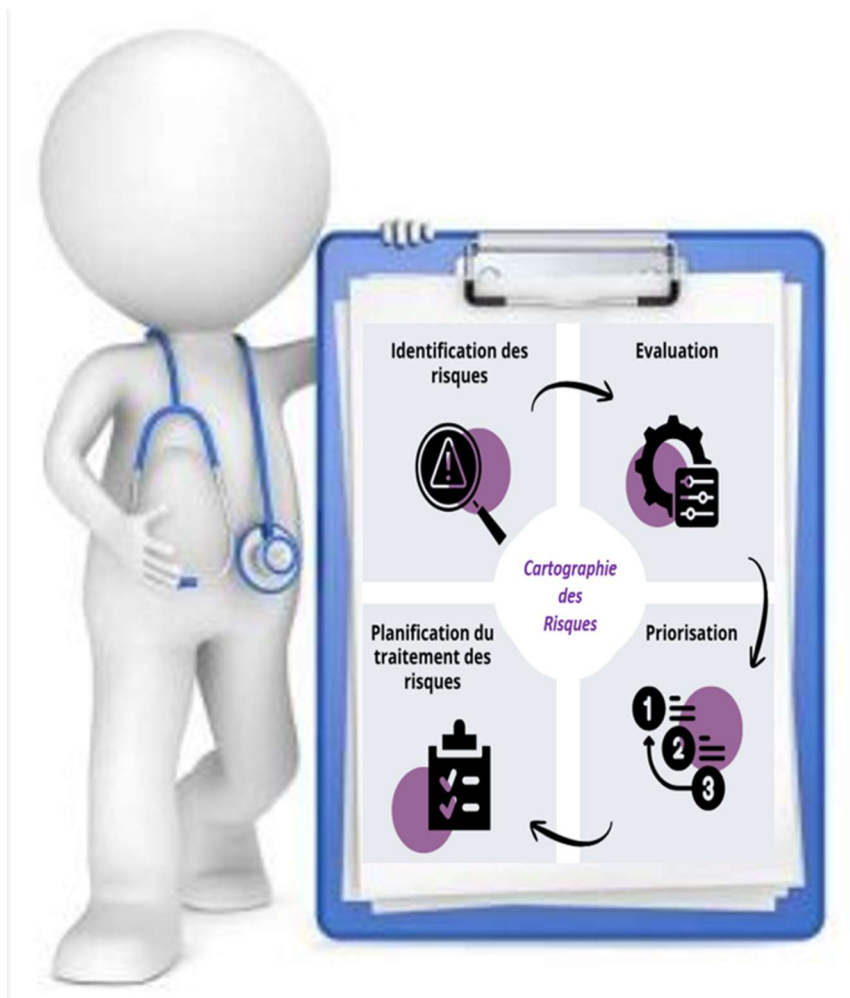




La cartographie, Outil d'acculturation



La cartographie des risques, outil d'acculturation

Etablir une cartographie des risques permet de recenser les vulnérabilités auxquelles est soumise une organisation, et partant, de prioriser ses actions correctrices. La construction de cette cartographie relève d'une démarche séquencée comme le détaille Jean-Marc Benard, entre définition des notions de base, du périmètre concerné, et identification des risques et impacts associés (en distinguant sinistralité brute ou nette).

Dans chaque activité, quelle que soit l'organisation, la présence de vulnérabilités est incontestable. En effet, comment peut-on imaginer une société ou un monde sans danger ?

Les vulnérabilités font partie de notre fonctionnement et de notre quotidien, et nous nous en accommodons avec une approche plus ou moins rigoureuse.

Alors, faut-il se faire peur ? Faut-il être anxigène ? Faut-il s'alerter ? Faut-il en parler ?

La réponse se trouve dans la vision que l'on souhaite en avoir. La vision négative serait celle qui fait peur et la vision positive, celle synonyme de prise de conscience tout simplement. Attention, le terme « simplement » pourrait laisser croire à une facilité que tout à chacun pourra mesurer à sa juste valeur en fait, l'idée serait de nous interdire de cacher les vulnérabilités et, au contraire, de s'obliger à les exposer. En effet, les recenser et les afficher permet de réduire les erreurs involontaires généralement porteuses de conséquences significatives, graves ou parfois irréversibles notamment lorsque l'humain est concerné.

