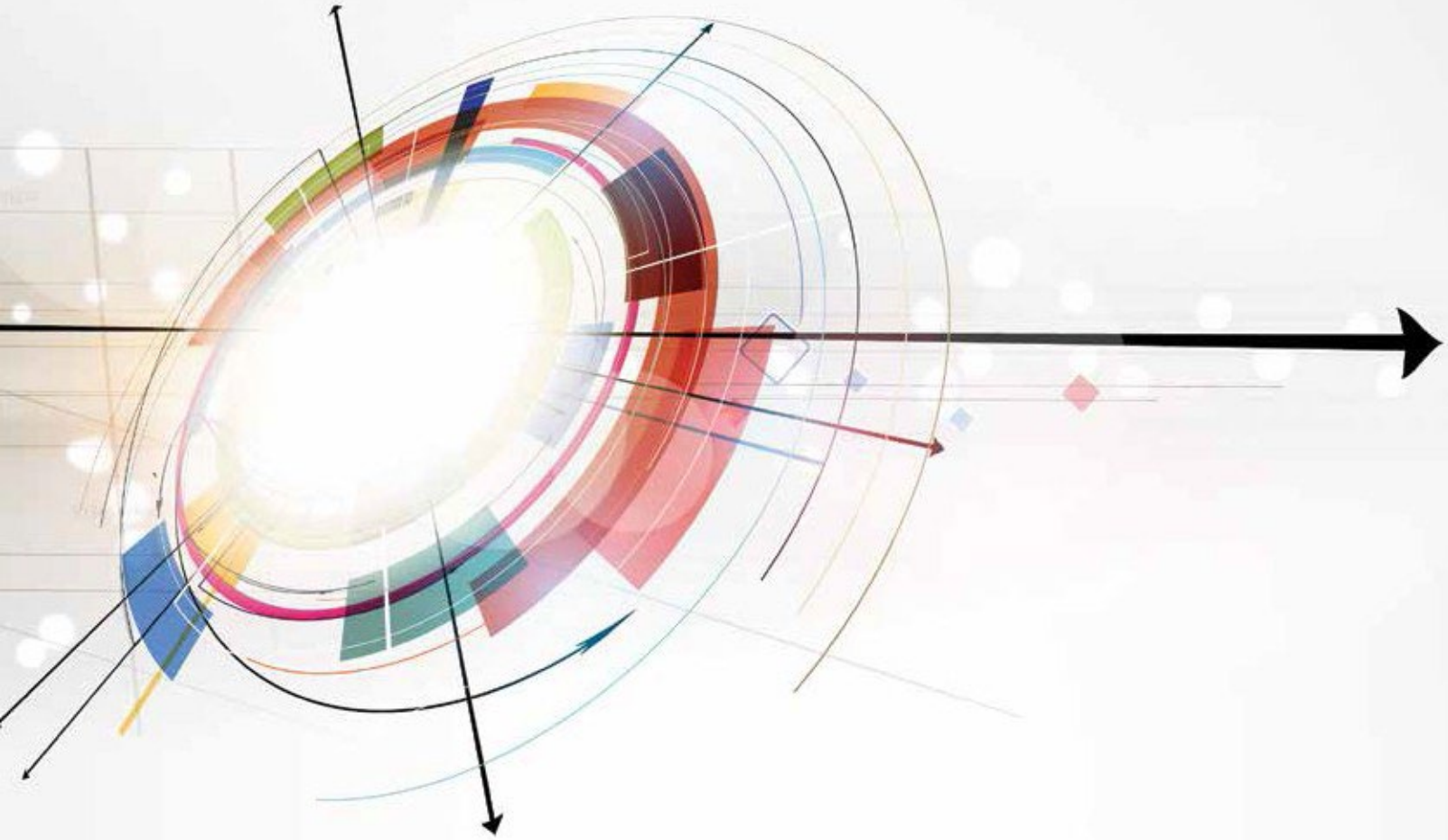


PERSPECTIVES INTERNATIONALES

Audit interne et conformité : la clarté et la collaboration au service d'une gouvernance renforcée

The Institute of Internal Auditors

Numéros précédents

Pour accéder aux numéros précédents des Perspectives internationales, visitez le site à l'adresse suivante www.theiia.org/GPI.

Avis des lecteurs

Envoyez toutes vos questions et observations à l'adresse : globalperspectives@theiia.org.

Table des matières

Remerciements

L'IIA remercie les membres et parties prenantes ayant contribué à la rédaction de ce numéro : Mark Carawan, Caroline Maurice, Vandana Siney, Karen Brady, Benito Ybarra, Mike Joyce, Stacey Schabel, Mani Sulur, Jee Kymm, Dana Lawrence, Geoff Rusnak, Paul Ricci, Senthil Kumar, Marta Budavari, Kathryn Reimann, Emily Wright, Akash Singh, Nora Ilmoni, Christine Ong, Calum Owen, Trygve Sørlie, Francis Nicholson et Jill Austin, ainsi que l'IIA-Australie.

À propos de l'IIA

Porte-parole mondial de la profession d'audit interne, l'Institut des auditeurs internes (Institute of Internal Auditors, IIA) est une autorité reconnue et un leader incontesté dans la formation et la formulation de normes, lignes directrices et certifications. Fondé en 1941, l'IIA compte actuellement quelque 200 000 membres dans plus de 170 pays et territoires. Son siège se situe à Lake Mary (Floride) aux États-Unis. Plus d'informations sont disponibles sur le site www.globaliia.org.

Avertissement

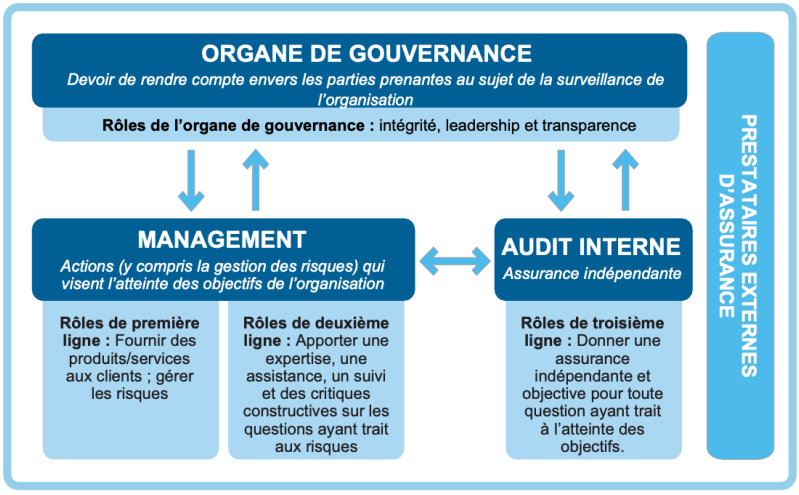
Les opinions exprimées dans les Perspectives internationales ne sont pas nécessairement celles des contributeurs individuels ayant collaboré à l'élaboration du présent document ni celles de leurs employeurs.

Introduction

Parfois confus, le rapport entre audit interne et conformité soulève des questions cruciales : le premier peut-il être responsable de la seconde ? La fonction Conformité a-t-elle la primauté de ces sujets dans l'ensemble de l'organisation ? Est-il envisageable que la conformité fasse partie des prérogatives du responsable de l'audit interne ?

Cette publication a pour but de clarifier ces interrogations complexes, afin d'éviter toute confusion et de ne laisser aucune place à d'éventuelles lacunes ou redondances. On y démontrera qu'une compréhension précise est essentielle, que la collaboration est vivement encouragée et que l'indépendance de l'audit interne[1] revêt une importance fondamentale.

Il n'est pas question ici de traiter de l'audit de la conformité, mais plutôt de fournir au conseil d'administration, au management, aux professionnels de la conformité et aux responsables de l'audit interne un outil pour les aider à comprendre le rapport entre l'audit interne et la conformité, *Modèle des Trois Lignes* à l'appui (modèle dont les six principes et leurs modalités d'application à la conformité sont deuxième partie de cet exposé).



