Tierce partie

Exigences thématiques

Topical Requirement

The Institute of Internal Auditors

Traduit en collaboration par :

IFACI IIA France

Institute of Internal Auditors Belgium

Exigences thématiques relatives aux tierces parties

Le Cadre de référence international des pratiques professionnelles (International Professional Practices Framework®) comprend les Normes internationales d'audit interne (Global Internal Audit Standards™), les Exigences thématiques et les Lignes directrices internationales. Les Exigences thématiques sont obligatoires et doivent être utilisées conjointement avec les Normes, qui font autorité sur les pratiques requises.

Les Exigences thématiques définissent des attentes claires pour les auditeurs internes en fournissant une référence a minima pour l'audit de domaines de risques spécifiques. Le profil de risque de l'organisation peut obliger les auditeurs internes à prendre en considération d'autres aspects du sujet.

La conformité aux Exigences thématiques renforcera la cohérence des activités d'audit interne et améliorera leur qualité et leur fiabilité ainsi que leurs résultats. En fin de compte, les Exigences thématiques élèvent le niveau professionnel de l'audit interne.

Les auditeurs internes doivent appliquer les Exigences thématiques conformément aux Normes internationales de l'audit interne. La conformité aux Exigences thématiques est obligatoire pour les activités d'assurance et recommandée pour les activités de conseil. L'Exigence thématique est applicable lorsque le thème est l'un des suivants :

1. Le thème d'une mission figure dans le plan d'audit interne.
2. Le thème a été identifiée lors de la réalisation d'une mission.
3. Le thème d'une mission demandée ne figurait pas dans le plan d'audit interne initial.

L'applicabilité de chaque exigence de l'Exigence thématique doit être évaluée. Les éléments probants de ces évaluations doivent être documentés et conservés. Toutes les exigences individuelles peuvent ne pas s'appliquer à chaque mission ; si certaines d'entre elles sont exclues, une justification doit être documentée et conservée. La conformité à l'Exigence thématique est obligatoire et sera évaluée lors des évaluations de la qualité.

Tierces parties

Un tiers est une personne, un groupe ou une entité externe avec lequel une organisation (dite "l'organisation principale") établit une relation d'affaires pour obtenir des produits ou des services. La relation peut être formalisée par un contrat, un accord ou d'autres moyens. La présente Exigence thématique utilise le terme "tierce partie" pour désigner les vendeurs, les fournisseurs, les entrepreneurs, les sous-traitants, les prestataires de services externalisés, les autres agences et les consultants. Le terme inclut les accords entre un tiers et ses sous-traitants, souvent appelés sous-traitants "en aval".

L'Exigence thématique s'applique lorsque la fonction d'audit interne réalise des missions d'assurance sur des tierces parties et/ou des relations de sous-traitance, y compris celles qui se situent au quatrième rang

ou plus en aval, autorisées par le contrat ou l'accord conclu par la tierce partie avec l'organisation principale. Les auditeurs internes doivent classer les tiers et les autres parties en aval par ordre de priorité en fonction du risque, comme décrit dans la section relative à la gestion des risques ci-dessous. Les auditeurs internes doivent appliquer toutes les exigences indiquées par les résultats de l'évaluation des risques, et documenter les exclusions.

La présente Exigence thématique n'a pas pour objet de traiter des relations, intérêts ou engagements externes indirects avec l'organisme principal, tels que les régulateurs, les agents, les fiduciaires / membres de conseil d'administration, ou des relations internes, telles que celles avec des salariés.

Le terme "tierce partie" peut être défini et utilisé différemment selon le secteur d'activité ou d'autres contextes. Les auditeurs internes disposent d'une certaine flexibilité et doivent s'appuyer sur leur jugement professionnel pour adapter l'Exigence thématique à la définition de tierce partie donnée par l'organisation principale.

L'organisation principale (l'organisation qui conclut un accord avec une tierce partie) reste tenue de rendre compte des risques liés à la réalisation de ses objectifs, même lorsqu'elle fait appel à un tiers pour l'aider à atteindre un ou plusieurs objectifs. Travailler avec des tierces parties présente des risques qui doivent être identifiés, évalués et gérés par des processus appropriés de gouvernance, de gestion des risques et de contrôle, comme indiqué dans la présente Exigence thématique. Si une tierce partie manque à ses engagements contractuels, se comporte de façon non éthique ou connaît une interruption de ses activités, l'organisation principale peut en subir les répercussions. Les catégories et les exemples de risques liés à des tierces parties comprennent :

