AUDIT INTERNE

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Relations de l'audit interne avec les autres fonctions d'Assurance

Modèle d'interaction

Traduit et adapté par :

FUNDACIÓN MAPFRE

AUDIT INTERNE

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Relations de l'audit interne avec les autres fonctions d'Assurance

Modèle d'interaction

FUNDACIÓN MAPFRE

Instituto de Auditores Internos de España

Traduit et adapté par :

ifaci
institut français de l'audit et du contrôle internes

This article was reprinted with permission from the Marco de Relaciones de Auditoria Interna con otras Funciones de Aseguramiento, published by Instituto de Auditores Internos de España – La fábrica de pensamiento, and has been translated from Spanish to French.

Copyright © 2013 by Instituto de Auditores Internos de España – La fábrica de pensamiento. No parts of this material may be reproduced in any form without the written permission of COSO.

Permission has been obtained from the copyright holder, Instituto de Auditores Internos de España, C.I.F. G-78253176, C/ Danta Cruz de Marcenado, 33 1°, registration n° 55.432, Spain, to publish this translation, which is the same in all material respects, as the original unless approved as changed. No parts of this document may be reproduced, stored in any retrieval system, or transmitted in any form, or by any means electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of The IIA Spain.

This document was translated by IIA France (IFACI – Institut France de l'Audit et du Contrôle Internes) on May 2014.

ISBN : 978-2-915042-64-1

Dans ce cadre, l'*Instituto de Ciencias del Seguro* de la *FUNDACIÓN MAPFRE* développe et encourage des activités d'éducation et de recherche dans les domaines de l'assurance et de la gestion des risques. Entre autres, l'Institut élabore périodiquement des rapports et publie des ouvrages sur l'assurance et la gestion des risques, dans le but de contribuer à une meilleure connaissance de ces thématiques.
Ces ouvrages peuvent servir de référence à des novices dans le monde de l'assurance ou comme source d'information pour l'approfondissement de thèmes spécifiques. C'est dans ce contexte que s'inscrit le soutien accordé à la publication de ce guide pratique, intitulé *Relations de l'audit interne avec les autres fonctions d'assurance*, et publié par la *FÁBRICA DE PENSAMIENTO, think tank* de l'*Instituto de Auditores Internos de España* (Institut des Auditeurs internes d'Espagne).
La *FUNDACIÓN MAPFRE* propose également des formations dont certaines sont réalisées en collaboration avec l'*Universidad Pontificia de Salamanca*. L'Institut favorise les aides à la recherche dans les domaines scientifiques du risque et de l'assurance. Il dispose en outre d'un Centre de documentation spécialisé dans les assurances et la gestion des risques qui soutient ses activités. Pour plus d'information : www.fundacionmapfre.org\cienciasdelseguro.

La *FÁBRICA DE PENSAMIENTO* de l'*Instituto de Auditores Internos de España* a publié le présent guide pratique, intitulé *Marco de Relaciones de Auditoria Interna con otras Funciones de Aseguramiento* pour répondre aux attentes des auditeurs internes et des lecteurs qui, indépendamment de leur position hiérarchique dans l'organisation, souhaitent acquérir une vision claire des différentes formes de prestations d'assurance.

Ce guide montre que l'existence de cartographies de prestataires de services d'assurance améliore la coordination des différentes lignes de maîtrise, assure l'optimisation des ressources de l'organisation, et permet de donner un niveau d'assurance approprié à la direction générale et au Conseil.

Ce document complète et renforce le modèle des « trois lignes de maîtrise », qui définit d'audit interne comme fonction d'évaluation de l'efficacité de la deuxième ligne, et de coordination de l'ensemble des prestataires internes d'assurance pour répondre à l'impératif d'efficience.

Je félicite les auteurs, membres de la commission technique, pour avoir maintenu le niveau d'excellence auquel les publications de la *FÁBRICA DE PENSAMIENTO* nous ont habitués. Au nom de l'*Instituto de Auditores Internos de España,* je remercie sincèrement la *FUNDACIÓN MAPFRE* pour son parrainage.

José Manuel Muries
Président de l'*Instituto de Auditores Internos de España*

L'Institut Français de l'Audit et du Contrôle Interne (IFACI) favorise la diffusion des normes internationales de l'audit interne et des meilleures pratiques contribuant à l'amélioration des dispositifs de gouvernance, de gestion des risques et de contrôle interne.

L'IFACI est affilié à *The Institute of Internal Auditors* (The IIA) et participe activement aux initiatives de l'ECIIA (*European Confederation of Institutes of Internal Auditing)*. La traduction de cette publication illustre la coopération entre les instituts du réseau de l'IIA. Le choix de cette thématique n'est pas anodin tant la question de la coordination des fonctions d'assurance et du rôle de l'audit interne est cruciale pour l'efficacité d'un système intégré de gestion des risques. Avec une approche très pragmatique, ces travaux s'insèrent naturellement dans la série de publications proposées par l'IIA et l'IFACI sur le même thème.

Le réseau de l'IIA est riche de multiples compétences et produit des livrables d'une grande qualité sur lesquels l'IFACI doit capitaliser. Ces travaux complètent ceux que nous conduisons et nous permettent de mieux répondre aux attentes de la profession et d'anticiper ses besoins. Nous poursuivrons donc à l'avenir la mise à disposition de ressources publiées au sein du réseau, notamment en Europe. Je remercie tout particulièrement les auteurs de la *FÁBRICA DE PENSAMIENTO* pour le présent document et les réviseurs réunis par l'IFACI pour son adaptation.

Philippe Mocquard
Délégué Général de l'IFACI

Auteurs

MEMBRES DE LA COMMISSION TECHNIQUE DE L'IIA ESPAGNE

COORDINATION : **Óscar del Olmo, CIA, CRMA, CFE.** IBERDROLA
Paz Argamentería, CRMA. INVERSIS
Francisco José Narváez. GRUPO FUERTES
Yolanda Cortés, CIA, CRMA. VOCENTO
Lucila Carnicero. DELOITTE
Eduardo Cuesta, CISA, CISM. MAPFRE
Angel Juárez. BDO
José Ignacio Domínguez, CRMA, ROAC
José Luis Solís, ROAC, CRMA, TEC. EY
Rafael Muriel. LIBERBANK
Mónica Albadalejo, CIA, CRMA. BANCO ESPIRITO SANTO

TRADUCTION ET ADAPTATION EN FRANÇAIS

Marie-Elisabeth ALBERT, CIA
Julien CORNUCHE, CIA
Benoît HAREL, CIA, CRMA
Béatrice KI-ZERBO, CIA
Yann LE BOURTHE, CIA
Jacques RENARD

Table des matières

Introduction 06

Objectif et étendue des travaux de la commission 09

Recensement des fonctions d'assurance 10

Conditions nécessaires à l'efficacité d'une fonction d'assurance 11

Procédures d'audit interne relatives à l'efficacité des autres fonctions d'assurance 12

Périmètre et rôle de l'audit interne par rapport aux autres fonctions d'assurance 14

Pistes pour une collaboration efficiente entre l'audit interne et les autres fonctions d'assurance. Cartographie des services d'assurance 15

Glossaire 18

Annexes 20

- Annexe 1. Contrôle interne 20
- Annexe 2. Contrôle interne relatif au reporting financier 22
- Annexe 3. Sécurité des systèmes d'information 24
- Annexe 4. Sécurité physique des actifs et des personnes 26
- Annexe 5. Conformité réglementaire 28
- Annexe 6. Gestion des risques 30
- Annexe 7. Système de management intégré 32
- Annexe 8. Responsabilité sociale et réputation de l'entreprise 34

Introduction

Toute fonction se doit d'optimiser l'utilisation de ses ressources. Il en est de même pour l'audit interne qui doit par ailleurs veiller à maintenir un niveau approprié d'assurance.

Nous avons créé, au sein de l'*Instituto de Auditores Internos de España,* une série de commissions techniques chargées de développer des prises de position qui clarifient le positionnement des auditeurs internes et les aident à analyser les enjeux stratégiques futurs. Le présent guide pratique s'inscrit dans ce contexte.

La crise renforce la nécessité d'améliorer l'utilisation efficiente des ressources. L'audit interne n'y fait pas exception et doit également veiller à maintenir un niveau approprié d'assurance. Pour atteindre cet objectif, il lui faut coordonner son activité avec les autres fonctions d'assurance de l'organisation, et tirer parti des travaux existants.