Les pages qui suivent devraient aider le lecteur à appréhender finement la conformité ainsi que la gestion des risques associés sous tous ses aspects, en lien avec le *Modèle des Trois Lignes*[2], à les évaluer et à les mettre en œuvre efficacement dans leur structure de gouvernance (tous lieux, secteurs d'activité, tailles et niveaux de complexité ou de maturité confondus). Des auditeurs internes ainsi que des responsables de la conformité et/ou de la gestion des risques ont accepté de partager les problématiques de conformité auxquelles ils ont été confrontés dans leur pratique dans l'objectif de faciliter l'évaluation des activités de conformité relativement aux 6 principes du *Modèle* (pages 10 à 18).

---

[1] La conformité, en tant que composante essentielle d'une gouvernance durable, est un axe fort des recommandations formulées par la présidence italienne du B20 à l'intention des ministres du G20 dans son document intitulé *B20 Italy Integrity & Compliance Policy Paper 2021*. Le point 2.1 page 11 notamment fait mention du rôle de l'audit interne tel que décrit dans le *Modèle des Trois Lignes*.

[2] Dans certains pays et certains secteurs, les rôles et les responsabilités en matière de conformité et de gestion des risques associés sont définis de manière très précise et font l'objet d'une législation et d'une réglementation foisonnantes, d'une vaste jurisprudence et de nombreuses recherches académiques. Le lecteur est invité à consulter les études détaillées qui existent sur le sujet, comme celles de l'American Law Institute : *Principles of the Law, Compliance, Risk Management, and Enforcement* No. 1 et *Principles of the Law, Compliance and Enforcement* No. 2.

Devoir de rendre compte, actions et assurance

Dans le *Modèle des Trois Lignes*, on découvre comment le *devoir de rendre compte* de l'organe de gouvernance, les *actions* du management et l'*assurance indépendante* de l'audit interne forment le socle d'une gouvernance efficace. On retient également de quelle manière ses six principes facilitent l'évaluation des différents rôles et responsabilités au sein de l'organisation. L'application des fondamentaux du *Modèle* et de ses principes varie d'une organisation à l'autre en fonction de ses objectifs, de ses ressources et de sa situation. Le *Modèle* aide chaque organisation à identifier les structures, à concevoir les processus et à attribuer les responsabilités optimales pour réaliser ses objectifs, à commencer par la gestion des risques de conformité, dont la responsabilité incombe au management[3] tout en demeurant le fruit d'un effort collectif.

Dans la palette des attentes et exigences de conformité dont l'organisation doit tenir compte, on distingue les contraintes externes (lois, réglementations, etc.) et les contraintes internes (règles/politiques, standards/normes, procédures, codes de conduite, etc.). Ces obligations peuvent être formalisées et explicitement définies ou au contraire tacites, comme c'est le cas des attentes d'ordre social, éthique ou culturel. Ce vaste éventail de considérations mouvantes sera regroupé ci-après sous l'expression « attentes et exigences ».

Les parties prenantes attendent de l'organisation qu'elle accomplisse ses objectifs et qu'elle maximise la valeur dans un cadre à la fois légal et éthique. Par conséquent, les organisations se donnent les moyens de suivre de près la conformité dans plusieurs domaines clés (la liste qui suit est loin d'être exhaustive) : santé et sécurité ; emploi ; protection des données et de la vie privée ; forme juridique et droit du commerce ; réglementation sectorielle ; normes de qualité ; lutte contre la fraude et la corruption ; protection des investisseurs et des consommateurs ; reporting financier et fiscalité ; codes de conduite. Dans le cadre d'un questionnement global sur l'efficacité de la gouvernance, la conformité peut s'appréhender sous l'angle du triptyque « devoir de rendre compte – actions – assurance » décrit dans le *Modèle des Trois Lignes*, et y trouver sa concrétisation.

Conformité : de quoi parle-t-on ?

Entre autres obligations externes, les organisations doivent impérativement mener leurs activités dans le cadre (autrement dit, dans le respect) de la législation en vigueur. Du dialogue social à la fiscalité, ces exigences de conformité couvrent un vaste périmètre. Or, si certains secteurs sont lourdement réglementés et scrutés par des autorités en tout genre, d'autres le sont beaucoup moins. Néanmoins, que ce soit dans le secteur public ou dans le secteur privé, difficile de trouver une organisation qui échappe à toute contrainte externe en matière de conformité.

Parallèlement, les organisations conçoivent et instaurent des attentes internes sous la forme de règles et procédures, et définissent des normes de comportement et de conduite éthique. Dans certains secteurs

[3] Dans le présent document, le terme « management » est employé au sens large pour désigner les rôles qui ne relèvent pas de la responsabilité de l'organe de gouvernance ou de l'audit interne.

réglementés, il s'agit d'ailleurs d'une injonction externe. Devant un tel millefeuille d'exigences, le concept de « conformité » devient protéiforme. Il est donc utile d'envisager cette notion sous tous ses aspects, vastes et interconnectés, mais néanmoins distincts, et de réfléchir au traitement qu'en font les organisations. La conformité peut ainsi être pensée comme un *résultat*, une *catégorie de risque*[4], un *rôle*, une *fonction* ou un *service*[5] de l'organisation, ou encore comme un *ensemble d'activités*.

Examinons ces facettes une par une.

La conformité comme résultat

Les organisations prennent diverses mesures pour appliquer les différents textes de référence, autrement dit, « pour être en conformité ». Dans bien des cas, le respect de certaines attentes et exigences est une condition *sine qua none* de la poursuite des activités et des objectifs stratégiques.

La conformité comme catégorie de risque

Le Cadre de référence international des pratiques professionnelles (CRIPP) définit le risque comme la « *possibilité que se produise un événement qui aura un impact sur la réalisation des objectifs* ». Un impact qui pourra être soit positif, soit négatif. Par conséquent, l'évaluation des risques implique d'examiner non seulement les attentes et exigences en matière de conformité, mais aussi la probabilité d'un manquement et son impact potentiel sur les objectifs.

Dans un cas comme dans l'autre, les organisations sont confrontées à des risques dont l'impact pourra prendre la forme d'un gain ou d'une pénalité, d'ordre matériel ou non. Prenons l'exemple des normes ISO, qui visent entre autres à favoriser l'efficacité opérationnelle. Si une organisation décide de se conformer à ces préconisations facultatives de l'Organisation internationale de normalisation, sa réputation n'en sera que meilleure. Dans le cas contraire, elle ne pourra prétendre à ces effets positifs ; pire, elle risque de se trouver prise en défaut et de se voir infliger des pénalités diverses (amendes, retrait d'agrément, sanctions, mise en liquidation, poursuites civiles ou pénales, perte de financement ou de subventions). Par ailleurs, l'absence de conformité est susceptible de nuire à la réputation de l'organisation en ce qu'elle peut provoquer le mécontentement des parties prenantes ou du public, par exemple.

Pour définir les mesures appropriées (politiques/règles, procédures, limites, contrôles, etc.)[6], il convient d'identifier, de quantifier et d'évaluer le risque de conformité, mais aussi de déterminer les niveaux d'appétence et de tolérance de l'organisation vis-à-vis de ce risque.

---

[4] Sous cette catégorie englobante, on désigne en fait une classification qui subdivise le risque de conformité en risques spécifiques et risques connexes s'agissant de la législation et de la réglementation en vigueur, ainsi que des règles internes et normes de comportement.

[5] La définition de ces rôles peut se faire en fonction de risques spécifiques : responsable des risques de conduite, responsable des risques liés à la protection des données, etc.

