



# Above SECURITE

1919, boul. Lionel-Bertrand,  
Bureau 203  
Boisbriand, Qc. J7H 1N8  
Canada  
Téléphone :  
450-430-8166  
Sans frais :  
866-430-8166  
Télécopieur :  
450-430-1858  
info@abovesecurite.com

La tranquillité d'esprit

## Liste de vérification du dirigeant d'entreprise pour la sécurité de l'information



Traduction libre de la définition de Gouvernance selon le *IT Governance Institute* :

« Série de responsabilités et de pratiques exercées par le conseil d'administration et la haute direction dans le but d'assurer la direction stratégique qui mène à l'atteinte des objectifs, tout en s'assurant que les risques soient gérés de façon appropriée et que les ressources de l'entreprise soient utilisées de façon responsable ».

Dans cet ordre d'idée, Above Sécurité vous propose une liste de vérification que les dirigeants peuvent utiliser pour mieux exercer la Gouvernance TI de leur organisation.<sup>1</sup>

### Responsabilité de la gestion des risques reliés à l'information

- Vos risques informationnels sont-ils gérés, comment, par qui?
- Les responsabilités sont-elles clairement définies ?
- Votre organisation alloue-t-elle des ressources dédiées uniquement à la gestion des risques informationnels ou à la sécurité de l'information ?
- Quel budget est alloué à la sécurisation de vos actifs informationnels?
- Combien de temps est réellement consacré à la gestion des risques informationnels ou à la sécurité de l'information?
- Au niveau exécutif, qui assume la responsabilité finale de l'implantation de la gestion des risques informationnels, physiques et informatiques?
- Discutez-vous de sujets reliés à la gestion des risques informationnels lors des réunions du conseil d'administration ?

### Proactivité en gestion des risques informationnels

- **Les risques sont-ils évalués de façon régulière ?**
- **Une fois les risques identifiés, quelles actions concrètes sont prises pour les gérer ?**
- **Votre organisation utilise-t-elle une expertise externe pour obtenir des audits objectifs ?**
- **La fréquence de ces audits convient-elle à la fluctuation de votre niveau de risque?**
- **Les audits incluent-ils la révision de votre plan de continuité des affaires et de votre plan de recouvrement TI ?**

<sup>1</sup> Cette liste de vérification est fournie à titre indicatif comme matière à réflexion et à discussion et ne peut se substituer à un audit professionnel.

## Politiques de gestion des risques informationnels

- ◆ Dans votre organisation, y a-t-il une politique de gestion des risques informationnels, de sécurité ou un manuel d'usage acceptable pour les utilisateurs?
- ◆ Chaque membre de votre personnel reçoit-il ce manuel?
- ◆ Est-il mis à jour sur de façon régulière ?
- ◆ Ces politiques sont-elles appliquées partout dans l'entreprise, à l'intérieur de vos chaînes d'approvisionnement et chez vos partenaires d'affaires?
- ◆ Demandez-vous à vos partenaires de gérer leurs risques informationnels en égards à vos informations?
- ◆ Y a-t-il une politique clairement documentée pour maintenir à jour les réseaux, les serveurs, les équipements et logiciels de protection, et les systèmes?

## Protection de vos actifs informationnels

- ◆ Connaissez-vous tous vos actifs informationnels?
- ◆ À quelle fréquence vos actifs informationnels sont-ils sauvegardés ?
- ◆ Le département de TI pourrait-il restaurer ces sauvegardes dans un délai raisonnable pour ne pas nuire à vos activités d'affaires ?
- ◆ Combien de fois ce système est-il testé? Quand a eu lieu le dernier test?
- ◆ Les leçons apprises sont-elles incorporées dans les séances et les manuels de formation ?

## Formation et conscientisation

- ◆ Votre organisation déploie-t-elle un programme de formation continue en gestion des risques informationnels ?
- ◆ Cette formation couvre-t-elle les meilleures pratiques et l'usage acceptable qui peut être fait des systèmes d'information?
- ◆ Cette formation comporte-t-elle la définition des responsabilités de l'utilisateur?
- ◆ À quelle fréquence ces sessions de formation sont-elles dispensées?
- ◆ Inclut-elle vos partenaires, vos entrepreneurs, et vos fournisseurs ?



**Exemples de mandats réalisés par Above Sécurité  
dans les derniers 6 mois :**

Bancaire et Financier	Révision d'une politique de sécurité
	Plan de continuité des affaires incluant un plan de recouvrement après désastre
	Mandat d'investigation forensique (cybercrime)
	Test d'intrusion sur une application e-banking
	Inventaire des actifs informationnels-conformité à Bâle 2
Santé et Pharmaceutique	Revue de l'architecture et de la configuration réseau
	Test d'intrusion d'une application web
Manufacturier et Distribution	Formation sur le développement de code sécuritaire
	Accompagnement en plan de relève informatique
Technologie et Énergie	Accompagnement en renforcement d'architecture réseau
	Audit de sécurité
	Revue opérationnelle
	Test d'intrusion d'un site web transactionnel
	Service de gestion de la surveillance réseau

**Notre clientèle**

Forte de plus de 300 entreprises situées dans 22 pays, notre clientèle s'étend sur les trois Amériques, l'Europe, les Caraïbes et l'Afrique du Nord. Notre clientèle se compose d'entités gouvernementales et d'entreprises privées des secteurs financiers, des assurances, de la santé, de l'énergie et des télécommunications.

***Above Sécurité peut devenir votre partenaire stratégique dans la gestion de vos risques informationnels.***

***Téléphonez-nous pour rencontrer l'un de nos spécialistes.***



Pour obtenir de plus amples renseignements sur nos services de gestion des risques informationnels, communiquer avec nous :

**Above Sécurité Inc.**  
1919 Lionel Bertrand, bureau 203  
Boisbriand (Québec) J7H 1N8  
Canada

Tél. 450-430-8166  
Fax. 450-430-1858  
Courriel : [info@abovesecurite.com](mailto:info@abovesecurite.com)

[www.abovesecurite.com](http://www.abovesecurite.com)