Ce guide propose une synthèse de différentes publications sur ce thème et des retours d'expérience des membres de la commission technique.

Selon les Normes internationales pour la pratique professionnelle de l'audit interne : « Afin d'assurer une couverture adéquate et d'éviter les doubles emplois, le responsable de l'audit interne devrait partager des informations et coordonner les activités avec les autres prestataires internes et externes d'assurance et de conseil. » (cf. Norme 2050 – Coordination).

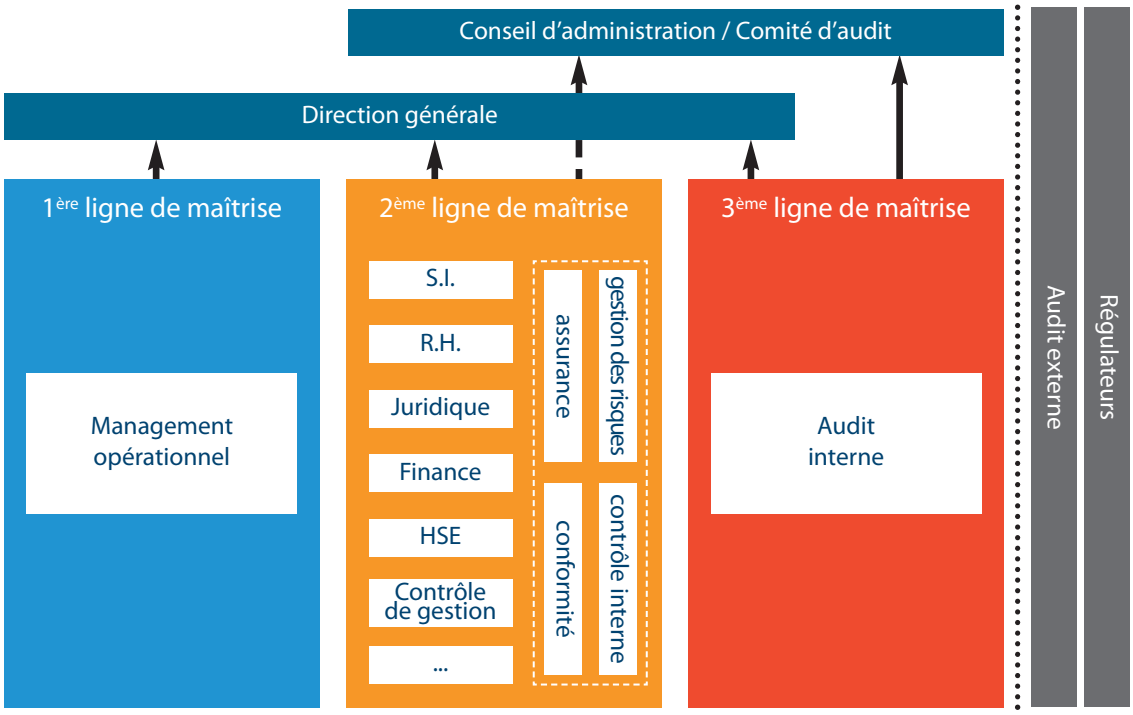
Le Cadre de référence international des pratiques professionnelles de l'audit interne de l'*Institute of Internal Auditors* (IIA) propose un ensemble de lignes directrices (modalités pratiques d'application, guides pratiques, prises de position) qui précisent et facilitent la mise en œuvre de la Norme 2050. Selon la modalité pratique d'application 2050-3 : « Pour fournir au Conseil une assurance concernant la gouvernance, le management des risques et le contrôle interne, l'auditeur interne peut s'appuyer sur les travaux d'autres prestataires internes ou externes de services d'assurance ou utiliser leurs travaux. ». D'autres documents complètent cette MPA :

- Modalités pratiques d'application : 2050-1 Coordination ; 2050-2 Cartographie des services donnant une assurance sur les dispositifs de contrôle et de management des risques.
- Guide pratique : *Reliance by Internal Audit on Other Assurances providers*, décembre 2011.
- Guide pratique : *Coordinating risk management and assurance,* mars 2012.
- Prise de position : *Les trois lignes de maîtrise pour une gestion des risques et un contrôle efficaces,* janvier 2013. Afin de positionner l'audit interne au sein de l'organisation, le présent guide utilise comme référence le modèle des trois lignes de maîtrise proposé et développé par l'IIA.

Commentaire IFACI

D'autres documents complètent ces références :

- Position Paper – Corporate Governance Insights, 2012, ECIIA
- Prise de Position – L'urbanisme du contrôle interne, 2008, IFACI
- Prise de position – Trois lignes de maîtrise pour une meilleure performance, 2013, IFACI / AMRAE



DÉFINITION DES ACTIVITÉS D'ASSURANCE

Les Normes définissent les activités d'assurance comme l'« examen objectif d'éléments probants, effectué en vue de fournir à l'organisation une évaluation indépendante des processus de gouvernement d'entreprise, de management des risques et de contrôle. »

Selon la prise de position « *Les trois lignes de maîtrise pour une gestion des risques et un contrôle efficaces* », les fonctions de gestion des risques et de conformité qui composent la deuxième ligne de maîtrise s'assurent de la conception et du fonctionnement efficace de la première ligne de maîtrise. Dans ce modèle, les fonctions de la deuxième ligne peuvent intervenir directement sur le développement des dispositifs de gestion des risques et de contrôle interne. Néanmoins, elles ne peuvent en aucun cas offrir aux organes de gouvernance une assurance indépendante concernant l'efficacité des dispositifs de gestion des risques et de contrôle interne. L'assurance indépendante est du ressort de la troisième ligne de maîtrise, l'audit interne.

CLASSIFICATION DES PRESTATAIRES DE SERVICES D'ASSURANCE

Le bon fonctionnement et la coordination des relations de l'audit interne avec les autres fonctions d'assurance présentent des avantages.

Tout service d'assurance implique trois catégories de parties prenantes :

- les personnes chargées des opérations, de l'exécution du processus, du fonctionnement du système, etc., et celles chargées de la supervision : gestion des risques, conformité, etc. ;
- les personnes chargées de l'évaluation : le prestataire de services d'assurance ;
- les utilisateurs de l'évaluation, qu'ils soient internes (direction générale ou Conseil) ou externes.

Il existe trois types de prestataires, classés selon le bénéficiaire des services d'assurance, leur niveau d'indépendance par rapport à réalisation des activités évaluées, et la robustesse de leur conclusion :

a) **Les prestataires internes qui rendent compte à la direction générale** et/ou en font partie : personnes chargées de l'auto-évaluation du contrôle, auditeurs QESH (qualité, environnement, sécurité, hygiène), gestionnaires des risques, fonctions relatives à l'évaluation du gouvernement d'entreprise, au reporting financier, à la conformité, etc..

b) **Les prestataires qui rendent compte au Conseil,** parmi lesquels l'audit interne.

c) **Les prestataires qui rendent compte aux parties prenantes externes** tels que l'auditeur externe qui informe les actionnaires.

S'APPUYER SUR LES INFORMATIONS DES TIERS

La décision de s'appuyer sur les travaux d'autres prestataires de services répond à plusieurs objectifs :

- couvrir des domaines pour lesquels l'audit interne ne disposent pas des compétences nécessaires ;
- transmettre des connaissances ;
- améliorer la couverture des risques au-delà du plan d'audit interne ;
- éviter les doubles emplois et créer des synergies en termes d'utilisation et d'optimisation des ressources.

Le bon fonctionnement et la coordination des relations de l'audit interne avec les autres fonctions d'assurance présentent notamment les avantages suivants :

- élargissement de la couverture des risques, sans augmentation du temps consacré à la mission d'audit interne ;
- augmentation de la réactivité des dispositifs de gestion des risques ;
- amélioration du niveau d'assurance par la mobilisation de l'expertise appropriée ;
- limitation du phénomène de saturation ;
- efficience accrue par l'élimination des doubles emplois ;
- conformité renforcée grâce aux efforts conjoints.