[6] Le Committee of Sponsoring Organizations of the Treadway Commission (COSO) édite des référentiels de management des risques et publie des documents de leadership éclairé. On retiendra notamment ses nouvelles lignes directrices portant sur l'application du cadre de référence relatif au management des risques de l'entreprise (ERM) à la gestion des risques de conformité.

La conformité comme rôle ou service de l'organisation

Il n'est pas rare que la conformité désigne un rôle ou un service instauré dans l'optique soit de répondre à des attentes et exigences particulières, soit d'exercer une surveillance, un contrôle, un regard critique, un suivi, de fournir une expertise ou une assurance, ou encore de procéder à des tests dans le domaine de la conformité. Comme détaillé dans le *Modèle des Trois Lignes*, ces missions relèvent de certains rôles de première ou de deuxième ligne, tout en demeurant dans le giron du management ; selon leurs spécificités, ces rôles peuvent d'ailleurs être amenés à fournir un appui spécialisé, notamment en matière de gestion des risques, aux rôles de première ligne et aux cadres dirigeants.

Sous réserve des exigences légales et réglementaires, et en fonction de la taille, de la complexité et du secteur d'activité de l'organisation, un manager délégué à la conformité peut, selon sa fiche de poste, être rattaché à l'une des nombreuses autres fonctions existant au sein de l'organisation : direction exécutive (qu'il s'agisse de la direction générale, de la direction des risques, de la direction opérationnelle, de la direction juridique ou autre) et ses différents échelons hiérarchiques, et/ou rattachement direct à l'organe de gouvernance ou à l'un de ses comités compétents. Dans certains cas, sous réserve des éléments précités et de l'existence d'un mécanisme propre à assurer l'indépendance de la fonction d'audit interne, un poste ou un service de conformité peut être placé sous la responsabilité du responsable de l'audit interne, ou encore de la personne chargée de superviser tant les activités de conformité que celles d'audit interne. Pour évaluer l'adéquation des responsabilités de chaque rôle lié à la conformité avec les attentes et exigences en la matière, il est recommandé d'appliquer les six principes du *Modèle des Trois Lignes*. En application de ce dernier, si l'analyse met en évidence un potentiel conflit d'intérêts ou une perte d'objectivité ou d'indépendance, il convient de prendre des mesures pour remédier à la situation. L'organe de gouvernance doit également être informé pour délibération et prise éventuelle de mesures complémentaires (signalement au régulateur, par exemple, le cas échéant).

La conformité comme ensemble d'activités

La conformité peut désigner les processus et contrôles visant à assurer, soutenir, surveiller, superviser, vérifier, tester, éprouver ou conforter la conformité. Les personnes chargées de l'exécution de ces missions veillent à ce que l'organisation et son personnel se conforment aux attentes et exigences applicables.

Dans l'organisation, la conformité résulte de l'agrégation des actions et des comportements de chaque personne travaillant pour ou avec l'organisation, pour peu qu'ils soient en adéquation avec son rôle et son degré de responsabilité.

La responsabilité des processus, procédures et contrôles de routine dont l'objectif est de satisfaire à un certain niveau d'attentes et d'exigences avec un degré acceptable de certitude peut être dévolue à diverses composantes de l'organisation ; elle peut même être externalisée. Le *Modèle des Trois Lignes* précise que la répartition du pouvoir de décision entre les acteurs impliqués, en matière d'activités de conformité, est un facteur clé pour l'évaluation de l'adéquation (voir en annexe la liste détaillée des rôles et activités concernés).

Le Modèle des Trois Lignes

Conformité

L'organe de gouvernance est l'ultime garant de la gouvernance de l'organisation, laquelle repose autant sur ses actions et comportements que sur ceux du management et de l'audit interne[7].

Si l'organisation assigne les responsabilités relatives à la conformité en fonction de sa situation et en tenant compte d'éventuelles prescriptions externes, elle ne doit pas pour autant négliger d'évaluer l'adéquation du cadre qu'elle aura mis en place au regard des six principes du *Modèle des Trois Lignes*. Cette évaluation pourrait révéler que certaines responsabilités relèvent de l'organe de gouvernance, d'autres du management (notamment la conformité et la gestion des risques), d'autres enfin de l'audit interne.

La fourniture de produits et de services aux clients et la mise à disposition d'un service support conformément aux attentes et exigences sont du ressort de la première ligne. En leur qualité de spécialistes, les rôles de deuxième ligne ont pour tâche de fournir une surveillance et des conseils avertis, d'évaluer les risques (notamment agrégés ou au sein d'un portefeuille) et de piloter la gestion des risques (suivi, surveillance, tests), tout en apportant un contrepoids crédible à la première ligne. L'audit interne, dans son rôle de troisième ligne, est garant d'une assurance indépendante, y compris sur le fait que la deuxième ligne porte bien un regard critique sur les actions de la première ligne. Ces trois lignes doivent se coordonner, communiquer et collaborer pour travailler efficacement et s'assurer que leurs activités se complètent utilement de manière à couvrir tout le spectre des missions, sans se chevaucher ou engendrer conflits et incompatibilités.

Pour ce qui est de la deuxième ligne, le schéma illustrant le *Modèle* ne mentionne aucun rôle ou service de conformité précis, ni aucune fonction ou responsabilité spécifique. Il fait ressortir les liens entre les principaux rôles de gouvernance, sans imposer un quelconque organigramme.

Détermination des responsabilités attribuables aux rôles et activités de conformité

Devoir de rendre compte, actions et assurance sont les ingrédients essentiels de la gouvernance. L'instauration de services spécialisés dans la gestion des risques, la conformité, l'éthique, le développement durable, la sécurité, la protection des données, les questions juridiques, le contrôle de gestion, etc., et la définition de leurs attributions dépendent de nombreux facteurs : complexité de l'organisation, taille, secteur d'activité, ressources, réglementation, législation, culture,

[7] La structure de l'instance de gouvernance varie selon le pays ou le territoire, le cadre réglementaire et la structuration de l'organisation même. Le terme « organe de gouvernance » englobe tout type de structure, quels que soient le pays, le territoire ou le secteur d'activité de l'organisation concernée, qu'elle soit publique ou privée. Entre autres missions qui peuvent lui incomber, l'organe de gouvernance fixe le cap de l'organisation, il définit sa vision, sa mission, ses valeurs et son appétence pour le risque, et enfin, il est destinataire de rapports du management sur les résultats escomptés, prévisionnels et effectifs, ainsi que sur les risques et leur gestion.

appétence/tolérance au risque de l'organe de gouvernance, et surtout, objectifs et responsabilités dévolus aux différents rôles au sein des services spécialisés.

Sauf obligation réglementaire applicable à certains secteurs, les organisations ne sont pas tenues de se doter d'une fonction de conformité à part entière. Et de fait, nombre d'entre elles n'ont ni service ni référent chargé de s'occuper de ces questions.

Cela n n'entrave pas nécessairement l'efficacité de leur gouvernance ni ne les empêche de se conformer aux attentes et exigences qui pèsent sur elles, pour peu qu'elles distribuent les rôles et les responsabilités en matière de conformité de manière cohérente et que chacun endosse le rôle qui lui est réservé.

En règle générale, plus les organisations grossissent, se complexifient, accumulent des ressources ou font l'objet d'une réglementation stricte, plus elles cherchent, de leur propre chef ou sous le coup d'une obligation externe, à attribuer des responsabilités et des ressources spécifiques à des rôles et services distincts pour gérer les diverses formes de conformité.

Par ailleurs, il arrive que plusieurs rôles soient attribués à une même personne. Dans ce cas, il convient d'évaluer le degré de compatibilité entre les différents rôles et de définir précisément les responsabilités qui s'y rattachent, ainsi que la surveillance et l'assurance dont ils feront l'objet. Dans certains cas, il sera nécessaire d'obtenir l'aval de l'organe de gouvernance et du régulateur.

