LES FONDAMENTAUX

Guide pratique de la Conformité en assurance

Les enjeux pour la gestion des risques et le contrôle interne

Odilon Audouin
Alexandre Liaskovsky

L'ARGUS EDITIONS de l'assurance

SOMMAIRE

ANNEXES

III – Le cycle vertueux de la Conformité

Une synthèse des bonnes pratiques observées chez différents organismes (et chez certaines banques) montre qu'un processus de gestion des risques de non-conformité complet et efficace repose généralement sur huit étapes successives. C'est ce que nous appelons le cycle vertueux de la Conformité.

Ces étapes décrites ci-après se déroulent les unes après les autres et se répètent à l'infini. Elles constituent, pour ainsi dire, l'objectif permanent de tout responsable de la Fonction conformité.

A – Étape 1 : identification des obligations (veille réglementaire, y compris prospective) et leurs attendus – recherche des meilleures pratiques

Connaître ses obligations peut parfois s'avérer aussi difficile que de les respecter. Cette étape d'identification des nouvelles réglementations ou des mises à jour des réglementations existantes applicables aux activités d'assurance est le point d'entrée de la Conformité.

La Fonction conformité devra ainsi veiller à bien comprendre les textes, à les « décortiquer »... et à en extraire les principaux attendus, afin d'être en capacité de les restituer sous une forme compréhensible et opérationnelle par les métiers.

Important :

La veille réglementaire nécessite d'être organisée et structurée au sein d'un processus « processus de veille réglementaire ». Elle répond à des besoins souvent plus larges que ceux de la Fonction conformité et de nombreux acteurs y participent. La direction juridique et les lignes métiers sont, à ce titre, des acteurs clés dans le processus de veille, sur lesquels la Fonction conformité peut utilement s'appuyer.

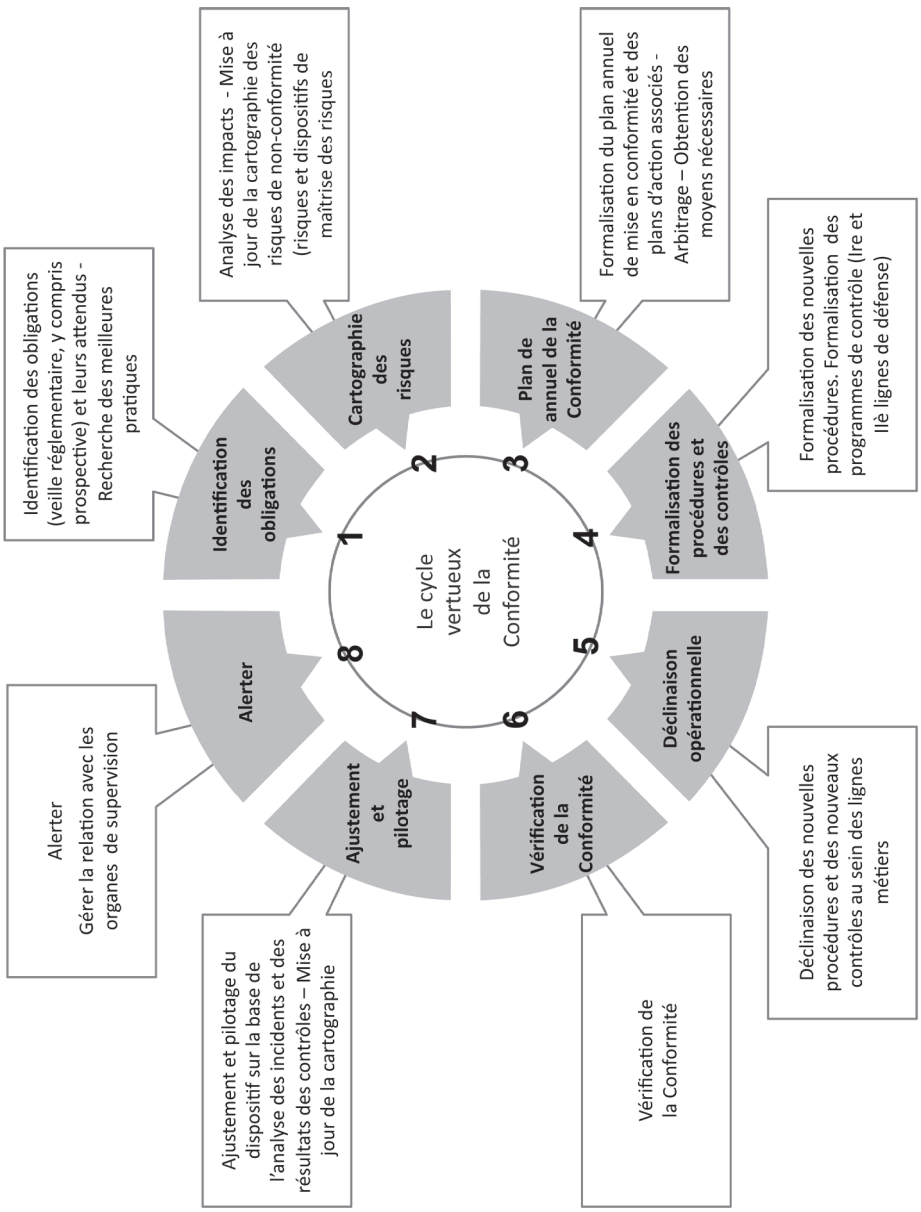
La formalisation du « nouveau » processus de veille réglementaire commence par un travail de recensement des actions de veille existantes au sein de l'entreprise. Les rôles des différents acteurs pourront être définis dans un deuxième temps, à chaque stade du processus. Une section entière est dédiée au processus de veille réglementaire dans le chapitre III relatif aux outils de la Fonction conformité.