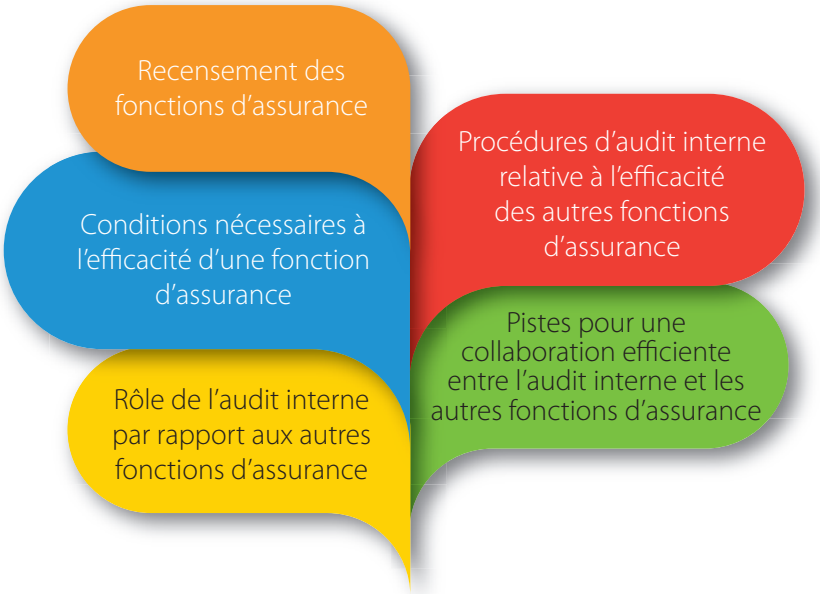
S'appuyer sur les autres prestataires comporte également des risques, tels que :

- les déficiences du contrôle, liées au fait que le périmètre couvert par le prestataire est insuffisant ;
- l'absence d'identification des problèmes, due au manque d'indépendance du prestataire ;
- l'accroissement des risques jugés non significatifs ou leur analyse hors contexte par l'audit interne.

Objectif et étendue des travaux de la commission

Nous avons élaboré un guide pratique des relations entre l'audit interne et les autres fonctions d'assurance interne qui permet :

- **de procéder au recensement** (non exhaustif) **des fonctions d'assurance ;**
- **d'identifier les conditions nécessaires à l'efficacité d'une fonction d'assurance ;**
- **d'élaborer des procédures d'audit interne relatives à l'efficacité** des autres fonctions d'assurance ;
- **de définir le rôle de l'audit interne par rapport aux autres fonctions d'assurance, les « lignes jaunes » à ne pas franchir ainsi que les domaines exclusifs d'intervention** de l'audit interne.
- **d'envisager des pistes pour une collaboration efficiente entre l'audit interne et les autres fonctions d'assurance,** qui renforcent les principales normes d'assurance et l'efficacité, et évitent les doubles emplois.



Recensement des fonctions d'assurance

Seules sont abordées les fonctions internes qui rendent compte à la direction générale ou au Conseil.

Il est très complexe d'élaborer un modèle organisationnel unique concernant les prestataires internes de services d'assurance. Cela dépend de leur degré de maturité, du secteur d'activité et du contexte. Nous considérons néanmoins qu'indépendamment de la question de la fonction responsable de la prestation d'assurance, il existe un ensemble d'activités qui doivent être réalisées et par conséquent être intégrées dans le cadre des « organisations ou fonctions internes ».

En particulier, nous avons identifié les activités et fonctions d'assurance suivantes, en lien avec les domaines suivants :

1. **Contrôle interne :** assurance portant sur le contrôle interne de l'entreprise. Il englobe les objectifs opérationnels, de conformité et de reporting.
2. **Contrôle interne relatif au reporting financier :** assurance portant sur le système de contrôle interne des processus d'élaboration du reporting financier.
3. **Sécurité des systèmes d'information :** assurance portant sur l'infrastructure technique et garantissant la confidentialité, l'intégrité et la disponibilité de l'information.
4. **Sécurité physique des actifs et des personnes :** assurance portant sur l'intégrité des actifs et des personnes, et garante de la continuité des activités[1].
5. **Conformité réglementaire :** assurance portant sur la conformité à des obligations concernant notamment la protection des données personnelles, la lutte contre le blanchiment et le financement du terrorisme, le règlement général de l'autorité des marchés financiers, des codes de déontologie, la responsabilité pénale des entreprises et des dirigeants ou des directives sectorielles spécifiques.
6. **Gestion des risques :** assurance portant sur la gestion adéquate des risques susceptibles d'affecter de manière significative les activités de l'entreprise.
7. **Système de management intégré :** assurance portant sur la conformité à la réglementation en matière de qualité, d'environnement, de prévention des risques professionnels, et de recherche, développement et innovation (RDI).
8. **Responsabilité sociale et réputation de l'entreprise :** assurance portant sur la transparence des activités de l'entreprise et des relations avec les parties prenantes.

[1] *Les nouvelles lois et les bonnes pratiques en matière de sécurité s'orientent vers une gestion intégrée et coordonnée de la sécurité, en mettant l'accent, non pas sur la protection physique ou logique d'un domaine spécifique, mais plutôt sur la protection globale d'un actif.*

Conditions nécessaires à l'efficacité d'une fonction d'assurance

Selon le Guide pratique de l'IIA, *Reliance by Internal Audit on other assurance providers,* paru en décembre 2011, les principes et éléments permettant d'évaluer les travaux des prestataires d'assurance interne et de déterminer leur fiabilité sont les suivants :

1. **Objectif de la mission :** l'objectif de la mission des prestataires d'assurance doit être précisé et être clair et pertinent au regard du périmètre et des objectifs de la mission d'audit interne.
2. **Objectivité du prestataire de services :** les prestataires d'assurance doivent démontrer leur impartialité et leur objectivité.
3. **Compétences techniques :** l'évaluation dépend de l'expérience et de l'expertise du prestataire. Ce principe est d'autant plus important que le prestataire n'est pas indépendant.
4. **Pratiques et méthodologies :** l'existence de politiques, procédures et programmes utilisés dans la réalisation de leur mission doit être évaluée. Les travaux doivent être planifiés, supervisés, documentés et examinés de manière satisfaisante, et être étayés par des éléments probants et suffisants. L'accès aux informations nécessaires pour émettre les conclusions est effectif.
5. **Communication des résultats et mesures correctives :** des procédures de communication des résultats des missions d'assurance à la direction sont en place, avec pour objectif l'adoption de mesures correctives et un suivi de leur mise en œuvre.

Procédures d'audit interne relatives à l'efficacité des autres fonctions d'assurance

La décision de s'appuyer sur le travail d'autres fonctions d'assurance doit être fondée sur une évaluation préalable de l'audit interne. Le bien-fondé de cette décision repose sur quatre facteurs :

1. **Objectivité de la fonction d'assurance par rapport à l'activité supervisée :**
   a. chaîne de responsabilité et niveau hiérarchique auquel est subordonnée la fonction d'assurance ;
   b. niveau d'indépendance dans la détermination des programmes de travail et dans l'accès aux éléments probants;
   c. politiques et pratiques permettant d'éviter des conflits d'intérêts dans le cas où certains membres de la fonction d'assurance auraient auparavant occupé des responsabilités opérationnelles.

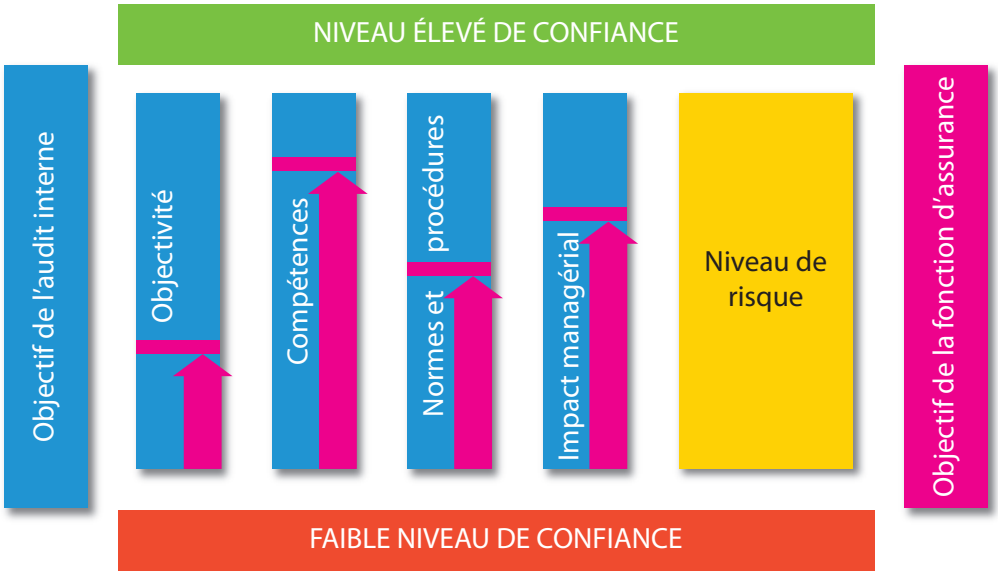
2. **Compétences professionnelles des membres de la fonction d'assurance :**
   a. formation et expérience professionnelle des membres de la fonction d'assurance ;
   b. obtention de certificats professionnels et programmes de formation continue.

