des risques ?
- Comment évaluer l'impact d'un sinistre majeur sur les objectifs stratégiques ?
- Comment évaluer les conséquences financières d'un sinistre majeur ?
- Quels enseignements tirer de l'évolution de la sinistralité antérieure ?

Outils d'identification des risques

L'une des principales difficultés du risk management est d'identifier les risques d'un groupe de façon objective et rationnelle. Il est indispensable d'aboutir à la réalisation d'une cartographie des risques faisant ressortir en priorité les méta-risques émergents.

Le risk manager n'a pas le droit de fonder sa cartographie sur un ressenti subjectif basé sur sa personnalité et son vécu professionnel. Il doit au contraire appuyer sa démarche sur plusieurs outils d'identification des risques qu'il va utiliser dans une optique de circularisation (la réponse apportée par ces outils doit en effet converger). Nous étudierons donc dans ce chapitre les outils suivants :

- l'audit documentaire ;
- les entretiens ;
- les visites de sites ;
- les questionnaires.

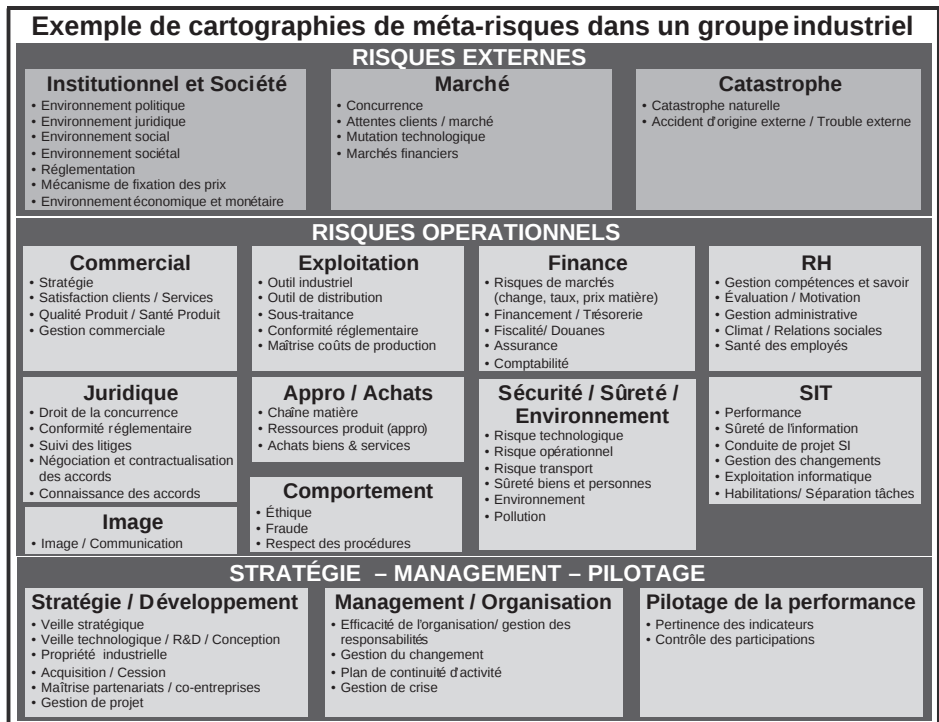
Audit documentaire et audit en risk management

L'audit documentaire est un outil essentiel en vue d'une identification rationnelle et objective des risques.

Dans la phase amont, l'auditeur va demander un certain nombre de documents, qu'il exploitera partiellement avant d'aller sur le terrain (phase de « travail à plat »).

Pendant la phase de déroulement de l'audit, l'auditeur va confronter ses sources documentaires avec les informations collectées via les interviews et la visite de sites.

En phase post-mission (rédaction du rapport), le risk manager préconisera ; compte tenu de ses conclusions, un certain nombre d'ajustements concernant les informations qu'il a collectées en phase initiale (modifications de clauses contractuelles, renégociation des clauses assurance, consultation du marché assurance, etc.).



Exemple de cartographie des méta-risques

Audit documentaire pré-mission

Dans la phase documentaire pré-mission, le risk manager va demander à l'entité auditée de lui transmettre un certain nombre de documents. La liste des documents à transmettre dépend de fait du type de risque à auditer.

Cependant, il s'avère possible de lister de façon générique les principaux documents demandés :

- programme d'assurance national ou international ;
- transmission des clauses des principaux contrats ;
- états analytiques et tableaux de bord ;
- états financiers certifiés ;
- experts techniques et expertises préalables de capitaux ;
- procédures de sécurité et de gestion de crise (si existantes) ;
- tests des plans de reprise d'activité ;
- schéma directeur des systèmes d'information ;
- plan de protection des informations.