La mise en place d'une veille prospective, c'est-à-dire l'ensemble des moyens permettant à la Fonction conformité d'identifier les nouveaux textes avant leur publication, doit également être envisagée. Elle permet à l'entreprise de se préparer à la mise en conformité dans de meilleures conditions, et, dans certains cas, d'en dégager un avantage concurrentiel. La veille prospective consiste également à identifier sur la Place les meilleures réponses qui auraient déjà pu être apportées à la réglementation.

Exemple :

Il s'agira, pour la Fonction conformité, d'obtenir des informations d'un confrère ou de participer à des initiatives de Place qui visent à proposer un format de « réponse » commun à l'ensemble des acteurs de la Place aux nouvelles exigences réglementaires. Ce partage de l'information et ces échanges constituent une bonne pratique, car cela permet également de s'assurer de la bonne interprétation des textes et des attendus par l'entreprise.

Les 8 étapes du cycle vertueux de la Conformité



B – Étape 2 : analyse des impacts – mise à jour de la cartographie des risques de non-conformité

Lorsque les nouvelles obligations et leurs attendus ont été identifiés, il convient de mener une première analyse de leurs impacts sur l'entreprise.

Suggestion :

Ce travail peut être mené par la Fonction conformité mais l'implication des lignes métiers et des directions supports permettra, sans aucun doute, d'obtenir de meilleurs résultats.

À ce stade du cycle vertueux de la Conformité, il s'agit davantage d'identifier et de mesurer des « macro-impacts » (grands processus métiers et supports impactés), et en particulier de déceler les enjeux significatifs en termes de systèmes d'information, de ressources humaines et d'organisation. La cartographie des risques de non-conformité qui permet de faire apparaître les risques de l'entreprise et son degré d'exposition à chacun d'entre eux, selon les dispositifs de maîtrise des risques déployés, doit être mise à jour. Une section complète est consacrée à la cartographie des risques dans le chapitre III relatif aux outils de la Fonction conformité.

