FICHE « MESURER LES RISQUES » SOURCES

23 octobre 2023

Recueil de différentes sources :

Introduction

Un risque est un évènement incertain et futur dont la survenance prive l'entreprise d'une ressource et l'empêche d'atteindre un ou plusieurs de ses objectifs [source :Deloitte 2016].

Les organismes de tous types et de toutes dimensions confrontés à des facteurs et des influences internes et externes ignorent si et quand ils vont atteindre leurs objectifs. L'incidence de cette incertitude sur l'atteinte des objectifs d'un organisme constitue le «risque». Toutes les activités d'un organisme comprennent des risques. Les organismes gèrent le risque en l'identifiant, en l'analysant, et en évaluant ensuite la nécessité de le modifier par un traitement afin de satisfaire aux critères de risque [source : ISO 31000].

Evaluation du risque

Après avoir dressé et validé une liste des risques de l'entreprise (Registre des risques), l'étape suivante consiste à procéder une évaluation de chaque risque retenu.

Sur la base des résultats de l'analyse du risque, le but de l'évaluation du risque est d'aider les décideurs à déterminer les risques nécessitant un traitement et la priorité dans la mise en oeuvre des traitements. L'évaluation du risque consiste à comparer le niveau de risque déterminé au cours du processus d'analyse aux critères de risque établis lors de l'établissement du contexte. Sur la base de cette comparaison, il est possible d'étudier la nécessité d'un traitement [ISO 31000]

Evaluer un risque consiste lui attribuer des critères d'importance, afin de classer le risque par ordre de priorité.

Pour mesurer un risque il faut tenir compte de 2 critères :

- La gravité qui mesure l'importance des impacts envisagés en cas de survenance du risque.
- La probabilité que ce risque survienne.

Source : *La cartographie des risques - 2ème édition - IFACI*

A minima, deux critères sont appréciés pour coter le risque brut : la fréquence et l'impact :
Risque brut = Fréquence x Impact

Le risque résiduel mesure le risque après mise en place des éléments de maîtrise :
Risque résiduel = Fréquence x Impact x Elément de maîtrise

Ou Risque résiduel = Risque brut – contrôle.

Les échelles d'évaluation facilitent la hiérarchisation des risques et in fine les arbitrages sur des actions à mener. ~~Les échelles paires à quatre niveaux sont à privilégier.~~

FICHE « MESURER LES RISQUES » SOURCES

23 octobre 2023

LA FREQUENCE

Comment déterminer la fréquence de survenance du risque ? Par l'estimation de l'occurrence des événements pouvant être à l'origine du risque. L'échelle de mesure de la fréquence doit être établie et adaptée à la structure.

Ci-après sont proposées deux illustrations de mesure de la fréquence.

Illustration 1 : Echelle de mesure de la fréquence

Cotation	Fréquence	Elément de mesure
1	Exceptionnel	Occurrence quasi nulle (<1%) sur 2 ans
2	Rare	Occurrence possible mais peu probable (1 à 10%) sur 2 ans
3	Probable	Occurrence plausible (10 à 50%) sur 2 ans
4	Très probable	Occurrence très probable (>50%) sur 2 ans

Illustration 2 : Echelle de mesure de la fréquence

Cotation	Fréquence	Elément de mesure
1	Rare	Fréquence de l'ordre d'1 à 2 fois en 3 ans
2	Modéré	Fréquence de l'ordre d'1 fois par an
3	Occasionnel	Fréquence pluriannuelle (quelques fois par an, de l'ordre du trimestre, du mois)
4	Fréquent	Fréquence quotidienne ou hebdomadaire

L'IMPACT

Quelle est la conséquence si le risque se concrétise ? L'unité de recherche propose de décliner les impacts en 3 principales catégories1, à savoir :
• l'impact financier (ex : perte financière, baisse des revenus, hausse des coûts), direct ou indirect, immédiat ou à terme. L'annexe 4 vous propose une liste non-exhaustive d'impacts financiers ;
• l'impact juridique (ex : responsabilité civile et/ou pénale, sanctions légales et/ou professionnelles, etc.) ;
• l'impact sur l'image (dégradation de l'image, réputation remise en cause).

ATTENTION : Une estimation systématique des conséquences financières, basée sur des scénarios de risques précis peut être un exercice très lourd et complexe. Il est en effet difficile d'exiger une évaluation financière précise de tous les impacts (humains, conformité, réputation, etc.).
Pour faciliter l'exercice d'évaluation, il est toutefois souhaitable d'établir des critères objectifs pour chaque niveau de gravité.

Ces trois principales catégories d'impact sont adaptées au secteur assurantiel. En fonction du domaine d'activité des entreprises, d'autres catégories d'impact peuvent être pertinentes. Par exemple, les impacts environnementaux peuvent être appropriés à l'industrie (nucléaire, minière, pétrolière) ou encore les impacts sur la vie humaine peuvent être envisagés dans les secteurs des travaux publics, de la sécurité (armée, police), ou l'industrie minière.

L'échelle de mesure de l'impact doit être établie et adaptée à l'organisme. Ci-après sont proposées deux illustrations de mesure de l'impact. D'autres évaluations de l'impact financier sont proposées en annexe 4.

Illustration 1 : Echelle de mesure de l'impact

Cotation	**Impact**	**Impact financier**	**Impact image**	**Impact légal réglementaire**
1	Faible	< 10 000 euros	Impact local	Observation des autorités de tutelle
2	Modéré	Entre 10 000 à 100 000 euros	Impact régional	Avertissement des autorités de tutelle Mise en cause juridique devant une juridiction autre que pénale
3	Significatif	Entre 100 000 à 500 000 euros	Impact national Un seul canal	Blâme des autorités de tutelle Mise en cause devant une juridiction pénale
4	Elevé	> 500 000 euros	Impact national Couverture large	Sanction des autorités de tutelles Condamnation pénale