Une fois ces documents collectés (dans les faits, le risk manager ne collecte qu'une partie des informations en pré-mission), il s'assure de la fiabilité des informations

transmises en utilisant les techniques de circularisation (demande d'information parallèle à l'externe, vérification de la certification des comptes, vérification de la non-rétroactivité des contrats, etc.).

Enfin, il commence à analyser les documents qui sont directement exploitables (analyse des clauses de contrats, analyse financière, etc.).

Audit documentaire pendant la mission

L'objectif du déroulement de la mission sur le terrain est de confronter l'identification des risques identifiés en phase post-mission d'audit avec les risques réellement tracés via interviews et/ou questionnaires et visites de sites.

Exploitation documentaire post-mission

L'exploitation documentaire post-mission va se traduire par des préconisations substantielles faites par le risk manager. Ainsi, les principales préconisations possibles sont les suivantes :

- souscription d'une nouvelle police d'assurance ;
- modification de clauses contractuelles ;
- signatures de contrats de back-up¹ ;
- rédaction de nouvelles procédures ;
- modification du contenu des procédures existantes.

Entretiens

La technique d'entretien s'avère être une technique essentielle à l'identification objective et rationnelle des risques, et ce, tout particulièrement en culture d'entreprise latine.

L'objectif de cet entretien est : d'une part, de s'assurer de la connaissance par les opérationnels des dispositifs de risk management mis en œuvre par l'entreprise ; d'autre part, d'évaluer avec eux les risques potentiels qui pourraient affecter les processus métiers et les risques du groupe.

L'interview se déroule en trois grandes étapes.

Analyse du passé

Le risk manager interviewe l'audité sur les cas de sinistres ou de gestion de crise qu'il a été amené à vivre dans le passé en adoptant un questionnement du type :

« Avez-vous été amené à vivre dans le passé une situation de crise ? Si oui, quels sont, de votre point de vue, les dispositifs mis effectivement en œuvre par le groupe pour gérer cette situation ? »

L'objectif de cette question est de savoir si les dispositifs mis en œuvre par le groupe sont connus et effectivement communiqués aux opérationnels.

1. Back-up : mise à disposition de ressources logistiques en cas de sinistre.

Projection sur le futur

L'objectif de cette partie de l'entretien consiste à identifier les risques potentiels que les opérationnels ont identifiés et qui n'ont pas été reportés au niveau du risk management.

La structure de questionnement est la suivante : « Avez-vous identifié ou pensé à des risques qui pourraient se matérialiser ? Êtes-vous déjà passé sur le “fil du rasoir” ? De votre point de vue, si le risque se matérialisait, le groupe saurait-il mettre en œuvre les dispositifs adéquats ? »

L'objectif de cette question est d'aller vérifier sur le terrain si le ressenti de l'opérationnel est confirmé ou non. Cette logique de questionnement peut permettre une priorisation de mesures correctrices à mettre en œuvre.

Simulation d'une situation de crise

L'objectif de cette dernière étape de l'interview consiste à construire avec l'audité le contenu opérationnel de son plan de reprise d'activité en cas de situation de crise.

La structure de simulation à adopter est la suivante :

« Vous arrivez sur votre lieu de travail à 7 h 45. Sur place votre siège social est détruit à 100 %. Le préfet, les médias, les salariés, la protection civile, les pompiers sont présents. Les camions arrivent avec les composantes. Que faites-vous ? »

L'objectif de cette simulation est de décrire les moyens logistiques qui devront être mis en œuvre en cas de situation de crise en vue d'assurer la continuité de l'exploitation des processus critiques.

L'exercice a pour objectif de décrire et d'identifier :

- les processus critiques qui devront être redéployés en cas de situation de crise ;
- les actifs stratégiques (machines-outils, moules, etc.) qui devront être protégés en priorité en cas de sinistre ;
- les hommes clés qui devront être déplacés sur le site de secours ;
- les ressources non utilisées avant sinistre (m^2 , m^3 , véhicules disponibles, etc.) ;
- les contrats de back-up avec les sous-traitants, fournisseurs, constructeurs informatiques, etc.

Visites de site

La visite de site est un outil essentiel en termes d'identification des risques. Elle permet par exemple d'observer les attitudes et les comportements des salariés en matière de respect des consignes de sécurité. Elle permet, d'autre part, à l'auditeur d'observer des dysfonctionnements ou des anomalies concernant l'organisation de l'entreprise pouvant générer des dommages potentiels.

Elle permet aussi de réactualiser des éléments liés à l'audit documentaire (exemple d'un plan de masse ne correspondant plus à la configuration réelle actuelle du site).

Questionnaires

L'identification des risques à partir des questionnaires est très utilisée dans les organisations anglo-saxonnes et présuppose l'existence d'un dispositif de risk management mûr et efficace.