3. **Existence de politiques, de procédures et de programmes écrits relatifs à l'exercice des fonctions d'assurance :**
   a. existence de politiques, de procédures et de programmes pour l'exercice de l'activité d'assurance ;
   b. procédures internes garantissant la qualité des documents de travail, des rapports et des recommandations ; existence de supports documentaires de conclusions fondées sur des éléments probants et sur le suivi des recommandations ;
   c. procédures de supervision et d'examen des activités des collaborateurs de la fonction ; évaluation annuelle de l'activité du personnel.

4. **Production de rapports comprenant des conclusions et des recommandations qui sont suivies jusqu'à leur mise en œuvre :**
   a. existence de procédures de communication des résultats des missions d'assurance à la direction afin que les mesures correctives soient prises ;
   b. existence de procédures de suivi des recommandations émises et des mesures adoptées pour pallier les défaillances.

Enfin, l'audit interne doit mettre en œuvre ses propres procédures d'analyse et de révision de ces travaux, afin de disposer de preuves concernant la qualité et la rigueur de ces activités d'assurance.

Afin de garantir la performance et la qualité de l'activité d'audit interne, il est nécessaire de procéder à des évaluations périodiques, tant internes qu'externes, comme le souligne la Norme 1300, *Programme d'assurance et d'amélioration qualité*, contenue dans le *Cadre de référence international des pratiques professionnelles de l'audit interne*.



Afin de garantir la qualité de l'activité d'audit interne, il est nécessaire de procéder à des évaluations périodiques, tant internes qu'externes.

Schéma : Facteurs à prendre en compte dans la détermination du niveau de confiance
Adapté à partir du Guide pratique de l'IIA, Reliance by internal audit on other assurance providers

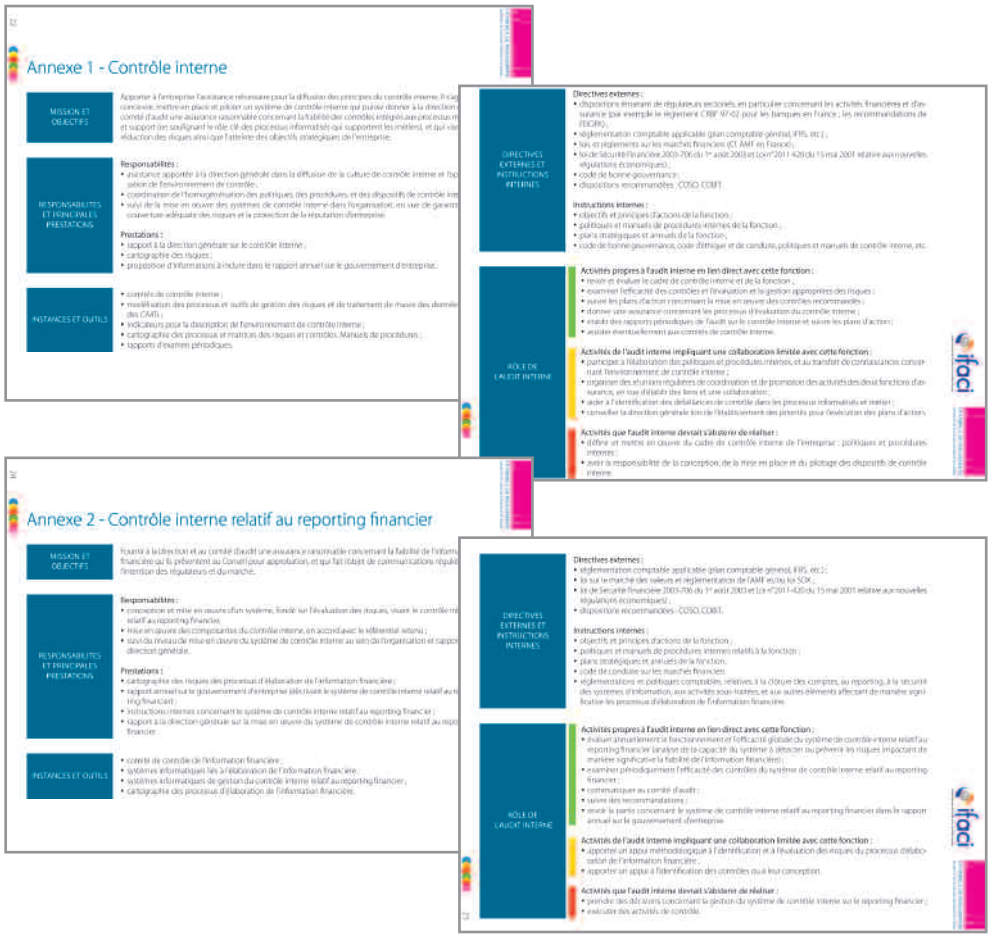
Plus les **objectifs** des prestataires (internes et externes) sont alignés avec ceux de l'audit interne, plus les auditeurs internes trouveront que les travaux des prestataires d'assurance sont pertinents.
Le niveau de confiance accordé à ces travaux variera selon les 4 éléments présentés dans le schéma ci-dessus. Malgré une indépendance moindre que celle de l'audit interne (notamment du fait de leur rattachement hiérarchique), les fonctions d'assurance peuvent faire preuve **d'objectivité**.

Cette faiblesse peut être partiellement compensée par le niveau de **compétence**, le recours à des **procédures** ou à des **normes** rigoureuses permettant d'étayer en temps opportun les constats ainsi que la capacité à avoir un **impact** sur la management du fait d'une plus grande proximité ou d'une réactivité facilitée par la surveillance en continu des risques et la mise en œuvre des mesures de traitement.

Périmètre et rôle de l'audit interne par rapport aux autres fonctions d'assurance

Il est fréquent que certaines activités réalisées par d'autres fonctions d'assurance soient redondantes, et même qu'elles relèvent du périmètre de l'audit interne, ou inversement. Il peut également arriver que l'on confonde le rôle de l'audit interne avec celui des autres fonctions d'assurance.

Afin de contribuer à clarifier le rôle et le périmètre de l'audit interne par rapport à chacune des autres fonctions d'assurance, nous proposons une série d'annexes qui décrivent les activités qui relèvent de l'audit interne et qui ne doivent pas être réalisées par des tiers, et des limites que ne doit pas franchir l'audit interne (pages 22 à 37).


Annexe 1 - Contrôle interne

MISSION ET OBJECTIFS

RESPONSABILITÉS ET PRINCIPALES PRESTATIONS

INSTANCES ET OUTILS

DIRECTIVES EXTERNES ET INSTRUCTIONS INTERNES

RÔLE DE L'AUDIT INTERNE

Annexe 2 - Contrôle interne relatif au reporting financier

MISSION ET OBJECTIFS

RESPONSABILITÉS ET PRINCIPALES PRESTATIONS

INSTANCES ET OUTILS

DIRECTIVES EXTERNES ET INSTRUCTIONS INTERNES

RÔLE DE L'AUDIT INTERNE

Traduction et adaptation - IFACI

Pistes pour une collaboration efficiente entre l'audit interne et les autres fonctions d'assurance. Cartographie des services d'assurance

L'une des principales responsabilités du Conseil est de s'assurer que les processus sont mis en œuvre conformément aux critères définis pour l'atteinte des objectifs. Pour ce faire, le Conseil dispose de plusieurs sources de prestation d'assurance mais elles peuvent laisser des zones de risques non couvertes ? Il est donc nécessaire de savoir si les processus de gestion des risques fonctionnent efficacement, et si les risques principaux ou critiques encourus par l'entreprise sont ramenés à un niveau acceptable.

L'élaboration d'une **cartographie des services d'assurance** constitue une bonne représentation de la coordination des différentes activités d'assurance en permettant de visualiser l'effort commun et de réduire les risques.