Illustration 2 : Echelle de mesure de l'impact

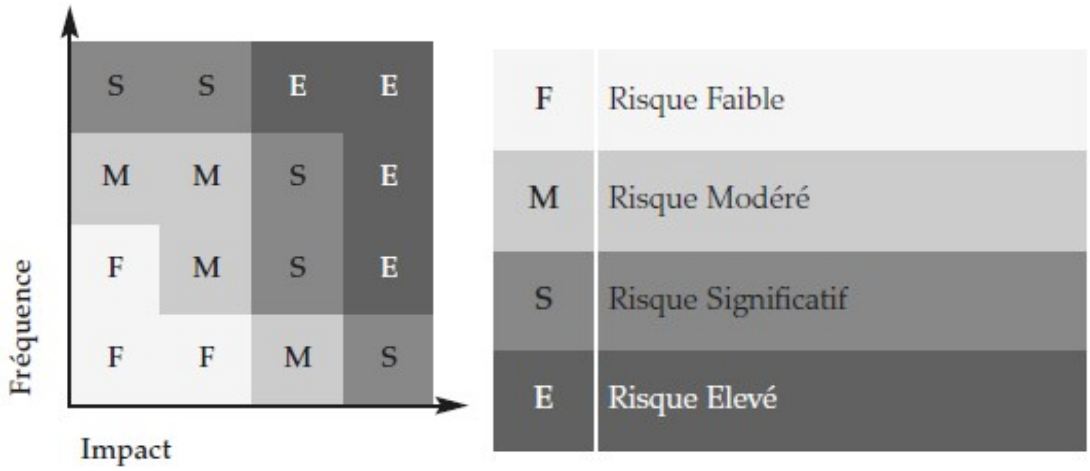
	Impact	**Financier (résultat)**	**Image / réputation ou encore réglementaire**
1	Limité	< 10% du résultat annuel	Attention de tiers (presse, groupes de pression, etc.) sur des sujets jugés sensibles
2	Significatif	10% à 50% du résultat annuel	Communication défavorable dans des médias sur une partie de l'entreprise et à un niveau local
3	Majeur	50% à 100%	Couverture médiatique plus large, mais n'entraînant pas d'effet majeur
4	Critique	> au résultat annuel	Attaque médiatique ayant des conséquences significatives sur l'image et la réputation du Groupe

Comment définir les seuils financiers dans les échelles de mesure d'impact ?

Les différents seuils à retenir doivent être « discriminants » et permettre une distribution des risques régulière sur l'ensemble des seuils retenus : si tous les risques évalués se situent sur le même niveau, l'échelle retenue ne sera pas utile à la bonne hiérarchisation des risques.

LE RISQUE BRUT

L'impact et la fréquence permettent de déterminer la cotation brute ou inhérente du risque.



ATTENTION : Pour certains, cette étape est considérée comme une étape intermédiaire. Ils préfèrent directement raisonner sur le risque résiduel, en intégrant les éléments de maîtrise dès les premiers travaux d'évaluation des risques. Ils résolvent ainsi une limite cognitive des acteurs qui n'arrivent pas à raisonner sur les risques en faisant abstraction des éléments de maîtrise existants.

LES ELEMENTS DE MAITRISE

L'élément de maîtrise se définit comme le moyen existant ou à mettre en place pour permettre de réduire ou d'éliminer le risque. Il peut porter aussi bien sur la fréquence que sur l'impact du risque à titre préventif ou correctif. Ainsi, à chaque risque est associé un ou plusieurs éléments de maîtrise.
Il est entendu qu'un même élément de maîtrise peut venir agir sur plusieurs risques.
Ces éléments de maîtrise sont constitués généralement de :

- missions, tâches données aux collaborateurs,
- manuels de procédures, modes opératoires,
- niveaux de savoir-faire des collaborateurs,
- tableaux de bord,
- systèmes informatiques,
- organigrammes ou structures clairement définis et formalisés,
- directives, consignes, règles claires et écrites,
- actions de vérifications : auto-contrôle, contrôle humain, contrôle automatique,
- séparation des tâches,

• délégations de pouvoirs formalisées.
L'échelle d'appréciation des éléments de maîtrise doit être établie et adaptée à l'organisme.

Illustration 1 : Echelle d'appréciation des éléments de maîtrise

Cotation	Niveau de maîtrise	Elément de mesure
1	Maitrisé	Dispositifs mis en place permettant de réduire la fréquence ou l'impact du risque à un niveau satisfaisant : règles écrites et détaillées, contrôles formalisés et appliqués (indicateurs de suivi et de contrôle, évaluation des procédures, etc.).
2	Acceptable	Dispositifs mis en place permettant de réduire notablement la fréquence ou l'impact du risque : règles écrites mais à compléter, éléments de maîtrise existants et pertinents, formalisés mais à compléter.
3	Insuffisant	Dispositifs mis en place ne permettant pas de réduire significativement la fréquence ou l'impact du risque : règles orales, éléments de maîtrise partiellement existants ou pertinents et peu formalisés.
4	Faible	Absence d'élément de maîtrise : pas ou peu de règle, on se fie à l'expérience, pas ou peu de remontées d'informations, pas ou peu de sensibilisation du personnel aux risques.

LE RISQUE RESIDUEL

Le risque résiduel est la criticité que présente le risque après prise en compte de l'effet protecteur des éléments de maîtrise en place.
Risque résiduel = Fréquence x Impact x Elément de maîtrise
Le poids du risque ainsi déterminé permet une hiérarchisation des principaux risques et une priorisation des plans d'actions peut être établie.

Illustration 1 : Echelle de mesure du risque résiduel

L = risque faible, géré par les procédures en place	L'impact sur l'atteinte des objectifs n'est pas préoccupant, le risque est sous contrôle
M = risque modéré, un suivi spécifique doit être organisé	L'impact sur l'atteinte des objectifs est limité. Des actions doivent être entreprises mais ne sont pas urgentes.

S = risque significatif, une alerte au senior management est nécessaire	L'impact sur l'atteinte des objectifs est significatif. Nécessité de prendre des actions immédiates pour limiter le risque.
H = risque élevé, action immédiate requise	L'impact sur l'atteinte des objectifs est d'une telle ampleur que les objectifs ne seront très probablement pas atteints. Nécessité de prendre des actions immédiates pour limiter le risque, et alerter la direction.

ATTENTION : Les risk managers peuvent mobiliser des critères complémentaires à l'impact et à la fréquence pour affiner l'évaluation des risques. Par exemple :

- la vélocité,
- la volatilité,
- le fait qu'il soit plus ou moins contrôlable,
- la capacité.

FICHE « MESURER LES RISQUES » SOURCES

23 octobre 2023

***Source** : Guide « Contrôle interne » - ACPR*

https://acpr.banque-france.fr/sites/default/files/20220311_guide_controle_interne.pdf

Cartographie des risques

Le système de contrôle interne comprend une cartographie des risques de la société.

Cette cartographie doit être suffisamment complète pour pouvoir appréhender les principaux risques ou les accumulations de risques auxquels l'organisme est exposé. À ce titre, le système de contrôle interne interagit avec la fonction de gestion des risques, puisque le calcul de l'intensité des risques prend en compte les effets d'atténuation permis grâce aux contrôles mis en œuvre.