Le questionnement permet de réaliser des benchmarks intersites et intragroupe, et de produire à ce titre des rosaces de performance permettant d'identifier les centres de risque¹ n'appliquant pas à la lettre les procédures de sécurité et de gestion de crise.

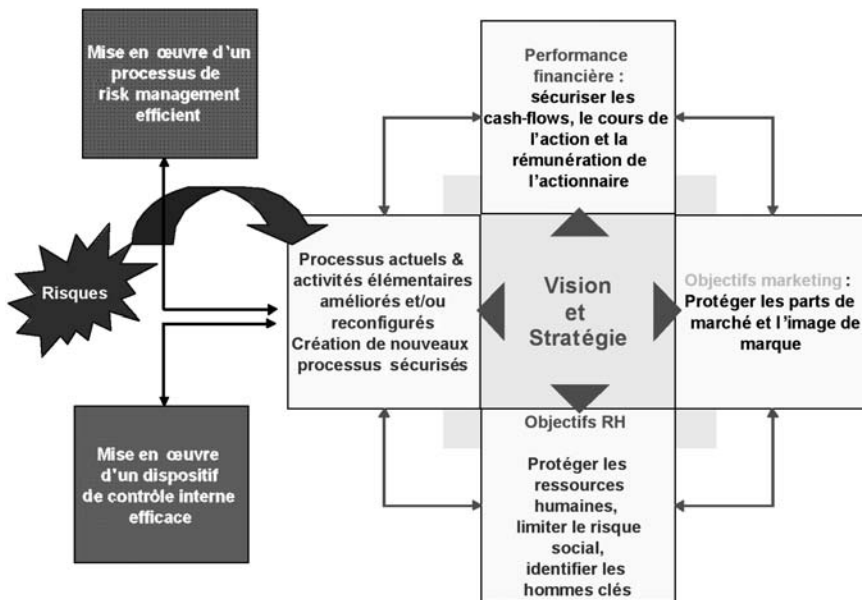
Ce dispositif est inadapté dans le cas de la construction d'un dispositif de risk management et, dans cette hypothèse, on privilégiera les techniques d'interviews.

Simulation de l'impact d'un sinistre majeur sur les objectifs stratégiques

L'objectif de cette étape est de simuler l'impact d'un sinistre maximum possible (c'est-à-dire d'un sinistre étant la résultante de plusieurs faits générateurs, majoré par des circonstances aggravantes) sur les processus et/ou les objectifs stratégiques de l'entreprise.

Ainsi, par exemple, le retrait d'un produit du marché (du fait de dommages corporels subis par un consommateur) affecterait :

- les parts de marché ;
- la rentabilité commerciale ;
- le cours de l'action (si le groupe est coté) ;
- la continuité des processus (obligation d'arrêter la production du produit incriminé).



Impact d'un sinistre majeur sur les objectifs stratégiques d'un groupe

L'objectif du risk management consiste donc à tout mettre en œuvre à titre préventif pour prévenir le risque ; mais, ce dernier avéré, le groupe doit mettre en place un

1. Entité organisationnelle (usine, magasin) regroupant des risques homogènes.

dispositif de gestion de crise auquel il a réfléchi à titre préventif, et gérer la situation de crise dans un délai très rapide. Dans notre exemple, les outils de gestion de crise mis en œuvre seraient les suivants :

- cellule de crise ;
- communication de crise vis-à-vis des consommateurs et du réseau ;
- plan de retrait des produits du marché avec mise en œuvre d'un processus d'indemnisation du consommateur ; ou fabrication d'un produit de substitution.

Ces procédures de gestion de crise ont bien sûr un caractère confidentiel, à l'exception du plan d'urgence, qui doit être communiqué aux autorités de tutelle, pour les risques RHP (risques hautement protégés) susceptibles de générer une atteinte à l'environnement.

Simulation des conséquences financières d'un sinistre majeur

L'objectif assigné à cette étape est d'identifier les scénarii de crise qui pourraient affecter la remise en cause de la pérennité du groupe. La quantification des sinistres majeurs a pour intérêt de permettre l'identification des scénarii inacceptables en vue de définir des priorités dans le dispositif de risk management.

Il s'agit donc de quantifier pour chaque scénario de crise (sont analysés en priorité les scénarii correspondant aux faits générateurs figurant en exclusion) les conséquences financières d'un sinistre maximum possible en chiffrant les quatre composantes suivantes :

- pertes matérielles (en quoi le sinistre affecte-t-il les actifs de l'entreprise ?) ;
- pertes d'exploitation (en quoi la situation de crise affecte-t-elle le compte de résultat ?) ;
- pertes humaines (en quoi le sinistre génère-t-il des dommages corporels chez les salariés ?) ;
- coût de la responsabilité civile et éventuellement pénale (quelle sera la valorisation de préjudices corporels, matériels et immatériels causés aux tiers ?).