Le cumul des rôles multiplie les risques d'incompatibilité et de conflit d'intérêts, et empêche d'y voir clair pour ce qui est du devoir de rendre compte et de la prise de responsabilité. Afin de ne pas excéder l'appétence de l'organisation pour le risque, il pourra être nécessaire d'agir pour remédier à cette situation, voire d'avertir l'organe de gouvernance et le régulateur.

La conformité, fruit d'un effort collectif

Même lorsque la gestion de la conformité est confiée à un rôle ou à un service donné, il faut admettre que toutes les activités de conformité ne sont pas concentrées en une seule et même main. La conformité est l'affaire de tous, à tous les échelons de l'organisation. La responsabilité et le devoir de rendre compte sont partagés par l'ensemble des rôles et structures hiérarchiques et managériales, dans un souci de garantir la conformité, d'atténuer les risques de cet ordre, et de s'assurer du respect des attentes et des exigences.

La conformité aux attentes et exigences internes comme externes est souvent gérée par des personnes ou des cellules spécialisées en dehors de tout service qui se consacrerait pleinement à cette tâche. Il se peut que leurs rôles et responsabilités respectifs soient étroitement définis par la réglementation sectorielle, par un individu, ou sur la base d'attentes ou d'exigences spécifiques. Par exemple : la conformité aux dispositions législatives et réglementaires en matière de ressources humaines se trouve gérée par les RH, tandis que la conformité aux exigences en matière de reporting financier et de fiscalité relève de la direction financière.

Comme évoqué plus haut, il se peut que les responsabilités liées à la conformité et les missions de surveillance, de suivi et de test qui en découlent soient réparties entre plusieurs services. Il est alors d'autant plus important de faire appel aux six principes pour déterminer les prérogatives et les responsabilités de chaque rôle en matière de conformité.

Gage de transparence, une gouvernance efficace passe par une communication, une coordination et une collaboration aussi bien informelle que formelle. Toutefois, si les échanges informels au sein des structures de gouvernance et de contrôle devaient nuire à l'identification, au signalement et au traitement en bonne et due forme des problématiques de conformité, ils risqueraient de miner l'efficacité des structures formelles de gouvernance et de contrôle et de brouiller les cartes en matière de devoir de rendre compte et de responsabilité.

Pour juger de l'efficacité d'un modèle de gouvernance, il est donc essentiel d'analyser la structure de gouvernance formelle mise en place pour assurer la conformité, mais aussi les canaux informels de communication, de prise de décision et d'action afin d'évaluer si, où et quand le deuxième mécanisme bride le premier. Certes, le *Modèle des Trois Lignes* encourage les échanges tant formels qu'informels, qu'il voit comme des moteurs de communication, de coordination et de collaboration. Toutefois, les structures informelles de gouvernance peuvent conduire à entraver la conformité, à éluder les contrôles – compromettant ainsi l'efficacité de la gestion des risques associés – et à brouiller les pistes en matière de responsabilité et de devoir de rendre compte. En appliquant le *Modèle des Trois Lignes* pour identifier les rôles, les responsabilités et les actions, les organisations sont assurées de mettre en place un cadre de gouvernance efficace, qui passe notamment par l'élaboration de mesures de protection visant à limiter les risques liés aux pratiques de gouvernance, prises de décision et actions informelles, susceptibles d'occasionner des manquements en matière de conformité.

Mettre en place un programme de conformité efficace, ce n'est pas seulement favoriser l'adoption et le respect d'une structure de gouvernance et de contrôle à la fois formelle et documentée, c'est aussi se donner les moyens d'instaurer et de diffuser une culture de la conformité et du contrôle, pour une efficacité accrue du *Modèle des Trois Lignes*.

Application des six principes

Le *Modèle des Trois Lignes* promeut une démarche d'évaluation et d'alignement des rôles et responsabilités bâtie sur des principes, démarche qui tient compte de la situation de l'organisation et en particulier des attentes et exigences qui lui sont propres en matière de conformité. Les six principes qui composent ce *Modèle* servent à mieux cerner la notion de conformité (comme résultat, comme catégorie de risque, comme rôle ou service, et comme ensemble d'activités) ainsi que son apport au cadre de gouvernance (voir le *Modèle des Trois Lignes* pour prendre connaissance de ces principes dans leur intégralité).

Principe n° 1 : Fixer des exigences de gouvernance

Le premier principe décrit les exigences minimales de gouvernance des différents acteurs comme suit :

- Organe de gouvernance : devoir de rendre compte, vis-à-vis des parties prenantes, sur l'atteinte de l'objet de l'organisation ;
- Management : pilotage d'actions (y compris en matière de gestion des risques et de conformité) pour réaliser les objectifs de l'organisation, grâce aux ressources à disposition ;
- Fonction d'audit interne indépendante : fourniture d'une assurance et de conseils dans tous les domaines afin de garantir la transparence et une surveillance efficace, et de favoriser la confiance et l'amélioration continue.

L'organe de gouvernance est l'ultime garant du respect des normes sociales et des standards généralement admis. Le management doit gérer les risques de conformité ou de non-conformité sans perdre de vue le niveau d'appétence pour le risque fixé par l'organe de gouvernance. Cela peut impliquer de créer des rôles individuels ou de monter des équipes entières chargées de traiter certains aspects de la conformité, mais aussi de définir précisément les prérogatives en matière de prise de décision entre la première ligne, responsable des risques, et la deuxième ligne, qui interroge les choix de la première ligne et la pousse à toujours tenir compte de l'appétence de l'organisation pour le risque. L'audit interne apporte au management et à l'organe de gouvernance une assurance sur l'adéquation et l'efficacité des dispositifs de contrôle à des fins de conformité et leur prodigue des conseils dans une optique d'innovation et d'amélioration continue.

Exemples concrets

> **La santé est un secteur fortement réglementé, et de ce fait, la prestation de service est presque toujours très strictement encadrée. Les professionnels de la santé ont l'obligation de veiller à ce que chaque acte soit dûment autorisé et documenté. Les personnes ou services chargés de la conformité informent les services cliniques de la nécessité liée à l'autorisation et à la documentation d'une procédure donnée mais, en fin de compte, c'est aux soignants, en première ligne, qu'il revient de mettre en œuvre les processus, de procéder aux contrôles appropriés et de garantir le respect des exigences.**
>
> – Responsable de la conformité et de l'audit interne, États-Unis

> **Dans mon secteur, on classe les principaux risques de conformité de l'organisation et l'on**

répertorie les exigences réglementaires majeures, puis on ajuste les activités, les dispositifs de contrôle et de suivi, et les responsabilités de façon à répondre à ces exigences d'une manière qui soit proportionnée aux risques identifiés. Par exemple, une organisation peut nommer un responsable anti-blanchiment, un responsable de la protection des données, un responsable anti-corruption ou autre pour satisfaire aux exigences réglementaires. Elle peut aussi attribuer des responsabilités (quant aux produits, aux informations à déclarer, au recrutement, à la gestion des réclamations, etc.) et se doter de ressources visant à garantir la conformité et la gestion de ces grands domaines de risque. Des rapports réguliers sont adressés à l'organe de gouvernance, et toutes les activités font l'objet d'un audit interne indépendant.

– Responsable de la conformité, Royaume-Uni

La course à l'adoption de normes environnementales, sociales et de gouvernance (ESG) illustre bien les défis auxquels font face les organisations aujourd'hui. L'organe de gouvernance doit demander au management de lui rendre des comptes quant à la bonne application de la stratégie, des normes sociales et des standards édictés par ses soins. Dans la mesure où les enjeux ESG touchent tous les recoins de l'organisation et l'ensemble de ses parties prenantes (collaborateurs, fournisseurs, clients), l'organe de gouvernance doit veiller à ce que le management articule correctement les risques ESG menaçant l'organisation avec le cadre réglementaire et législatif et avec les règles et procédures internes (sans oublier les indicateurs de performance y afférents, et des données fiables, authentiques et comparables témoignant du respect de ces attentes et exigences internes). De plus, le management comme l'organe de gouvernance voudront avoir ou auront besoin d'une assurance quant à la réalisation des objectifs de conformité en matière ESG. Il conviendra de réaliser une cartographie détaillée des responsabilités et devoirs de rendre compte au sein de l'organisation pour bien identifier les rôles et services concernés et les activités menées pour satisfaire aux exigences ESG.