À l'issue de cette étape, les principaux impacts sont identifiés et la cartographie est à jour, ce qui signifie que le niveau d'exposition de l'entreprise au risque de non-conformité est matérialisé.

C – Étape 3 : formalisation du plan de mise en conformité – arbitrages – obtention des moyens nécessaires à la mise en conformité

La Fonction conformité va chercher, lors de cette étape, à compléter les travaux de l'étape précédente en formalisant des plans de mise en conformité pour les situations dans lesquelles les risques de non-conformité sont élevés. Ces plans consistent à hiérarchiser les actions à engager et à donner de la visibilité aux parties prenantes sur les principaux impacts de la mise en œuvre à la réglementation. La formalisation des plans de conformité, corrélés aux travaux d'analyse des impacts, doit en principe mettre la gouvernance opérationnelle en situation de pouvoir arbitrer sur les actions à engager. Ces décisions sont prises en fonction de l'appétit de risque (ou appétence au risque) de l'entreprise qui va considérer le niveau de tel ou tel risque « net » comme acceptable ou non. Cette phase d'arbitrage est toujours nécessaire, compte tenu des contraintes en matière de ressources humaines et de moyens financiers disponibles pour la mise en conformité.

Exemple :

Une entreprise pourra décider de privilégier sur l'année à venir la mise en conformité sur les contrats non réglés et de reporter à l'année suivante la mise en conformité au regard des obligations issues de la loi Informatique et Libertés, en raison du risque de contrôle de l'ACPR auquel s'expose l'organisme sur la première thématique.

Cette étape est très importante pour le responsable de la Fonction conformité, car il obtient ici sa feuille de route et, dans le même temps, négocie les moyens nécessaires à son action.

D – Étape 4 : formalisation des nouvelles procédures – formalisation des programmes de contrôles (Ire et IIe lignes de défense)

La mise en conformité de l'entreprise implique la formalisation de nouvelles procédures et le renforcement ou la création de contrôles. Une bonne pratique consiste à formaliser une procédure « chapeau » ou « faîtière » (c'est-à-dire adressant toutes les activités et tous les métiers), que les lignes métiers devront ensuite décliner opérationnellement en tenant compte de leurs spécificités (voir étape 5). Cette étape vise également à formaliser les programmes de contrôle de la Conformité qui seront utilisés par les contrôleurs de Ier et de IIe niveaux.

E – Étape 5 : déclinaison des nouvelles procédures et des nouveaux contrôles au sein des lignes métiers

Cette étape clé est également l'une des plus difficiles. La déclinaison consiste à formaliser de nouvelles procédures et de nouveaux contrôles au sein des lignes métiers, à partir des éléments de la procédure chapeau, mais surtout à les déployer pour qu'ils soient appliqués au quotidien par les lignes métiers. Lorsque ce qui doit être déployé a été conçu par les lignes métiers elles-mêmes, les chances de succès sont plus élevées. Si ce qui doit être déployé a été élaboré uniquement « en chambre » par la Fonction conformité, les chances de déploiement sont très faibles. Le nouveau dispositif doit donc être défini par les lignes métiers en lien étroit avec la Fonction conformité, qui s'assurera que les exigences de la réglementation sont correctement prises en compte. La réussite du déploiement et sa bonne application dépendent de plusieurs leviers, comme la formation, qui doivent être adressés comme un projet de « conduite du changement ». Une partie est dédiée à ce sujet dans la dernière section de ce chapitre.

F – Étape 6 : vérification de la Conformité

Remarque :

Paradoxalement, la directive Solvabilité II consacre l'apparition d'une « fonction de vérification de la conformité » alors qu'il ne s'agit que d'une des étapes du cycle vertueux de la Conformité. Celle-ci ne peut avoir lieu, en effet, qu'après avoir déployé les dispositifs au sein de l'ensemble des activités concernées de l'entreprise (nouvelles procédures et nouveaux contrôles). Une bonne approche consiste d'ailleurs à consacrer les premiers efforts à la définition et à la mise en place des nouveaux dispositifs, puis, dans un deuxième temps, à la vérification de leur conformité.