Estimation des pertes matérielles

L'objectif de cette première simulation est d'estimer l'impact d'un sinistre majeur sur les immobilisations sous contrôle (au sens des normes IAS 16 et 17 pour lesquelles l'entreprise porte l'ensemble des risques et des responsabilités, quelle que soit leur qualification juridique) et sur les stocks.

Deux cas de figure se présentent dans le cadre de cette estimation :

- soit l'entreprise est dans un référentiel comptable autre qu'IFRS (International Financial Reporting Standard) et, dans ce cas de figure, elle doit faire réaliser une expertise préalable de capitaux des biens en propriété, en location, en location financièrement, mais aussi des biens confiés ou des actifs qu'on lui a transférés dans le cadre d'un contrat de concession ou d'affermage ;
- soit l'entreprise est en IFRS (International Financial Reporting Standard) et a opté pour la réévaluation des actifs et, dans ce cas, la valorisation des actifs au prix du marché sert de base à l'estimation des pertes matérielles.

Dans les deux cas de figure, l'estimation des pertes matérielles se fait en multipliant la valeur des capitaux par une estimation du pourcentage de destruction de l'actif.

Estimation des pertes d'exploitation

L'estimation des pertes d'exploitation est réalisée par centre de risque (ce qui correspond en contrôle de gestion à une entité organisationnelle du type « centre de profit » ou « centre de responsabilité »).

La méthodologie consiste dans un premier temps à construire un compte de résultat du centre de risque avant sinistre. L'objectif à ce niveau est de segmenter le compte de résultat en quatre grandes masses :

- chiffre d'affaires ou prix de transfert¹ ;
- charges variables qui seront sensibles à l'impact du sinistre ;
- charges fixes que l'entreprise continuera à supporter post-sinistre ;
- résultat analytique du centre de risque avant sinistre (différence entre produits et charges opérationnelles).

Dans un deuxième temps, à structurer un compte de résultat de l'entité post-sinistre :

- estimation du chiffre d'affaires ou des prix de cession post-sinistre (impact du sinistre sur le CA dépendant de l'existence d'un plan de reprise d'activité ou non, testé de surcroît régulièrement) ;
- estimation de l'impact du sinistre sur les charges variables (dont les achats) ;
- estimation du sinistre sur les nouveaux coûts générés par la situation de crise (frais supplémentaires d'exploitation, frais d'expertise, honoraires, frais de démolition, frais de décontamination, etc.).

Le résultat analytique post-sinistre est donc égal à la différence entre le CA et les charges opérationnelles post-sinistre (charges variables après sinistre, maintien des frais fixes supportés avant sinistre, nouveaux frais directement imputables à la situation de crise et nécessaires au redéploiement de l'activité).

La perte d'exploitation sera égale à la différence entre le résultat opérationnel du centre de risque avant sinistre (basé sur les prévisions budgétaires de l'exercice) et l'estimation du résultat analytique du même centre de risque post-sinistre.

Quantification des pertes humaines

La quantification des pertes humaines (c'est-à-dire des dommages affectant les salariés de l'entreprise : décès, accidents de travail, invalidité, etc.) se décompose en :

- indemnisation de type Sécurité sociale ;
- indemnisation via la souscription d'une police d'assurance collective pour le compte des salariés (en intégrant les capitaux maximaux prévus dans la police d'assurance).

1. Échanges économiques internes au groupe.

Valorisation du coût de la responsabilité civile et pénale

La quantification du coût de la remise en cause de la responsabilité civile passe par l'analyse de la jurisprudence existante au niveau international.

Dans l'hypothèse de l'inexistence d'une telle jurisprudence, l'auditeur appliquera une démarche qualitative en construisant une grille qualitative graduée de la façon suivante :

- 0 : impact nul ;
- 1 : impact faible ;
- 2 : impact financier moyen ;
- 3 : impact financier majeur ;
- 4 : impact financier inacceptable.

L'estimation du coût de la responsabilité pénale passe par une analyse des différentes pénalités par type d'infraction.

Quantification du coût résiduel à la charge de l'entreprise

L'objectif de cette étape du dispositif consiste à sommer par scénario le coût des quatre typologies de pertes : matérielles, exploitation, humaines et responsabilité civile (RC) ; et à le comparer au montant indemnisable prévu dans le programme d'assurance. La différence entre ces deux montants correspond au risque résiduel, qui peut être considéré par les autorités de gouvernance comme étant acceptable ou inacceptable.

