Le risk assessment pour le secteur financier : un accélérateur de transformation de la fonction conformité

Comment améliorer l'efficacité des fonctions conformité grâce à l'exercice d'évaluation des risques ?

pwc

L'essentiel en bref

Les institutions financières doivent faire face à un environnement réglementaire en mutation constante dans lequel toute mauvaise conduite peut entraîner des pénalités financières et des poursuites judiciaires.

La pression des régulateurs est croissante et se traduit par des amendes importantes, pouvant atteindre plusieurs milliards d'euros pour les acteurs les plus importants. Cette pression n'est plus l'apanage des autorités américaines : les régulateurs européens sont de plus en plus actifs au travers de nouvelles réglementations à portées extraterritoriales et d'un intérêt renouvelé pour les investigations comme l'illustre l'amende de 4,5 milliards d'euros infligée à la banque suisse UBS pour fraude fiscale par les tribunaux français. En plus des régulateurs, les institutions financières sont également scrutées à la fois de l'intérieur (lanceurs d'alerte) et de l'extérieur (ONG, activistes environnementaux, associations). La conformité devient dès lors un élément central de la protection des institutions financières, et voit le champ de ses responsabilités s'étendre. Pour y faire face, la fonction conformité s'est généralement développée rapidement au cours des dernières années, et doit maintenant rationaliser son organisation et accroître son efficacité. C'est donc bien deux défis, d'apparence contradictoires, qui doivent être relevés : des responsabilités accrues et un besoin de rationalisation. L'exercice d'évaluation des risques de non-conformité, le *risk assessment*, est un élément clé en réponse à ces défis.

Le *risk assessment* est un puissant outil de supervision, mais aussi un facteur de la transformation de la fonction conformité.

Pour couvrir le spectre des risques de conformité, la fonction conformité doit étendre sa capacité de pilotage à l'ensemble des activités et zones géographiques de l'institution financière, même si elles ne sont pas considérées comme essentielles. En effet, plusieurs affaires récentes sont liées à des activités annexes ou à des entités considérées comme "mineures", comme le montre l'enquête en cours qui concerne plus de 200 milliards d'euros de transactions suspectes via la succursale estonienne de Danske Bank, qui, si elle est concluante, serait l'un des plus grands scandales de blanchiment d'argent de l'histoire.

Le risk assessment permet de mesurer le risque résiduel de non-conformité d'une organisation, en évaluant les risques inhérents à chaque activité ainsi que la qualité et l'efficacité du dispositif de contrôle couvrant ces risques. Les résultats du *risk assessment* doivent être utilisés pour revoir et améliorer en permanence le dispositif de surveillance et en particulier la bibliothèque des contrôles. Inversement, les résultats des contrôles doivent alimenter le *risk assessment*, pour l'évaluation des facteurs atténuants (ou "mitigants"), créant ainsi un cercle vertueux. Protéger l'entreprise en anticipant plutôt qu'en réagissant après coup participe à mettre la fonction conformité au cœur de l'organisation.

Pour mettre en œuvre un risk assessment, il est préférable de s'appuyer sur une plateforme déjà éprouvée.

Dérouler des campagnes annuelles de *risk assessment* peut s'avérer consommateur en termes de ressources, à moins de pouvoir s'appuyer sur un outil éprouvé, capable de s'adapter à une organisation spécifique. Les institutions financières ont plusieurs options à leur disposition, allant des développements en interne aux outils proposés par certaines FinTechs, sans oublier les solutions proposées par les grands acteurs traditionnels de l'industrie financière. PwC propose un dispositif d'évaluation des risques comprenant non seulement une plateforme intégrée avec des outils de suivi et de reporting, mais également des questionnaires d'évaluation des risques et des modèles de collecte de données reposant sur une double expertise métier et réglementaire, une taxonomie des risques et un moteur de notation. Capitaliser sur un dispositif efficace d'évaluation des risques n'aide pas seulement à évaluer les risques et accroître la supervision : c'est l'opportunité de faire du *risk assessment* la pierre angulaire de la transformation de la fonction conformité.