Nous proposons que la cartographie des services d'assurance soit réalisée par l'audit interne, puisque c'est sur lui que repose la compréhension des exigences d'assurance du Conseil et la définition des rôles et du niveau d'assurance. L'objectif principal d'une cartographie des services d'assurance est, en premier lieu, de présenter au Conseil et à la direction générale, à un instant donné, le niveau d'assurance global par rapport aux principaux risques susceptibles d'affecter l'entreprise. Il s'agit, en deuxième lieu, d'identifier la fonction prestataire d'assurance et, enfin, d'évaluer les risques par catégorie en fonction du niveau d'assurance fourni.

Ces informations peuvent constituer la base à partir de laquelle l'audit interne oriente son plan annuel vers les domaines de risques dont le niveau d'assurance ne semble pas approprié.

L'audit interne détermine les activités selon la cartographie des services d'assurance ainsi élaborée, et met l'accent sur les risques présentant un déficit de supervision.

Processus d'élaboration de la cartographie des services d'assurance

L'élaboration de la cartographie des services d'assurance se décompose en trois étapes :

- **Étape 1 : Identification des processus ou activités pertinents de l'entreprise,** afin de garantir l'intégrité de la cartographie des services d'assurance. Une « **cartographie des processus** » est élaborée en identifiant pour chacun d'entre eux le responsable de l'activité, et la fonction d'assurance exercée par le deuxième niveau de contrôle.
- **Étape 2 : Identification des risques portant sur les processus ou activités.** L'objectif est d'associer aux processus correspondants les principaux risques auxquels est confrontée l'entreprise et qui ont été identifiés dans le modèle des risques.

  C'est à cette étape que sont intégrés les critères (limites ou indicateurs) permettant de mesurer les risques par rapport à la valeur souhaitable. Ces critères sont déterminés en fonction de l'appétence pour le risque et de la tolérance au risque tels que définis par le Conseil[2].
- **Étape 3 : Identifions des fonctions qui donnent une assurance sur chacun des risques. Evaluation du niveau d'assurance fourni par chaque fonction en lien avec chacun des risques sous sa supervision. Tout ceci constitue la « cartographie des services d'assurance ».**

  L'audit interne, selon la cartographie des services d'assurance ainsi élaborée, détermine les activités sur lesquelles pèsent des risques présentant un déficit de supervision, que cette dernière soit absente ou insuffisante.

1 ÉLABORATION DE LA CARTOGRAPHIE DES PROCESSUS

2 ASSOCIATION DES RISQUES AUX PROCESSUS

3 ÉLABORATION DE LA CARTOGRAPHIE DES SERVICES D'ASSURANCE

[1] *Voir le document de LA FÁBRICA DE PENSAMIENTO sur la définition et la mise en œuvre de l'appétence pour le risque : Definición e implantación de Apetito de Riesgo.*

EXEMPLE DE CARTOGRAPHIE DES SERVICES D'ASSURANCE

Catégorie de risques	RISQUE		2e LIGNE DE MAÎTRISE								3e LIGNE DE MAÎTRISE
	Intitulé	Description	Contrôle interne	Contrôle relatif au reporting financier	Sécurité des systèmes d'information	Sécurité physique des actifs	Conformité réglemen-taire	Gestion des risques	Système de mana-gement intégré	RSE et réputation	Audit interne
Stratégiques											
Opérationnels											
Conformité											
Reporting											

Le niveau d'assurance, ainsi que l'activité fournissant l'assurance, seraient indiqués de différentes couleurs dans les cellules où se recoupent le risque et la fonction

Glossaire

ABE
Autorité Bancaire Européenne (autorité indépendante de l'Union Européenne qui œuvre afin de garantir un niveau de règlementation et de surveillance prudentielles efficace et cohérent dans l'ensemble du secteur bancaire européen)

ACPR (ou tout autre organe de supervision de banque et de l'assurance)
Autorité de Contrôle Prudentiel et de Résolution

AEMF
Autorité Européenne des Marchés Financiers

AMF
Autorité des Marchés Financiers en France ou tout autre régulateur jouant le rôle de commission nationale régulant les marchés de valeurs

CAAT
Computer Assisted Auditing Techniques (Techniques d'audit assistées par ordinateur, TAAO)

CEI
Commission électrotechnique internationale

COBIT
Control Objectives for Information and Related Technology. Référentiel relative aux SI publié par l'ISACA (www.isaca.org)

COSO
Committee of Sponsoring Organizations of the Treadway. Commission a notamment produit des référentiels sur le contrôle interne et la gestion des risques

CRBF 97-02
Règlement n°97-02 du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement

Directive européenne 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques

EBA
European Banking Authority (Autorité bancaire européenne, ABE)

EFQM
European Foundation for Quality Management (Fondation européenne pour le management par la qualité)

EIOPA
European Insurance and Occupational Pensions Authority (Autorité européenne des assurances et des pensions professionnelles)

ESMA
European Supervision Market Authority (Autorité européenne des marchés financiers, AEMF)

FBF
Fédération Bancaire Française ou tout autre association professionnelle sectorielle

IFRS
Normes internationales d'information financière

IIA
Institute of Internal Auditors

ISO
Organisation internationale de normalisation.

LCBFT
Lutte contre le blanchiment de capitaux et le financement du terrorisme

Loi Informatique et Libertés
Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

MiFID
Markets in Financial Instruments Directive (Directive sur les marchés d'instruments financiers, MIF)

OHSAS
Occupational Health and Safety Assessment Series (Système de management de la santé et de la sécurité au travail)

PCI-DSS
Payment Card Industry - Data Security Standard (Norme de sécurité des données pour l'industrie des cartes de paiement)

PNUE
Programme des Nations Unies pour l'environnement

RSE
Responsabilité sociale des entreprises

SI
Systèmes d'information

Solvabilité II
Directive 2009/138/CE du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice

SOX
Loi Sarbanes-Oxley 107-204 du 30 juillet 2002 sur la réforme de la comptabilité des sociétés cotées et la protection des investisseurs

Annexe 1 - Contrôle interne

MISSION ET OBJECTIFS	Apporter à l'entreprise l'assistance nécessaire pour la diffusion des principes du contrôle interne. Il s'agit de concevoir, mettre en place et piloter un système de contrôle interne qui puisse donner à la direction et au comité d'audit une assurance raisonnable concernant la fiabilité des contrôles intégrés aux processus métier et support (en soulignant le rôle clé des processus informatisés qui supportent les métiers), et qui visent la réduction des risques ainsi que l'atteinte des objectifs stratégiques de l'entreprise.
RESPONSABILITES ET PRINCIPALES PRESTATIONS	Responsabilités : • assistance apportée à la direction générale dans la diffusion de la culture de contrôle interne et l'optimisation de l'environnement de contrôle ; • coordination de l'homogénéisation des politiques, des procédures, et des dispositifs de contrôle interne ; • suivi de la mise en œuvre des systèmes de contrôle interne dans l'organisation, en vue de garantir une couverture adéquate des risques et la protection de la réputation d'entreprise. Prestations : • rapport à la direction générale sur le contrôle interne ; • cartographie des risques ; • proposition d'informations à inclure dans le rapport annuel sur le gouvernement d'entreprise.
INSTANCES ET OUTILS	• comités de contrôle interne ; • modélisation des processus et outils de gestion des risques et de traitement de masse des données par des *CAATs* ; • indicateurs pour la description de l'environnement de contrôle interne ; • cartographie des processus et matrices des risques et contrôles. Manuels de procédures ; • rapports d'examen périodiques.

DIRECTIVES EXTERNES ET INSTRUCTIONS INTERNES

Directives externes :

- dispositions émanant de régulateurs sectoriels, en particulier concernant les activités financières et d'assurance (par exemple le règlement CRBF 97-02 pour les banques en France ; les recommandations de l'EIOPA) ;
- réglementation comptable applicable (plan comptable général, IFRS, etc.) ;
- lois et règlements sur les marchés financiers (Cf. AMF en France) ;
- loi de Sécurité Financière 2003-706 du 1er août 2003 et Loi n°2011-420 du 15 mai 2001 relative aux nouvelles régulations économiques) ;
- code de bonne gouvernance ;
- dispositions recommandées : COSO, COBIT.