FICHE « MESURER LES RISQUES » SOURCES

23 octobre 2023

***Source** : Auditeur interne et contrôleur permanent - Eyrolles*

Echelle de mesure de la fréquence

Cotation	**Fréquence**	**Elément de mesure**
1	Impossible	Presque jamais
2	Très basse	Une fois par période de 2 ans
3	Basse	Une fois par an
4	Modérée, occasionnelle	Une fois par semestre
5		Une fois par trimestre
6		Une fois par mois
7	Haute	Une fois par semaine
8		Une fois par jour
9	Très haute	Quelques fois par jours
10		Fréquemment chaque jour

Grille de degrés de gravité

Cotation	**Impact**
1	Mineur
2	
3	Moyenne
4	
5	Critique
6	
7	Très critique
8	
9	Catastrophique
10	

FICHE « MESURER LES RISQUES » SOURCES

23 octobre 2023

***Source** : La gestion des risques en assurance - L'argus de l'assurance*

Afin d'être cohérentes et efficaces, les techniques d'évaluations s'appuient de façon pragmatique sur la définition du risque. En effet, le risque (…) défini comme « la possibilité qu'un évènement se produise et ait une incidence sur la réalisation des objectifs ou sur les principaux actifs de l'entreprise ».
Dans cette définition, deux termes sont fondamentaux pour travailler sur l'appréciation du niveau de risque : la « possibilité » et « l'incidence ».

Afin d'évaluer le risque, il va être nécessaire de se prononcer sur la possibilité de réalisation du risque et donc sur le caractère potentiel de sa survenance d'une part, et sur le niveau d'incidence en cas de survenance d'autre part.

Nous proposons par la suite de qualifier le « probabilité » le critère qui va permettre d'évaluer la possibilité de survenance du risque et « d'impact » le critère permettant d'évaluer son incidence.
Ainsi l'évaluation du risque s'appuiera sur le principe suivant :

RISQUES = PROBABLITE x IMPACT

(…)

Notion de risque brut
Notion de risque résiduel/net

Quelques exemples d'échelles de probabilités :

PROBABILITE			
1	Improbable	1 fois sur 500	> tous les 10 ans
2	Rare	1 fois sur 100	Tous les 10 ans
3	Peu fréquent	1 fois sur 20	Tous les ans
4	Occasionnel	1 fois sur 5	Tous les mois
5	Fréquent	1 fois sur 2	Tous les jours

	PROBABILITE	**DESCRIPTION**
1	Rare	Peu susceptible de se produite (1 à 2 fois en 3 ans) ou moins de 2% de chances de survenir
2	Peu probable	Susceptible de survenir environ une fois par an ou entre 2% et 10% de chances de survenir
3	Probable	Susceptible de survenir plusieurs fois par an ou entre 10% et 2à% de chances de survenir
4	Très probable	Susceptible de survenir régulièrement ou plus de 20% de chances de survenir

FICHE « MESURER LES RISQUES » SOURCES

23 octobre 2023

Exemple d'échelles d'impacts

	Impact	Financier	Image / Qualité de service	Légal
1	Faible	Moins de 100 K€	Visible uniquement en interne > aucun impact sur le niveau de satisfaction	Sans impact ou conséquences internes uniquement
2	Modéré	100 K€ à 500 K€	Visible par peu d'adhérents ou bénéficiaires	Sanctions administratives : URSSAF, FISC…. Observations des CAC Observations de l'autorité de contrôle
3	Significatif	500 K€ à 2 M€	Visible par de nombreux bénéficiaires et par les entreprises adhérentes	Engagement d'une procédure de sanction par les autorités de contrôle/tutelles Réserve des CAC Condamnation civile ou pénale faible
4	Elevé	Supérieur à 2 M€	Visible par un nombre significatif d'adhérents et/ou Mise en cause de la mutuelle dans le secteur d'activité : visible dans la presse spécialisée, par les autorités de contrôle et tutelles, l'environnement politique…	Sanction lourdes par les autorités de contrôle/tutelles : mise sous tutelle, retrait d'agrément… Condamnation civile ou pénale forte/privation de liberté

Exemple de cotation des éléments de maîtrise :

	Synthèse de l'efficacité des actions de maîtrise
1	Risque sans action de maîtrise
2	Les actions de maîtrise sont inadaptées
3	Les actions de maîtrise sont inefficaces
4	Risque couvert avec de rares possibilités de défaillance
5	Risque parfaitement couvert

FICHE « MESURER LES RISQUES » SOURCES

23 octobre 2023

Source *: Une méthodologie pour donner aux risques opérationnels et de non-conformité une dimension plus stratégique - Revue banque*

https://www.revue-banque.fr/fonctions-support/une-methodologie-pour-donner-aux-risques-operation-EORB20372

Une méthodologie pour donner aux risques opérationnels et de non-conformité une dimension plus stratégique

Il n'y a pas que les risques financiers à prendre en compte dans une « stratégie risques », mais aussi les risques opérationnels et de non-conformité. Voici une démarche pour en établir une cartographie cohérente et en lien avec l'appétit aux risques fixé par les dirigeants.

On peut considérer que toutes les banques disposent d'une cartographie des risques, c'est-à-dire un document dans lequel elles formalisent leur profil de risque. En revanche, leur qualité et leur utilité réelles peuvent être très variables d'un établissement à l'autre. D'abord centrées autour des risques très opérationnels, les cartographies ont progressivement intégré des risques de non-conformité. Mais le choix de nombre d'établissements d'associer coûte que coûte des événements de natures très différentes dans un même support finit par l'alourdir et dégrader sa cohérence et, de ce fait, limiter son exploitation. Ce manque de lisibilité explique probablement pourquoi la cartographie des risques reste souvent réservée à un cercle de spécialistes. Elle n'a pas pleinement trouvé sa place auprès des dirigeants, en tant qu'instrument de pilotage d'une stratégie globale des risques. C'est pourtant l'une de ses utilités. Voici une méthode pour mieux atteindre cet objectif.

Étape 1 : une cartographie séparée entre risques opérationnels et de non-conformité

En matière de risques à cartographier, on peut distinguer deux familles : les risques strictement opérationnels et les risques de non-conformité, tels que définis dans la réglementation [1]. Historiquement, la démarche adoptée pour élaborer une cartographie des risques est celle conçue pour capter les risques de nature strictement opérationnelle, c'est-à-dire les événements assimilables à des incidents, ou qui surviennent à la suite d'une forme de défaillance des processus. Cette démarche n'est pas adaptée aux risques de non-conformité.