Un environnement réglementaire mouvant

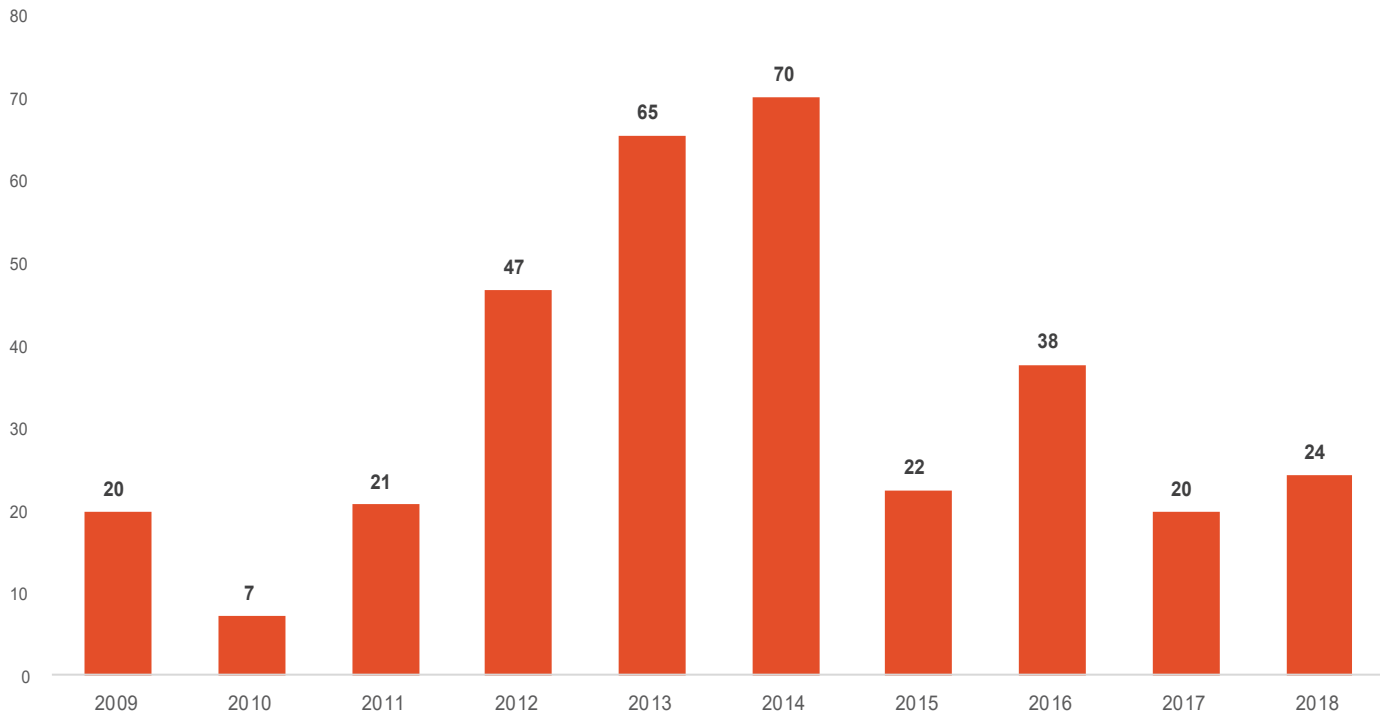
Faire face à la pression croissante des régulateurs

Des coûts liés à la non-conformité en hausse

L'augmentation des amendes imposées par les régulateurs exerce une pression énorme sur les institutions financières
Depuis la crise des subprimes, les institutions financières ont dû s'habituer à payer des amendes plus fréquentes et dont les montants peuvent être astronomiques.
En effet, les établissements bancaires ont payé plus de 330 milliards d'euros depuis 2009 pour régler des litiges liés à la non-conformité. Le pouvoir de réglementation en matière de conformité s'accroît aussi nettement : les régulateurs et les autorités sont de plus en plus prescriptifs quant à ce qu'ils attendent des programmes de conformité des entreprises. Ils ont développé des outils plus performants et renforcé leurs équipes.

Les institutions financières doivent rapidement répondre aux nouvelles exigences, malgré le manque de profils qualifiés, les contraintes technologiques et un éventail plus large de risques à couvrir. Les programmes de conformité cherchent donc des moyens de limiter les coûts de mise en œuvre tout en évitant d'avoir à payer des amendes et leurs coûteuses mesures correctives associées. De plus, les institutions financières doivent être conscientes des effets secondaires de la non-conformité : étant donné l'importance des réseaux sociaux et des chaînes d'information en continu, tout incident peut s'intensifier rapidement jusqu'à devenir viral, au point de nuire à la réputation de l'entreprise et d'entraîner une perte de clients.

