

Depuis le 1^{er} janvier 2009, l'organe de révision est tenu de vérifier l'existence de ce qu'on appelle un Système de Contrôle Interne (ci-après SCI) et de le confirmer dans son rapport aux actionnaires.

Dans le cadre d'un SCI, la formalisation recourt souvent à des référentiels, tels que le COSO (Committee of the Sponsoring Organizations of the Treadway Commission), sans doute l'un des plus répandus de par le monde.

La dématérialisation des processus au sein des entreprises, par l'intégration de systèmes d'information complexes, renforce la nécessité d'une analyse de risques afin de garantir via un SCI la fiabilité des informations financières, mais également de prévenir tout incident de quelque nature qu'il soit sur les systèmes d'information pouvant impacter les résultats financiers.

Ces nouvelles obligations soulèvent de nombreuses questions juridiques relatives aux mécanismes technologiques et organisationnels des contrôles d'un système d'information.

Cette formation s'adresse aux CIO, CSO, aux administrateurs d'entreprises, aux auditeurs, aux contrôleurs, mais également à toute personne confrontée à un SCI et à la Gouvernance du système d'information.

OBJECTIFS :

- Appréhender les cadres juridiques et normatifs appliqués à un SCI sur SI
- Identifier les responsabilités lors de l'établissement et de la gestion d'un SCI
- Sensibiliser et responsabiliser les employés et décideurs confrontés à un SCI
- Découvrir quelques scénarios pratiques

DUREE : 8h00

NIVEAU : tout public

Le séminaire est animé par **Nicolas Rosenthal**, expert juridique qui dispose d'une vaste expérience tant de la conformité de systèmes d'information que de la Gouvernance d'entreprise.

E-DROIT est un Cabinet juridique de conseils dans le domaine de la gouvernance d'entreprise et la conformité réglementaire des systèmes d'information. Nous vous accompagnons dans les défis posés par l'environnement réglementaire grâce à l'analyse liée aux lois émergentes, à l'usage des technologies et à l'impact sur votre entreprise.

PROGRAMME :

8H15 LE NOUVEAU CADRE DU SYSTEME DE CONTRÔLE INTERNE

- Les principes et objectifs d'un SCI (Système de Contrôle Interne) sur le MSI (Management d'un Système d'Information)

La révision du statut juridique des Sociétés dans le Code des Obligations

- Le contrôle ordinaire confronté au contrôle restreint
- Le régime du contrôle optionnel
- Les responsabilités du Conseil d'Administration et de l'organe de révision
- L'évaluation des risques et de l'établissement du SCI

La Circulaire FINMA 2008/24 sur la surveillance et le contrôle interne

- L'importance des notions de révision interne, contrôle interne et *compliance*
- La dérégulation ? « comply or explain »
- Le texte de la Circulaire FINMA 2008/24 : principes et exceptions
- Les obligations lors de la constitution d'un Comité d'Audit

Cas pratique

Les participants analyseront, avec le formateur, les marges de manœuvres du Conseil d'Administration pour les entreprises et du Comité d'Audit pour les banques

L'analyse des risques et la matérialisation d'un SCI du système d'information

- La nouvelle norme ISO/CEI 27005 «Gestion du risque des systèmes d'information»
- L'annexe A de la norme ISO/CEI 27001 «Exigences pour un système de gestion de sécurité de l'information»
 - Chapitre 11 : Contrôle d'accès
 - Chapitre 13 : Gestion des incidents
 - Chapitre 14 : Gestion du plan de continuité de l'activité
 - Chapitre 15 : Conformité (*compliance*)
- La norme ISO/CEI 20000 « Gestion des changements »
- COSO : les principes et objectifs
- NAS 890 : la norme d'audit suisse sur la vérification de l'existence d'un SCI

Cas pratique

Les participants analyseront, avec le formateur, les composantes du SCI sur le système d'information

12H15 Pause

14H00 MISE EN PLACE D'UN SCI SUR UN SYSTEME D'INFORMATION

Informations sur l'organisation, le contenu du séminaire et sa facturation
Email : secretariat@e-droit.ch

La nouvelle norme ISO 38500 sur la Gouvernance du système d'information

Etude détaillée du cadre de bonne gouvernance des technologies de l'information par l'entreprise :

- Identification des responsabilités, établissement d'une stratégie, modalités d'acquisition d'un SI, mesure des performances du SI, conformité du SI, comportement humain

Etude détaillée du modèle de bonne gouvernance des technologies de l'information par l'entreprise :

- Evaluation ; Orientation : Surveillance

Etablissement d'une politique de contrôle interne

- Les niveaux de contrôles du contrôle permanent
- Les caractéristiques d'un contrôle en particulier
- Les contrôles sur risques majeurs et le point de surveillance fondamental (PSF)
- Les indicateurs su suivi d'un contrôle
- L'efficacité et l'efficience d'un contrôle
- Les responsabilités d'exécution d'un SCI

Les participants étudieront, avec l'aide du formateur, l'établissement d'une procédure définissant un contrôle d'une opération à risque sur le système d'information

- Exemples d'analyses de risques
- Exemples de risques et incidents couverts
- Les responsabilités et champ d'application
- La fréquence et la sélectivité du contrôle
- La matérialisation du contrôle et son éventuel archivage
- Le suivi d'exécution du contrôle

18H00 Clôture du séminaire par la remise d'une attestation de formation