Approche pour le risque opérationnel

Pour évaluer ce risque, il s'agit de dérouler linéairement les étapes d'un processus opérationnel (voir Schéma 1), afin d'identifier puis de mesurer les risques potentiels assimilables à des incidents, par exemple dus à la faiblesse ou au non-respect de procédures, de ruptures informatiques, etc.

Toute activité génère par nature des risques opérationnels potentiels. La question porte donc sur les fragilités du mode de gestion mis en œuvre par centre de responsabilité et d'en mesurer l'impact en cas de survenance.

Cette cartographie mesure un risque, dont on cherche à mesurer l'impact en cas de survenance au travers du facteur « fréquence » et du facteur « coût unitaire ». Chaque service métier de l'entreprise est responsable de ses activités et de ses risques.

Aucun critère de mesure n'est parfait, mais l'utilisation de l'étalon monétaire pour les risques opérationnels (risques mesurés en euros) s'explique : la survenance d'un incident génère des coûts directs et indirects, pour corriger les causes et conséquences de l'incident et pour prendre en compte le manque à gagner direct. L'impact réel peut être bien sûr plus étendu, mais l'étalon monétaire reste le moins mauvais critère. Il offre l'avantage d'une bonne comparabilité entre différents événements. Il s'agit plus d'une analyse modélisée que d'une prédiction divinatoire (voir un exemple de cartographie dans le graphique 1).

Une méthodologie différente pour la non-conformité

Ici, la question n'est plus de connaître la fragilité de la gestion, mais d'estimer si l'on répond pleinement, partiellement ou pas du tout à une obligation de conformité. En d'autres termes, il faut appréhender une situation dans laquelle une offre de services ne produirait pas un résultat conforme : par rapport aux lois-règlements, aux attentes du superviseur, aux règles déontologiques, aux normes professionnelles et aux décisions des instances de gouvernance.

Prenons par exemple, dans le cadre de la protection de la clientèle, la loi Eckert, qui se décompose elle-même en plusieurs contraintes distinctes (voir schéma 2).

L'analyse est plus complexe et la responsabilité de l'action est collective puisque éclatée entre plusieurs acteurs : front-office, middle ou back office, DSI et même la sécurité financière.

C'est ensuite à un tiers arbitre – logiquement la fonction Conformité – d'estimer, de manière transversale, si le dispositif de l'entreprise peut être considéré comme respectant les obligations de la loi.

En l'occurrence, le risque n'est pas potentiel, il est avéré. Certes temporairement caché, il est susceptible d'être révélé à tout moment par un client, un autre tiers ou les pouvoirs publics, lors d'un contrôle de l'ACPR par exemple. Il s'agit donc d'évaluer si l'on est globalement conforme, ou plutôt non conforme, notamment au vu des attentes des pouvoirs publics. Ces différences de concept et d'axe d'analyse expliquent le besoin de produire deux cartographies différentes.

La question de l'évaluation relève de la même logique. La plupart du temps, il existe bien un impact monétaire, mais qui ne représente qu'une partie de l'impact réel. L'enjeu est ailleurs : subir une sanction associée à une perte de réputation pouvant limiter l'activité économique au sens large :

– de la part des pouvoirs publics : une sanction disciplinaire ou pénale (de la personne morale ou de personnes physiques), une limitation d'exercice, accompagnées ou non d'une amende pécuniaire [2] ;

– de la part de clients, du public et du marché : une perte d'image pouvant jouer sur la marge de manœuvre future de l'entreprise (sur les activités, le financement…), avec des conséquences financières très difficiles à modéliser.

Puisque l'impact monétaire n'est pas assez pertinent, ne l'utilisons pas. Si l'on s'accorde pour dire que les conséquences pour l'établissement sont une sanction disciplinaire par le superviseur, une sanction judiciaire par les tribunaux ou une perte d'image et de réputation (voire une combinaison des trois), pourquoi ne pas utiliser ces critères pour mesurer l'impact d'une non-conformité, en les classant par exemple sur une échelle de 1 à 5, allant de risque limité à « risque critique » (voir graphique 2) ?

Étape 2 : développer une correspondance avec la notion d'appétit au risque

Dans le secteur bancaire, le temps où l'on élaborait une cartographie des risques a minima, uniquement pour respecter une obligation réglementaire, est révolu. On a compris l'importance – pour les fonctions clés et les métiers – de disposer d'un document formalisant le profil de risque de chaque établissement. Il permet de structurer le dispositif de contrôle interne et de justifier de son principe de proportionnalité.

L'importance croissante de certains risques opérationnels ou la pression continue des réglementations devrait pousser les dirigeants effectifs, comme l'organe de surveillance, à appréhender pleinement les risques opérationnels et de non-conformité dans sa stratégie risques.

Poussés par la réglementation, les risques financiers ont déjà été pilotés de la sorte : les risques de crédit ou de marché depuis Bâle II et, plus récemment, les risques de liquidité depuis Bâle III.

Le régulateur français nous y conduit aussi. Il suffit de se référer au récent arrêté du 21 février 2021 évoquant la notion de stratégie à définir pour l'informatique et le risque informatique [3], en pratique une sous-catégorie de risque opérationnel. La stratégie risques sert à sécuriser l'atteinte des objectifs stratégiques de l'entreprise dans une approche top-down. Elle se matérialise notamment par la fixation de seuils d'appétit aux risques, accompagnée par un système de cotation adapté.

À chaque stratège, ses seuils de tolérance

On peut résumer la notion d'appétit aux risques par le niveau et le type de risques que l'établissement peut et souhaite assumer dans ses expositions et ses activités, compte tenu de ses objectifs stratégiques, avec les contraintes réglementaires telles que définies dans le pilier 3 de Bâle III. Il s'agit notamment de la fixation de limites et de règles de tolérance, ainsi que des moyens de suivi permettant d'en vérifier le respect. L'arrêté du 3 novembre 2014 actualisé précise aussi le contenu de l'appétit aux risques [4].

En pratique, il s'agit concrètement de demander aux organes de gouvernance de positionner leurs seuils de tolérance de l'appétit aux risques sur la grille de cotation des risques opérationnels et sur la grille de cotation des risques de non-conformité réalisée précédemment. Le plus simple est alors de le traduire en code couleur (voir graphique 3). Cela permet en outre de bâtir une cartographique des risques consolidée.

On laisse ainsi de côté le débat sur la prise en compte ou non de l'étalon monétaire ou d'un autre critère de mesure ; on retient la notion de criticité par rapport à l'appétit aux risques dans le cadre de la stratégie risques. Une fois cet exercice fait, les instances de gouvernance auront défini la cible à respecter en matière de risques opérationnels et de non-conformité. Il sera ensuite à la charge des fonctions clefs de surveiller leur application correcte par les métiers sur le terrain.

