MAÎTRISER LES RISQUES DES TIERS

Adopter une gestion des risques efficace avec les Tiers

ifaci
institut français de l'audit et du contrôle internes

GROUPE DE TRAVAIL
MAÎTRISER LES TIERS

INTRODUCTION

Les fiches de ce guide pratique portent sur la méthodologie applicable pour chaque composante du processus de gestion des risques dans le cadre de la maîtrise des Tiers, ie. la gouvernance des Tiers, la veille relative aux Tiers, la connaissance des Tiers et des risques inhérents et le pilotage opérationnel.

Ce guide a vocation à partager la connaissance opérationnelle et les bonnes pratiques à mettre en place sur un sujet très prégnant dans les entreprises de toute nature. Par « Tiers », nous entendons le recours à un prestataire pour effectuer une tâche incombant à l'Entreprise. Cette dernière demeure ultimement responsable du risque, il ne peut jamais être transféré au mandataire. La nécessité d'encadrer les travaux réalisés par le Tiers pour compte de l'Entreprise est essentielle. De plus, le risque inhérent à l'externalisation est à considérer dans le cadre de la gestion des risques de l'Entreprise.

Successivement seront abordés :

- La **gouvernance des Tiers**: elle est le lien entre la stratégie arrêtée, la politique décidée relative aux Tiers et le niveau de tolérance au risque souhaité. L'organisation subséquente à mettre en place afin de traduire au plan opérationnel les risques, définir les bons niveaux de reporting sur la base des tableaux de bord convenus sont des éléments à déterminer. La communication sera ajustée à la comitologie prévalente au sein de l'Entreprise,
- La **veille relative aux Tiers** : elle doit permettre de se tenir informé en priorité des évolutions juridiques, réglementaires, sociétales, éthiques etc. dans l'objectif de protéger l'Entreprise et, au besoin, de rentrer en conformité rapidement. Elle fera l'objet d'une communication, d'un échange et d'une décision aussi des comités ad-hoc en vue de maintenir un bon niveau de gouvernance,
- La **connaissance des Tiers et des risques inhérents** : elle répond aux obligations imposées par la conformité s'agissant de la connaissance des intermédiaires. Cette dernière permet d'identifier, de mesurer et d'accepter le risque inhérent au Tiers mais aussi s'apprécie au fil du temps et en fonction de l'évolution du cadre de référence interne à l'entreprise,
- Le **pilotage opérationnel** : il visera à approfondir les indicateurs à mettre en place pour piloter valablement les Tiers et en effectuer une revue sur base régulière.

Si le pilotage opérationnel prend toute son ampleur une fois le Tiers en place, les trois autres composantes sont à aborder tout au long du processus.

Ainsi, la gestion des risques relative aux Tiers sera efficiente.

REMERCIEMENTS

En tant que pilote du groupe de travail, je suis honoré de vous proposer ce premier guide réalisé dans cette période troublée et parfois difficile au sein de nos entreprises.

Les échanges au sein du groupe de travail Workplace IFACI «Maitriser les Tiers» furent riches et variés avec les moyens de collaboration à distance.

Je tenais à remercier les contributeurs d'avoir consacré du temps et des efforts pour nous livrer leur réflexion sur des composantes de la gestion des risques des Tiers et toutes les personnes qui ont contribué aux différents ateliers, et celles qui ont interagi via le Workplace de l'IFACI, tout particulièrement Nelly Thieriot, Pascale Mirigay et Nathalie Sadeyen.

Un grand merci à toute l'équipe du service des adhérents IFACI de nous avoir accompagné pour que cela puisse se concrétiser.

Eric Chemama.

CONTRIBUTEURS

Eric Chemama

Auditeur en systèmes d'information, concepteur-formateur , Eric Chemama, ingénieur en informatique, a été Manager de projets informatiques au sein de grandes banques françaises et accompagne les entreprises dans la mise en place de dispositifs maîtrise des risques SI. Il dirige depuis 2012 le Cabinet EMC Conseil et Formation, spécialisé en audit et contrôle internes.

Astrid Boulon

Internal Audit Manager / Group Inspection at ODDO BHF, AMF Certification, Rouen Business School

Maxence Vadon

Contrôleur interne - Entité PIlotage du Contrôle permanent chez MACIF; membre du Comité Externalisation Groupe AEMA - Faculté de Droit de Montpellier - Master droit bancaire et financier

Christiane Legat

CFSA, Présidente du Groupe Professionnel Banque de l'IFACI et travaux en cours avec l'ECIIA pour, entre autres, développer les relations avec les régulateurs; une carrière internationale dans le monde bancaire au service des méTiers de l'Audit Interne et du Contrôle Interne; une expérience en matière de gouvernance, risques, conformité, contrôle mise au service de différents types de structures.

DISCLAIMER

Ce document est le fruit du Groupe de travail «Maîtriser les Tiers» de l'IFACI. Les Groupes de travail de l'IFACI ont pour objectif d'échanger sur des thématiques spécifiques d'un secteur d'activité, d'un domaine, ou d'une fonction. Ces échanges peuvent, le cas échéant, faire l'objet de publications destinées aux professionnels de la gestion du risque, auditeurs et contrôleurs internes du secteur concerné.

Ces publications sont réalisées sous la responsabilité des membres du Groupe de travail, et leur contenu technique n'engage ni les organisations auxquelles appartiennent les participants de ce Groupe, ni l'IFACI.

Le Groupe de travail «Maîtriser les Tiers» a élaboré ce document à titre informatif et pédagogique. L'IFACI n'a pas exercé de vérification exhaustive de son contenu. Cette publication n'a pas vocation à apporter de réponses définitives à des cas précis, et est uniquement destinée à servir de guide.

L'IFACI, ainsi que le Groupe de travail «Maîtriser les Tiers» déclinent toute responsabilité pour les cas où des lecteurs se fieraient exclusivement à ce guide ou ne trouveraient pas satisfaction dans cet ouvrage.

TABLE DES MATIÈRES

Cliquez sur une rubrique pour y accéder.