La vérification de la Conformité consiste à sélectionner un thème de la Conformité à contrôler (en cohérence avec le plan de Conformité élaboré à l'issue de la cartographie des risques), puis à dérouler le programme de contrôle. Plusieurs options sont concevables en ce qui concerne le rattachement des contrôleurs qui vont exécuter les programmes de contrôles. La pratique montre qu'ils peuvent être des collaborateurs de la Fonction conformité ou être rattachés au contrôle interne, qui constitue, comme évoqué plus haut, une direction « partenaire ».

G – Étape 7 : ajustement et pilotage du dispositif sur la base de l'analyse des incidents et des résultats des contrôles – mise à jour de la cartographie

Le dispositif de maîtrise des risques de non-conformité doit être réévalué régulièrement afin de s'assurer qu'il est toujours adéquat. En effet, de nouveaux risques peuvent apparaître, et les contrôles existants peuvent s'avérer défaillants ou inadaptés. La mise à jour de la cartographie doit être réalisée a minima annuellement mais il existe d'autres moyens de s'assurer de sa pertinence à fréquence plus régulière. La collecte et l'analyse des incidents, qui font l'objet d'une partie dédiée dans le chapitre III relatif aux outils de la Fonction conformité, est l'un de ces leviers. Elle doit permettre au responsable de la Conformité d'identifier de nouveaux foyers d'exposition au risque de non-conformité (incidents récurrents) et de « challenger » l'évaluation des dispositifs de maîtrise de risques réalisée dans le cadre de la cartographie (par exemple, en cas de survenance d'un incident majeur sur un processus dont le risque net est faible). La remontée des alertes directement par les collaborateurs, lorsqu'un dispositif d'alerte professionnelle (« whistleblowing ») a été mis en place, est également une source d'identification des risques de non-conformité. Ce dispositif fait l'objet de développements plus précis dans le cadre du chapitre IX relatif à l'Éthique et à la conduite des affaires.

H – Étape 8 : alerter – gérer la relation avec les organes de supervision

En matière de supervision interne, l'article R. 354-4-1 du Code des assurances applicable au 1er janvier 2016 rappelle que la Fonction conformité doit conseiller le directeur général ou le directoire ainsi que le conseil d'administration ou le conseil de surveillance. Il faut également qu'elle soit en mesure de les alerter. Il revient au top management de définir les modalités de remontée des informations qu'il souhaite connaître. La mise en place d'indicateurs de pilotage, qui repose sur des logiques de seuils de montant et/ou de gravité des incidents, peut être un moyen de mise en œuvre opérationnel des alertes. Pour ce qui concerne la supervision externe, la relation avec l'ACPR (et les autres autorités de supervision) est un élément essentiel de l'efficacité du dispositif. Il est ainsi fortement conseillé de communiquer et d'échanger régulièrement avec les autorités de contrôle, y compris en dehors du cadre des contrôles.

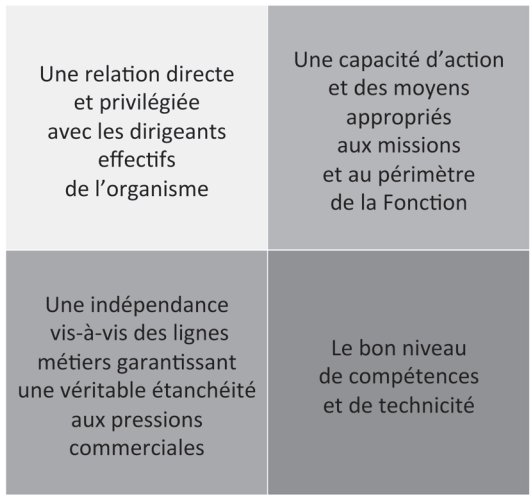
Section II – Les principes organisationnels et la politique de la Fonction conformité

I – Les principes communs à toutes les Fonctions clés

En 2014, lors de la présentation des résultats de la dernière enquête de préparation à Solvabilité II, l'ACPR annonçait que 92 % des répondants avaient mis en place une Fonction conformité contre 81 % l'année précédente. Il reste à préciser ce qui est concrètement mis en œuvre au-delà de la nomination d'un collaborateur et l'ajout d'une fonction dans un organigramme.