Alors, sachant qu'une vulnérabilité ou un danger génère automatiquement une alerte ou un risque et que ce dernier s'évalue en impact, un recensement le plus exhaustif possible de l'ensemble des vulnérabilités conduit à construire une cartographie des risques. De par les impacts calculés, cette cartographie se matérialise dans une matrice et oriente ainsi une hiérarchisation des priorisations.

Définir les notions

Avant de raisonner cartographie, définissons quelques termes utilisés afin de bien comprendre le besoin et les enjeux.

- L'incident se caractérise comme un dysfonctionnement, une anomalie ou une défaillance quel que soit le sous-jacent.
- Le risque correspond à une alerte issue d'un danger plus ou moins prévisible inhérent à une situation ou une activité. Il est avéré lorsque l'incident s'est réellement produit, il est potentiel lorsque celui-ci est connu mais non avéré. Le risque imprévisible devient un aléa.
- L'impact est une conséquence issue d'une alerte ou d'un risque et se recense en deux catégories, l'impact financier et l'impact d'image.
- Les dispositifs de maîtrise des risques recensent les moyens nécessaires afin de diminuer ou d'éviter les impacts associés. Ils se positionnent sur deux niveaux, le

dispositif de prévention qui réduit la fréquence annuelle d'un incident ou décale dans le temps la fréquence d'un incident considéré comme rare (au-delà d'une année), et le dispositif de protection qui réduit ou évite la gravité de l'impact d'un incident lorsque ce dernier est avéré.

- La cartographie se définit comme le recensement des risques qui apporte une connaissance précise et actualisée des vulnérabilités de l'organisation et de son environnement. Il est à noter que les risques imprévisibles ne peuvent pas intégrer une cartographie de par la difficulté de les recenser et de l'impossibilité de les évaluer.

Déterminer le périmètre minimal concerné

Quelle que soit son activité (entreprise, industrie, service, association, collectivité, etc.), une organisation nécessite des moyens basiques pour fonctionner. Ils se résument à trois besoins indissociables : les moyens humains, ensuite les moyens matériels, puis les processus pour exécuter et réaliser. Enfin, comme toute organisation est exposée vis-à-vis de son environnement, elle a nécessairement besoin de se protéger contre tout ce qui gravite autour d'elle.

Le périmètre observé pour l'identification des risques se retrouve ainsi balisée par ces éléments : il se compose de l'ensemble des vulnérabilités sur les personnes, sur les biens et systèmes d'information, sur les processus et sur les événements extérieurs.

Répertorier les risques.

A partir du moment où le périmètre est ciblé, les vulnérabilités sont corrélées aux alertes, en d'autres termes, aux risques constatés ou détectés.

Avant de reprendre chaque item du périmètre cité ci-dessus afin d'affecter les risques associés, précisons les catégories génériques de la sphère risque (figure 1). En effet, certains risques sont prévisibles alors que d'autres deviennent imprévisibles puisqu'aléatoires.

Trois catégories apparaissent et traduisent une équivalence financière mesurable prévisible ou imprévisible.

- La catégorie risque principal se définit comme le risque aléatoire dont la prévisibilité est difficile de par l'absence de connaissance du futur ou de par une volumétrie trop importante. Pour le secteur bancaire, il correspond au risque de crédit où le risque de non remboursement est aléatoire. Sa protection financière est caractérisée par une charge de risque calculée essentiellement à partir de statistiques historiques.

- La catégorie risques de gestion financière correspond aux risques imprévisibles de la gestion financière de la trésorerie de l'organisation. Elle dépend essentiellement de critères externes de nature économique, politique, géographique, sectorielle, etc. Qu'ils soient de taux, de marché, de liquidité ou de change, sa protection financière réside principalement sur l'utilisation d'instruments sur les marchés dérivés.

- La catégorie risques opérationnels est souvent considérée, par manque de connaissance, comme cloisonnée à un périmètre restreint. Or, elle repose sur tous les autres risques non cités ci-dessus. De ce fait, contrairement aux deux précédentes, cette catégorie rassemble un nombre démultiplié et illimité de risques considérés comme connus, donc envisageables. Sa protection repose sur la mise en place des dispositifs de maîtrise des risques correspondants.