Gouvernance des Tiers 8
- Introduction 8
- Définitions 8
- Composition de la gouvernance des Tiers 9
- Structurer sa gouvernance à partir d'une Politique écrite 9
- S'organiser autour d'un processus transverse 10
- S'appuyer sur une comitologie opérationnelle et décisionnelle 11
- S'aider de tableaux de bord 11
- Reporter pour s'améliorer 12
- Facteurs de réussite 12

Veille relative aux Tiers 14
- Introduction 14
- Prévenir les risques vis-à-vis des Tiers 14
- Déterminer et combiner les méthodes 15
- Arrêter un Timing 16
- Informer les acteurs internes 17
- Autres idées à retenir 17
- Facteurs de réussite 18

Connaissance des Tiers et des risques inhérents 19
- Introduction 19
- Définitions 19
- Identifier les risques avec méthode 20
- Actualiser la connaissance des risques en continu 21
- Responsabiliser les acteurs de la connaissance des risques 22
- Évaluer et comparer le niveau des risques 23
- Adopter une démarche reliée à une nomenclature des risques 24
- Points d'attention 25

Pilotage opérationnel **26**
- Introduction 26
- Acteurs du Pilotage opérationnel 26
- Définitions 27
- Mettre en place des mesures d'analyse au regard des objectifs fixés 27
- Faire bon usage des mesures 29
- S'appuyer sur une comitologie opérationnelle 29
- Collecter et analyser l'information fournie par le Tiers pour conserver une vue constante de l'activité 30
- Contrôler son Tiers pour garder la maitrise de son activité 31

GOUVERNANCE DES TIERS

INTRODUCTION

Qu'elle soit motivée par une recherche de flexibilité des moyens de production ou davantage d'efficacité opérationnelle, **l'externalisation**[1] est utilisée de façon croissante par les établissements. Cette externalisation est par ailleurs source de risques : accroissement des risques opérationnels ou encore difficultés d'accès à l'information pertinente à des fins de contrôle des activités sous-traitées.

Ainsi, l'établissement qui externalise doit se prémunir face à ces risques au travers d'une robuste gouvernance robuste d'administration des Tiers, devant amener à l'application d'une stratégie préalablement définie. Aussi, conduire une analyse de risques complète est essentiel pour être en mesure de définir les mesures et les dispositifs de contrôle interne à exiger du prestataire ou à mettre en œuvre au sein de l'Entreprise.

DÉFINITIONS

Entité : Toute organisation responsable
Activités externalisées : les activités pour lesquelles l'entreprise assujettie confie à un Tiers, de manière durable et à titre habituel, la réalisation de prestations de services ou d'autres tâches opérationnelles.

1 Externalisation : Confier à une entreprise extérieure à l'Entreprise

COMPOSITION DE LA GOUVERNANCE DES TIERS

STRUCTURER SA GOUVERNANCE À PARTIR D'UNE POLITIQUE ÉCRITE

Une Politique écrite a pour objectif de formaliser les grandes orientations fixées par les instances décisionnelles en matière de Pilotage d'une activité essentielle à la bonne gestion de l'entreprise ou d'un organisme. Qu'elle soit imposée par une réglementation (cf. Politique Solvabilité 2 sur la sous-traitance en matière d'assurance) ou à l'initiative de l'entité, elle doit aboutir à une stratégie à mettre en œuvre et à respecter par les directions opérationnelles.

La Politique dédiée à la maitrise des Tiers consistera ainsi à définir la notion de Tiers pour l'entité, de rappeler les principes de responsabilité et les macro risques associés au Tiers, de fixer les critères pour les classer et pour évaluer l'importance ou la criticité de l'activité confiée par rapport à l'entité, de cadrer les phases majeures du processus interne gérant la relation avec eux, de définir les rôles, responsabilités et habilitations en interne et enfin de prévoir la circulation de l'information et des reporting internes et externes le cas échéant.

Il en ressortira une stratégie dédiée sur le recours aux Tiers sous forme d'orientations et conforme aux objectifs stratégiques de l'entité. Ces orientations porteront notamment sur les activités susceptibles d'être ou non confiées à des Tiers et dans quelles conditions.

Idée à retenir n°1

Il convient de faire approuver la **Politique**[2] écrite par l'instance décisionnelle et de la mettre à jour régulièrement notamment en utilisant les reporting remontés.

S'ORGANISER AUTOUR D'UN PROCESSUS TRANSVERSE

Au sein de l'entreprise, les intervenants sur le périmètre de la gestion des Tiers sont nombreux et incluent différentes directions telles que celles des risques, de la conformité, des contrôles permanents, de la finance, des achats, etc. Il incombe alors à l'entreprise de créer une organisation dédiée à la supervision de la relation avec le prestataire afin d'assurer la pleine responsabilité de toutes les obligations qui lui incombe. Afin d'assurer une organisation transverse et de qualité, l'entreprise devra formaliser :

- Un processus de sélection, de contractualisation, de suivi et contrôle des Tiers, de reporting;
- Des procédures opérationnelles de déclinaison de Politique des processus définis;
- Un dispositif de contrôle interne incluant une cartographie des risques spécifiques à la gestion des Tiers, un plan de contrôle et de suivi des plans d'action notamment.

Idée à retenir n°2

Il convient de formaliser les documents cadres à la gestion des risques des Tiers et de les communiquer à l'ensemble des parties prenantes.

2 Politique : Ensemble de principes, de normes, de comportement, qui sont émis par l'instance décisionnelle.

S'APPUYER SUR UNE COMITOLOGIE OPÉRATIONNELLE ET DÉCISIONNELLE

Le recours à des Tiers peut concerner une pluralité d'activités d'une entité et implique, par conséquent, de nombreux acteurs internes. Il convient de créer un comité regroupant ces acteurs opérationnels ainsi que des fonctions de contrôles et de gestion des risques.

Ce comité qui doit se réunir de façon périodique a pour rôle d'organiser et de mettre en œuvre opérationnellement la Politique écrite et d'effectuer son suivi.

À côté de son rôle de coordination, ce comité peut disposer de pouvoirs décisionnels (validation du recours à des Tiers, arbitrage de litiges,), ou simplement consultatifs (avis ou visa sur un projet de recours).