La Fonction conformité obéit à plusieurs principes communs avec les autres Fonctions clés.

Les principes communs aux Fonctions clés de Solvabilité II



A – Une relation directe et privilégiée avec les dirigeants effectifs

Les Fonctions clés rendent des comptes directement à la gouvernance opérationnelle et à la gouvernance institutionnelle.

Les Fonctions clés ont des obligations spécifiques sur les thèmes dont elles ont la charge vis-à-vis des dirigeants et de la gouvernance institutionnelle : conseiller et alerter.

B – Une capacité d'action et des moyens appropriés

La Fonction conformité, à l'instar du contrôle périodique (audit interne), doit pouvoir agir librement et notamment accéder à toutes les informations qu'elle juge utile de connaître au sein de l'entreprise. Ce droit doit cependant s'exercer intelligemment, par le biais d'un protocole, afin d'éviter de trop nombreuses sollicitations des opérationnels.

Les Fonctions clés doivent disposer des moyens humains et techniques nécessaires à la bonne réalisation de leurs missions. Sur ce sujet, le train est en marche mais il existe de nombreuses Fonctions conformité encore insuffisamment dotées en ressources humaines et financières.

C – Une indépendance vis-à-vis des lignes métiers

La Fonction conformité doit être indépendante, c'est-à-dire libre des influences qui pourraient entraver son objectivité, son impartialité ou encore son indépendance. Cette condition est généralement satisfaite lorsque la Fonction est positionnée à un niveau suffisamment élevé dans la hiérarchie et qu'elle a été confiée à une personne qui ne détient aucune fonction opérationnelle, c'est-à-dire principalement commerciale.

La Fonction conformité devrait également être investie d'un « droit de véto », c'est-à-dire la possibilité de stopper ou d'empêcher une opération ou une transaction, quel que soit l'enjeu

qu'elle présente ou le bénéfice que pourrait en tirer l'entreprise (par exemple, la faculté de s'opposer à la mise sur le marché d'un nouveau produit). En pratique, force est de constater qu'il est rare que les entreprises dotent le responsable de la Conformité de telles prérogatives. Ce dernier doit, à tout le moins, être en mesure de donner un avis, favorable ou défavorable, sur certaines décisions de l'entreprise qui présentent un impact sur son exposition au risque de non-conformité. Cet avis doit pouvoir être tracé, en particulier via les comptes-rendus des comités auxquels il participe.

D – Le bon niveau de compétences et de technicité

Si les missions et les enjeux de la Fonction conformité sont, aujourd'hui, mieux compris qu'hier, les attentes vis-à-vis de celle-ci sont également plus fortes. Le niveau de compétence et de technicité de la personne en charge de la Fonction conformité et de ses collaborateurs revêt donc une importance cruciale, et conditionne souvent le succès de ses actions. Le responsable de la Fonction conformité doit, par ailleurs, être légitime aux yeux de tous, au sein de l'entreprise mais également à l'extérieur, pour assurer les missions qui lui sont confiées. Les compétences qui semblent nécessaires à la Fonction conformité sont illustrées ci-après dans la section III.

Par ailleurs, même si les scandales récents, chez les organismes d'assurance ou les banques, ont toujours impliqués des collaborateurs qui avaient le niveau d'honorabilité requis (sur la base de l'analyse de leur historique professionnel)… les organismes d'assurance doivent déployer des mesures raisonnables qui permettent de s'assurer que le responsable de la Fonction désigné n'a fait l'objet d'aucun manquement significatif à des règles externes ou internes, et qu'il s'est toujours conformé, dans sa carrière professionnelle, à des standards éthiques et de bonne conduite élevés.