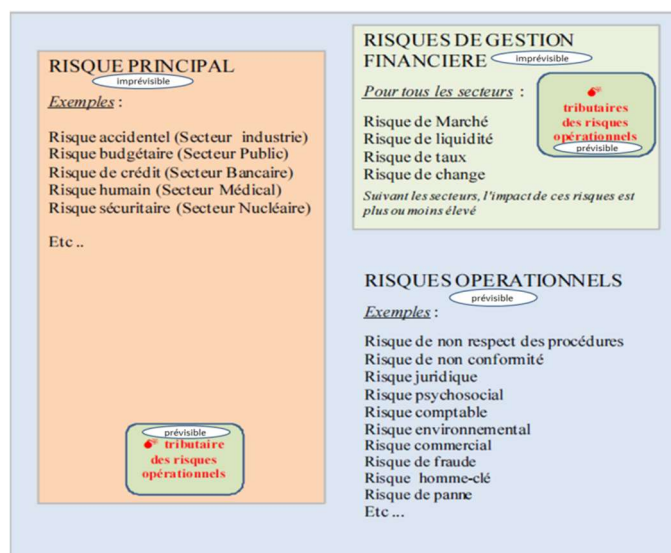


Figure 1

La notion « tributaire des risques opérationnels » précisée dans les risques principaux et de gestion financière doit être comprise comme des situations autres qu'imprévisibles. Pour exemple, une erreur réalisée lors de passation d'un ordre sur le marché boursier (gestion financière) n'est pas un risque aléatoire, le respect de la procédure aurait dû l'éviter, c'est donc un risque opérationnel.

La cartographie repose sur des risques connus et prévisibles.

Etant donné que le périmètre est complet et que la cartographie s'appuie sur des risques connus et prévisibles, elle devient en quelque sorte globale. De ce fait, sur ce périmètre, nous pouvons répertorier les différents risques ; bien sûr, la liste évoquée est non exhaustive mais permet d'avoir un aperçu étendu.

Sur les personnes, les risques correspondent aux risques physiques, intellectuels, psychosociaux, déontologiques, d'absentéisme, commercial, mais aussi ceux sur les compétences, la formation, la malveillance interne, etc.

Sur les biens et systèmes d'information, ils reposent sur le matériel, l'immatériel, le mobilier, l'immobilier, l'énergie, la mécanique, etc.

Sur les processus et procédures, ce sont essentiellement les défauts d'actions de contrôle mis en cause notamment sur le fonctionnement des activités, la réglementation, la conformité, la sécurité, la comptabilité, etc.

Enfin, sur les événements extérieurs, les risques trouvent leur origine sur l'environnement, la malveillance externe, les prestataires et fournisseurs, les médias, etc.

Les types de risque et les besoins associés

Une fois les risques répertoriés, il faut ensuite les classer afin d'apporter des éléments d'évaluation. Le classement des risques permet de mettre en place une méthodologie d'évaluation cohérente et pertinente.

On distingue d'abord les risques classés comme fréquents ou courants. On les répertorie sur le critère du nombre d'incidents détectés et constatés sur l'année d'observation. En d'autres termes, ils correspondent aux risques susceptibles de se produire une à plusieurs fois par an. Puis, on identifie les risques classés comme rares. À l'inverse des risques fréquents, ceux-ci sont susceptibles de ne pas se produire sur l'année d'observation.

Ce classement est important puisqu'il détermine les modalités d'évaluation.

Avant de décrire la méthodologie, il est nécessaire de préciser également les besoins. Ceux-ci reposent sur deux notions pour apporter toute la transparence de la gestion afin de piloter en toute connaissance de cause.

- La première notion est celle de l'évaluation de la sinistralité brute. Elle calcule la valeur réelle des vulnérabilités sans dispositif et permet d'établir une hiérarchisation des priorités. Cette notion possède aussi la faculté de donner une valeur concrète de chaque vulnérabilité qui permet de diffuser des degrés de sensibilisation.

