Exigences thématiques relatives aux tiers

Public Consultation Draft

Le Cadre international des pratiques professionnelles (International Professional Practices Framework®) comprend les Normes internationales de l'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 constituent la base faisant autorité pour les pratiques requises.

Les Exigences Thématiques définissent des attentes claires pour les auditeurs internes en fixant un niveau de référence minimum pour l'audit de thèmes de risques spécifiques. Le profil de risque de l'organisation peut rendre nécessaire pour les auditeurs internes de prendre en compte d'autres aspects du sujet. La conformité aux Exigences Thématiques renforcera la cohérence des services d'audit interne et améliorera la qualité et la fiabilité des services et des résultats de l'audit interne. En fin de compte, les Exigences Thématiques réhaussent la profession d'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 services d'assurance et recommandée pour les services de conseil. L'Exigence Thématique est applicable lorsque le sujet est l'un des suivants :

A. L'objet d'une mission dans le plan d'audit interne.
B. Identifié lors de l'exécution d'une mission.
C. L'objet d'une demande de mission ne figurant 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 ne s'appliquent pas nécessairement à chaque mission ; si des exigences sont exclues, une justification doit être consignée dans la documentation 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 qui une organisation entretient une relation commerciale. Une relation avec un tiers peut être formalisée par un contrat, un accord ou d'autres moyens afin de fournir des produits ou des services à l'organisation. L'utilisation du terme "tiers” peut avoir des significations différentes selon le secteur d'activité ou d'autres contextes. Le présent guide utilise le terme "tiers" pour désigner les vendeurs ou les fournisseurs, les entrepreneurs ou les sous-traitants, les prestataires de services externalisés, les autres agences et les consultants, et inclut les accords entre un tiers et ses sous-traitants.

Cette exigence thématique n'a pas pour objectif de traiter des relations indirectes, des intérêts ou des implications avec l'organisation principale, tels que les employés, les partenaires financiers, les régulateurs, les agents ou les administrateurs.

Bien que l'organisation principale puisse faire appel à un tiers pour l'aider à atteindre un ou plusieurs de ses objectifs commerciaux, elle reste responsable des risques liés à la réalisation de ces objectifs. Si le contrat ou l'accord d'un tiers avec l'organisation lui permet de sous-traiter à un quatrième ou à d'autres parties, cette exigence thématique s'applique également pour assurer la gouvernance et la supervision de ces relations sous-traitées. Dans ces cas, les auditeurs internes doivent appliquer toutes les exigences indiquées par les résultats d'une évaluation des risques. Les exclusions doivent être documentées.

Travailler avec des tiers (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 un tiers ne respecte pas ses engagements contractuels, participe à des pratiques non éthiques ou connaît une interruption de ses activités, l'organisation principale peut subir des répercussions. Les catégories et exemples de risques liés aux tiers incluent :

- Opérationnels, tels que des interruptions de service ou la non-réalisation des objectifs commerciaux.
- Cybersécurité, comme la compromission de données sensibles.
- Financiers, tels que l'insolvabilité d'un fournisseur.
- Conformité aux exigences réglementaires locales, nationales et internationales applicables.
- Juridique, tel que les conflits d'intérêts, les différends et les litiges liés aux violations de contrat.
- Réputationnel, tel que les dommages causés à l'environnement ou aux clients, consommateurs ou parties prenantes de l'organisation principale.

Le cycle de vie des tiers comprend la sélection, la contractualisation, l'intégration, la surveillance et la cessation d'activité. Les auditeurs internes doivent tenir compte de ces phases lors de l'évaluation des 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 tiers

Cette exigence thématique offre une approche cohérente et complète pour évaluer la conception et de la mise en œuvre des processus de gouvernance, de gestion des risques et de contrôle des tiers. Les exigences représentent un seuil minimal pour cette évaluation dans une organisation.

Gouvernance : Évaluation et analyse de la gouvernance des tiers

Exigences :

Les auditeurs internes doivent évaluer les aspects suivants de la gouvernance des tiers au sein de l'organisation, y compris la supervision du conseil d'administration :

A. Une approche formelle est établie, mise en œuvre et régulièrement revue pour déterminer s'il convient de contracter avec un tiers afin d'aider à atteindre un objectif commercial en fournissant un produit ou un service. L'approche comprend des critères appropriés pour définir et évaluer les ressources disponibles pour atteindre les objectifs.

B. Des politiques, des procédures et des processus sont établis pour définir, évaluer et gérer les relations et les risques avec les tiers tout au long de leur cycle de vie. Les politiques, procédures et processus sont alignés avec les exigences réglementaires applicables et sont régulièrement revus et mis à jour pour renforcer l'environnement de contrôle.

C. Les rôles et responsabilités en matière de gestion des tiers au sein de l'organisation sont définis, en précisant qui sélectionne, dirige, gère, communique avec et contrôle les tiers, et qui doit être informé des activités des tiers. Un processus existe pour garantir que les individus affectés aux rôles et responsabilités liés aux tiers possèdent les connaissances, compétences et capacités appropriées.