Instructions internes :

- objectifs et principes d'actions de la fonction ;
- politiques et manuels de procédures internes de la fonction ;
- plans stratégiques et annuels de la fonction ;
- code de bonne gouvernance, code d'éthique et de conduite, politiques et manuels de contrôle interne, etc.

RÔLE DE L'AUDIT INTERNE

Activités propres à l'audit interne en lien direct avec cette fonction :

- revoir et évaluer le cadre de contrôle interne et de la fonction ;
- examiner l'efficacité des contrôles et l'évaluation et la gestion appropriées des risques ;
- suivre les plans d'action concernant la mise en œuvre des contrôles recommandés ;
- donner une assurance concernant les processus d'évaluation du contrôle interne ;
- établir des rapports périodiques de l'audit sur le contrôle interne et suivre les plans d'action ;
- assister éventuellement aux comités de contrôle interne.

Activités de l'audit interne impliquant une collaboration limitée avec cette fonction :

- participer à l'élaboration des politiques et procédures internes, et au transfert de connaissances concernant l'environnement de contrôle interne ;
- organiser des réunions régulières de coordination et de promotion des activités des deux fonctions d'assurance, en vue d'établir des liens et une collaboration ;
- aider à l'identification des défaillances de contrôle dans les processus informatisés et métier ;
- conseiller la direction générale lors de l'établissement des priorités pour l'exécution des plans d'action.

Activités que l'audit interne devrait s'abstenir de réaliser :

- définir et mettre en œuvre du cadre de contrôle interne de l'entreprise : politiques et procédures internes ;
- avoir la responsabilité de la conception, de la mise en place et du pilotage des dispositifs de contrôle interne.

Annexe 2 - Contrôle interne relatif au reporting financier

MISSION ET OBJECTIFS	Fournir à la direction et au comité d'audit une assurance raisonnable concernant la fiabilité de l'information financière qu'ils présentent au Conseil pour approbation, et qui fait l'objet de communications régulières à l'intention des régulateurs et du marché.
RESPONSABILITES ET PRINCIPALES PRESTATIONS	**Responsabilités :** • conception et mise en œuvre d'un système, fondé sur l'évaluation des risques, visant le contrôle interne relatif au reporting financier ; • mise en œuvre des composantes du contrôle interne, en accord avec le référentiel retenu ; • suivi du niveau de mise en œuvre du système de contrôle interne au sein de l'organisation et rapport à la direction générale. **Prestations :** • cartographie des risques des processus d'élaboration de l'information financière ; • rapport annuel sur le gouvernement d'entreprise (décrivant le système de contrôle interne relatif au reporting financier) ; • instructions internes concernant le système de contrôle interne relatif au reporting financier ; • rapport à la direction générale sur la mise en œuvre du système de contrôle interne relatif au reporting financier.
INSTANCES ET OUTILS	• comité de contrôle de l'information financière ; • systèmes informatiques liés à l'élaboration de l'information financière ; • systèmes informatiques de gestion du contrôle interne relatif au reporting financier ; • cartographie des processus d'élaboration de l'information financière.

DIRECTIVES EXTERNES ET INSTRUCTIONS INTERNES

Directives externes :

- réglementation comptable applicable (plan comptable général, IFRS, etc.) ;
- loi sur le marché des valeurs et réglementation de l'AMF et/ou loi SOX ;
- loi de Sécurité Financière 2003-706 du 1er août 2003 et Loi n°2011-420 du 15 mai 2001 relative aux nouvelles régulations économiques ;
- dispositions recommandées : COSO, COBIT.

Instructions internes :

- objectifs et principes d'actions de la fonction ;
- politiques et manuels de procédures internes relatifs à la fonction ;
- plans stratégiques et annuels de la fonction ;
- code de conduite sur les marchés financiers ;
- réglementations et politiques comptables, relatives à la clôture des comptes, au reporting, à la sécurité des systèmes d'information, aux activités sous-traitées, et aux autres éléments affectant de manière significative les processus d'élaboration de l'information financière.

RÔLE DE L'AUDIT INTERNE

Activités propres à l'audit interne en lien direct avec cette fonction :

- évaluer annuellement le fonctionnement et l'efficacité globale du système de contrôle interne relatif au reporting financier (analyse de la capacité du système à détecter ou prévenir les risques impactant de manière significative la fiabilité de l'information financière) ;
- examiner périodiquement l'efficacité des contrôles du système de contrôle interne relatif au reporting financier ;
- communiquer au comité d'audit ;
- suivre des recommandations ;
- revoir la partie concernant le système de contrôle interne relatif au reporting financier dans le rapport annuel sur le gouvernement d'entreprise.

Activités de l'audit interne impliquant une collaboration limitée avec cette fonction :

- apporter un appui méthodologique à l'identification et à l'évaluation des risques du processus d'élaboration de l'information financière ;
- apporter un appui à l'identification des contrôles ou à leur conception.

Activités que l'audit interne devrait s'abstenir de réaliser :

- prendre des décisions concernant la gestion du système de contrôle interne sur le reporting financier ;
- exécuter des activités de contrôle.

Annexe 3 - Sécurité des systèmes d'information

MISSION ET OBJECTIFS	Définir et élaborer des dispositifs, des stratégies, des solutions organisationnelles et des systèmes d'information permettant de réaliser, préserver, protéger et garantir les principales caractéristiques de la sécurité de l'information (confidentialité, intégrité et disponibilité).
RESPONSABILITES ET PRINCIPALES PRESTATIONS	**Responsabilités :** • élaboration d'un cadre de gouvernance de la sécurité des systèmes d'information et définition de normes en la matière ; • élaboration des contrôles et dispositifs garantissant l'adoption des mesures nécessaires en matière de sécurité des systèmes d'information, et élaboration de tests de sécurité, en vue d'identifier les vulnérabilités des systèmes ; • appui aux investigations informatiques pour la détection et la prévention des fraudes. **Prestations :** • plan directeur de sécurité ; • cartographie des risques liés à la sécurité des systèmes d'information ; • politiques, normes et procédures en matière de sécurité des systèmes d'information ; • rapports sur les tests de sécurité, tant internes (boîte blanche) qu'externes (boîte noire).
INSTANCES ET OUTILS	• comités de sécurité ; • outils informatiques de codage des systèmes, contrôles et surveillance des incidents de sécurité ; • systèmes de prévention (antivirus et pare-feu) et détection des intrusions ; • systèmes de contrôle d'accès aux systèmes. Matrices d'autorisation et types d'accès aux systèmes ; • protocoles sécurisés de communication.

DIRECTIVES EXTERNES ET INSTRUCTIONS INTERNES

Directives externes :

- législation en matière de protection des données à caractère personnel (Loi Informatique et Libertés & directive européenne sur la protection des données personnelles) ;
- obligation sectorielle en matière de continuité d'activité (par exemple, article 14 du CRBF 97-02 pour les banques) ;
- législation sur la monnaie électronique (PCI-DSS) ;
- dispositions recommandées : COSO, COBIT, normes de la série ISO/CEI 27000 et ISO 17799.

Instructions internes :

- politiques et manuels de procédures internes relatifs à la fonction ;
- plans stratégiques et annuels des systèmes d'information ;
- politique de sécurité des systèmes d'information ;
- Plan de Secours Informatique (PSI). Dispositif réglementaire relatif à la sécurité des systèmes d'information ;
- code d'éthique et de conduite.

RÔLE DE L'AUDIT INTERNE

Activités propres à l'audit interne en lien direct avec cette fonction :

- examiner et évaluation de chaque domaine de responsabilité de la fonction de sécurité des systèmes d'information ;
- suivre les plans d'action sur la sécurité des systèmes d'information résultant de mission d'audit antérieures.

Activités de l'audit interne impliquant une collaboration limitée avec cette fonction :

- élaborer le plan annuel d'audit des systèmes d'information. Eléments supplémentaires à prendre en compte pour l'identification d'éventuelles missions d'audit ;
- aider à l'identification des faiblesses de la sécurité des systèmes d'information ;
- organiser des réunions régulières de coordination et de promotion des activités des deux fonctions d'assurance, en vue d'instaurer des liens et une collaboration.

Activités que l'audit interne devrait s'abstenir de réaliser :

- définir et mettre en œuvre le dispositif réglementaire relatif à la sécurité des systèmes d'information ;
- définir les contrôles et actions y afférents.