- Les risques stratégiques, comme la capacité à réaliser la mission principale et/ou les objectifs de haut niveau de l'organisation ou à gérer l'impact de fusions et acquisitions.
- Les risques réputationnels comme les dommages causés à l'environnement ou aux relations de l'organisation principale avec ses clients et ses parties prenantes et à leur confiance envers elle.
- Les risques éthiques, comme les manquements à l'intégrité, les conflits d'intérêts, les pots-de-vin et la corruption.
- Les risques opérationnels, tels que ceux menaçant la sécurité physique et celle de l'information, le risque d'initié, les perturbations de service et la non-réalisation des objectifs.
- Les risques financiers, tels que l'insolvabilité et la fraude des tierces parties.
- Les risques de non-conformité aux exigences réglementaires locales, nationales et internationales applicables.
- Les risques cyber et autres formes de menaces pesant sur les données, telles que la compromission et la fuite de données sensibles.
- Les risques associés aux technologies de l'information, comme le défaut de soutien aux opérations critiques.
- Le risque juridique, tel que les conflits d'intérêts, les différends et les litiges liés à des violations de contrat.
- Le développement non durable, notamment sur le plan environnemental, social et dans le domaine de la gouvernance. Il s'agit par exemple des risques liés à l'impact d'une organisation sur l'environnement naturel et des risques concernant ses interactions avec les communautés.
- Le risque géopolitique, comme les conflits/sanctions commerciaux et l'instabilité politique.

Le cycle de vie d'une tierce partie comprend la sélection, la contractualisation, l'intégration, le suivi et le désengagement. Les auditeurs internes doivent tenir compte de ces étapes lorsqu'ils évaluent les exigences relatives aux processus de gouvernance, de gestion des risques et de contrôle.

Évaluation et analyse des processus de gouvernance, de gestion des risques et de contrôle des tierces parties

Cette Exigence thématique offre une approche cohérente et complète pour évaluer la conception et la mise en œuvre des processus de gouvernance, de gestion des risques et de contrôle des tierces parties. Les exigences constituent une base a minima pour l'évaluation.

GOUVERNANCE

Exigences :

Les auditeurs internes doivent évaluer les aspects suivants de la gouvernance de l'organisation principale vis-à-vis des tierces parties, y compris la surveillance exercée par le conseil d'administration :

A. Une approche formelle est établie, mise en œuvre et examinée périodiquement pour déterminer s'il convient de passer un contrat avec une tierce partie. L'approche comprend des critères appropriés pour définir et évaluer les ressources nécessaires et disponibles afin d'atteindre les objectifs associés à la fourniture d'un produit ou d'un service.

B. Des politiques et des procédures sont établies pour définir, évaluer et gérer les relations et les risques avec les tierces parties tout au long de leur cycle de vie. Les politiques et procédures sont alignées avec les exigences réglementaires applicables et sont périodiquement examinées et mises à jour afin de renforcer l'environnement de contrôle.

C. Les rôles et responsabilités de l'organisation en matière de gestion des tierces parties sont définis et précisent qui sélectionne, dirige, gère, communique et suit les tierces parties et qui doit être informé de leurs activités. Un processus est en place afin de garantir que les personnes auxquelles sont attribués des rôles et responsabilités liés aux tierces parties disposent des compétences appropriées.

D. Des protocoles de communication avec les parties prenantes concernées sont définis et prévoient de rendre compte en temps utile de l'état des résultats, des risques et de la conformité (en particulier les violations des lois et règlements) des tierces parties prioritaires. Les tierces parties sont classées par ordre de priorité en fonction du risque. Les parties prenantes concernées peuvent être le conseil d'administration, la direction générale, les achats, les activités opérationnelles, la gestion des risques, la conformité, le service juridique, les technologies de l'information, la sécurité de l'information, les ressources humaines, etc.

GESTION DES RISQUES

Exigences :

Les auditeurs internes doivent évaluer les aspects suivants de la gestion des risques liés aux tierces parties au sein de l'organisation :

A. Les processus de gestion des risques liés aux tierces parties et à leurs services sont normalisés et complets, comprennent la définition des rôles et des responsabilités et prennent suffisamment en compte les principaux risques pertinents pour l'organisation (tels que les risques stratégiques, réputationnels, éthiques, opérationnels, financiers, de conformité, les risques cyber, de

technologie de l'information, juridiques, de développement non durable et géopolitiques). Le respect des processus est suivi et des actions correctives sont mises en œuvre en cas d'écart.