Idée à retenir n°3

Afin que la Politique et la stratégie soient effectives, il convient de désigner, au côté du comité, une direction en charge du Pilotage des processus dédiés qui doit disposer des pouvoirs de décision sur la manière de l'organiser. Cette Direction (de préférence non opérationnelle) s'appuiera sur les travaux de ce comité.

S'AIDER DE TABLEAUX DE BORD

Le recensement des Tiers de l'entreprise est une étape cruciale au bon déroulement du dispositif de contrôle interne. Recourir à un Tiers ne doit pas être source d'augmentation du niveau de risque intrinsèque des activités concernées.

Alors, le dispositif de suivi des prestataires doit à minima se concentrer autour :

- D'un tableau de recensement des Tiers. Il peut se baser sur une analyse visant à classer les Tiers par niveau de risque brut / net et par niveau de criticité de l'activité externalisée;
- D'un tableau d'indicateurs de contrôle et de suivi de la qualité du Tiers. Afin de décliner le dispositif de maîtrise des risques adéquat, il est de bonne pratique d'effectuer un **risk assessment**[3] au préalable.

3 Risk assessment : Processus consistant à évaluer les risques

Idée à retenir n°4

Afin de permettre un Pilotage efficace, il convient de s'aider de tableaux de bord de pilotage devant être mis à jour régulièrement.

REPORTER POUR S'AMÉLIORER

Pour rendre efficiente la gouvernance et ajuster la stratégie associée, divers types de reporting doivent être mis en place :

- Des reporting opérationnels périodiques à exiger du Tiers notamment sur des éléments statistiques sur l'activité confiée, des indicateurs de qualité, des contrôles et incident;
- Ces reporting opérationnels doivent être analysés en interne et les principaux constats doivent être consolidés au niveau central;
- Des reporting sur les incidents identifiés en interne dans le cadre des relations avec le Tiers. Ces reporting peuvent s'appuyer sur les bases internes de remontée d'incidents;
- Des reporting sur le suivi et l'évaluation de la qualité du Tiers (rapport d'audit sur place, d'enquêtes satisfaction initiées par une Direction Achats, veille et vérifications sur la situation financière, administrative réglementaire du Tiers).

Ces divers reporting sont essentiels et tout particulièrement si certains rapports sur la maîtrise des Tiers sont exigés par des autorités administratives ou par les organes de gouvernance.

Idée à retenir n°5

Il convient d'analyser et d'exploiter ces différents reporting. Ils révèlent le niveau de dépendance et des risques associés de l'entité face à ses Tiers et permettent d'ajuster le cas échéant sa stratégie autour du recours à des Tiers.

FACTEURS DE RÉUSSITE

Un RACI (rapport annuel sur le contrôle interne) permettant de distinguer clairement les responsabilités en interne de gestion de la relation opérationnelle avec un Tiers, et le rôle de pilotage des activités gérées par des Tiers dans l'optique de mener la stratégie définie.

Une veille, fréquente et exhaustive des Tiers de l'Entreprise (cf. chapitre Veille).

Une gouvernance qui repose également sur un Pilotage opérationnel efficace (cf. chapitre Gouvernance).

Poursuivre votre lecture ....

Lien vers les autres travaux du Groupe :

-->Pour plus d'informations sur la phase de sélection du processus, voir la fiche Connaissance des Tiers et des risques inhérents.

--> Pour plus d'informations sur les différents types de reporting opérationnels, voir la fiche Pilotage opérationnel.

VEILLE RELATIVE AUX TIERS

INTRODUCTION

La veille est un terme très général. Différents types de veille comme la veille scientifique, réglementaire, juridique, financière, stratégique, sociétale, environnementale, concurrentielle... existent.

L'objectif de toute veille est de se tenir informé, d'être informé en priorité pour action.

Les catégories de veille dépendent du milieu dans lequel la veille doit être effectuée (entreprise, banque, services, secteur public, état, assurance, industrie...)

La veille réglementaire ou juridique consiste en une surveillance des évolutions législatives et réglementaires permettant de connaitre les normes en vigueur. Quant à la veille commerciale ou financière par exemple, elle consiste en une surveillance des changements de situation, de stratégie ou de règles et normes financières. Dès lors, la veille stratégique englobera plusieurs types de veille pour permettre d'orienter la stratégie globale d'une organisation (concurrents, R&D...).

Idée à retenir n°1
La veille relative aux Tiers est une veille thématique qui sera protéiforme dans la mesure où elle englobera différents aspects tels que ceux réglementaires, légaux, commerciaux, de conformité... Elle sera structurée afin de répondre aux contrôles comme prévu par les trois lignes de défense.

PRÉVENIR LES RISQUES VIS-À-VIS DES TIERS

La veille est une **surveillance**, un repérage des évolutions, des informations stratégiques qui permettront à une institution/une entreprise d'avoir une bonne connaissance de l'environnement dans lequel elle évolue afin de bâtir sa stratégie, **d'anticiper** les évolutions à venir et donc **d'adapter** son offre et **de calibrer** ses propositions.

Dans un esprit de développement durable, la veille est donc un élément essentiel pour **prévenir les risques** en anticipant les contraintes environnementales ou sociétales. Elle s'inscrit dans le système global de prévention des risques.

La veille est un atout essentiel pour une **gestion des risques efficace** qui permet à une entreprise de réagir face à des évolutions à venir ou des menaces portant sur son environnement. La veille est indépendante et notamment indépendantes de la direction des risques. Elle est rattachée à un directeur exécutif. La maximisation de l'utilité de la veille est obtenue par une bonne relation avec les autres départements de la structure pour intervenir a-priori et permettre de mettre en place une sorte de règle des quatre yeux.

Idée à retenir n°2

La veille relative aux Tiers permettra de sous-traiter à des Tiers dans le respect des obligations qui s'imposent au secteur d'activité auquel appartient le délégant; ceci en ayant connaissance des risques afin de les étudier préalablement comme par exemple les conflits d'intérêt et de couvrir le délégant par exemple par une déclaration sur l'honneur du Tiers quant à sa probité. Elle permettra aussi de tenir informé régulièrement le délégataire de ses obligations et des contraintes qu'il a à respecter dans le cadre de la prise en charge des processus externalisés.