- La seconde notion est l'évaluation de la sinistralité nette. Elle apporte une lecture directe sur l'efficacité des dispositifs de prévention et protection en place.

Le croisement entre la sinistralité brute et la sinistralité nette permet d'identifier les points de faiblesse de l'organisation.

À partir de ces besoins, nous pouvons calculer les impacts. Chaque risque génère un ou plusieurs impacts. Comme défini un peu plus haut, les impacts se recensent en deux catégories : l'impact financier et l'impact d'image. Longtemps laissé de côté, l'impact d'image devient une donnée à part entière face à l'évolution de notre société où l'information n'a plus de limite géographique et devient pratiquement instantanée.

La méthodologie d'évaluation des impacts

L'impact financier est la résultante de la multiplication entre la fréquence et la gravité d'un incident. L'impact d'image se définit comme la résultante d'un risque de notoriété, médiatique ou de réputation. Son évaluation se réalise à partir de critères qui, cumulés, génère des niveaux d'alertes plus ou moins significatifs.

Déterminons la méthodologie et ciblons les données des modalités de calcul.

- Les données du dispositif de protection, éléments de base d'analyse du risque fréquent.

Le dispositif de protection permet de réduire la gravité d'un ou plusieurs risques avérés. Ceux-ci sont considérés comme risques fréquents puisque susceptibles de se produire à minima une fois sur l'année en cours. Les incidents sont connus et les éléments de ce dispositif apportent des données financières concrètes pour mesurer l'efficacité. Plus précisément, dans une base de collecte d'incidents, les dysfonctionnements doivent être enregistrés en sinistralité brute, c'est à dire à partir du montant potentiel maximum que l'organisation peut subir. Suivant la durée de vie de l'incident, celui-ci se clôture en prenant en compte les récupérations financières et/ou l'enregistrement des pertes. De ce fait, la sinistralité brute représente le montant maximum que peut subir l'organisation et la sinistralité nette exprime le coût comptable. La différence correspond à l'efficacité des dispositifs, de prévention pour la volumétrie et de protection pour la gravité.

- Les données du dispositif de prévention, éléments de base d'analyse du risque rare.

Par définition, les risques rares ne se produisent pas dans l'année d'observation. Les incidents sont prévisibles et les données du dispositif de prévention apportent les attributs d'appréciation pour déterminer l'efficacité. Contrairement aux risques fréquents, l'objectif n'est pas de réduire la volumétrie (nulle dans l'année observée) mais de mettre tout en œuvre afin de décaler dans le temps sa survenance donc d'enrichir suffisamment le dispositif de prévention. En règle générale, la sinistralité brute d'un risque rare se détermine par une fréquence de 1 (même si une volumétrie un peu plus importante est parfois possible dans certains cas) et d'une gravité unitaire pratiquement identique à la sinistralité nette. Sachant qu'une actualisation se planifie à minima annuellement, la révision du dispositif s'assure que son efficacité est reconduite chaque année.

La hiérarchisation des risques

Les données évaluées, la cartographie se met en place et prend forme. Elle se concrétise par une matrice basée sur les risques bruts.

Plusieurs matrices ont été élaborées depuis des années afin de cibler les risques majeurs, acceptables ou encore mineurs comme par exemple la matrice de Prouty qui croise fréquence moyenne et gravité moyenne de chaque risque. Ces matrices apportent des éléments de réflexion afin d'établir un diagnostic pour d'éventuelles actions sur la fréquence et/ou sur la gravité. Mais, en considérant qu'il existe deux impacts, financier et d'image, n'est-il pas judicieux de reconsidérer cette matrice avec des axes d'abscisses et ordonnées qui reposent sur l'impact financier et l'impact d'image (figure 2).

Le croisement des évaluations déclenche ainsi une visualisation plus précise où l'impact image peut prendre une importance capitale même si l'impact financier semble être mineur.