– Responsable de la conformité, États-Unis

Principe n° 2 : Assurer une surveillance adéquate de la gouvernance

Le deuxième principe définit les rôles de l'organe de gouvernance relatifs à :

- la gouvernance,
- la supervision du management,
- l'institution d'une fonction d'audit interne et la supervision de son efficacité.

L'organe de gouvernance est l'ultime garant de la gouvernance de l'organisation et, à ce titre, il s'assure que les structures et processus adéquats sont en place – y compris un cadre de conformité et de supervision du rôle de l'audit interne.

L'organe de gouvernance doit déterminer le degré de confiance qu'il exige, ainsi que celui qu'il accorde au respect des attentes et exigences visant le niveau d'exposition au risque et l'impact potentiel de ce dernier sur les objectifs stratégiques. Pour fixer le niveau de tolérance ou d'appétence pour le risque de conformité, il devra superviser la capacité du management à mener ses activités et la faculté des rôles et services concernés à s'acquitter de leurs responsabilités en matière de conformité.

L'organe de gouvernance devrait par ailleurs s'assurer que l'audit interne est convenablement positionné

et outillé pour fournir une assurance et des conseils indépendants et efficaces au sujet de la conformité. Pour asseoir son autorité et son indépendance, le responsable de l'audit interne doit rendre compte à l'organe de gouvernance, à un comité d'audit indépendant, ou à tout comité équivalent rattaché à l'organe de gouvernance.

Exemples concrets

Un organe de gouvernance opérant est capable de faire advenir le changement et de se faire entendre dans toute l'organisation. Dans certains cas, les signalements et les rapports à l'organe de gouvernance sont certes systématiques, mais la rapidité et l'efficacité de sa supervision et de son pilotage dépendront de la fraîcheur et de la qualité de l'information qui lui est communiquée, le risque étant toujours d'agir avec retard, sur la base de renseignements dépassés. L'audit interne devrait s'assurer que l'organe de gouvernance a une bonne visibilité des risques gérés par l'organisation, et qu'il est ainsi en mesure d'anticiper, de superviser et de guider la gestion de ces risques. La fonction Conformité joue un rôle de deuxième ligne important : elle demande au management de démontrer l'efficacité de ses mesures de conformité et de contrôle, et elle fournit à l'organe de gouvernance des éclairages sur l'efficacité de la gestion des risques de conformité, dans le respect de l'appétence pour le risque.

– Responsable de la conformité, Singapour

Dans la santé comme dans bien d'autres secteurs, le service de conformité peut se retrouver chargé de la gestion quotidienne de certains éléments du programme de conformité (organisation de formations, suivi de la *hotline*, promulgation du code de déontologie, vérification d'antécédents, etc.). Si certaines de ces activités ont pour objet la mise en œuvre de la conformité, d'autres portent plutôt sur la fixation de règles, le suivi de la conformité et de son efficacité, et la production de rapports destinés au management et à l'organe de gouvernance. Mais attention, si le service de conformité est rattaché au responsable de l'audit interne, la fonction d'audit interne ne pourra fournir une assurance indépendante quant à l'efficacité du programme de conformité. Dans ce cas, il est possible de mandater un tiers indépendant qui remplira ce rôle auprès de l'organe de gouvernance.

– Responsable de la conformité et de l'audit interne, États-Unis

L'organe de gouvernance doit : i) veiller à ce que les risques de conformité soient pleinement évalués/englobés dans le plan d'audit interne, ii) appréhender le périmètre pluriannuel de l'audit interne en tenant compte des principaux risques d'ordre réglementaire et des priorités du régulateur, et iii) passer en revue les résultats des activités/rapports de conformité.

– Responsable de l'audit interne, Royaume-Uni

En matière de gestion des risques de conformité, l'organe de gouvernance donne le *la* au management et à l'audit interne. Pour s'acquitter pleinement de son devoir de supervision, il doit donc pouvoir amplement examiner, de manière aussi fréquente que régulière, des données quantitatives et qualitatives transmises par ces deux interlocuteurs et reflétant l'état de la conformité dans l'organisation. L'organe de gouvernance doit inscrire à son ordre du jour un point récurrent sur l'ensemble des activités de gestion des risques de conformité afin d'en adopter une vision prospective, et non une simple vue rétrospective centrée sur les manquements, les failles et les mesures prises pour y remédier.

– Responsable de la conformité, Royaume-Uni

Principe n° 3 : Définir les rôles du management au sein des première et deuxième lignes

Le troisième principe détaille les rôles du management (situés tant au sein de la première que de la deuxième ligne, ces rôles peuvent être fusionnés ou séparés selon les ressources à disposition, les objectifs poursuivis, la réglementation, etc.).

Le management englobe les rôles de première et de deuxième ligne. La première ligne est chargée de fournir des produits et/ou services aux clients. La deuxième ligne, elle, a pour fonction d'apporter un œil expert, d'évaluer les risques (notamment agrégés ou au sein d'un portefeuille) et de piloter la gestion des risques, tout en formulant des critiques constructives à l'égard de la première ligne.

Il est possible de créer un service à part entière, comme une fonction Conformité, ou de nommer un chef de service (dans des organisations plus petites et moins complexes, il s'agira d'un poste isolé qui fera office de référent) rattaché soit directement à l'organe de gouvernance, soit indirectement *via* l'un de ses comités. En parallèle, ledit chef de service ou référent pourra aussi être subordonné au directeur général (CEO) ou à tout autre membre désigné du management. Un rattachement ou une obligation de rendre compte à l'organe de gouvernance peut conférer une plus grande indépendance à cette personne. Cependant, il ne faut pas oublier que l'indépendance se caractérise entre autres par l'absence de prise de décision. Or, toute personne dans un rôle de conformité détient un certain degré de responsabilité en matière de décisions de gestion (du choix de faire affaire avec un client à l'approbation de nouveaux produits, en passant par l'autorisation d'une exception à la règle, etc.). Ainsi, le fait d'être rattaché à l'organe de gouvernance ou à l'un de ses comités ne saurait garantir une indépendance parfaite. La fonction d'audit interne et son responsable, outre le fait qu'ils sont hiérarchiquement indépendants du management, ne prennent aucune décision opérationnelle de gestion, ce qui renforce leur degré d'indépendance.

Voici donc un descriptif succinct des rôles des différentes lignes :

- Rôles de première ligne : ces rôles fournissent des produits et services de manière conforme à la législation et la réglementation, aux codes de conduite, aux règles de l'organisation, etc. Le management demeure responsable de la conformité.
- Rôles de deuxième ligne : le référent ou le service chargé de la conformité pose un cadre, exerce une supervision, fournit des conseils, un suivi et une surveillance, entreprend des tests, formule des critiques constructives au management, et dispose généralement d'un pouvoir opérationnel de décision et de gestion des risques (choix de faire affaire avec un client, approbation de nouveaux produits ou services, validation des transactions, autorisation d'un dépassement ou d'une exception à la règle, etc.).
- Rôles de troisième ligne : l'audit interne apporte de manière unilatérale une assurance indépendante quant à la conformité, à l'efficacité des efforts du management en la matière, et aux missions du référent ou du service Conformité en matière de suivi de cette question et de surveillance/contrôle de la gestion des risques y afférents. L'audit interne n'a aucun pouvoir de décision de gestion et rend compte de manière indépendante à l'organe de gouvernance.