DÉTERMINER ET COMBINER LES MÉTHODES

La veille consiste, en toute indépendance, pour des professionnels de l'information et experts de la matière, à collecter **en continu** des informations, les **analyser** et effectuer des projections par rapport au secteur d'activité de l'entreprise concernée. C'est un **dispositif organisé visant à anticiper**.

Aujourd'hui, avec les moteurs de recherche, les bases externes (exemple : celle de Transparency International sur les indices de perception de la corruption) et surtout la montée en puissance de l'intelligence artificielle, la collecte/la fourniture des informations est grandement facilitée.

Des consolidateurs d'information d'ordre public comme PROVIGIS (solution de conformité des fournisseurs) facilitent la collecte d'information.

Restent (1) la partie la plus délicate qui est la synthèse/l'analyse de toutes ces informations et surtout (2) la partie prospective. Cette dernière nécessite une très bonne connaissance de l'entreprise et des risques portés par le business afin de pouvoir identifier/déterminer :

- ceux qui évolueront et dans quelle proportion,
- ceux qui disparaitront et à quel horizon,
- ceux qui apparaitront. Les risques naissants seront à quantifier et à pondérer alors qu'aucun historique n'existe au sein de l'entreprise.

La complexification, par exemple, des réglementations notamment dans le domaine financier, apparait comme un risque important auquel la veille doit s'attacher tout particulièrement.

Idée à retenir n°3

La veille ne doit pas s'arrêter dès lors que l'activité est externalisée, il est nécessaire de garder le contrôle des activités externalisées. Pour cela, le délégant devra être en mesure de démonter sa capacité à internaliser l'activité externalisée ou la négociation de contrats identiques avec une autre structure en mesure de reprendre l'externalisation au pied levé. De la même manière, si le délégataire décide à son tour de devenir délégant, il doit en informer le primo délégant et lui prouver qu'il est en capacité à gérer les risques comme souhaité initialement par le délégant et en conformité avec les termes du contrat signé à l'origine entre les parties.

ARRÊTER UN TIMING

- La veille est utilisée ab initio.

En effet, la décision d'externaliser est une décision qui relève des organes de gouvernance et une politique d'externalisation doit être approuvée par les instances. Compte tenu des risques nouveaux générés par cette décision, il est recommandé d'avoir effectué la veille préalablement

Avant de contracter avec un Tiers, il est nécessaire d'avoir procédé aux contrôles de conformité sur le Tiers; la veille nous permettra de savoir ce que le délégant peut collecter comme par exemple, un accord de confidentialité (**NDA**[4]) à signer par les personnes exécutant la prestation et ce qu'il n'a pas le droit de collecter, comme les informations personnelles relatives aux personnes exécutant la prestation. Lors de la contractualisation, la veille juridique relative aux Tiers permettra de connaitre les mentions obligatoires à inscrire dans les contrats comme par exemple les normes de performance, les droits d'auditabilité mais aussi les obligations en matière d'externalisation à un autre Tiers. Elle permettra également de savoir quels sont les documents à collecter comme par exemple le K-Bis.

- La veille est utilisée au cours de la vie des contrats d'externalisation.

La veille notamment sur la probité, la santé financière, l'application des règles déontologiques par le délégataire est essentielle. De celle-ci, résultera la décision de continuer ou d'internaliser à nouveau la prestation. Le respect des obligations en matière de plan de continuité des activités : le délégant doit être informé des conditions de restauration de ses informations sur site externe lors des phases de test.

4 NDA : Non Disclosure Agreement

- La veille est utilisée pour mettre un terme au contrat d'externalisation.

Lorsqu'il est décidé de mettre un terme à la décision d'externalisation, la veille est importante car des obligations parfois évolutives au fil du temps s'imposent tant au délégant qu'au délégataire (exemple : récupération des archives...).

INFORMER LES ACTEURS INTERNES

Dans le cadre de la gouvernance, sont définis des reportings dédiés à la veille afin d'informer les différents acteurs de la comitologie de la structure et également afin de mettre à jour les politiques de la structure et en suivant les procédures.
Cette remontée d'information est indispensable afin que les effets positifs attendus surviennent.

Par ailleurs, dans certains cas et notamment si les prestations rendues par les Tiers sont considérées comme significatives voire essentielles, alors un reporting doit avoir lieu auprès de l'organe de direction.

Il est enfin fait un reporting sur les conséquences financières si la veille n'a pas été suivie d'effet et donc qu'un risque opérationnel ait été pris par l'établissement conduisant à une perte.

AUTRES IDÉES À RETENIR

- La veille règlementaire, technologique et concurrentielle intra ou intersectorielle permet d'identifier les opportunités de marchés et les avantages compétitifs potentiels (innovations notables, nouveaux services ou produits).

- En termes fonctionnels, la veille est souvent incluse dans un département rattaché au domaine de la conformité mais il y a aussi la veille technique qui existe au sein de chaque département. Par exemple, le département comptable doit bénéficier d'une unité de veille afin d'apprécier les évolutions, par exemple, celles relatives aux normes comme les IAS et les adapter au contexte de l'entreprise.

- L'externalisation d'une prestation rendue par un Tiers est possible à condition que le délégant en soit informé préalablement et que les indicateurs définis et mis en place pour mesurer la qualité de la prestation soient respectés par le sous-traitant du délégataire.

- Pour les structures de petite taille, il n'est pas toujours possible de mobiliser les moyens nécessaires pour mener une veille de qualité. Dès lors, des abonnements à des services de veille sont possibles voire une mutualisation des veilles pour un même domaine d'activité.

FACTEURS DE RÉUSSITE

Une bonne communication entre les départements de risques et de veille est un gage de succès pour l'entreprise.

Une grande réactivité des différents départements pour mettre à jour la cartographie des risques de l'établissement et pour ajuster les pondérations de risque permettra une meilleure allocation du capital, denrée rare et chère dans certains secteurs.