Annexe 4 - Sécurité physique des actifs et des personnes

MISSION ET OBJECTIFS	Sauvegarder les actifs physiques de l'entreprise, la sécurité physique des collaborateurs et des responsables de l'organisation, et gérer les risques pouvant être partagés dans le cadre de polices d'assurance adaptées. Il s'agit également, en particulier dans le cas d'organisations soumises à une réglementation sur les infrastructures critiques, de minimiser les risques liés au terrorisme, à la prolifération des armes de destruction massive et au crime organisé.
RESPONSABILITES ET PRINCIPALES PRESTATIONS	**Responsabilités :** • définition et mise en œuvre de la politique de sécurité de l'organisation concernant les actifs critiques et le personnel ; • gestion, coordination et supervision du fonctionnement des services de sécurité internes et externes ; • planification et exécution des plans de formation en matière de sécurité, en conseillant, en tant que de besoin, les différents services de l'organisation. **Prestations :** • cartographie des risques liés à la sécurité physique des actifs et des personnes ; • plan stratégique de sécurité, politiques et procédures d'action interne et externe ; • rapports périodiques sur les polices d'assurances (biens et événements couverts, franchises).
INSTANCES ET OUTILS	• comités des risques ; • politiques de gestion des assurances de l'organisation ; • outils informatiques d'analyse actuarielle des risques assurables ; • outils informatiques de gestion et de contrôle des risques. Modèles aléatoires et statistiques ; • manuels de procédures internes de sécurité physique des actifs et des collaborateurs.

DIRECTIVES EXTERNES ET INSTRUCTIONS INTERNES

Directives externes :

- Réglementation relative à la sécurité privée ;
- obligation sectorielle en matière de continuité d'activité (par exemple, article 14 du CRBF 97-02 pour les banques ;
- dispositions recommandées : suite ISO/CEI 27000.

Instructions internes :

- politiques et manuels de procédures internes relatifs à la fonction, aux déclarations de sinistres, à la sécurité et au contrôle des accès, etc. ;
- plans stratégiques et annuels de la fonction ;
- politiques générales de souscription des assurances ;
- manuels de sécurité à destination des salariés dans les pays à risques spécifiques.

RÔLE DE L'AUDIT INTERNE

Activités propres à l'audit interne en lien direct avec cette fonction :

- donner une assurance concernant les processus de gestion des risques ;
- évaluer les processus de gestion des risques liés à la sécurité physique des actifs et des personnes ;
- évaluer l'élaboration des rapports sur les risques critiques et revoir leur gestion.

Activités de l'audit interne impliquant une collaboration limitée avec cette fonction :

- participer à l'élaboration de la cartographie des risques : identification et évaluation des principaux risques ;
- conseiller la direction concernant le traitement des risques identifiés dans ce domaine ;
- contribuer à la mise en œuvre et au maintien du cadre et de la politique de gestion des risques, en appui au Conseil via le comité d'audit.

Activités que l'audit interne devrait s'abstenir de réaliser :

- définir des risques pouvant ou non être partagés ;
- mettre en place des processus de gestion des risques liés à la sécurité physique des actifs et des personnes ;
- prendre des décisions concernant l'assurance des risques ou leur traitement ;
- assumer des responsabilités en matière de gestion de ces risques.

Annexe 5 - Conformité réglementaire

MISSION ET OBJECTIFS	Identifier les obligations découlant des lois et règlements, superviser le niveau de conformité à ces obligations, coordonner la conception et la mise en œuvre de plans d'actions correctives, évaluer l'éventuel impact de l'évolution du cadre réglementaire sur les activités de l'entreprise et définir un programme de conformité en conséquence.
RESPONSABILITES ET PRINCIPALES PRESTATIONS	**Responsabilités :** • identification des obligations réglementaires découlant des lois et règlements du secteur, et évaluation de l'impact des changements dans la réglementation sur les activités de l'entreprise ; • élaboration et définition du programme de conformité sur la base de l'inventaire des évolutions réglementaires ; • suivi du niveau de conformité aux obligations réglementaires, identification des déficiences et de leurs responsables, et coordination avec les services impliqués dans la conception et la mise en œuvre de plans d'actions correctives. **Prestations :** • cartographie des risques réglementaires ; • procès-verbaux du comité de conformité réglementaire et du comité dédié à la lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT) ; • rapport périodique sur la conformité réglementaire à l'intention de la direction générale.
INSTANCES ET OUTILS	• code de conduite ; • dispositifs d'alerte ; • manuels de procédures internes ; • inventaire des évolutions réglementaires.

DIRECTIVES EXTERNES ET INSTRUCTIONS INTERNES

Directives externes :

- dispositions émanant de régulateurs sectoriels (Comité de Bâle sur le contrôle bancaire, Banque centrale européenne, ABE, EBA, AEMF, banque de France, AMF, ACPR), concernant principalement les activités financières et d'assurance, notamment :
  - la directive MIF 2004/39/CE et sa transposition, lois et règlements sur les marchés financiers, sur l'organisation du contrôle interne (règlement CRBF 97-02), et sur la lutte contre le blanchiment de capitaux et le financement du terrorisme,
  - loi sur l'intermédiation en assurance, règlement relatif à l'organisation et la supervision des assurances privées, directive Solvabilité II, réglementation de la DGSFP, réglementation de l'EIOPA ;
- législation relative à la protection des données à caractère personnel ;
- code pénal ;
- dispositions recommandées : FBF, EIOPA, COSO.

Instructions internes :

- objectifs et principes d'actions de la fonction ;
- politiques et manuels de procédures internes relatifs à la fonction ;
- plans stratégique et annuels de la fonction ;
- manuels et politiques internes : prévention des risques pénaux, lutte contre le blanchiment de capitaux et le financement du terrorisme, réglementation concernant les instruments financiers, loi de protection des données, code d'éthique et de conduite, dispositifs d'alerte, etc.

RÔLE DE L'AUDIT INTERNE

Activités propres à l'audit interne en lien direct avec cette fonction :

- évaluer de façon périodique et indépendante l'efficacité de la mise en œuvre des activités incombant à la fonction de conformité réglementaire ;
- analyser la clarté et la transparence des activités incombant à la fonction ;
- communiquer les informations à la fonction conformité concernant tout constat d'audit interne relatif à des risques de non-conformité réglementaire.

Activités de l'audit interne impliquant une collaboration limitée avec cette fonction :

- établir une relation avec les superviseurs et les régulateurs ;
- participer à l'élaboration de la cartographie des risques : identification et évaluation des risques principaux ;
- participer à la coordination de la gestion des risques relatifs à la conformité réglementaire ;
- contribuer au maintien du cadre de gestion des risques et à la définition de la stratégie de gestion des risques en appui au Conseil.

Activités que l'audit interne devrait s'abstenir de réaliser :

- mettre en place des processus de gestion des risques de non-conformité ;
- définir les degrés d'appétence pour le risque de non-conformité ;
- avoir des responsabilités en matière de gestion des risques de non-conformité réglementaire, en particulier par la prise de décisions en réponse à des situations sensibles ou par la réalisation de contrôles de premier niveau.

Annexe 6 - Gestion des risques

MISSION ET OBJECTIFS	Adopter, appliquer et maintenir les procédures et politiques de gestion des risques permettant de fournir les informations pertinentes sur la situation des risques de l'organisation à la direction générale et aux organes de gouvernance, afin que ces derniers aient connaissance des conséquences sur la réalisation des objectifs de l'organisation.
RESPONSABILITES ET PRINCIPALES PRESTATIONS	**Responsabilités :** • coordination des processus d'identification et d'évaluation des risques grâce à l'élaboration et à l'actualisation de la cartographie des risques, en tenant compte de la menace potentielle sur la réalisation des objectifs de l'organisation ; • coordination des processus de mesure des risques et des contrôles et des procédures nécessaires à leur atténuation dans le cadre de l'appétence pour le risque et des seuils de tolérance au risque définis par le Conseil ; • élaboration des mécanismes de communication périodique de l'évolution et du suivi des risques, en particulier des plus critiques ou s'étant matérialisés, et information sur leurs conséquences et leur impact économique. **Prestations :** • cartographie des risques de l'organisation ; • rapport sur le suivi des risques, leur matérialisation et les plans d'action ; • information sur la gestion des risques dans le rapport annuel sur le gouvernement d'entreprise.
INSTANCES ET OUTILS	• comités des risques ; • politiques de gestion des risques et manuels de procédures ; • outils informatiques de gestion et de contrôle des risques ; • cartographie des risques et des processus.