Grâce au *Modèle des Trois Lignes*, l'organisation est en mesure de se conformer aux attentes et exigences, de contribuer à une gouvernance efficace et durable, et de lutter contre les agissements illicites et la corruption. La conformité doit être fondée sur la transparence, afin de placer la barre à un niveau

convenable dans l'organisation. En outre, un programme de conformité efficace et vecteur de transparence est propre à inspirer confiance aux parties prenantes externes (actionnaires, administrations publiques, autorités de régulation et places boursières, fournisseurs et chaîne d'approvisionnement).

Exemples concrets

Les rôles de première et deuxième ligne doivent collaborer efficacement en vue d'identifier les risques de conformité qui pèsent sur l'organisation, de les gérer et de piloter leur atténuation. Ils ne doivent en aucun cas se défausser sur l'audit interne. Les tâches de suivi, de test et de contrôle sont et demeurent de leur ressort.

– Responsable administratif, États-Unis

Les responsables de la conformité doivent épauler l'organisation en s'assurant que les processus et les contrôles sont bien alignés. Ces rôles de deuxième ligne sont amenés à lui fournir des conseils en diverses occasions. À ce titre, les indicateurs clés de performance et de risques sont utiles pour aider l'organisation à identifier et gérer les risques liés à l'efficacité des contrôles.

– Responsable de la conformité, Mexique

De nombreux secteurs sont régis par une myriade de règlements complexes. Lorsque des exigences ou des évolutions réglementaires touchent une fonction, quelle qu'elle soit, le service Conformité peut apporter expertise et conseils. Par exemple, dans la santé, le management des différents services cliniques a pour tâche de concevoir et de mettre en œuvre les contrôles visant à garantir la conformité. Du fait de son expertise, le service Conformité est bien placé pour évaluer le respect des exigences.

– Responsable de la conformité, États-Unis

L'assimilation des responsabilités et des obligations relatives aux attentes et exigences en matière de conformité, ainsi que leur bonne exécution par le référent ou le service chargé de cette question, sont un enjeu crucial, que les grandes entreprises arrivent à bien gérer. Pour cela, il est nécessaire d'établir un cadre très clair de contrôle et de gestion des risques, de bien définir les rôles, responsabilités et rattachements hiérarchiques, et d'aménager des circuits de remontée d'information *via* un mécanisme de gouvernance solide. À défaut, la supervision de la conformité devient un exercice confus et difficile à réaliser.

– Responsable de la conformité, Royaume-Uni

La conformité est l'affaire de tous. Dans les secteurs fortement réglementés, comme la santé, cette responsabilité incombe à chaque soignant et peut l'obliger à observer des consignes d'autorisation et de documentation pour telle ou telle procédure. Si c'est au service de conformité qu'il revient d'élaborer les règles, processus et contrôles applicables aux différentes procédures, ou d'assumer la responsabilité desdites procédures, il ne sera pas en mesure de fournir une assurance objective. En revanche, s'il est en position de conseil vis-à-vis des exigences réglementaires associées à une procédure, son objectivité ne s'en trouvera pas nécessairement entamée.

– Responsable de la conformité et de l'audit interne, États-Unis

Principe n° 4 : Définir le rôle de la troisième ligne

Selon le quatrième principe, l'audit interne a pour rôle de fournir une assurance et des conseils indépendants.

Le *Modèle des Trois Lignes* insiste sur ce qu'il définit comme une composante fondamentale de la gouvernance : le besoin d'assurance quant à l'adéquation et l'efficacité des modalités de traitement des risques et des dispositifs de contrôle, y compris relatifs à la conformité (atteinte, suivi, supervision) et à la gestion des risques associés. Cet impératif est du ressort de l'audit interne, seule composante de l'organisation en capacité de fournir une assurance indépendante du management, dans la mesure où il applique avec compétence des processus systématiques et rigoureux, et où il peut apporter expertise et éclairages.

La fonction de conformité et la fonction d'audit interne peuvent trouver le moyen de travailler main dans la main au service de l'organisation tout en restant efficaces dans leur rôle respectif.

Compte tenu de la structuration des différents rôles et devoirs de rendre compte au sein de l'organisation, il n'est pas impossible de trouver d'autres sources d'assurance qui, une fois agrégées, peuvent venir enrichir la vision interne. Toutefois, il est important d'analyser et d'évaluer ces différents rôles et leur alignement par rapport au *Modèle des Trois Lignes* afin de jauger la qualité et l'objectivité des sources en question.

L'audit interne rend compte en premier lieu à l'organe de gouvernance et préserve son indépendance vis-à-vis du management. Cette disposition est essentielle pour comprendre les rôles d'assurance et la position particulière qu'occupe l'audit interne au sein de la structure de gouvernance. Si l'indépendance et l'objectivité de la fonction se trouvent menacées, le responsable de l'audit interne doit en informer l'organe de gouvernance pour qu'il prenne des mesures correctives.

Pour appliquer le *Modèle des Trois Lignes* comme il se doit, les auditeurs internes doivent, lorsqu'ils évaluent l'efficacité des rôles et services de conformité, se montrer ouverts à la communication, à la coordination et à la collaboration, et promouvoir une culture de la conformité et du contrôle.

Exemples concrets

> **Lorsque l'on évalue la gestion du risque de conformité, il est essentiel de s'attarder sur l'efficacité des mesures d'atténuation. Il est important de conduire une solide évaluation des différents risques liés à la conformité et de s'interroger sur l'adéquation des activités menées pour les atténuer. Sinon, on risque de dépenser beaucoup d'énergie sans pour autant parvenir à prémunir l'organisation contre les risques de non-conformité.**
>
> – Responsable de l'audit interne, Afrique du Sud

> **Pour les auditeurs internes, il est particulièrement difficile de faire apparaître explicitement dans leurs travaux et leurs rapports d'audit les différents cas de non-conformité (violations de la législation ou réglementation en vigueur, ou encore non-respect des règles, normes ou codes de conduite). Une telle assurance nécessite d'avoir accès à des ressources suffisamment qualifiées pour évaluer efficacement et consigner dans un rapport les efforts visant à atteindre le résultat**

souhaité en matière de conformité.

– Responsable de l'audit interne, Royaume-Uni

Principe n° 5 : Préserver l'indépendance de la troisième ligne

Le cinquième principe souligne l'importance de l'indépendance de l'audit interne.

En tant que rôle de troisième ligne, l'audit interne a plusieurs particularités qui concourent à en faire une fonction indépendante : sur le plan fonctionnel, elle est indépendamment rattachée à l'organe de gouvernance ou à l'un de ses comités, et surtout, elle ne prend aucune décision de gestion.

Si elles sont souvent rattachées à l'organe de gouvernance ou à l'un de ses comités, les fonctions de gestion des risques (de conformité notamment) ont généralement dans leurs attributions un pouvoir de prise de décision de gestion, notamment en ce qui concerne la prise de risque et la reddition de comptes, ainsi que dans la gestion de ces risques, leur atténuation et leur contrôle.

La deuxième ligne peut conserver le droit de formuler des critiques utiles et constructives à l'égard de la première ligne. Cependant, l'indépendance de l'audit interne vis-à-vis de la prise de décision de gestion est un marqueur fort qui distingue la troisième ligne des deux autres, comme expliqué dans le troisième principe.

Exemples concrets

Pour éviter de se retrouver tiraillés, les auditeurs internes ne doivent pas avoir conçu ou exécuté des dispositifs de contrôle, ni pris part à des décisions de gestion. Leur rôle est d'observer, de tester et d'évaluer si les risques clés ont été identifiés et maîtrisés comme prévu. Ils ne doivent avoir ni biais ni préjugés.