Dans l'hypothèse où le comité des risques estime que le risque résiduel est inacceptable, il s'avère indispensable de réfléchir sur la mise en œuvre de financements alternatifs, n'affectant pas la trésorerie courante de l'entreprise en cas de réalisation du risque.

Étude de la sinistralité antérieure

L'étude de la sinistralité antérieure (sur des séries chronologiques consécutives *a minima* de cinq ans) vise à :

- identifier d'éventuelles tendances structurelles en termes de sinistralité (concentration d'accidents du travail par exemple) ;
- permettre une renégociation ultérieure avec les assureurs (en comparant la sinistralité effective avec celle prise en compte par les assureurs).

Les principaux sinistres analysés, tant en fréquence qu'en termes de gravité, sont les suivants :

- sinistralité dommages aux biens ;
- sinistralité flotte automobile ;
- sinistralité informatique ;
- sinistralité responsabilité civile ;
- sinistralité accidents du travail.

Modalités de mise sous contrôle des risques

La méthodologie d'audit en risk management est une approche transverse visant à s'assurer de la mise sous contrôle des risques de sinistralité de l'entreprise, tant à titre préventif que curatif, en déclinant un triple dispositif :

- contrôle interne des risques et procédures de gestion de crise ;
- contrôle technique et investissements de sécurité ;
- contrôle financier des risques intégrant l'autofinancement, le transfert des risques et le recours aux financements alternatifs à l'assurance.

Contrôle technique et sécurité

La mise en œuvre d'un dispositif de prévention mature passe par la réalisation d'investissements de sécurité et par l'engagement de charges d'exploitation au titre de la sécurité correspondant *a minima* aux exigences réglementaires.

Les principaux sous-domaines concernés sont les suivants :

- sécurité informatique ;
- sécurité des biens ;
- sécurité des personnes ;
- sécurité atteinte à l'environnement.

Procédures de sécurité et de gestion de crise

La mise en œuvre d'un dispositif de corporate risk management efficace passe par la rédaction de procédures de sécurité de base et de gestion de crise.

Bien évidemment l'efficacité de telles procédures doit être régulièrement testée.

Procédures de sécurité de base

La mise en œuvre d'un dispositif de corporate risk management mature passe par la rédaction et l'application de procédures de type « management des risques » telles que :

- procédures de sécurité informatique physiques et immatérielles et plan de protection des informations ;
- procédures de sécurité environnementale ;
- plan d'organisation des secours.

Les principaux scénarii de gestion de crise

La construction des scénarii de crise a pour objectif d'anticiper la combinaison optimale d'outils de gestion de crise à mettre en œuvre en cas de sinistre majeur.

Les principaux scénarii analysés sont les suivants :

- gestion de crise produit avec retrait des produits du marché ;
- atteinte à l'environnement ;
- mise en examen d'un mandataire social ;
- offre publique d'achat hostile ;
- attentat ;
- grève interne ou externe, voire mélange des deux typologies (grande spécialité française !) ;
- boycott de la marque ;
- situation de crise informatique ;
- mort d'un homme clé.

Il est évident que cette liste doit être adaptée en fonction du secteur d'activité, ainsi :

- dans le secteur bancaire, on simulera l'impact du scénario hold-up ;
- dans le secteur aéronautique, on évaluera les conséquences du crash d'un avion ;
- dans le secteur aéronautique, on estimera les conséquences de l'explosion d'une fusée ou d'une navette embarquant des satellites.

Procédures de gestion de crise

Les procédures de gestion, systématiquement rédigées à titre préventif, et testées en vue d'évaluer leur efficacité, ont pour objectif de permettre la continuité de l'exploitation des processus critiques d'un centre de risque (exemple d'une usine), dans des délais très rapides sur d'autres sites internes au groupe ou à l'extérieur du groupe via des contrats de back-up signés avec des constructeurs informatiques, fournisseurs et sous-traitants captifs, et éventuellement avec des concurrents.

Le risk manager doit donc réfléchir à titre préventif à la construction de ces cinq outils de gestion de crise, qui seront combinés en fonction du scénario de crise analysé, à savoir :

- le plan de retrait des produits du marché ;
- la communication de crise interne et/ou externe pouvant être offensive ou défensive ;
- le plan de reprise d'activité ;
- le plan d'urgence concernant les risques d'atteinte à l'environnement ;
- la cellule de crise conçue tant en termes organisationnels que logistiques.

Plan de retrait des produits

La réflexion préventive concernant l'organisation d'un plan de retrait des produits du marché concerne en priorité les entreprises ayant une stratégie marketing de biens de grande consommation et tout spécifiquement celles travaillant dans les secteurs pharmaceutique, agroalimentaire, automobile.