CONNAISSANCE DES TIERS ET DES RISQUES INHERENTS

INTRODUCTION

Les organisations publiques ou privées doivent étendre leur méthode d'analyse des risques pour une connaissance exhaustive des risques vis-à-vis de la relation d'affaires avec un Tiers prestataire, fournisseur ou mandataire.

Les étapes classiques de la gestion des risques doivent intégrer les causes probables de risque et leurs impacts générés de manière directe ou indirecte sur leurs Tiers. Ces risques sont alors qualifiés d'exogènes et peuvent survenir à tout moment dans la relation d'affaires, y compris après la clôture.

On considère 4 étapes pour appréhender ces risques :

- Identifier les risques;
- Évaluer les risques;
- Analyser les risques;
- Corréler les risques.

Conduire un processus d'identification et d'évaluation des risques est essentiel pour être en mesure :

- de gérer les risques dans le processus d'appel à un Tiers et tout au long de la relation d'affaires;
- de corréler les risques identifiés pour aider à la décision; en prenant différents critères par exemples, le prix, les délais et l'éthique, pour aider à la sélection d'un Tiers;
- d'informer la gouvernance;
- de définir les mesures et les dispositifs de contrôle interne à exiger ou à mettre en œuvre au sein de l'entreprise;
- de revoir et amender les termes des contrats.

DÉFINITIONS

[Connaissance] : « *Faire ou avoir fait l'expérience permettant une représentation mentale de quelque chose, avoir l'idée, la notion d'une chose* » (Larousse).

[Risque] : probabilité qu'un événement se produise pouvant nuire à l'entreprise et aux actifs de celle-ci.

[Appétence] : tendance qui porte vers ce qui peut satisfaire les penchants naturels

[Evaluation du risque résiduel] : l'évaluation des risques résiduels constitue un ensemble de mesures favorisant la diminution des risques potentiels et pouvant impacter négativement les objectifs de l'entreprise.

IDENTIFIER LES RISQUES AVEC MÉTHODE

Le périmètre de maîtrise du risque ne s'arrête pas à la porte de l'Entreprise. Cette dernière s'expose à des risques en sollicitant un Tiers et/ou en mettant en place une relation d'affaires durable.
L'entreprise doit **identifier les risques vis-à-vis de la relation d'affaires avec le Tiers en distinguant** :

- le Tiers et ses caractéristiques propres dans son environnement; le simple fait de solliciter un tiers pour une prestation ou fourniture de biens et/ou de services ponctuels;
- les engagements pris;
- **la (les) activité(s)** qui ont été externalisées; l'externalisation d'une activité ou fonction qui se retrouve donc susceptible de modifier significativement l'exposition aux risques des activités menées en interne.

Il n'y a pas de méthode idéale mais un ensemble d'approches et de techniques, basées sur l'expérience, enrichies des exercices formels de cartographie des risques. Mais celles-ci ne peuvent suffire à connaître de manière pertinente les risques auxquels le Tiers et par voie de conséquence l'entreprise sont exposés. L'identification des risques peut être réalisée en combinant plusieurs lectures du risque :

- Identification en se basant sur l'atteinte des objectifs de l'entreprise;
- Identification en se basant sur les risques déjà survenus; les incidents et problèmes recensés en interne et dans des bases externes;
- Nomenclature de risques possibles afin de voir si ceux-ci concernent les processus en partage avec le Tiers;
- Identification basée sur les actifs importants (données, sites, savoir-faire...) et des menaces pesant sur eux;
- Identification à partir des facteurs environnementaux et de l'exposition aux menaces externes;
- Analyse des impacts sur le fonctionnement normal de la production et du service aux clients finaux;
- Identification des risques par l'analyse des activités en cas d'externalisation; les risques inhérents aux activités sous traitées : défaillances, disponibilité, dépendance, ségrégation des clients, homme clé, conformité, systémique;

Idée à retenir n°1

Le profil de risque des activités et de l'entreprise change lorsque celle-ci concentre des services au sein d'un même Tiers et/ou que la relation devient durable et régulière.

Idée à retenir n°2

L'application notamment des seuils définis comme pour le devoir de vigilance ne restreint pas l'applicabilité qu'à la porte de l'entreprise. Elle peut concerner le non-respect des règles en matière de corruption, des règles liées au RGPD et à leurs relations avec les sous-traitants, des règles et engagements en matière d'environnement,...

Idée à retenir n°3

La stratégie de l'entreprise et les axes opérationnels sont également des référentiels utiles pour l'entreprise et des mesures de l'atteinte des objectifs; l'entreprise peut s'engager dans une politique du respect des individus et par conséquent hiérarchiser les risques critiques lors de la sélection du Tiers et durant toute la relation.

ACTUALISER LA CONNAISSANCE DES RISQUES EN CONTINU

L'entreprise porte d'abord son attention sur une connaissance précise des risques dès la sélection d'un Tiers fournisseur ou prestataires (cf. figure 1). Cette prise de connaissance souvent dénommée par l'acronyme KYS (« Know your supplier ») doit être proportionnelle aux enjeux des relations fournisseurs et à l'importance de la relation.

Elle démarre par la connaissance des Tiers et par la compréhension de la nature de la relation que l'entreprise va établir (achats, ventes, subventions, prestation financière, ...).

Figure 1.

Une gestion des risques efficace demande une actualisation régulière, programmée et/ou déclenchée à partir d'événements issus de la Veille et/ou d'informations de la part de la gouvernance.

Idée à retenir n°4

Des marqueurs d'un renouvellement anticipé de cotation doivent être identifiés (nouveau pays, changement de l'actionnariat,).

Idée à retenir n°5

L'entreprise doit régulièrement apprécier les critères de risque tout au long de la relation lui permettant de comparer les fournisseurs/les prestataires appartenant à la même famille de Tiers (ex : fournisseurs de matières premières).