Un reporting plus aisé

Avec ces deux grilles de cotation harmonisées, les fonctions clefs – direction des risques et direction de la conformité – disposent des outils de mesure nécessaires, à la fois pour :

– conduire chaque exercice de cartographie des risques avec les métiers ;

– regrouper tous les risques dans une cartographie consolidée à des fins d'analyse ;

– coter les risques lors des contrôles permanents de second niveau et de constater les écarts éventuels par rapport aux limites fixées par les organes de gouvernance.

Ces fonctions clefs pourront ainsi fournir aux instances de gouvernance un reporting régulier des risques réels relevés au sein de la banque et cotés selon les limites de tolérance de l'établissement.

Pour les acteurs qui ne l'ont pas encore fait, une telle démarche, assez simple à mettre en œuvre, donne aux instances de gouvernance les moyens de piloter des risques jusque-là peut-être un peu sous-estimés. Les changements rapides de l'environnement bancaire – les néo-banques et la transformation des modèles de banque – mettent au premier plan les risques opérationnels et de non-conformité. Cette méthodologie permet aussi aux fonctions clefs de second niveau de se rapprocher autour de règles communes et, pourquoi pas, de les faire adhérer l'ensemble des fonctions clefs, avec le contrôle périodique, à ce référentiel commun. Cet effort de simplification contribuerait aussi à une meilleure compréhension du contrôle interne et à une appropriation de la culture risques par tous les acteurs de la banque. Ce serait donc un progrès, avant même de s'attaquer à un autre sujet : la cartographie portant sur la sécurité du système d'information. Le risque croissant dû à la complexité des systèmes et à la cyber-sécurité en fait un autre thème majeur.

[1]Le risque de non-conformité est décrit dans l'article 10-p de l'arrêté du 3 novembre 2014 actualisé.

[2]La prise en compte du seul montant de l'amende infligée par l'ACPR lors d'un contrôle n'est pas suffisante ni suffisamment pertinente pour mesurer l'impact de la non-conformité. Son paiement ne constitue pas un solde de tout compte, car l'établissement reste redevable des actions de remédiation contenues dans la lettre de suite du SGACPR. Sa mise en œuvre sous contrainte engendrera un coût réel beaucoup plus élevé que l'amende elle-même. Il ne faut pas oublier non plus le fait de se retrouver sous surveillance par les pouvoirs publics et l'impact d'image auprès de ces mêmes pouvoirs publics et du marché.

[3]Art. 270-1 de l'arrêté du 21 février 2021 modifiant l'arrêté du 3 novembre2014.

[4]Article 224 de l'arrêté du 3 novembre 2014 actualisé : l'appétit pour le risque ainsi que les limites globales de risques qui en résultent sont fixés et revus, autant que nécessaire et au moins une fois par an, par les dirigeants effectifs et approuvés par l'organe de surveillance, qui consulte, le cas échéant, le comité des risques, en tenant compte notamment des fonds propres de l'entreprise et, si c'est nécessaire, des fonds propres consolidés ou sous-consolidés et de leur répartition au sein du groupe, adaptée aux risques encourus

FICHE « MESURER LES RISQUES » SOURCES

23 octobre 2023

Graphique 1. Mode d'évaluation des risques opérationnels

Exemple de grille de cotation des risques opérations (fréquence X impact unitaire)

	Moins d'une fois tous les 5 ans	Moins d'une fois par an	Moins d'une fois par trimestre	Moins d'une fois par mois	Moins d'une fois par semaine	Plus d'une fois par semaine
0 - 5 K€	1	2	3	6	10	15
5 - 25 K€	4	5	8	12	18	20
25 - 100 K€	7	9	11	16	23	26
100 - 500 K€	13	14	17	19	28	31
500 - 5 M€	16	17	26	30	33	35
5 M€ et plus	24	25	29	32	34	36

Graphique 2. Mode d'évaluation des risques de non-conformité

Exemple de grille de cotation des risques de non-conformité

A) Intensité du risque →	1- NS ou limitée	2-Notable	3-Forte	4-Très forte	5-Critique
C) Sanction disciplinaire par le superviseur ACPR Hypothèse en cas de contrôle sur place →	**Si contrôle sur place** NS	**Si contrôle sur place** Apparition de doute sur la conformité. Situation dans une zone grise mais conforme aux pratiques de place	**Si contrôle sur place** **Lettre de suite simple** non-conformité partielle ou de priorité moyenne	**Si contrôle sur place** Entre **Lettre de suite avec mise en demeure** et **1er niveau de sanction** (avertissement)	**Si contrôle sur place** **Sanction plus lourde** (blâme et plus)
D) Sanction pénale	/	*Scénario à décrire*	*Scénario à décrire*	*Scénario à décrire*	*Scénario à décrire*
E) Image et réputation	/	*Scénario à décrire*	*Scénario à décrire*	*Scénario à décrire*	*Scénario à décrire*
F) Non-application des décisions des instances de gouvernance	Impact éventuel assimilable à une perte d'opportunité (risque stratégique) → Choix de ne pas mesurer l'impact mais de signaler le cas				

À chacun des cinq pas de risque du tableau ci-dessus doit correspondre un scénario d'impact clair et compréhensible pour les dirigeants comme pour les responsables métier : le nombre de pas et les degrés de criticité sont à adapter à la situation ou à la perception de chaque entreprise.

FICHE « MESURER LES RISQUES » SOURCES

23 octobre 2023

Graphique 3. Méthode de consolidation des cartographies des risques

Équivalence des niveaux selon le code couleurs entre chaque tableau

Exemple de seuils de tolérance de l'appétit aux risques

Couleur	Signification du risque	Tolérance au risque
vert	Risque NS ou limité	Risque accepté, dans le cours normal des affaires
jaune	Risque notable	Risque accepté, doit être limité
orange	Risque fort	Risque toléré
rouge	Risque très fort	Au-delà du risque de tolérance
noir	Risque critique	Non tolérable, pouvant mettre en péril certains équilibres de l'établissement