– Responsable de l'audit interne, Australie

L'organe de gouvernance est le principal interlocuteur de la fonction d'audit interne ; étant donné son indépendance au sein de l'organisation, celle-ci n'a pas besoin de prendre des gants pour lui communiquer résultats et recommandations. Elle n'est en aucun cas tenue de montrer les mécanismes de contrôle et les personnes chargées de leur exécution sous un jour favorable. Son rôle ultime est de dépeindre la réalité sans fard.

– Responsable de l'audit et de la conformité, États-Unis

Les rôles de deuxième ligne chargés de la conformité fixent les règles, conseillent l'entreprise au sujet de la conception des dispositifs de contrôle, lui fournissent conseils et avis sur son appétence pour le risque, et lui apportent une assurance. Les référents ou services de conformité peuvent se voir déléguer des fonctions opérationnelles relevant de la première ligne. Dans ce cas, leur indépendance n'est plus assurée. L'audit interne est la seule fonction pleinement indépendante dans la mesure où elle se tient éloignée de la prise de décision qui caractérise les première et deuxième lignes.

– Responsable de la gestion des risques de l'entreprise et de l'audit interne, États-Unis

Principe n° 6 : Créer et protéger la valeur grâce à la collaboration

Le sixième et dernier principe rappelle l'importance de la coordination et de la collaboration entre tous ces rôles.

Une gouvernance efficace repose non seulement sur une affectation adéquate des responsabilités, mais aussi sur l'harmonie entre les différentes fonctions, rendue possible par la coordination, la collaboration et la communication. L'organe de gouvernance s'appuie sur les rapports du management et de l'audit interne, entre autres, pour exercer sa mission de supervision et aiguiller le management dans la réalisation des objectifs, la gestion des risques et la création de valeur. Ensemble, tous ces rôles (organe de gouvernance, première, deuxième et troisième lignes) contribuent à la création et à la protection de valeur, dès lors qu'ils sont en phase les uns avec les autres ainsi qu'avec les intérêts prioritaires des parties prenantes. Par conséquent, la communication claire des responsabilités en matière de conformité, les pouvoirs décisionnels, les obligations de reporting, l'appétence pour le risque, les classifications communes, la bonne définition des unités ou entités chargées de l'évaluation, le reporting de la performance et des risques au regard des attentes et exigences, ainsi que les programmes de test et d'assurance sont autant d'éléments propres à améliorer la coordination et la collaboration.

Exemples concrets

La protection des données est un bon exemple de coordination et de collaboration. Seule ou en concertation avec le service juridique, selon les organisations, la fonction Conformité identifie les exigences réglementaires, les fait connaître à l'organisation et veille à la mise en œuvre de processus et de contrôles appropriés. Les équipes opérationnelles (opérations, systèmes d'information, sécurité des données, etc.) se chargent d'exécuter les activités, y compris si besoin celles de suivi, de signalement et de reporting. La cellule chargée de la sécurité des données et les équipes de conformité mettent en place un suivi dans les principaux domaines de risque afin de s'assurer que les équipes opérationnelles suivent bien les procédures, et qu'elles s'acquittent convenablement de leurs tâches de surveillance et de reporting. Lors de l'audit des différentes fonctions, l'audit interne évalue le cadre de gestion des risques applicables (y compris de conformité) ainsi que les processus et contrôles mis en place par les équipes opérationnelles.

– Responsable de la conformité, Royaume-Uni

Les enjeux ESG sont un excellent exemple de coordination et de collaboration à l'échelle de l'organisation au regard de la mise en conformité par rapport aux attentes et exigences. Pour atteindre leurs objectifs en matière d'ESG, les première, deuxième et troisième lignes doivent travailler ensemble, sous l'égide de l'organe de gouvernance, tout en restant chacune dans leur rôle. Dans cette optique, les différents rôles et fonctions chargés de la conformité seront amenés à s'associer à d'autres services internes :

- **L'organe de gouvernance a pour mission de fixer la stratégie et l'appétence pour le risque, et de donner le *la* en matière de culture et de comportement.**
- **Le management intègre les attentes et exigences ESG dans la gouvernance et les activités de l'organisation.**
  - **Il fournit des conseils, un cadre et des exigences relatives au contenu, à la conception et à la mise en œuvre des structures, systèmes et processus utiles à la planification stratégique**

et opérationnelle, à la fixation d'objectifs, à la collecte de données, à la prise de décision et au reporting dans le domaine ESG.

- **Il évalue les risques associés à la mise en conformité avec les normes et exigences ESG externes, ainsi qu'avec les règles et objectifs internes.**
- **Il élabore les normes, cadres, principes ou modèles qu'il conviendra d'adopter pour la mesure, le suivi et le reporting des impacts liés à la mise en conformité ESG.**
- **Il évalue l'exactitude et la cohérence des informations et des méthodes employées pour collecter les données utilisées dans le cadre du reporting sur le développement durable et les enjeux ESG.**
- **Il fixe les modalités et les processus d'évaluation, définit le seuil de matérialité, liste les indicateurs pertinents (KPI) et met en place des méthodes, des lignes directrices et des outils (internes comme externes) aux fins du reporting.**

- **L'audit interne fournit une assurance indépendante à l'organe de gouvernance sur les activités susmentionnées et sur l'atteinte des objectifs ESG par le management, ainsi qu'au management sur la conformité au regard des attentes et des exigences applicables.**

– Responsable de la conformité, Royaume-Uni

La conformité en quelques points

Dix enseignements à retenir

1. La responsabilité de la conformité n'est pas nécessairement endossée par un référent, un service ou un manager donné. Certaines organisations n'ont pas la capacité ou n'éprouvent pas le besoin de se structurer ainsi. Souvent, c'est lorsqu'elles grandissent, se complexifient, se retrouvent soumises à une réglementation plus stricte ou plus pointue, fassent l'objet d'une attention accrue, commencent à opérer dans des environnements en mutation rapide (sur le plan réglementaire, commercial ou autre) ou à intégrer des enjeux similaires qu'elles décident d'affecter des personnes, des équipes, des systèmes et/ou d'autres ressources à la conformité et de lui ménager une place spécifique dans leur organigramme. Dans certaines organisations, il peut s'agir de ressources externes (par exemple, via l'externalisation de certaines expertises ou tâches de suivi de la conformité).

2. Lorsque l'on applique les six principes du *Modèle des Trois Lignes* pour évaluer les rôles liés à la conformité, il est utile de se rappeler les résultats que chaque rôle doit viser :

- Respect de la législation et de la réglementation, des dispositions contractuelles, des règles, procédures, codes de conduite ou autres exigences dans la fourniture de produits et de services.
- Apport d'un œil expert, évaluation des risques (notamment agrégés ou au sein d'un portefeuille), pilotage de la gestion des risques et formulation de critiques constructives à l'égard de la première ligne afin de promouvoir la mise en conformité de l'organisation avec les codes et normes de conduite, exigences et attentes applicables.
- Évaluation de l'adéquation et de l'efficacité du programme de conformité.

- Formulation de critiques éclairées sur l'efficacité du programme de conformité et de ses composantes au sein de l'organisation.

3. Toutes les questions liées à la conformité ne sont pas nécessairement traitées par un seul rôle ou service au sein de l'organisation[8]. Dans certains cas, cette dernière doit définir par écrit le périmètre des rôles ou services de conformité, et préciser les rôles chargés de garantir le respect d'autres attentes et exigences. Cela est tout aussi important pour les petites structures (dans lesquelles une même personne peut se voir attribuer des responsabilités de plusieurs types et où certaines responsabilités peuvent être externalisées) que pour les grandes organisations, où plusieurs rôles ou services peuvent se partager les différentes tâches de conformité.