Coûts des contentieux et litiges bancaires depuis 2009 (en milliards d'euros)

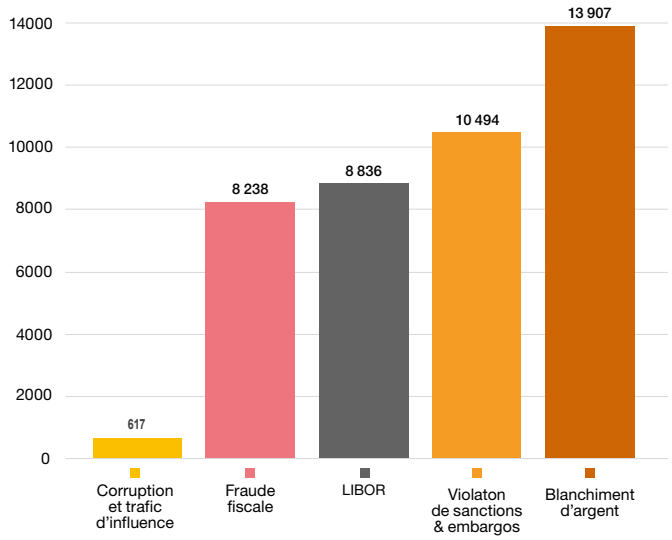


Légende : Montant des amendes payées par les principales banques européennes et américaines depuis 2009 pour non-conformité (Sources : media, rapports annuels des entreprises)

Un paysage réglementaire en mutation : vers un environnement de conformité mondial

Plus les régulateurs deviennent matures, plus la coopération internationale s'intensifie. Les États-Unis ne sont pas les seuls à distribuer des amendes partout dans le monde. L'Europe est également de plus en plus active, comme on l'a vu en France avec l'affaire de fraude fiscale d'UBS, où la banque Suisse a été condamnée à payer une amende de 4,5 milliards d'euros en février 2019. Les réglementations ont également plus fréquemment une portée extraterritoriale. Par exemple, Sapin 2, la loi française de lutte contre la corruption entrée en vigueur en 2017, s'applique à toute société implantée en France, directement ou par l'intermédiaire d'une succursale, ayant plus de 500 salariés et dont le chiffre d'affaires dépasse 100 millions d'euros. Les institutions financières doivent également faire face à des menaces potentielles émanant d'ONG et d'activistes, désireux de mettre en lumière toute mauvaise conduite. En parallèle, les institutions financières doivent faire preuve d'une attitude exemplaire en interne afin de se prémunir de tout manquement provenant de l'intérieur de l'organisation. En effet, aux États-Unis, 69 % des signalements de lanceurs d'alerte proviennent de collaborateurs actuels ou d'ex-collaborateurs de l'entreprise (2018).*