D. Les protocoles de communication avec les parties prenantes concernées sont définis et incluent la communication de l'état de la performance, des risques et de la conformité des tiers prioritaires. Les parties prenantes concernées peuvent inclure le conseil d'administration, la direction générale, les opérations, la gestion des risques, les ressources humaines, la sécurité de l'information, les services juridiques, la conformité, les achats et autres, etc.

GESTION DES RISQUES : Évaluation et évaluation de la gestion des risques liés aux tiers

Exigences :

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

A. Les processus de gestion des risques pour les tiers sont normalisés et complets, comprennent des rôles et des responsabilités définis et abordent de manière suffisante les principaux risques (financiers, opérationnels, stratégiques, cybersécurité, conformité, réputationnels, éthiques, durabilité, géopolitiques et juridiques). Le respect des processus est suivi et des actions correctives sont mises en œuvre en cas de déviation.

B. Les risques liés aux tiers tout au long du cycle de vie sont identifiés et évalués. L'évaluation des risques est utilisée pour classer et hiérarchiser les tiers et pour prioriser les réponses aux risques. L'évaluation est revue et mise à jour périodiquement.

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

D. Des processus sont en place pour gérer et, si nécessaire, escalader les problèmes liés aux tiers, en assurant la responsabilité des résultats et en augmentant la probabilité de respecter les termes des contrats ou autres accords. Si un tiers ne répond pas aux préoccupations escaladées, des processus sont en place pour la remédiation, y compris la résiliation si nécessaire. pouvant aller jusqu'à la résiliation.

CONTRÔLES : Évaluation des processus de contrôle des tiers

Exigences :

Les auditeurs internes doivent évaluer les contrôles suivants pour les tiers prioritaires, y compris les processus de la direction pour l'évaluation et la surveillance continues des tiers de l'organisation :

A. Un dossier d'affaires documentée et approuvée ou tout autre document pertinent décrit et justifie la nécessité et la nature de la relation avec un tiers.

B. Un processus de diligence raisonnable solide pour la recherche et la sélection des tiers est en place. Le processus comprend des critères pour des aspects importants, tels que la révision des protocoles de cybersécurité, le contrôle des antécédents financiers et la vérification des coordonnées bancaires.

C. La passation et l'approbation des marchés sont effectuées conformément aux politiques, procédures et processus de gestion des risques liés aux tiers de l'organisation et comprennent une collaboration avec les services appropriés de l'organisation.

D. Les contrats ou accords définitifs sont examinés et approuvés par toutes les parties prenantes concernées, y compris le service juridique et le service de la conformité le cas échéant ; ils sont signés par les personnes autorisées des deux parties et conservés en toute sécurité. Tous les contrats sont attribués à un gestionnaire de contrat ou à un administrateur qui en assume la responsabilité.

E. Une liste précise, complète et actualisée de toutes les relations avec des tiers est maintenue à jour, par exemple dans un système centralisé de gestion des contrats.

F. Des processus documentés d'intégration sont établis et suivis pour permettre aux tiers de respecter les termes du contrat ou de l'accord.

G. Des processus de contrôle permanent existent pour évaluer si les tiers prioritaires respectent les termes du contrat ou de l'accord tout au long du cycle de vie et s'ils s'acquittent de leurs obligations contractuelles. Les processus comprennent la vérification de la fiabilité des informations fournies et la réévaluation des performances à intervalles réguliers ainsi qu'à chaque modification de l'accord.

H. Des protocoles sont établis pour initier des actions correctives si un tiers 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 profondes des incidents.

I. Les dates de renouvellement des contrats sont surveillées et des mesures de renouvellement sont prises si nécessaire.

J. Pour les tiers prioritaires, un plan formalisé de désengagement est mis en œuvre et suivi. Les processus incluent la manière de :
   - Mettre fin à l'activité du tiers.
   - Remplacer le tiers si nécessaire.
   - Réattribuer la garde et renvoyer ou détruire les données sensibles de l'organisation qui sont stockées
     Chez les tiers
   - Révoquer l'accès du tiers aux systèmes, outils et installations.

À propos de l'Institut des auditeurs internes

L'Institut des auditeurs internes (IIA) est une association professionnelle internationale qui compte plus de 260.000 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, consultez le site www.theiia.org.

Avertissement

L'IIA publie ce document à des fins informatives et éducatives. Ce matériel n'est pas destiné à fournir des réponses définitives à des circonstances individuelles spécifiques et doit donc être utilisé uniquement comme un guide. L'IIA recommande de consulter un expert indépendant pour toute situation spécifique. L'IIA décline toute responsabilité envers toute personne qui placerait une confiance exclusive dans ce matériel.

Droit d'auteur

Février 2025

