

La Cartographie unique des Risques



La cartographie unique des risques

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 anxieux ? 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 ferait peur et la vision positive, celle dont il faut seulement en prendre conscience. Attention, le terme « seulement » pourrait envisager une facilité que tout à chacun pourrait 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 impacté.

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

Mais d'abord, de quoi parlons-nous exactement ?

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. Le risque est avéré lorsque l'incident s'est réellement produit, il est potentiel lorsque celui-ci est connu mais non avéré. Il est à noter qu'un risque imprévisible devient un aléa.

L'impact est une conséquence issue d'une alerte ou d'un risque, il se recense en deux catégories, impact financier et impact image.

Le dispositif de prévention est un moyen de réduire la fréquence annuelle d'un incident ou de décaler dans le temps la fréquence d'un incident considéré comme rare (au-delà d'une année).

Le dispositif de protection est un moyen de réduire ou d'éviter la gravité de l'impact d'un incident lorsque ce dernier est avéré.

La cartographie unique 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 des risques imprévisibles ne peuvent pas intégrer une cartographie unique de par la difficulté de les recenser et de l'impossibilité de les évaluer.

Prenons du recul et observons le périmètre concerné.

Quelle que soit l'organisation, celle-ci nécessite des moyens basiques pour fonctionner qui se résument à trois besoins indissociables et un moyen de protection. Ainsi, nous distinguons des moyens humains, des moyens matériels et des processus pour faire fonctionner le ou les activités. Comme toute organisation est exposée vis-à-vis de l'extérieur, celle-ci a donc nécessairement besoin de se protéger contre tout ce qui gravite autour d'elle.

A partir de ces éléments, le périmètre observé devient naturel et se compose donc de l'ensemble des vulnérabilités sur les biens et systèmes d'information, sur les personnes, sur les processus et sur les événements extérieurs.

Désormais, les risques peuvent être identifiés.

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. 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 : elle se définit comme le risque aléatoire où sa 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 imprévisible. Sa protection est caractérisée par une charge de risque calculée essentiellement à partir de statistiques historiques.

- La catégorie risques financiers : elle 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 réside principalement sur l'utilisation d'instruments sur les marchés dérivés.

- La catégorie risques opérationnels : souvent par manque de connaissance, elle est considérée comme cloisonnée à un périmètre restreint. Or, elle repose sur tous les autres risques non cités ci-dessus. De ce fait, contrairement aux deux catégories précédentes, cette catégorie rassemble un nombre démultiplié et illimité de risques considérés comme connus, donc prévisibles.

La cartographie unique repose sur des risques connus.

La cartographie s'appuie sur des risques connus et prévisibles. Sur le périmètre observé, 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, mais aussi ceux sur les compétences, 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 la réglementation, la conformité, la sécurité, etc.

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

Les types de risque et les besoins associés

Les risques répertoriés, il faut ensuite les classer afin d'apporter des éléments d'évaluation.

L'objectif de classer ces 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 les besoins. En fait, 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.

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 image. Longtemps laissé de côté, l'impact 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

L'impact financier est la résultante de la multiplication entre la fréquence et la gravité d'un incident. L'impact 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.

- Données du dispositif de protection, éléments de base d'analyse du risque fréquent :

Les risques fréquents correspondent aux risques susceptibles de se produire à minima une fois sur l'année en cours. Le dispositif de prévention ayant la faculté de réduire la fréquence et le dispositif de protection la gravité, nous utilisons les données issues de ces dispositifs pour en déterminer l'efficacité. Ainsi, 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 vie de l'incident, celui-ci se clôture en prenant en compte les récupérations financières et/ou l'enregistrement des pertes.

En d'autres termes, la sinistralité brute représente le montant maximum que peut subir l'organisation et la sinistralité nette le coût comptable. La différence correspond à l'efficacité des dispositifs, de prévention pour la volumétrie et de protection pour la gravité.

- 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. Ainsi, les éléments d'évaluation se caractérisent notamment par une fréquence nette d'un en nombre, la gravité s'évalue donc unitairement. 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) et d'une gravité unitaire.

La hiérarchisation des risques

À partir des données d'évaluation, la cartographie se met en place et prend forme. Elle se matérialise 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'éventuels actions sur la fréquence ou la gravité. Mais, en considérant qu'il existe deux impacts, financier et image, n'est-il pas judicieux de reconsidérer cette matrice avec des axes d'abscisses et ordonnées qui reposent sur l'impact financier et impact image.

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.

Pour exemple, la matrice peut prendre la forme suivante :

FINANCIER

Significatif				
Fort				
Moyen				
Peu Significatif				
	Peu Significatif	Moyen	Fort	Significatif

IMAGE

Bien sûr, les niveaux d'impacts doivent être traduits suivant l'activité de l'organisation, impact financier par fourchette (à partir du calcul fréquence * gravité) et impact image par strate de perception (suivant les publics visés).

La cartographie unique des risques

La matrice étant définie et les évaluations réalisées, nous pouvons positionner les résultats en deux matrices différentes, une matrice pour les risques fréquents, une autre pour les risques rares avec pour chacun un comparatif sinistralité brute et sinistralité nette.

La distinction des risques fréquents et rares permet d'obtenir un visuel instantané sur l'efficacité des dispositifs entre le brut et le net, plus caractérisé pour les risques fréquents que pour les risques rares.

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

De ce fait, la meilleure visibilité pour un dirigeant reste une matrice de la cartographie unique en sinistralité brute. C'est la seule qui recense une hiérarchisation juste des principaux risques majeurs avant dispositifs. Elle aide à comprendre l'utilité de certaines actions de contrôle, de travaux d'optimisation, de protection, de sécurisation. En fait, elle apporte 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 (*).

(*) « Conscientisation des risques », Editions EDILIVRE, Paris – Réédition 2026 « La gestion des Risques », Editions BoD