L'organisation logistique d'un plan de retrait prévoit un simple arrêt de production et de commercialisation à titre préventif dans le cas de l'émission de signaux de pré-alerte (taux de réclamations clients anormal, taux de rebut, de refaçonnage élevé, etc., sur un produit ou une famille de produits).

Communication de crise

Il existe de nombreux registres de communication de crise, sur lesquels les groupes doivent réfléchir à titre préventif, soit en vue d'exonérer la responsabilité civile, soit de limiter l'impact de cette dernière au cas où elle serait mise en cause.

Il est ainsi possible d'opposer les axes de communication ci-dessous :

- interne et externe ;
- offensive et défensive ;
- réglementaire et stratégique.

Communication de crise interne et externe

La communication de crise externe est en général indissociable de la communication de crise interne.

En effet, la communication de crise externe, qu'elle soit institutionnelle ou opérationnelle, vise à sécuriser l'ensemble des parties prenantes, pour protéger les objectifs stratégiques du groupe. *A contrario*, la communication de crise interne vise surtout à permettre le déploiement des processus critiques sur des sites non sinistrés dans des délais très rapides si une situation de crise est déclenchée.

Communication de crise offensive et défensive

Les registres de communication de crise peuvent être offensifs en cas de rumeur ou en cas de remise en cause non fondée de la responsabilité civile du groupe. Ainsi, il est envisageable, dans le cas d'un scénario de crise produit, de développer une communication de crise offensive, dans l'hypothèse d'une relation de corrélation (existence d'un dommage corporel chez un consommateur, ne pouvant être associé à une marque commerciale spécifique de l'entreprise).

Par contre, en cas de remise en cause de la responsabilité civile du groupe, la communication de crise institutionnelle défensive a pour objectif de protéger les parts de marché, l'image de marque, alors que la communication de crise opérationnelle décrit au réseau de distribution ainsi qu'aux clients les modalités d'action (comment se faire indemniser, comment faire réparer le produit, comment avoir un produit de substitution... ?).

Plan de reprise d'activité/plan de continuité de l'exploitation

Le risk management minimise le rôle de l'assurance en cas de sinistre majeur. Son objectif n'est pas de rechercher des garanties confortables en cas de situation de crise, mais de permettre une reprise de l'activité dans les délais les plus rapides. Voici la méthodologie de construction de ces plans de reprise d'activité.

Concepts généraux sur les plans de continuité de l'exploitation

La continuité d'activité s'inscrit dans une démarche de pérennité de l'entreprise. Elle consiste à mettre en place des procédures et des moyens visant à assurer le fonctionnement

de ses activités, principales et cruciales, et la disponibilité des ressources indispensables au déroulement de ces activités.

La gestion de la continuité d'activité est une approche globale de management. Son objectif est d'identifier les impacts potentiels qui menacent le groupe et de la doter des capacités de répondre efficacement à des sinistres potentiels en sauvegardant ses activités vitales et critiques, sa réputation et les intérêts de ses clients et partenaires.

Définition de la notion d'activité vitale

C'est une activité dont l'exécution est fondamentale et obligatoire pour l'entreprise. En cas d'arrêt de cette activité, les impacts sont jugés inacceptables par le management :

- impact financier extrêmement lourd pour l'entreprise ;
- très forte dégradation de son image de marque auprès des clients et des partenaires ;
- impact réglementaire majeur sans possibilité de négociation avec les institutions légales.

Définition de la notion d'activité critique

Il s'agit d'une activité dont l'exécution est souhaitée pour le groupe, mais qui ne revêt pas de caractère obligatoire. Les impacts, en cas d'arrêt de ces activités, sont jugés très préoccupants voire inacceptables pour la stratégie de l'entreprise, mais ne compromettent pas sa survie en cas de crise :

- impact financier lourd pour l'entreprise ;
- impact stratégique majeur ;
- très forte dégradation de son image de marque auprès des salariés et des médias ;
- impact réglementaire majeur avec possibilité de négociation avec les institutions gouvernementales.

Définition de la notion d'activité sensible

Par activité sensible, il faut entendre une activité dont l'exécution est préférable pour le bon déroulement des opérations. Les impacts, en cas d'arrêt de ces activités, sont jugés préoccupants, mais potentiellement acceptables dans un contexte de crise :

- impact financier moyen pour l'entreprise ;
- impact stratégique nul ;
- dégradation significative de son image de marque auprès des salariés et des médias.

Le cycle de vie de la continuité d'activité

Processus cyclique

La démarche « continuité d'activité » est un processus cyclique à travers lequel le groupe :

- évalue la solidité de son organisation et la vulnérabilité de ses activités à des sinistres majeurs ;
- définit la stratégie de continuité de ses activités critiques après sinistre ;
- met en place les solutions de continuité pertinentes et les documente ;

- teste ses dispositifs, les maintient opérationnels et les révise à fréquence régulière ;
- informe ses personnels et les exerce à utiliser les solutions de continuité en cas de sinistre.