RESPONSABILISER LES ACTEURS DE LA CONNAISSANCE DES RISQUES

L'approche pour une bonne prise de connaissance des risques passe par des entretiens avec les Managers, les Pilotes de processus et les seniors Managers.
D'autres acteurs transverses contribuent à une centralisation de la connaissance des risques des Tiers, comme la Direction des achats, les Contract Managers ou les acteurs de la gestion du risque opérationnel.

Idée à retenir n°6

Il appartient au Responsable de processus d'identifier les risques inhérents à l'externalisation de la prestation. Il pourra s'appuyer sur les fonctions de support de l'entreprise pour collecter et évaluer les données du Tiers et formuler à cette occasion une cotation du risque fournisseur.

Idée à retenir n°7

La prise de connaissance et l'appréciation du niveau de risques liés aux Tiers et/ou aux prestations doivent être réalisées avec la contribution des différentes Directions et Services compétents (Opérations; Risques; IT; Conformité/ CP et Juridique par exemple). Ces acteurs peuvent s'appuyer sur des outils partagés pour coter le risque selon les domaines d'expertise.

Idée à retenir n°8

Le Responsable de Relation aura la responsabilité de constituer un dossier prestataire avec toutes les preuves. Il pourra alors disposer d'une documentation complète pour :

- identifier les risques majeurs inhérents à l'externalisation de la prestation;
- mettre à jour le dossier du prestataire;
- réunir, sur le prestataire, les informations liées à la formation, la sécurité, les conflits d'intérêts, les personnes concernées et les contrôles internes en vigueur;
- surveiller les engagements du prestataire par le biais de reporting, d'indicateurs qualité, de comités formalisés et de suivi des incidents.

ÉVALUER ET COMPARER LE NIVEAU DES RISQUES

Un dispositif de cotation permet de quantifier le risque et ainsi de comparer les Tiers entre eux selon les critères choisis, surveiller l'évolution dans le temps, par Tiers, par critère ou par famille de Tiers.
Un système de cotation opérationnelle enregistre et met en forme le travail d'analyse des fournisseurs; il conserve l'historique de cotation, ainsi que les éventuelles pièces justificatives venant corroborer les notes.

Idée à retenir n°9
Les approches d'identification et de cotation des Tiers s'appuient sur un ensemble de critères concourant à la cotation du risque des Tiers dont la défaillance serait susceptible de nuire gravement à la poursuite, à la sécurité ou à la conformité et/ou de remettre en cause les activités sous traitées et/ou avoir un impact sur la réputation de l'entreprise.

Idée à retenir n°10
Un dispositif de cotation du risque de corruption doit correspondre au mieux à la mission et aux objectifs de l'organisation, à la réalité de ses activités et doit être corrélé à la cartographie des risques de corruption; cette dernière permet d'évaluer le risque de corruption et conduit à déterminer le niveau de diligences à appliquer.

Idée à retenir n°11
Une cotation du risque « fournisseurs », comme celle adaptée à l'anticorruption et au respect des exigences de Sapin II peut être utile :

- à l'appui de la présentation d'une nouvelle stratégie fournisseurs : diversification des approvisionnements, par exemple.
- pour adapter les contrôles en cas de critère aggravant ou diminuant les risques,
- en cas de contrôle externe (audit, certification, ...), les données enregistrées tracent les analyses effectuées.

ADOPTER UNE DÉMARCHE RELIÉE À UNE NOMENCLATURE DES RISQUES

Le recours à tout Tiers et/ou toute prestation de service nécessite qu'une analyse préalable de risques soit établie de manière à ce que la fourniture, la prestation ponctuelle ou la relation d'affaires soient effectuées en « pleine connaissance de cause ».

On peut utiliser la nomenclature des risques afin de distinguer :

Les principaux risques liés au Tiers

- Les risques relatifs au prestataire (de par sa surface, sa notoriété, sa pérennité, ...);
- Les risques inhérents à la situation géographique voire géopolitique de la prestation;
- Les risques inhérents à la maîtrise de l'expertise du prestataire (et de sa potentielle « dilution » pour le donneur d'ordre);
- Le risque lié à la non-conformité réglementaire et sociale;
- Le risque de corruption;
- Le risque lié à la sécurité financière (blanchiment, embargo, ...);
- Le risque de concentration et de dépendance économique;
- Le risque lié à l'abus de position dominante de la part du client « donneur d'ordre » qui abuse de sa position vis-à-vis de prestataires pour leur imposer des exigences non conformes au droit du travail;
- Le risque systémique si le prestataire est commun à plusieurs donneurs d'ordre et qu'il subit une défaillance pouvant impacter l'ensemble d'un secteur;

Les risques liés aux engagements et à la fourniture, prestation ou externalisation

- Le risque de défaillance du prestataire : non-conformité de la prestation par rapport aux clauses techniques du contrat, fragilité financière, « risque pays » du prestataire (dans le cas de prestataires délocalisés en partie ou en totalité);
- Le risque lié au non-respect ou à une déficience du processus d'externalisation;
- Le risque lié à la non-réversibilité des activités externalisées et la perte de compétence associée;
- Les risques opérationnels liés à l'activité elle-même.

Les autres risques

- De manière systématique, l'entreprise doit prendre en compte les risques liés à toute forme d'externalisation comme le respect des réglementations en matière de déontologie, de secret professionnel, de droit du travail, de devoir de vigilance.

POINTS D'ATTENTION

- Les facteurs favorisant la survenance des risques sont propres d'abord au Tiers lui-même, à son exposition à l'environnement externe, à la concurrence et aux différentes règlementations sectorielles ou du pays d'exercice; des facteurs liés à l'usage des technologies de l'information, à la responsabilité sociale des entreprises sont susceptibles d'être appréhendés sans limite.

- Le risque notamment de perte de continuité d'activité montre combien il est important d'identifier où se situent les risques et leur traitement. Des dispositions doivent être prises pour identifier ce risque selon les situations différentes :
    - continuité d'activités totalement à la charge de l'entreprise;
    - continuité d'activités totalement à la charge du Tiers;
    - continuité d'activités reposant conjointement sur l'entreprise et sur le Tiers.