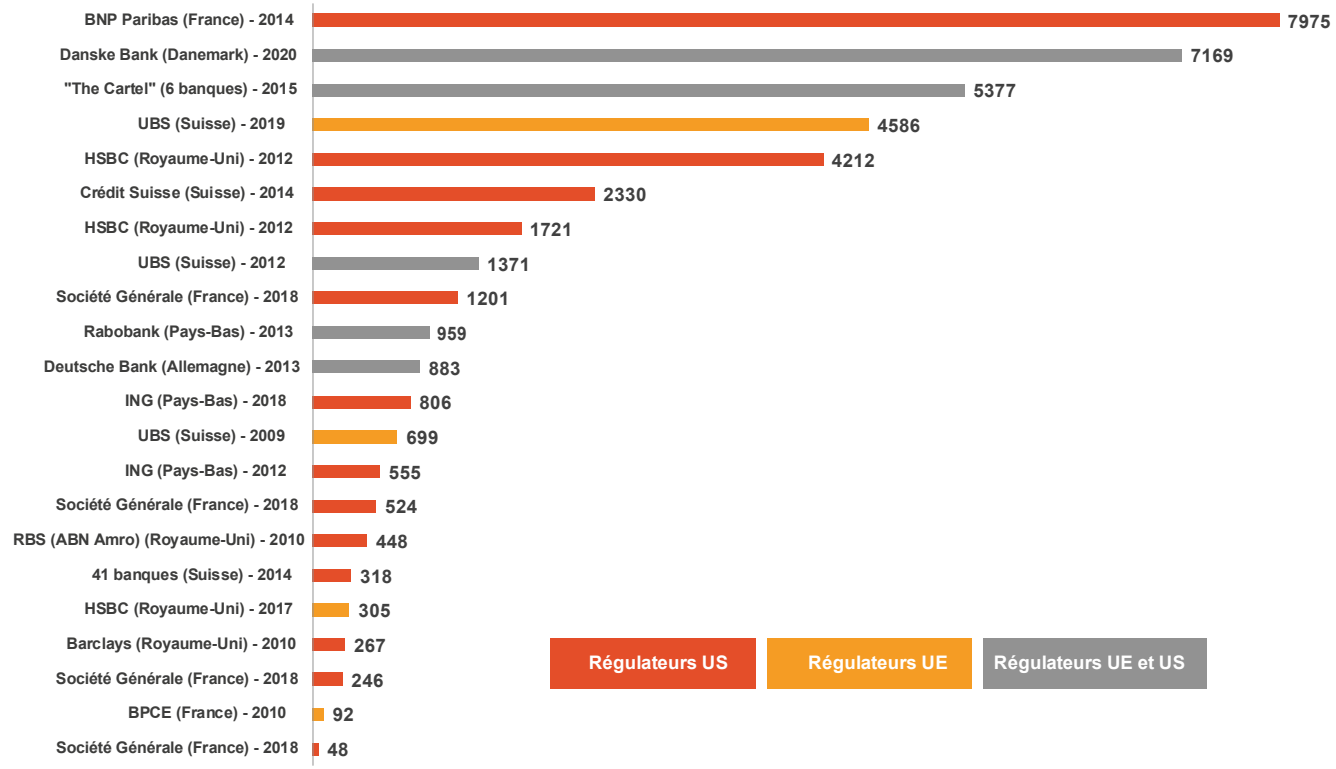
Répartition par type d'amendes (en millions d'euros)



Légende : Montants cumulés par type d'amendes (Source : étude PwC)

4,5 milliards : c'est le montant en euros que la banque Suisse UBS a été condamné en février 2019 à payer en France

Montants des plus importantes amendes (en millions d'euros) infligées pour non-conformité (2008-2019)



Légende : Principales amendes infligées pour non-conformité (2008-2019) (Source : analyse PwC)

*(Source : U.S. Securities and Exchange Commission's 2018 Annual Report to Congress - Whistleblower Program. https://www.sec.gov/sec-2018-annual-report-whistleblower-program.pdf)

La transformation de la fonction conformité et du rôle de responsable de la conformité

En une décennie, la fonction conformité a radicalement changé

Les attentes croissantes des régulateurs génèrent un besoin de ressources qualifiées en matière de conformité ainsi que des technologies avancées, en particulier pour la détection des fraudes et pour les processus d'entrée en relation avec les clients. A titre d'exemple, chez BNP Paribas, un mois après la condamnation par un juge américain à une amende de 8 milliards d'euros pour violation de sanctions (2015), le système de contrôle interne a été remodelé par l'intégration verticale de la fonction conformité et la revue de la gouvernance. En 2018, BNP Paribas a continué à renforcer ses équipes de conformité en ouvrant plus de 600 nouveaux postes*. Chez la plupart des grands acteurs de la place, les départements conformité ont également massivement développé leurs capacités de collecte et d'analyse de données, bien qu'il y ait encore beaucoup de travail à faire dans ce sens. La conformité ajoute à son rôle traditionnel d'« expertise » un rôle de surveillance qui doit s'appuyer sur des éléments quantitatifs pour être substantiel.

Le responsable de la conformité est devenu membre du comité exécutif

Le rôle du responsable de la conformité (ou «CCO» pour Chief Compliance Officer) évolue en même temps que la transformation de la fonction conformité. Les organisations prennent davantage conscience de l'importance du rôle du CCO. La rémunération de ce poste dans les institutions financières a ainsi sensiblement augmenté, avec un salaire moyen de 150 000 euros selon le cabinet de conseil Robert Half. Au-delà de leur mission principale qui consiste à protéger l'entreprise et ses actifs les plus importants, à savoir ses clients et sa réputation, les CCOs jouent également un rôle clé en apportant un éclairage lors des décisions business stratégiques.