4. Le référent ou le chef du service Conformité peut, en pratique et sous réserve des dispositions légales et réglementaires en vigueur, être rattaché à l'un des postes suivants dans l'organisation : direction exécutive (direction générale, direction des risques, direction opérationnelle, direction juridique, ou autre) et/ou organe de gouvernance ou l'un de ses comités. Dans certains cas, la fonction Conformité, peut, même si elle fait partie du management, être rattachée au responsable de l'audit interne. L'adéquation de ces rattachements peut être évaluée en partie en procédant à l'examen des responsabilités suivant le *Modèle des Trois Lignes* et les exigences légales et réglementaires applicables.

5. Le référent ou le chef du service Conformité peut être rattaché ou rendre compte à un ou plusieurs comités de l'organe de gouvernance ou aux personnes qui se trouvent à leur tête. Néanmoins, cela n'empêche pas la fonction Conformité de rester dépendante du management et n'exclut pas la nécessité d'une assurance indépendante fournie par l'audit interne.

6. Les responsabilités d'un référent individuel ou d'un service Conformité sont les suivantes (liste non exhaustive) : gestion globale du risque de conformité, suivi ou pilotage, tests, analyse, évaluation, conseil, assurance, fixation de règles, élaboration et mise en œuvre de systèmes et de dispositifs de contrôle, décisions de gestion, supervision et formation.

7. Les rôles et services de conformité peuvent également endosser des responsabilités étroitement ou directement liées à la fourniture de produits et services. Il est alors nécessaire de documenter clairement leurs responsabilités, leurs prérogatives et leur devoir de rendre compte (par exemple, la capacité à empêcher une non-conformité en interdisant une opération ou en bloquant une décision de gestion).

8. Il est recommandé de séparer la première et la deuxième ligne. La première ligne doit être comptable des risques qu'elle prend. La deuxième ligne doit de son côté établir et superviser le cadre et les standards destinés à aider la première ligne dans l'accomplissement de sa mission, et formuler des critiques constructives à son égard. En pratique, en fonction des exigences locales ou sectorielles, et selon la taille et la complexité de l'organisation, entre autres facteurs, ces rôles peuvent se trouver fusionnés. Dans ce cas, il convient d'en évaluer la compatibilité et d'atténuer les risques associés, éventuellement en ajustant la composition des rôles. La gestion des risques demeure l'apanage des rôles de première ligne et s'inscrit dans le périmètre d'action du management.

[8] La déontologie, le développement durable, le reporting financier, la protection des données, les ressources humaines et les obligations juridiques sont autant de sujets dont des ressources propres (en interne ou en externe) sont chargées d'assurer la conformité, ou la supervision et la gestion des risques (lesquelles peuvent porter sur des aspects spécifiques). À titre d'exemple, l'évolution des enjeux environnementaux, sociaux et de gouvernance (ESG) voit fleurir dans les organisations toute une série de nouveaux rôles, responsabilités, activités et services, dont le but est d'assurer la conformité à ces critères étendus.

9. Quelle que soit la manière dont l'organisation structure ses ressources chargées d'assurer le respect des obligations de conformité, c'est au management qu'il incombe de veiller à ce qu'elle satisfasse aux attentes et exigences qui lui sont propres, dans les limites de l'appétence pour le risque fixée par l'organe de gouvernance.

10. L'évaluation de l'efficacité du programme de conformité de l'organisation et des efforts requis pour se conformer aux attentes et exigences applicables est une responsabilité essentielle du rôle de conformité relevant de la deuxième ligne.

ANNEXE : Mise en cohérence des responsabilités attribuables aux rôles et activités de conformité

Les activités de conformité sont une composante essentielle de la gouvernance de l'organisation, de sa gestion des risques et de ses activités de contrôle interne. La responsabilité des actions nécessaires pour atteindre la conformité, la promouvoir, la vérifier et l'attester, de même que l'exécution de ces responsabilités, peut échoir à différents pans de l'organisation. Les personnes chargées des activités de conformité doivent définir les résultats escomptés en la matière et fixer les mesures appropriées pour en démontrer l'atteinte.

Voici une liste (non exhaustive) d'activités touchant à la conformité :

- Identification des lois et réglementations externes applicables, ainsi que des règles et politiques internes, standards, procédures, codes de conduite et normes de comportement en phase avec les objectifs de l'organisation.
- Détermination des critères de mesure du risque de conformité ou de non-conformité aux éléments précités.
- Évaluation des risques de conformité aux éléments précités, y compris risques à venir ou émergents.
- Conception, élaboration et mise en œuvre de processus et de dispositifs de contrôle pour la mise en conformité aux éléments précités.
- Exécution, tenue et gestion des processus et des dispositifs de contrôle pour la mise en conformité aux éléments précités.
- Évaluation, test et suivi de la mise en conformité aux éléments précités.
- Formulation de critiques constructives à l'égard du management concernant les risques de conformité.
- Gestion et maîtrise des risques de conformité.
- Identification des cas de conformité ou de non-conformité.
- Communication et signalement des cas de non-conformité.
- Production de rapports de conformité ou de non-conformité suivant les exigences internes et externes.
- Promotion d'une culture de la conformité.
- Sensibilisation au sujet via des actions de communication, de formation et de promotion.

- Fourniture de conseils sur les différents aspects de la conformité.
- Mise en place ou maintien d'un programme de déontologie ou d'un système d'alerte.
- Conception et mise en œuvre d'actions de formation et de sensibilisation à la conformité.
- Rôle d'interface entre les autorités de régulation et l'organisation.
- Établissement et entretien de relations avec les organisations professionnelles et les organismes sectoriels afin d'identifier les normes, codes ou lignes directrices applicables auxquels l'organisation et ses différentes fonctions devraient se conformer ou pourraient choisir d'adhérer, mais aussi pour faciliter la collecte et la communication d'informations à des fins de comparaison.
- Établissement et entretien de liens avec les organisations-cadres du secteur, qui peuvent décider de fixer des attentes ou des exigences concernant leurs infrastructures et exiger des utilisateurs et de leurs contreparties qu'ils s'y conforment.

Il est important que les responsabilités de chaque rôle et les résultats escomptés soient bien clairs. Certains de ces rôles et activités sont incompatibles avec d'autres, comme l'autorisation de transactions, le choix de faire affaire avec un client, ou d'autres décisions opérationnelles comportant des risques, dans le périmètre de la troisième ligne, comme détaillé dans le *Modèle des Trois Lignes*. Pour que l'audit interne puisse assumer de tels rôles, il est nécessaire de mettre en place des mesures de protection, telles que l'obtention de l'aval de l'organe de gouvernance ou du comité d'audit, le recours à un tiers pour la fourniture d'une assurance indépendante dans les domaines concernés, et, si besoin, la sollicitation de l'autorisation du régulateur.

Pareillement, même si elle est animée des meilleures intentions en matière de conformité dans le cadre de la fourniture de ses produits et services aux clients, l'organisation doit s'attacher à identifier les rôles compétents, lesquels seront non seulement chargés de prêter attention à la conformité, mais aussi de veiller à la surveillance et la gestion au sens large des risques de cet ordre. Les principes fondamentaux que sont la séparation des tâches et l'indépendance s'appliquent, de même que l'obligation de maîtriser les risques découlant d'une incompatibilité identifiée entre les rôles.

De même, lorsqu'elles identifient des lacunes ou des défaillances dans les activités de contrôle et de gestion des risques liés à la fourniture de produits ou de services, les personnes en position de supervision sont parfois tentées d'outrepasser leurs prérogatives et d'intervenir directement. L'inverse peut également être vrai, lorsque la première ligne se fie trop aveuglément aux rôles chargés d'assurer la supervision ou la gestion des risques. Une telle attitude la prive des bénéfices d'une supervision objective. Dans ce cas, il appartient au rôle de supervision d'identifier, de faire remonter et de suivre les lacunes ou les défaillances constatées, ainsi que les mesures prises par le management pour y remédier. Ces éléments doivent être mis en cohérence et documentés conformément aux rôles et responsabilités de gouvernance fixés.

The Institute of
Internal Auditors

theiia.org