Exemple de grille de cotation des risques de non-conformité

A) Intensité du risque ⇝	1-NS ou limitée	2-Notable	3-Forte	4-Très Forte	5-Critique
C) Sanction disciplinaire par le superviseur ACPR Hypothèse en cas de contrôle sur place ⇝	Si contrôle sur place NS	Si contrôle sur place Apparition de doute sur la conformité. Situation dans une zone grise mais conforme aux pratique de place	Si contrôle sur place **Lettre de suite simple** non-conformité partielle ou de priorité moyenne	Si contrôle sur place Entre **Lettre de suite avec mise en demeure** et **1re niveau de sanction** (avertissement)	Si contrôle sur place **Sanction plus lourde** (blâme et plus)
D) Sanction pénale	/	*Scénario à décrire*	*Scénario à décrire*	*Scénario à décrire*	*Scénario à décrire*
E) Image et réputation	/	*Scénario à décrire*	*Scénario à décrire*	*Scénario à décrire*	*Scénario à décrire*
F) Non-application des décisions des instances de gouvernance	Impact éventuel assimilable à une perte d'opportunité (risque stratégique) ⇝ Choix de ne pas mesurer l'impact mais de signaler le cas				

Exemple de grille de cotation des risques opérations (fréquence X impact unitaire)

	Moins d'une fois tous les 5 ans	Moins d'une fois par an	Moins d'une fois par trimestre	Moins d'une fois par mois	Moins d'une fois par semaine	Plus d'une fois par semaine
0 - 5 K€	1	2	3	6	10	15
5 - 25 K€	4	5	8	12	18	20
25 - 100 K€	7	9	11	16	23	26
100 - 500 K€	13	14	17	19	28	31
500 - 5 M€	16	17	26	30	33	35
5 M€ - et plus	24	25	29	32	34	36

Cartographie des risques consolidés

n° ligne	1er niveau : processus 2e niveau : sous-processus 3e niveau : plus détaillé	Intitulé événement de risque	Nature du risque (menu déroulant)	Pour mémoire : impact monétaire. Sert à calculer le risque brut			Niveau de risque attribué			Commentaires, analyses, modifications ou améliorations envisageables
				Unit	Fréq.	Glob.	Brut	DMR	Net	

FICHE « MESURER LES RISQUES » SOURCES

23 octobre 2023

***Source** : Optimind*

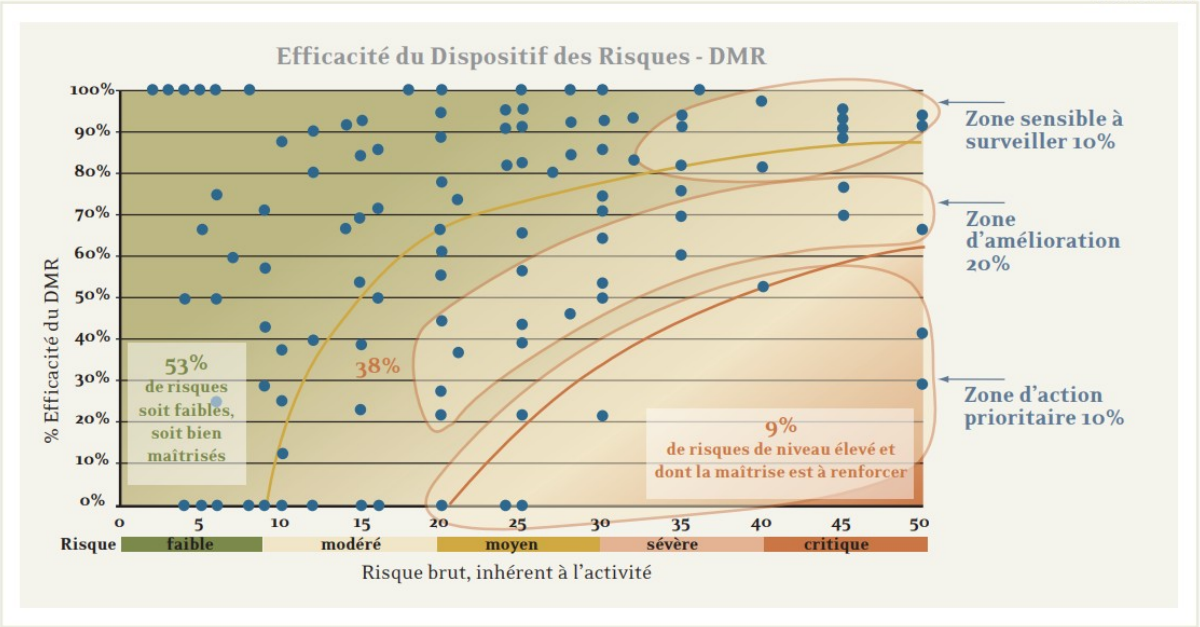
https://www.optimind.com/medias/documents/217/avril_dt_risques_operationnels_vf.pdf

Les axes d'analyse des résultats issus de la cartographie des risques conduisent notamment à étudier au cas par cas si le risque résiduel qui subsiste est acceptable ou non. Les approches de classification des risques alors mises en œuvre, permettent de déterminer les priorités afin d'améliorer le dispositif existant via l'élaboration de plans d'actions.

La cartographie, schéma A, fait ressortir majoritairement :
- les risques exogènes, rares et à fort impact pour lesquels l'entreprise n'a pas la maîtrise sur l'occurrence de l'événement mais peut en limiter l'impact avec notamment un plan de continuité de l'activité, PCA ;
- les risques au cœur de l'activité dont l'impact peut être fort et pour lesquels une bonne maîtrise est nécessaire au quotidien. Il s'agit alors, avec la mise en place d'indicateurs d'alerte, de s'assurer que ce dispositif reste à tout moment opérationnel et sans défaillance.

Il est à noter que certaines démarches de restitution introduisent des biais d'analyse non négligeables s'appuyant sur des matrices dites « de chaleur » mal conçues et aboutissant à une analyse erronée des risques, matrice 4 par 4 de fréquences et sévérités, scores issus de formules non justifiées, etc. La matrice ci-dessous, schéma B, est l'exemple même de ce qu'il vaut mieux éviter de réaliser.