La transformation de la fonction conformité : un défi en matière d'évaluation des risques

Après des années de croissance rapide des budgets et des équipes conformité, l'heure est aujourd'hui à une allocation intelligente des efforts, en priorité sur les plus grands risques. La fonction conformité se retrouve donc confrontée à un double défi quasi contradictoire : la nécessité de gérer l'extension de ses responsabilités et d'être capable d'anticiper les menaces, et en même temps l'impératif de rationaliser son organisation et de davantage concentrer ses efforts. Le *risk assessment* est un exercice puissant pour répondre à ces deux défis, s'il est conçu et exécuté correctement.

Sources :

** "Ces métiers présentent donc de fortes perspectives de recrutement : 150 postes sont à pourvoir en France et 540 à l'international rien que pour les Métiers de la Conformité de BNP Paribas en 2018" : https://business.lesechos.fr/directions-financieres/partenaire/partenaire-1730-la-conformite-des-metiers-incontournables-dans-le-secteur-bancaire-323014.php*

Piloter la fonction conformité grâce au *risk assessment*

Une approche normalisée et flexible pour identifier, mesurer et surveiller les risques de non-conformité

Disposer d'une vision d'ensemble des risques de non-conformité

Aujourd'hui, peu d'institutions financières disposent d'une vue d'ensemble de leurs risques de non-conformité. La complexité croissante de l'environnement commercial et l'imbrication des réglementations, couplés au très grand nombre de services offerts, rendent la tâche plus difficile. De nombreuses activités sont opérées en dehors de tout cadre géographique défini et recouvrent de multiples juridictions. Pour un service donné, la relation client peut avoir été initiée dans un pays, différent de celui où se trouve le client, tandis que le service est fourni dans un troisième lieu et exécuté dans un quatrième. Une institution financière est exposée à une grande variété de risques tels que ceux liés aux crimes financiers, la corruption, l'éthique, l'intégrité des marchés, la protection des clients et autres risques liés à la transparence fiscale et aux données personnelles. Construire une taxonomie des risques de non-conformité adaptée à l'entreprise et la mettre à jour régulièrement pour prendre en compte les risques émergents (cyber, environnementaux, etc.) est la première étape logique d'une bonne évaluation des risques.

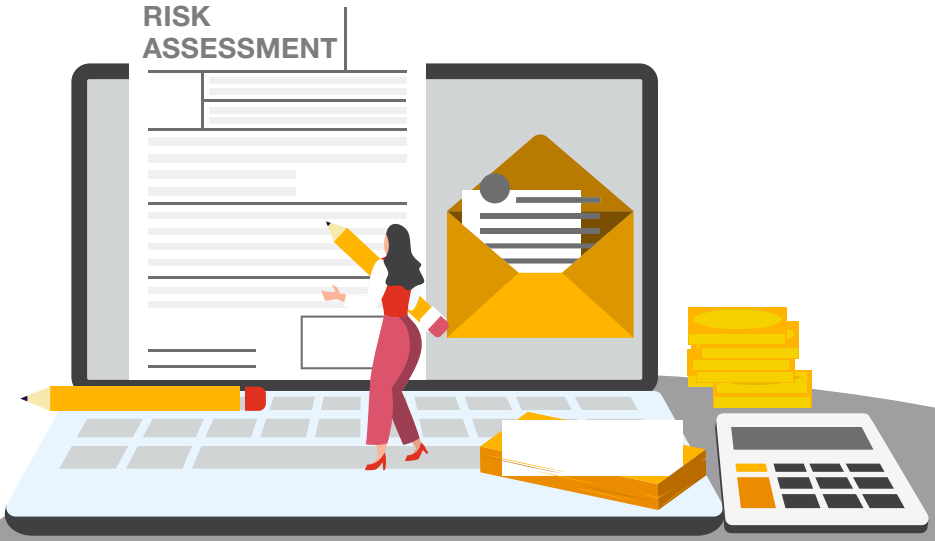
Renforcer la capacité de pilotage de la fonction conformité

Pour obtenir une vue d'ensemble des risques de non-conformité et détecter les zones les plus à risque, la fonction conformité doit avoir une couverture complète des activités et des zones géographiques de l'organisation.