- Les risques peuvent également se manifester de manière temporaire dans les phases de transition, de bascule vers le Tiers ou dans des phases de réversibilité. Ils peuvent également se produire à la livraison/réception d'un bien ou service.

PILOTAGE OPERATIONNEL

INTRODUCTION

Le pilotage opérationnel des activités du Tiers est le contrôle de sa performance par rapport aux attendus/objectifs fixés et moyens alloués et ceci à travers des tableaux de bord, d'indicateurs et de la mise en plan d'actions en cas d'écarts constatés.

Le pilotage opérationnel a pour objectif de :

1. Veiller à l'atteinte des objectifs des activités opérationnelles / des services et produits fournis par les Tiers
2. Veiller à la conformité du Tiers face à ses engagements financiers, éthiques, réglementaires et juridiques.
3. Etre en capacité d'arbitrer et d'aider à la décision
4. Satisfaire aux exigences et prendre en compte les risques.

Le pilotage opérationnel est mis en œuvre à travers un certain nombre de composantes :

- Instances et comités au sens large (cf. chapitre Gouvernance);
- Collecte et remontée des données du Tiers (plateforme, reporting périodique, ...);
- Indicateurs (en distinguant le pilotage individuel vs Tiers tous confondus);
- Contrôle sur place ou à distance (ex : contrôle à distance, certification par un Tiers ISO, reporting ISAE 3402...);
- Déclaration et exploitation des incidents (partage d'une base des incidents, reporting, incidents de sécurité (fuite d'info, cloud,..), ...);
- Aléas/changements (cf. chapitre Veille);
- Evaluation du Tiers (cotation , ré-évaluation, inventaire, ...) pour présentation des résultats produits à la Gouvernance

ACTEURS DU PILOTAGE OPÉRATIONNEL

Les Principaux acteurs de ce dispositif de pilotage sont :

- Les méTiers et leurs pilotes de processus assurant le suivi des relations avec le Tiers;
- Les risk manager pour une bonne prise en compte des exigences;
- Les services achats garants des conditions des engagements;
- Les sachants et experts de domaines support (IT, conformité,...,).

DÉFINITIONS

Pilotage opérationnel : Mise en place et analyse d'un ensemble de données et de mesures pour l'évaluation des risques des activités et des Tiers.

KPI : acronyme issu de l'anglais, signifiant key performance indicator. En français, on parle d'indicateur clé de performance (ICP). Un KPI permet de bien piloter et de mesurer l'efficacité des services et produits proposés par un Tiers.

KRI : Key Risk Indicator. En français, on parle d'indicateur clé de risque. Un KRI permet de vérifier le niveau de maîtrise des risques identifiés en suivant l'évolution des valeurs des résultats des dispositifs.

Pénalités : L'évaluation de mesures de services ou de non-respect des engagements peut occasionner l'application de pénalités financières restant à négocier avec les Tiers.

METTRE EN PLACE DES MESURES D'ANALYSE AU REGARD DES OBJECTIFS FIXÉS

Périmètre de ces mesures

Des mesures peuvent être établies sur les caractéristiques propres du Tiers et sur les données de l'activité confiée. On peut suivre et piloter les familles de données suivantes (non exhaustive) :

- Signalétique
- Données fiscales et sociales
- Équipe et compétences requises
- Suivi KPI, KRI des activités menées
- Alertes/plan d'actions
- Facturation (prix, qualité, délais,)
- Traitement des incidents

On peut apprécier la qualité des prestations, notamment par rapport au suivi des incidents et des anomalies mineures ou majeures. Les pilotes mettent en place les mesures nécessaires pour une amélioration continue des prestations sous-traitées sous forme :

- Qualitative avec description du problème, des causes et des possibilités de corrections;

- Quantitative avec des indicateurs de flux, de taux et de délai de résolution.

Dans la plupart des cas, les pilotes lancent des plans d'actions en regard des incidents et prennent les décisions nécessaires pour en réduire les impacts.

Différents types d'indicateurs

Ils peuvent être calculés en distinguant :

- Indicateurs individuels permettant le suivi de l'activité chez le Tiers
- Indicateurs macro sur l'ensemble ou sous ensemble des Tiers (cf. chapitre Gouvernance).

Règles de gestion applicables à ces mesures

- Les indicateurs sont souvent définis dans la partie « convention de services » ou annexes des dossiers contractuels;
- Ils sont calculés au moins mensuellement, parfois au quotidien ou hebdomadairement sur certaines prestations, puis repris dans des tableaux de bord, sur plusieurs mois glissants;
- Les indicateurs sont fournis par le prestataire à partir des méthodes de calcul et de mesure décrites dans les documents contractuels.

Idée à retenir n°1

Il faut veiller de manière systématique à faire une première analyse de ces indicateurs dans les documents supports des comités. Cette analyse donne lieu, en cas de problème, à des actions correctrices voire à des pénalités. Elle fait l'objet d'une appréciation globale avant mise en œuvre des pénalités.

Idée à retenir n°2

Ces mesures sont, la plupart du temps, validées par le pilote interne notamment avec des outils internes de mesure puis analysées en comité de pilotage;

Idée à retenir n°3

La satisfaction est parfois mesurée par une enquête interne. Elles sont menées auprès des utilisateurs finaux de la prestation; d'autres enquêtes restent dans le cercle des acteurs du pilotage de la prestation.

FAIRE BON USAGE DES MESURES

Pour permettre des interactions avec le Tiers, des indicateurs vont pouvoir être utilisés pour déterminer :

- La faisabilité d'application des pénalités et la bonne adéquation des indicateurs;
- La satisfaction client et les points d'amélioration;
- Les risques homme-clé, perte de compétences en interne, dépendance;
- La réalité de mise en œuvre des éléments d'un PCA suivant les types d'externalisation;
- La capacité de réinternaliser l'activité ou de passer chez un autre Tiers;
- Les perspectives de remise en cause du Tiers (fournisseur ou prestataire) ou les conditions d'une nouvelle contractualisation ou du lancement d'un nouvel appel d'offre;
- La capacité des Tiers à respecter les droits humains, l'environnement, la santé et la sécurité des personnes.