DIRECTIVES EXTERNES ET INSTRUCTIONS INTERNES

Directives externes :
- lois et règlements sur les marchés financiers (Cf. AMF en France);
- code de bonne gouvernance ;
- dispositions recommandées : COSO, COBIT, Norme ISO 31000.

Instructions internes :
- objectifs et principes d'actions de la fonction ;
- politiques de gestion des risques et orientations du comité d'audit et du Conseil concernant le suivi des systèmes de gestion des risques ;
- plans stratégiques et annuels de la fonction ;
- code d'éthique et code de conduite.

RÔLE DE L'AUDIT INTERNE

Activités propres à l'audit interne en lien direct avec cette fonction :
- donner une assurance relative à l'évaluation et à la gestion des risques ;
- évaluer les processus de gestion des risques, incluant les contrôles et les procédures ;
- évaluer et revoir l'élaboration de rapports sur les risques clés et examiner leur gestion.

Activités de l'audit interne impliquant une collaboration limitée avec cette fonction :
- participer à l'identification et à l'évaluation des principaux risques ;
- conseiller la direction concernant le traitement des risques identifiés ;
- contribuer à la coordination de la gestion des risques ;
- contribuer à la mise en œuvre et au maintien du cadre et de la politique de gestion des risques, en appui au Conseil, via le comité d'audit.

Activités que l'audit interne devrait s'abstenir de réaliser :
- définir l'appétence pour le risque ;
- mettre en place les processus de gestion des risques ;
- prendre des décisions dans le cadre de l'assurance des risques ou de leur traitement ;
- assumer des responsabilités en matière de gestion de ces risques.

Annexe 7 - Système de management intégré

MISSION ET OBJECTIFS	Intégrer au sein d'un seul système de gestion les exigences communes aux normes de qualité telles que l'EFQM, l'ISO 9001 :2008, l'ISO 14001 :2004 et l'OHSAS 18001 :2007 et viser l'amélioration continue de la qualité, de l'environnement, de la qualité de vie au travail.
RESPONSABILITES ET PRINCIPALES PRESTATIONS	**Responsabilités :** • étude et coordination des activités d'innovation et de développement afin de répondre aux attentes des clients internes ou externes, des collaborateurs et d'autres parties prenantes ; • renforcement de la culture d'amélioration continue des produits et de la gestion des processus de l'entreprise, et supervision du niveau de performance pour assurer la rentabilité du capital investi ; • suivi de la conformité à la réglementation, aux lois et autres accords sur l'environnement, la prévention des risques professionnels, etc., et suivi de l'amélioration des indicateurs financiers et extra-financiers (leadership, responsabilité sociale et environnementale, sécurité). **Prestations :** • plans d'audit en matière de qualité, d'environnement et de prévention des risques professionnels ; • rapports présentant les conclusions des audits ; • état des non-conformités et recommandations proposées.
INSTANCES ET OUTILS	• comités pour la qualité, l'environnement et la prévention des risques professionnels ; • outils informatiques pour la gestion documentaire des rapports d'audit et le suivi des non conformités ; • politiques, manuels de gestion et procédures du système de contrôle intégré ; • plans d'audit spécifiques en matière de qualité, d'environnement et de prévention des risques professionnels.

DIRECTIVES EXTERNES ET INSTRUCTIONS INTERNES

Directives externes :
- législation générale ou sectorielle relative à l'environnement, la prévention des risques professionnels, la qualité et la normalisation ;
- dispositions recommandées : Normes ISO, modèle de l'EFQM, norme OHSAS 18001 :2007 sur la prévention des risques professionnels.

Instructions internes :
- politiques et manuels de procédures internes relatifs à la fonction ;
- plans stratégiques et annuels de la fonction ;
- politiques de l'entreprise en matière de qualité, d'environnement et de prévention des risques professionnels ;
- système de management intégré de l'entreprise.

RÔLE DE L'AUDIT INTERNE

Activités propres à l'audit interne en lien direct avec cette fonction :
- formuler une opinion sur l'étendue et l'adéquation des plans d'audits spécialisés ;
- examiner la complémentarité avec les plans d'audits spécialisés, en s'assurant que les non conformités font l'objet d'un suivi ;
- évaluer les compétences professionnelles des auditeurs de la qualité, de l'environnement et de la prévention des risques professionnels.

Activités de l'audit interne impliquant une collaboration limitée avec cette fonction :
- réaliser des audits en collaboration avec les auditeurs de la qualité, de l'environnement et de la prévention des risques professionnels ;
- organiser des réunions régulières de coordination et de promotion des activités, en vue d'instaurer des liens et une collaboration.

Activités que l'audit interne devrait s'abstenir de réaliser :
- définir et approuver les politiques relatives à la qualité, l'environnement, et la prévention des risques professionnels ;
- concevoir et mettre en œuvre un système de management intégré.

Annexe 8 - Responsabilité sociale et réputation d'entreprise

MISSION ET OBJECTIFS	Gérer les actions de l'entreprise visant la transparence de l'information et les relations avec les parties prenantes dans des domaines comme le gouvernement d'entreprise, l'éthique des affaires, les droits de l'homme, les impacts sociaux des activités de l'entreprise et l'environnement.
RESPONSABILITES ET PRINCIPALES PRESTATIONS	**Responsabilités :** • suivi du positionnement de l'organisation dans la société, de l'image de marque de l'entreprise et de sa propriété intellectuelle, élaboration de rapports d'activité et collaboration à la réalisation du rapport annuel ; • étude, diagnostic et proposition de politiques et d'actions de mise en conformité avec les standards de référence, et adaptation des activités de l'entreprise aux exigences définies selon certains indicateurs de développement durable ; • coordination des plans d'action pour la réalisation des objectifs. **Prestations :** • rapport annuel de responsabilité sociale élaboré par l'équipe dirigeante ; • intégration des rapports de développement durable dans la communication d'entreprise ; • rapports d'évaluation sur les filiales, les prestataires et les sous-traitants.
INSTANCES ET OUTILS	• comité de développement durable ; • outils d'élaboration des rapports de responsabilité sociale (normes AA1000 et ISAE 3000), et outils de compilation et de consolidation de l'information au sein de l'organisation ; • cartographie des risques de réputation ; • politiques de ressources humaines intégrant l'égalité, la conciliation de la vie professionnelle et de la vie privée, etc., et politique gestion de l'image de marque et de la réputation de l'entreprise ; • plan annuel de responsabilité sociale ; • audit externe du rapport de responsabilité sociale d'entreprise et rapports externes sur le développement durable.

DIRECTIVES EXTERNES ET INSTRUCTIONS INTERNES	**Directives externes :** • dispositions recommandées : Nations Unies, *The International Integrated Reporting Framework* (www.theiirc.org), PNUE. **Instructions internes :** • objectifs et principes d'actions de la fonction ; • manuel de procédures internes de la fonction ; • plans stratégiques et plan directeur concernant la responsabilité sociale et la réputation d'entreprise.
RÔLE DE L'AUDIT INTERNE	**Activités propres à l'audit interne en lien direct avec cette fonction :** • donner une assurance concernant les processus de gestion de la responsabilité sociale et l'image de marque ; • évaluer les processus de gestion des risques de réputation et les impacts de cette activité sur la société ; • évaluer l'élaboration des rapports annuels et la fiabilité et l'intégrité de l'information contenue dans le document de référence. **Activités de l'audit interne impliquant une collaboration limitée avec cette fonction :** • participer à l'évaluation du degré de conformité aux standards de référence ; • conseiller la direction concernant l'élaboration du traitement des risques de réputation ; • réviser les dispositifs d'alerte ; • contribuer au maintien du cadre et de la stratégie de gestion du risque de réputation, en appui au Conseil. **Activités que l'audit interne devrait s'abstenir de réaliser :** • prendre des décisions concernant l'élaboration du rapport global destiné aux tiers ; • assumer des responsabilités en matière de gestion de ces risques.

Instituto de Auditores Internos de España
Santa Cruz de Marcenado, 33
28015 Madrid
Tel. : 91 593 23 45
Fax : 91 593 29 32
www.auditoresinternos.es

IFACI
98 bis, boulevard Haussmann
75008 Paris
Tél. : 01 40 08 48 00
Fax : 01 40 08 48 20
www.ifaci.com