Le cas de Danske Bank, qui met en lumière 200 milliards d'euros de transactions suspectes gérées par sa succursale estonienne entre 2007 et 2015, est un exemple récent de défaillance potentielle de la fonction conformité, provenant d'une filiale considérée comme "petite" au regard du groupe.

7 milliards : c'est le montant en euros que pourraient atteindre les amendes dans le cadre du plus grand scandale de blanchiment d'argent en Europe

Pour éviter ces écueils, la fonction conformité doit améliorer son dispositif de surveillance et élargir sa couverture des risques en ne se concentrant pas uniquement sur les activités « essentielles ». Les régulateurs savent que dans les environnements complexes d'aujourd'hui, le diable se trouve souvent dans les détails en termes de risques de conformité. En renforçant et en systématisant son approche des risques, la fonction conformité assumera pleinement son rôle de protecteur de l'organisation : elle disposera d'une vue holistique de ses risques et pourra détecter les domaines (types de risque, activités, zones géographiques) sur lesquels investir en priorité.



Le *risk assessment* : la pierre angulaire de la fonction conformité
Comment assurer une évaluation uniforme des risques à l'échelle de son organisation ? La clé du succès est d'adopter une approche structurée appuyée par la direction qui permet de susciter l'engagement des collaborateurs.

Qu'est-ce qu'un *risk assessment* ?

Une évaluation des risques de non-conformité (ou "compliance *risk assessment*" ou "*risk assessment*") est un exercice régulier, généralement annuel, qui permet d'identifier et de mesurer les risques de non-conformité d'une organisation à un moment donné dans le temps. Il évalue les risques encourus par chaque activité et/ou entité (appelés «risques inhérents») ainsi que la qualité et l'efficacité du dispositif de contrôle couvrant ces risques (appelés "mitigants"). La combinaison des risques inhérents et des mitigants permet de calculer un risque résiduel, qui représente l'exposition au risque.

Pourquoi un *risk assessment* ?

Un *risk assessment* doit constituer la base d'une approche avancée de gestion des risques. Au-delà de l'obligation réglementaire de disposer d'une cartographie des risques, le *risk assessment* est l'occasion d'identifier, d'analyser et de surveiller adéquatement les risques de conformité auxquels une organisation est confrontée. L'exercice de risk assessment permet de concevoir des plans d'action nécessaires pour la mise en œuvre de nouvelles mesures d'atténuation (mitigation), à la lumière de l'appétit au risque de l'entreprise. Dans un contexte de ressources limitées, il permet de concentrer les efforts sur les zones les plus à risques.

Concrètement, comment mesure-t-on les risques ?