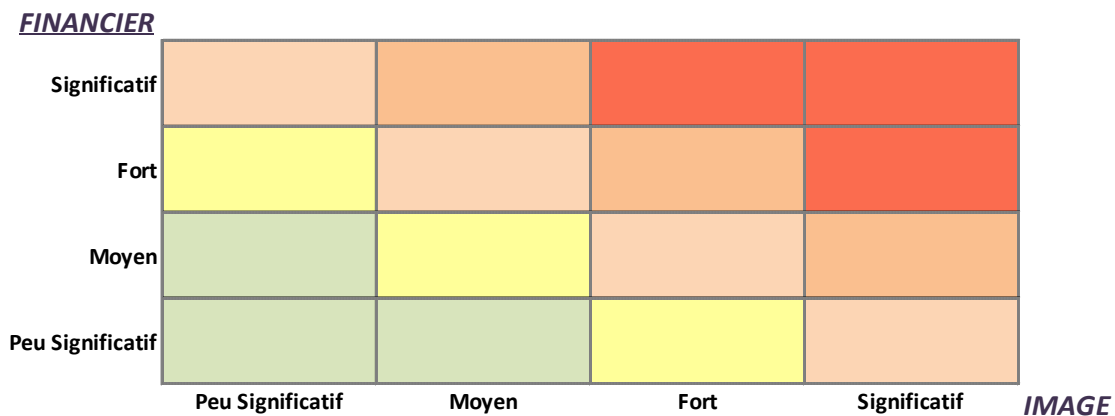


Figure 2

Bien sûr, les niveaux d'impacts doivent être traduits suivant l'activité de l'organisation, l'impact financier par fourchette (à partir du calcul fréquence * gravité) et l'impact d'image par strate de perception (suivant les publics visés). Prenons une illustration pour une grande collectivité territoriale. Un taux trop important d'absentéisme génère un *impact financier* « fort » de par le coût des remplacements temporaires pour assurer la continuité des activités, mais également un *impact image* « significatif » pour la population concernée face à un surplus de dépenses financières converti dans les impôts annuels. Dans un autre registre, un établissement bancaire refuse d'indemniser un client suite à une réclamation. Même si la banque peut être dans son droit juridiquement et malgré un *impact financier* « peu significatif », la situation peut générer un *impact d'image* « significatif » si le client interpelle les médias.

La cartographie des risques

La matrice définie et les évaluations réalisées, la cartographie des risques positionne les résultats dans une matrice où les risques fréquents et rares peuvent être distincts. En effet, suivant le classement des risques, la visualisation de l'efficacité des dispositifs sera plus caractérisée pour les risques fréquents que pour les risques rares.

Attention, une visibilité sur la seule cartographie à sinistralité nette est restrictive puisqu'elle minimise certaines activités, certes sécurisées par des dispositifs efficaces, mais sensibles et dangereuses en cas de modification d'organisation ou de fonctionnement.

De ce fait, la meilleure visibilité pour un dirigeant reste une matrice de la cartographie en sinistralité brute. C'est la plus rationnelle qui recense une hiérarchisation juste des vulnérabilités des différentes activités de l'organisation avant dispositifs de maîtrise. Bien sûr, comme précisé un peu plus haut, son croisement avec les sinistralités nettes aboutit à l'identification des points de faiblesse de l'organisation.

Outil de sensibilisation et de diffusion d'une culture risque

Que ce soit au niveau organisation sur les risques les plus importants ou au niveau activité locale pour les risques dédiés, la cartographie expose et classe un inventaire des vulnérabilités. C'est un outil indispensable pour le pilotage des activités d'une organisation. En effet, face à la hiérarchisation constituée, celle-ci situe son exposition aux risques au regard de ses activités. Avec les résultats obtenus par les évaluations des dispositifs, elle peut ainsi prioriser les actions correctrices, d'enrichissement ou de développement de ses activités.

De manière plus générique, elle facilite la compréhension de l'utilité de certaines actions de contrôle, de travaux d'optimisation, de protection, de sécurisation. En fait, elle participe à une prise de conscience et une sensibilisation nécessaire à l'intégration d'une gestion anticipative des risques et donc de la diffusion d'une culture risque (*).

(*) Lire aussi du même auteur, l'ouvrage : « *Conscientisation des risques* », Editions EDILIVRE, Paris, novembre 2014 – réédition sous le titre « *La Gestion des Risques* » aux Editions BoD – Mai 2026