Deux prérequis sont indispensables pour engager la démarche « continuité d'activité » :

- une stratégie d'entreprise clairement définie ;
- un *risk assessment* solide et exhaustif.

Les principaux résultats attendus (livrables)

Ce sont :

- une cartographie des risques ;
- un *business impact analysis*, une collecte des expressions de besoins des métiers, mettant en évidence les activités critiques ;
- une stratégie de continuité d'activité déclinée en fonction de différents scénarii de sinistres, et adressant les objectifs métiers, les priorités et les niveaux d'activité à recouvrir après un sinistre ;
- un inventaire des ressources critiques et le séquençage de leur montée en charge ;
- des plans de continuité d'activité décrivant les dispositifs mis en place et les procédures pour mettre en œuvre la stratégie ;
- des programmes de tests et des plans d'action correctifs ;
- des supports d'information, de sensibilisation et de formation.

Mettre en œuvre un plan de continuité d'activité

Le *business impact analysis* (BIA) est une démarche analytique dont l'objectif consiste à :

- identifier les activités vitales/critiques ;
- inventorier les ressources critiques nécessaires pour assurer la continuité de ces activités vitales/critiques ;
- définir les priorités de continuité et/ou de reprise après sinistre.

Pourquoi le fait-on ? Le BIA permet d'évaluer les impacts, pour l'entreprise, d'un sinistre touchant ses activités. La démarche doit être entreprise pour chacun des processus métiers conduits dans le groupe, identifiés dans la phase de cartographie des processus.

Les conséquences d'un sinistre sur les activités du groupe sont évaluées dans le temps selon différents types d'impacts :

- impacts financiers (évaluation quantitative) ;
- impacts non financiers (évaluation qualitative).

Bien que les sinistres auxquels la société doit se préparer soient de natures différentes et puissent influencer la gravité et/ou la rapidité d'apparition/de résorption des impacts, les bonnes pratiques recommandent de mener le BIA en adoptant certains postulats :

- toutes les activités sont interrompues sans possibilité de reprise ;
- l'entreprise seule est impactée par le sinistre ;
- tous les acteurs du marché continuent « *business as usual* ».

La démarche BIA est conduite par les coordinateurs des plans de continuité d'activité (PCA) sur la base d'interviews réalisées avec les propriétaires des processus métiers. Les informations collectées ainsi que les analyses d'impacts sont systématiquement validées par le management, qui est responsable de l'expression des besoins, de la définition des stratégies, de l'allocation des moyens humains et financiers nécessaires à la démarche et qui est propriétaire des plans de continuité.

La démarche BIA

Elle se déroule en étapes distinctes.

Étape 1 : cartographie des processus métiers

La compréhension de l'organisation commence nécessairement par une cartographie décrivant les activités de chacune des entités du groupe :

- identifier les principaux processus métiers ;
- inventorier les ressources requises pour mener à bien chacun de ces processus.

Cette cartographie est le préalable indispensable au déploiement de la démarche BIA et plus généralement de la démarche de continuité d'activité : l'analyse d'impact, la définition des objectifs de reprise et les expressions de besoin en termes de ressources sont construites au niveau de chaque processus métier.

À noter que, s'il existe déjà des descriptions de processus dans l'organisation, elles doivent être systématiquement réutilisées dans un souci de cohérence et d'efficacité.

La cartographie doit aussi mettre en lumière les périodes critiques de chaque processus, c'est-à-dire les périodes durant lesquelles un sinistre aurait les impacts les plus pénalisants pour l'entreprise (« scénario du pire »).

La définition des périodes critiques permet :

- de définir les stratégies de reprise en intégrant le scénario dans lequel un sinistre aurait lieu aux moments les plus critiques du processus ;
- d'informer, le cas échéant, les gestionnaires de crise des circonstances particulières liées à la période de déclenchement du sinistre.

Exemples de périodes critiques : arrêts comptables, cut-off, échéances à terme, etc.

Pour les besoins de cette cartographie, des ressources critiques doivent être identifiées. Les ressources critiques à identifier sont les ressources indispensables à l'accomplissement d'un processus métier qui doivent nécessairement être restaurées pour garantir la continuité des activités critiques suite à un sinistre.