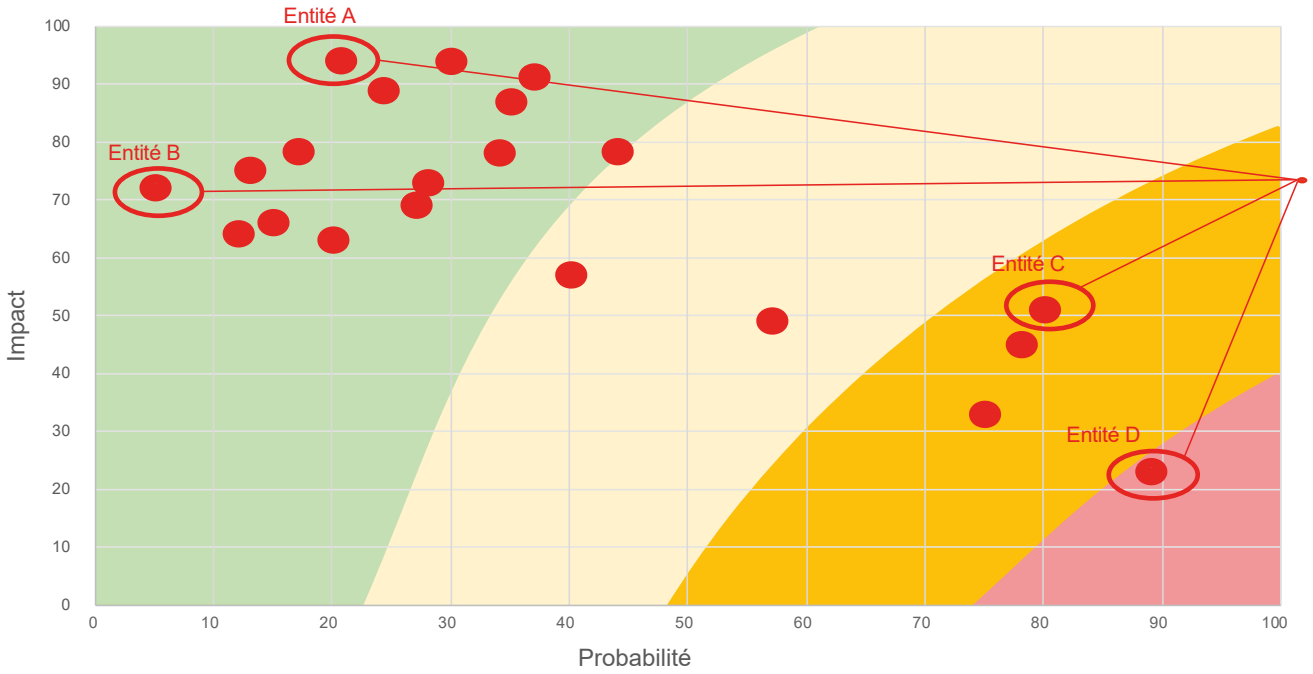
Deux méthodes existent pour évaluer les risques : soit une évaluation au travers de questionnaires, soit une évaluation basée sur la description par les métiers et la conformité des scénarios de risques pouvant se réaliser. Les questionnaires doivent intégrer un mix de questions qualitatives et quantitatives. Ces dernières années, les régulateurs ont mis l'accent sur l'ajout au processus d'évaluation de données non biaisées provenant directement des systèmes pour objectiver les résultats du *risk assessment*. Ces données portent notamment sur les clients, les produits et les transactions, mais également sur les dispositifs de couvertures des risques (taux de formation des collaborateurs, résultats des contrôles, etc.).

Ces données peuvent être renseignées de manière centralisée, lorsque c'est possible, ou remplies à un niveau plus granulaire de l'organisation.

En complément des questionnaires ou de l'analyse des scénarios, une méthodologie de scoring permet, via le jeu de pondérations et de mécanismes d'aggravations, de calculer les scores de risques et de contrôle des activités et des zones géographiques de l'institution. Cette méthodologie doit être clairement documentée pour pouvoir répondre à d'éventuelles requêtes des régulateurs.

Qui est impliqué ?

Un exercice de *risk assessment* implique l'ensemble de l'organisation, car il nécessite une connaissance précise des activités. Les fonctions opérationnelles, également appelées première ligne de défense, doivent être impliquées pour apporter une vision concrète des risques. En tant que deuxième ligne de défense, le département conformité est responsable du processus et challenge l'évaluation réalisée par les métiers. L'approche globale du *risk assessment* doit être clairement articulée entre la première et la deuxième ligne de défense et la description des rôles et des responsabilités de chacun doit figurer dans le document de méthodologie.