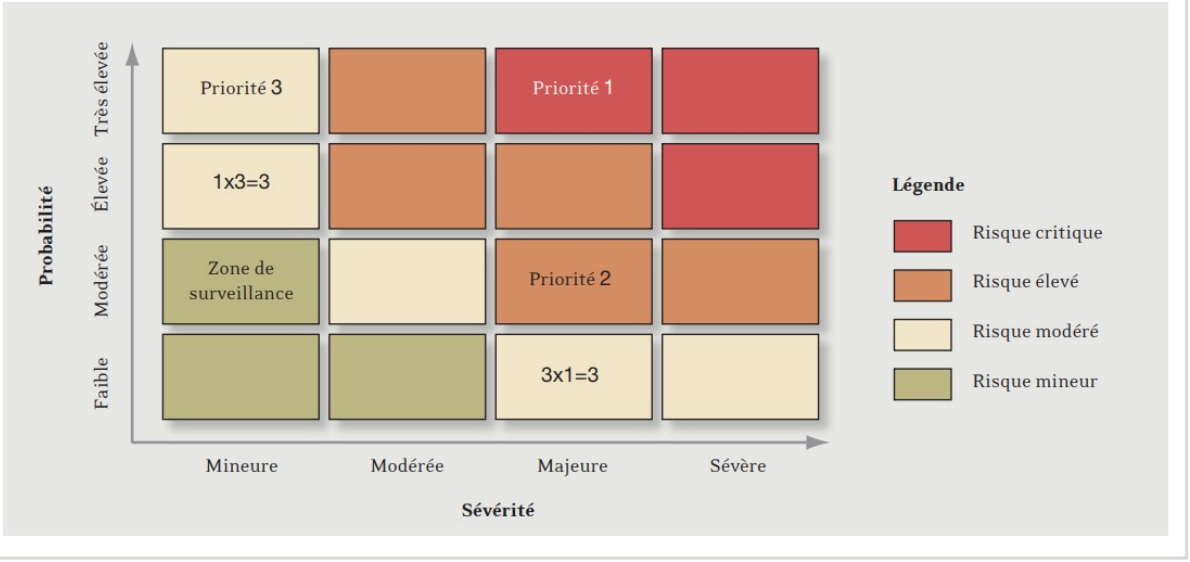
SCHÉMA A



FICHE « MESURER LES RISQUES » SOURCES

23 octobre 2023

SCHÉMA B



FICHE « MESURER LES RISQUES » SOURCES

23 octobre 2023

***Source** : Sia conseil*

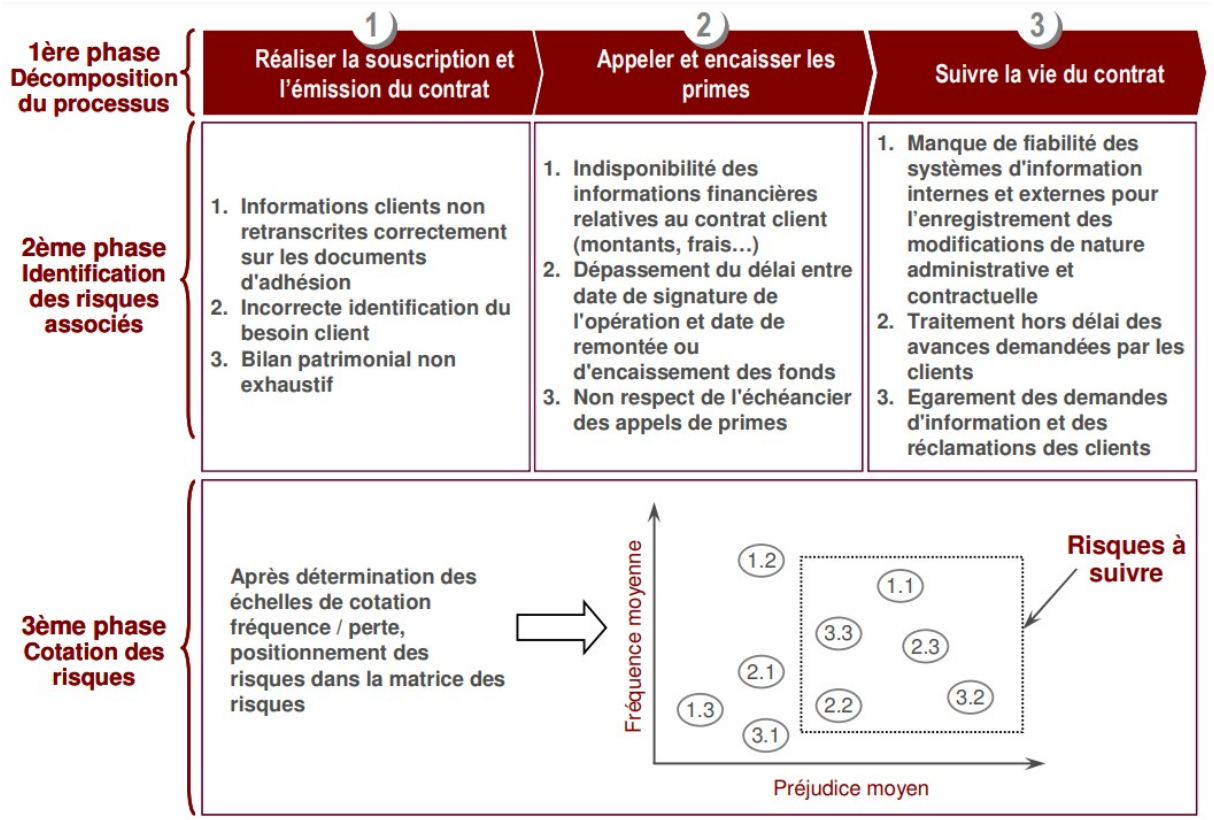
https://www.sia-partners.com/system/files/document_download/file/2020-06/insight_ro-solvency-ii.pdf

Cartographier les risques pour déterminer le profil de risque de l'établissement

Cette phase est une étape clé car elle détermine sensiblement la nature des incidents qui seront collectés et donc suivis par la suite. C'est également cet exercice qui permettra de définir une nomenclature des risques valable pour l'ensemble de l'organisation, cadre indispensable à une collecte efficace et homogène des incidents. La cartographie des risques consiste à formaliser les risques opérationnels dans les processus de la compagnie. Cet exercice passe par les phases suivantes :

• Décomposer en activité chaque processus de la compagnie ;
• Pour chaque activité, recenser les risques opérationnels associés ;
• Pour chaque risque, déterminer le niveau de fréquence et de sévérité (matrice des risques) ainsi que le niveau de performance du contrôle associé ;
• Déterminer, à partir des seuils fixés, le traitement global que l'on applique aux différents groupes derisques opérationnels.