On peut ainsi citer :

- besoins en personnel : nombre de personnes allouées au processus métier en production ;
- systèmes informatiques :
 - applications métiers,
 - progiciels intégrés,
 - disques partagés ;
- poste de travail : type de configuration requise (nombre et puissance des PC, nombre d'écrans, téléphonie normale ou spécialisée, etc.) ;

- télécoms : inventaire des moyens de communication nécessaires en plus de la téléphonie (fax, télex) ;
- sauvegardes vitales : ensemble des documents sur tout support dont l'absence après sinistre empêcherait de reprendre le processus métier ;
- dépendances : ensemble des services, fournis par un acteur interne ou externe, nécessaires à l'accomplissement du processus métier (qui ? quoi ?).

Étape 2 : l'évaluation des impacts

Typologies d'impacts

- pertes financières directes : c'est l'ensemble des pertes financières supportées par l'entreprise résultant de son incapacité à gérer ses processus métier ;
- pertes de revenus : impacts financiers dus à l'incapacité de l'entreprise de réaliser de nouvelles transactions tant que ses processus métiers restent dégradés (d'où perte d'opportunités) ;
- impacts réglementaires : risques de pénalités de la part des régulateurs et des autorités de tutelle à l'encontre de la société dans l'incapacité totale ou partielle de faire face à ses obligations réglementaires ;
- impacts légaux et juridiques : impacts potentiels ou pertes encourues à cause d'actions en justice ou de poursuites de la part de clients, suite à l'incapacité de l'entreprise à faire face à ses engagements contractuels ;
- impacts sur l'image et la réputation : préjudices portés à la crédibilité de l'entreprise vis-à-vis de ses clients, des investisseurs, de ses actionnaires, des agences de rating ou des médias, conduisant à une perte substantielle d'opportunités à venir ;
- impacts sur d'autres processus de l'entreprise : risques d'extension d'impacts sur d'autres processus du groupe, lorsque des impacts directs ne peuvent pas être mis directement en évidence. Ce type d'impacts est directement lié aux interdépendances entre les différentes activités du groupe.

La relation au temps

Le critère de temps est une dimension clé dans l'évaluation des impacts, car il permet de concentrer les efforts sur les activités dont les délais de reprise sont les plus critiques.

L'échelle de temps est construite selon :

- les impératifs de reprise définis par les régulateurs (en France et à l'international) ;
- les bonnes pratiques de l'industrie ;
- les délais contractuels de bascule des systèmes d'information et de mise à disposition des solutions de repli.

Chaque activité doit définir une échelle pertinente lui permettant de quantifier de manière homogène et cohérente ses pertes financières potentielles. Ces quantifications sont ensuite traduites en degrés d'impacts en fonction de leur importance :

- très élevé ;
- élevé ;
- moyen ;
- faible.

Il appartient au management de chaque entité de définir et valider cette échelle, car celle-ci sera utilisée pour définir les objectifs et arbitrer les priorités de reprise. Les impacts qui ne peuvent pas être quantifiés en termes financiers sont qualifiés selon le même type d'échelle.

Étape 3 : déterminer la stratégie – définition des objectifs de reprise

Une fois l'analyse d'impact réalisée, le groupe est en mesure de définir pour chacun des processus métiers étudiés :

- la période de temps maximale après le sinistre, au cours de laquelle chacune des ressources nécessaires à l'accomplissement d'un processus métier pour être opérationnelle doit être recouverte (*recovery time objectives [RTO]*) ;
- le niveau d'activité qui doit être repris pour chaque processus, ainsi que son évolution dans le temps sur une période d'un mois à compter de la survenance du sinistre.

La définition des objectifs de reprise doit permettre de comprendre la stratégie que les métiers souhaitent mettre en place pour assurer la continuité de leur activité avec un niveau acceptable de dégradation suite à un sinistre. La stratégie est ainsi formulée de manière simple : en cas de sinistre et pour chaque métier, quelles capacités le groupe veut-il conserver ou recouvrer, et à quelles échéances ?

Comme lors de l'analyse d'impact, la bonne pratique veut que la stratégie et les objectifs de reprise soient définis au regard du scénario le plus impactant pour le processus métier considéré (l'entreprise est la seule impactée, les autres acteurs du secteur opèrent normalement).

La définition des RTO repose obligatoirement sur la cartographie et l'analyse d'impact réalisée avec le BIA :

- implicitement, le RTO indique le niveau d'impact que le métier accepte de supporter (le seuil de tolérance) ;
- les périodes critiques identifiées lors de la cartographie des processus sont prises en compte dans la définition de la stratégie de reprise (objectifs et priorités en cas de sinistre survenant à la pire période).

Étape 4 : élaborer et mettre en place des solutions

Les métiers ayant défini leur stratégie de continuité d'activité et formulé leurs besoins en ressources critiques sont maintenant en mesure de :

- consolider les besoins de secours applicatifs en spécifiant aux maîtrises d'ouvrage informatique les besoins à couvrir en termes d'objectif de reprise et de restauration de données ;