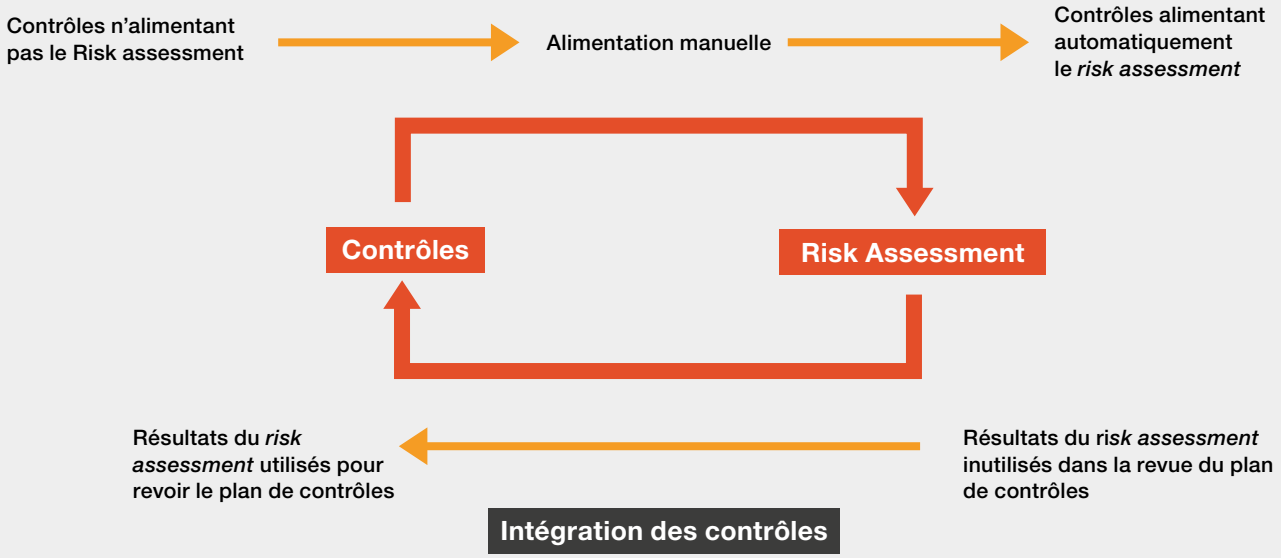


Légende : Exemple d'évaluation des risques de différentes entités d'un groupe bancaire dans le monde, pour un risque donné (Source : analyse PwC)

De la réaction à l'anticipation : l'intégration dans le dispositif de contrôle

Une fois les risques de non-conformité identifiés et évalués, les résultats du *risk assessment* doivent être utilisés pour renforcer la bibliothèque des contrôles sur les zones les plus *vulnérables. Réciproquement, les résultats des contrôles doivent faire partie de l'évaluation du dispositif de couverture pour un risque donné.*

Il apparaît donc clairement que les dispositifs de risk assessment et de contrôles sont étroitement liés. Une approche bien articulée met en place une boucle d'amélioration continue des contrôles en fonction des résultats du risk assessment, qui tiendront eux-mêmes compte des résultats des contrôles.



Légende : Exemple d'évaluation des risques de différentes entités d'un groupe bancaire dans le monde, pour un risque donné (Source : analyse PwC)

Mettre à profit des dispositifs existants pour accélérer la transformation de votre conformité

S'appuyer sur une plateforme de *risk assessment* adaptée à votre organisation

La mise en place d'un *risk assessment* et son exécution à une fréquence régulière peuvent représenter une charge de travail importante, surtout dans les premières années de conception et de calibrage de l'exercice. Il n'existe pas de véritables options sur étagère en termes d'outils ou de méthodologie, car les solutions de marché n'offrent pas suffisamment de possibilités d'adaptation aux besoins spécifiques des organisations.

PwC met à disposition de ses clients un dispositif d'évaluation des risques qui comprend non seulement une plateforme intégrée mais aussi des questionnaires d'évaluation des risques et des modèles de collecte de données.

La plupart des grands acteurs ont ainsi développé leurs propres solutions en internes ou utilisent des plateformes ad-hoc telles que celle développée par PwC pour les exercices de *risk assessment* : un outil flexible, adapté aux banques, aux compagnies d'assurance ou aux plateformes spécialisées des banques en ligne.

Contactez-nous

Vous souhaitez transformer votre fonction conformité et étudier la mise en place d'un dispositif d'évaluation des risques ? Nos experts "Financial Services Risk & Regulation" sont à votre disposition pour répondre à vos questions.

Géraud du Deschaux
Directeur, PwC France
geraud.dudeschaux@pwc.com
Tel : +33 1 56 57 83 66

Sébastien d'Aligny
Associé, PwC France
sebastien.daligny@pwc.com
Tél : +33 1 56 57 15 32

Rami Feghali
Associé, PwC France
rami.feghali@pwc.com
Tél : +33 1 56 57 71 27

Collaborateurs Financial Services Risk & Regulation ayant contribué à cette publication :
Ivan Takahashi, Senior Manager, PwC France
Nina Dolveck, Associate, PwC France
Victor Jessel, Senior Associate, PwC France
Dominik Schauerte, Directeur, PwC Allemagne

Pour en savoir plus :
pwc.fr/riskassessment