B. Les risques liés aux tierces parties tout au long du cycle de vie sont identifiés et évalués régulièrement. L'évaluation des risques est utilisée pour classer et hiérarchiser les tierces parties, y compris celles qui se trouvent en aval. Les réponses aux risques sont également classées et hiérarchisées. L'évaluation des risques est examinée et mise à jour périodiquement.

C. Les réponses aux risques sont adéquates et précises, proportionnées à leur classement. Les réponses aux risques sont mises en œuvre, examinées, approuvées, suivies, évaluées et ajustées si nécessaire.

D. Des processus sont en place pour gérer et, si nécessaire, porter à la connaissance de qui de droit, les problèmes liés aux tierces parties, assurant ainsi la prise en compte des résultats et augmentant la probabilité de respecter les termes des contrats ou autres accords. Si une tierce partie ne répond pas aux préoccupations remontées, des procédures sont en place pour permettre à la direction d'évaluer les risques liés à la poursuite de la relation commerciale et de prendre des mesures supplémentaires, de remédier à la situation ou de mettre fin à cette relation, si cela est justifié.

CONTRÔLES

Exigences :

Les auditeurs internes doivent évaluer les dispositifs de maîtrise suivants pour les tierces parties classées par ordre de priorité en fonction du risque qu'elles représentent. L'évaluation doit porter sur les processus d'évaluation et de contrôle en continu des tierces parties, mis en place par la direction de l'organisation :

A. Un processus solide de vérification préalable pour l'identification et la sélection des tierces parties est en place, avec une analyse de rentabilité documentée et approuvée ou tout autre document pertinent, décrivant et justifiant la nécessité et la nature d'une relation avec la tierce partie.

B. La contractualisation et l'approbation sont effectuées conformément aux politiques et procédures de gestion des risques liés aux tierces parties de l'organisation et intègrent la collaboration des entités concernées de l'organisation.

C. Les contrats ou accords définitifs sont examinés et approuvés par toutes les parties prenantes concernées, y compris les fonctions juridiques et de conformité, sont signés par les personnes autorisées des deux parties et conservés en toute sécurité. Chaque contrat est placé sous la responsabilité d'un gestionnaire ou d'un administrateur de contrat.

D. Une liste précise, complète et actualisée de toutes les relations avec des tierces parties est gérée, par exemple dans un système centralisé de gestion des contrats.

E. Des processus d'intégration documentés sont mis en place et suivis afin d'établir une base permettant aux tierces parties de respecter les termes du contrat ou de l'accord.

F. Des processus de suivi en continu permettent d'évaluer si les tierces parties respectent les termes du contrat ou de l'accord tout au long du cycle de vie et si elles s'acquittent de leurs obligations contractuelles. Les processus comprennent la vérification de la fiabilité des informations fournies et la réévaluation de la performance, de manière périodique et à chaque fois que l'accord est modifié.

G. Des protocoles sont établis pour les actions correctives à prendre quand une tierce partie ne répond pas aux attentes ou présente un risque accru ou inattendu. Les protocoles comprennent l'escalade des incidents en fonction de leur gravité, la réalisation de revues post-incidents et l'analyse des causes racines de ces incidents.

H. Les dates d'expiration et de renouvellement des contrats sont suivies et des mesures de renouvellement sont prises si nécessaire.

I. Un plan formalisé de sortie est mis en œuvre et suivi afin de garantir que les exigences contractuelles en termes de calendrier et d'attentes sont correctement prises en compte. Les processus incluent les modalités de :

- Mettre fin à la relation de la tierce partie.
- Remplacer la tierce partie si nécessaire.
- Réattribuer la garde et restituer ou détruire les données sensibles de l'organisation conservées chez la tierce partie.
- Supprimer l'accès de la tierce partie aux systèmes, outils et installations.

À propos de l'Institut des auditeurs internes

L'IIA est une association professionnelle internationale qui compte plus de 265 000 membres dans le monde et a délivré plus de 200 000 certifications Certified Internal Auditor® (CIA®) dans le monde entier. Fondée en 1941, l'IIA est reconnue dans le monde entier comme le leader de la profession d'audit interne en matière de normes, de certifications, d'éducation, de recherche et de conseils techniques. Pour plus d'informations, visitez le site theiia.org.

Droit d'auteur

Septembre 2025

The Institute of Internal Auditors

Siège mondial
The Institute of Internal Auditors
1035 Greenwood Blvd, Suite 401
Lake Mary, FL 32746, USA
Téléphone : +1-407-937-1111
Fax : +1-407-937-1101