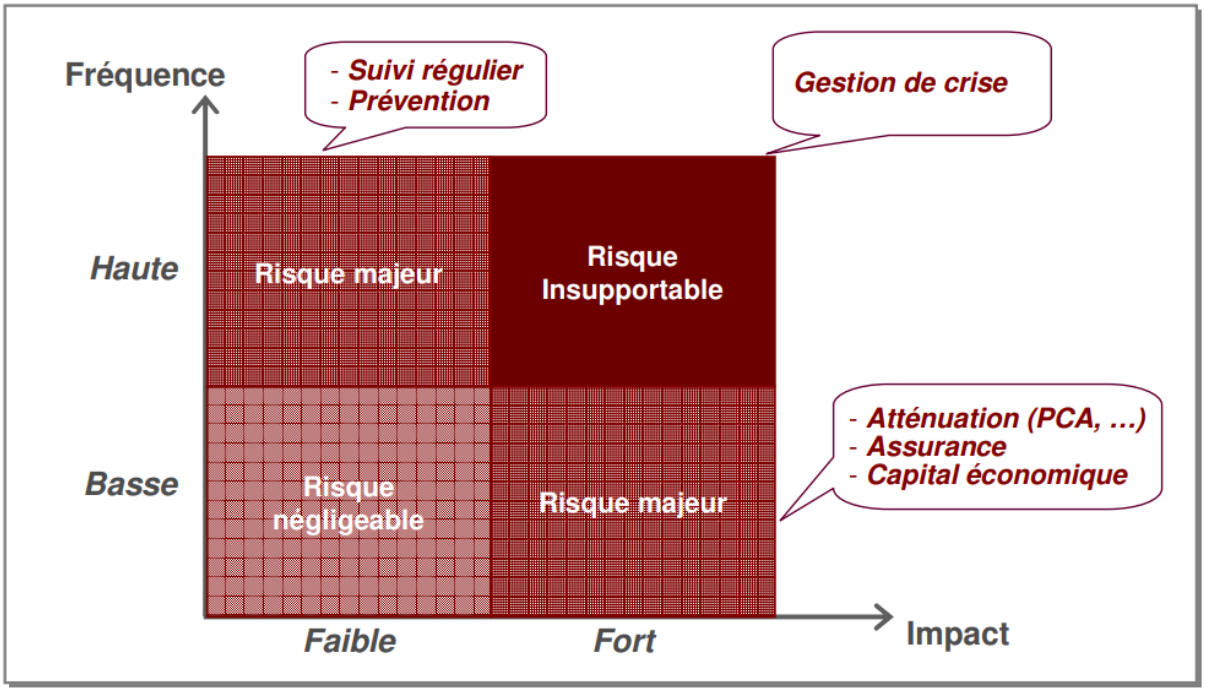
A titre d'exemple, le schéma ci-dessous illustre les phases de l'exercice de cartographie dans le cadre du domaine « assurances individuelles », pour le processus « Administrer les contrats individuels » :



FICHE « MESURER LES RISQUES » SOURCES

23 octobre 2023

L'objectif de la constitution de la matrice des risques est de définir, par ensemble de risques identifiés, les grandes actions à mettre en place pour les traiter :



Le recueil, la formulation, et la qualification des risques opérationnels en vue de la cartographie est une approche « bottom-up ». En effet, les risques opérationnels sont par nature diffus et existent dans chaque service, chaque entité et à tout niveau organisationnel de l'établissement.
La formulation et la centralisation des risques opérationnels par processus métier imposent donc de faire appel à des relais locaux qui pourront être désignés au sein des cellules de contrôle interne ou des cellules de déontologie existant dans chaque entité du groupe. Dans cet exercice, ces dernières pourront recueillir l'expérience des collaborateurs exposés aux risques opérationnels, par la mise en place de séries d'entretiens.

FICHE « MESURER LES RISQUES » SOURCES

23 octobre 2023

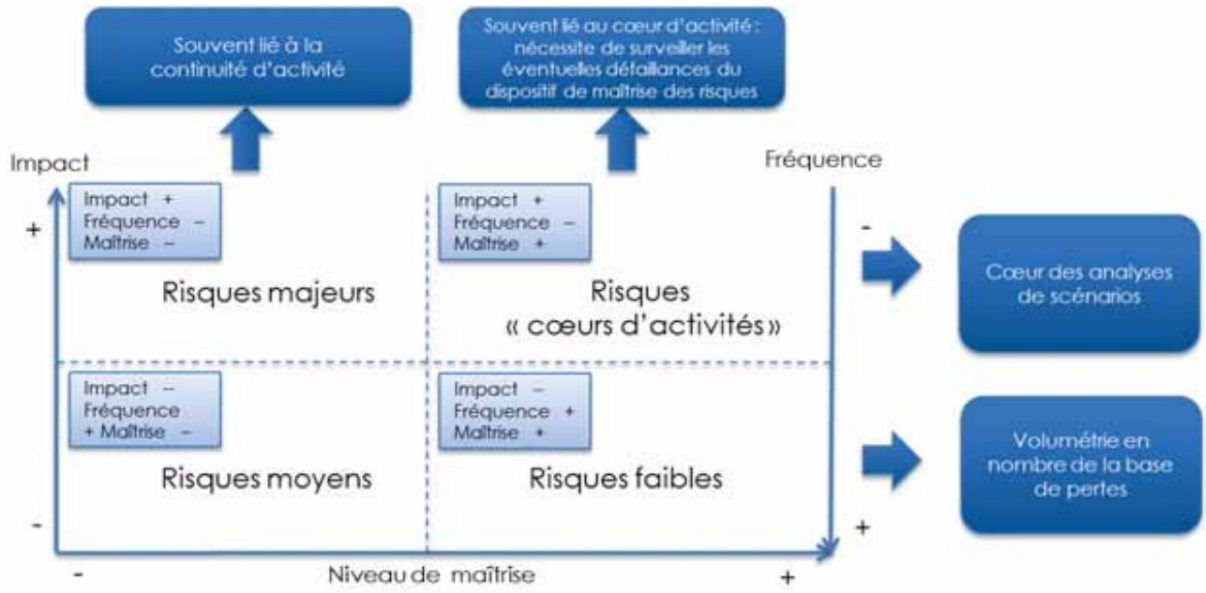
***Source** : Obsmétiers*

https://obsmetiers.rcp-pro.fr/fileadmin/observatoire_metiers/documents/etudes/Fiche_de_synthese.pdf

La cartographie des risques opérationnels permet d'identifier et recenser les principaux risques, internes ou externes, pouvant avoir un impact sur l'atteinte des objectifs fixés. Elle permet aussi d'évaluer les risques via la prise en compte de leur probabilité d'occurrence et de leur gravité potentielle, ainsi que de l'environnement et des mesures de maîtrise existantes.

C'est un outil pour visualiser l'exposition aux risques, délimiter les contours du profil de risques et identifier les zones à risque insuffisamment couvertes par le dispositif de maîtrise. Elle permet aussi de comparer et hiérarchiser les risques les uns par rapport aux autres.

Ce qui ressort le plus souvent des cartographies* :



FICHE « MESURER LES RISQUES » SOURCES

23 octobre 2023

AUTRES SOURCES :

Si vous disposez d'autres éléments, vous pouvez les déposer ici. ☺