Des grilles de cotation du risque lié à la relation d'affaires ou en matière de corruption constituent des éléments d'appréciation individuelle pour comparaison avec des prestataires/fournisseurs appartenant à la même famille de Tiers (fournisseur de matières premières, infogérance, prestataire d'éditique, cabinet d'avocats...)

S'APPUYER SUR UNE COMITOLOGIE OPÉRATIONNELLE AVEC LE TIERS

Afin d'assurer un suivi et une bonne organisation de l'activité externalisée, il convient de mettre en œuvre, de manière conventionnelle, divers comités gérant les relations directes entre le donneur d'ordre et son Tiers.

- Un comité communément appelé de pilotage ayant vocation à gérer la gouvernance de la relation. De récurrence moindre (une à quatre fois par an selon le niveau d'importance de l'activité pour le délégant), il sera en charge notamment de dresser un bilan d'activité traiter les orientations générales organisationnelles, fonctionnelles, les dysfonctionnements majeurs, valider les besoins d'évolution du contrat ou convention ou de l'activité ou arbitrer sur des divergences opérationnelles.

- Des comités opérationnels spécialisés tels que des comités de suivi Métier ou informatique le cas

échéant. De récurrence plus rapprochée (une fois par mois ou par trimestre) ils visent principalement à réaliser un suivi opérationnel et fonctionnel des activités externalisées, à suivre la qualité et la conformité des prestations et indicateurs. Ils seront en charge notamment de suivre la réalisation des objectifs et les contrôles ainsi que l'avancement des plans d'actions en rapport avec les activités opérationnelles, de traiter les problématiques opérationnelles, les incidents, d'identifier les écarts sur les indicateurs, d' établir des plans d'actions ou de progrès....

COLLECTER ET ANALYSER L'INFORMATION FOURNIE PAR LE TIERS POUR CONSERVER UNE VUE CONSTANTE DE L'ACTIVITÉ

À côté des différents comités, il convient de prévoir conventionnellement différents types de remontées d'information par le Tiers et ceci de manière périodique comme par exemple :

- Des remontées d'information sur l'activité. Cela se traduit notamment par l'accès donné au délégant aux outils de pilotage du Tiers ou par l'envoi de réporting opérationnels périodiques. Les informations opérationnelles portent en général sur le suivi de l'activité et des engagements et du niveau des indicateurs de services, de formalisation des contrôles effectués, des incidents, mais également sous la forme de flux statistiques, comptables pour alimenter diverses directions chez le délégant (comptabilité, contrôle interne, partenariat, achat...),

- Des remontées d'information sur la situation du prestataire. Il convient régulièrement de demander au Tiers la fourniture de certains éléments sur sa situation ou son organisation interne. Souvent cela se traduit par l'envoi d'un questionnaire pluridisciplinaire portant sur sa situation administrative (Kbis) , réglementaire (attestation URSSAF, liste des travailleurs étrangers, sur le renouvellement d'inscription pour les activités réglementées...), organisationnelle (dispositif contrôle interne; politique), sur son niveau de conformité par rapport à certaines réglementations (RGPD, SAPIN II, LCB/FT...) ou d'exigences de sécurité (plan de sécurité information ou PCA). Des justificatifs peuvent être demandés à l'appui des réponses. Il peut être rattaché à ces réponses un système d'évaluation de prestation.

Idée à retenir n°4

Il est essentiel que le mandant exploite et analyse l'ensemble des informations transmises en s'appuyant notamment sur ses sachants internes (RSSI, Contrôle interne, conformité, Délégué à la Pro-

tection des données.). Ceci lui permet d'une part de garder une vision constante de son activité déléguée et d'autre part d'évaluer le Tiers de manière régulière (en complément avec des enquêtes satisfaction interne). Ces analyses doivent ensuite être remontées pour consolidation à la direction ou l'instance en charge de la gouvernance des Tiers.

De plus en plus d'outils de gestion d'échanges d'informations existent entre le délégant et son délégataire sur le marché, soit pour répondre à un besoin sectoriel (courtage...), soit à portée généraliste.

CONTRÔLER SON TIERS POUR GARDER LA MAÎTRISE DE SON ACTIVITÉ

Les éléments opérationnels obtenus du Tiers sous forme déclarative nécessitent d'être corroborés par des contrôles initiés par le déléguant. Ces contrôles peuvent être effectués à distance (si accès aux outils du Tiers) ou sur place. La fréquence dépend du niveau de risque, de la nature et de l'importance de l'activité déléguée pour le délégant. Il convient d'établir une lettre de mission précisant les domaines à auditer et d'aboutir in fine à un rapport appuyé par des plans d'actions ou de recommandations.

Ces contrôles sur place peuvent être externalisés à des cabinets spécialisés à l'initiative du mandant ou même du Tiers (via un rapport ISA 3402).

Idée à retenir n°5
Prévoir dans la convention d'externalisation des clauses d'audit et d'accès à l'information au profit du mandant afin de faciliter les modalités d'intervention.

À propos

Porte-paroles de la profession d'audit interne, l'Institut Français d'Audit et de Contrôle internes (IFACI) et l'Institut des auditeurs internes (IIA) sont des autorités reconnues dans le domaine de la formation et de la formulation des normes, lignes directrices et certifications.

Copyright

Le copyright de ce guide pratique est détenu par l'IFACI.
Pour l'autorisation de reproduction, prière de contacter l'IFACI à l'adresse suivante :
institut@ifaci.com

IFACI

98bis, Boulevard Haussman
75008 PARIS, France
Téléphone : 01 40 08 48 00
Fax : 01 40 08 48 20
Site Web : www.ifaci.com
Courrier électronique : institut@ifaci.com

institut français de l'audit et du contrôle internes

GROUPE DE TRAVAIL
MAÎTRISER LES TIERS

MAÎTRISER LES RISQUES DES TIERS

Adopter une gestion des risques efficace avec les Tiers

Institut Français de l'Audit et du Contrôle Internes - 98bis, Boulevard Haussmann
75008 Paris - Tél. : 00 48 08 40 331+ Fax : 20 48 08 40 331+ - institut@ifaci.com