Nous reviendrons plus en détail sur le sujet de la compétence et de l'honorabilité (fit and proper), qui fait l'objet de dispositions spécifiques de la réglementation, dans le chapitre IX relatif à l'Éthique et à la conduite des affaires.

Important :

Le renforcement du risque pénal qui pèse sur les entreprises et ses dirigeants, expose le responsable de la Fonction conformité, à titre personnel cette fois-ci, à des risques nouveaux.
Le « Compliance Officer » (CO) – ou le « Chief Compliance Officer » (CCO) doit ainsi organiser sa propre protection, c'est-à-dire sa capacité à se défendre si l'entreprise souhaite lui faire porter la responsabilité d'un grave incident de non-conformité. Il doit donc être attentif à la formalisation et à la traçabilité de son devoir d'alerte (A-t-il alerté le top management sur les risques encourus par l'entreprise ? L'a-t-il invité à engager des actions correctrices ? Disposait-il des moyens de connaître les opérations à l'origine de l'incident ?). Une première protection repose sur la fiche de poste et/ou la lettre de mission. Celle-ci doit être validée au plus haut niveau de l'entreprise, et préciser clairement les rôles et responsabilités de chacun (« Who is responsible of what ? »).
Une deuxième protection consiste à matérialiser dans les comités des risques ou autres instances de gouvernance, l'éventuel désaccord avec la gouvernance opérationnelle.
Enfin, il reste également possible de démissionner en cas de désaccord profond.

Guide pratique de la Conformité en assurance

Solvabilité II impose aux organismes d'assurance de mettre en place une Fonction conformité, « fonction clé » du système de gouvernance intégrée aux dispositifs de contrôle interne et de gestion des risques.
Cette nouvelle obligation intervient dans un contexte de concurrence accrue, d'inflation des textes et de pression du régulateur sur les thèmes de la Conformité, comme la protection de la clientèle ou la lutte contre le blanchiment de capitaux et le financement du terrorisme.
La « Compliance » est entrée dans une nouvelle ère…
Le déploiement de la Fonction conformité oblige les organismes d'assurance à faire évoluer leur organisation, leur stratégie et leurs méthodes de travail. Afin de prévenir le risque de sanctions et d'atteinte à la réputation de l'entreprise, ils doivent adopter une conduite appropriée vis-à-vis de leurs clients, collaborateurs et partenaires.
Mais respecter la réglementation ne suffit plus. La Conformité s'inscrit dans une démarche proactive et nécessite d'anticiper les exigences à venir. Les acteurs qui sauront relever ce défi avec le niveau d'ambition adéquat en tireront, à n'en pas douter, un avantage concurrentiel indéniable.
Les opportunités de différenciation sont réelles !
Ce guide pratique détaille les enjeux de la Fonction conformité sur chacune des étapes du cycle de mise en conformité. Illustré de nombreux exemples et bonnes pratiques tirés de l'expérience des auteurs, il constitue l'outil incontournable de tous les acteurs de la « Compliance » : responsables et collaborateurs de la Fonction conformité, contrôleurs internes, risk managers, opérationnels, mais également dirigeants et administrateurs.

***Odilon Audouin**, Directeur au sein du département Risk Advisory de Deloitte Conseil, intervient depuis près de 20 ans auprès d'assureurs dans la sphère de la Compliance. Il est diplômé de l'ESC Tours-Poitiers, titulaire d'un MBA de l'ESSEC et certifié CAMS.*

***Alexandre Liaskovsky**, Consultant senior au sein du département Risk Advisory de Deloitte Conseil, intervient auprès d'assureurs sur divers projets de Conformité. Il est diplômé de Sciences Po. Paris et titulaire d'un Master de droit.*

www.argusdelassurance.com

9 782354 742133