CYBER-SÉCURITÉ POUR LES ORGANISATIONS PLUS PETITES

LISTE DE CONTRÔLE DU CONSEIL : LEADERSHIP DE LA CYBER-SÉCURITÉ

PRINCIPES FONDAMENTAUX DE LA GOUVERNANCE DES CYBER-RISQUES

☐ **En tant que groupe, évaluez régulièrement si le conseil peut répondre de manière affirmative aux questions suivantes :**

- Votre organisation a-t-elle satisfait aux exigences légales et réglementaires pertinentes, par exemple au RGPD ?
- Votre organisation a-t-elle quantifié ses cyber-expositions et testé sa résilience financière ?
- Votre organisation a-t-elle un plan d'amélioration en place pour garantir que les expositions s'inscrivent dans votre appétit au risque convenu ?
- Le conseil discute-t-il régulièrement des informations concises, claires et exploitables relatives à la cyber-résilience de l'organisation et fournies par la direction ?
- Votre organisation a-t-elle des plans de réponse aux incidents en place qui ont récemment été testés, y compris au niveau du conseil ?
- Les rôles des personnes clés responsables de la gestion des cyber-risques sont-ils clairs et alignés sur les trois lignes de défense ?
- Avez-vous obtenu une validation et une assurance indépendantes de la posture de cyber-sécurité de votre organisation, par exemple, via des tests, une certification ou une assurance ?

☐ **Si vous ne pouvez pas répondre de manière affirmative à un ou plusieurs des éléments ci-dessus, travaillez avec votre PDG, le RSSI, le personnel de l'organisation concerné et/ou des ressources externes pour résoudre le problème.**

SUPERVISION

☐ **Assurez-vous que le conseil d'administration est conscient de son rôle de responsable ultime pour le cyber-risque et la résilience de votre organisation.**

☐ **Déléguez la supervision à un comité du conseil spécifique si nécessaire.**

☐ **Assignez à un responsable de l'entreprise, généralement le responsable de la sécurité des systèmes d'information (RSSI), la responsabilité de signaler la capacité de votre organisation à gérer la cyber-résilience et les progrès dans la mise en œuvre des objectifs de cyber-résilience.**

☐ **S'assurer que ce responsable dispose d'un accès régulier au conseil d'administration, d'une autorité suffisante, de la maîtrise du sujet, de l'expérience et des ressources pour remplir ces obligations.**

☐ **Définissez annuellement la tolérance au risque de votre organisation, en assurant la cohérence avec votre stratégie d'entreprise et l'appétit au risque.**

☐ **Assurez-vous qu'un examen formel et indépendant de la cyber-résilience de votre organisation est effectué chaque année.**

☐ **Travaillez pour intégrer la cyber-résilience et l'évaluation des risques dans la stratégie commerciale globale de votre organisation, la gestion des risques, la budgétisation et l'allocation des ressources.**

☐ **Examinez régulièrement les risques concernant les tiers.**

☐ **Supervisez la création, la mise en œuvre, les tests et l'amélioration continue des plans de cyber-résilience, en vous assurant qu'ils sont harmonisés dans l'ensemble de votre organisation et que votre RSSI ou autre cadre responsable les signale régulièrement au conseil d'administration.**

☐ **Passez régulièrement en revue vos performances pour ce qui précède et tenez compte des conseils indépendants pour une amélioration continue.**

RESTER INFORMÉ

- ☐ **Lorsqu'une personne rejoint le conseil, assurez-vous qu'elle dispose des compétences et connaissances appropriées et actualisées pour comprendre et gérer les risques posés par les cyber-menaces.**
- ☐ **Sollicitez des conseils réguliers de la part de la direction sur l'exposition au risque actuelle et future de votre organisation, les exigences réglementaires pertinentes, et les références du secteur et de la société pour l'appétit au risque. Prévoyez de participer :**
  - aux séances d'information régulières sur les obligations créées par les nouvelles réglementations et législations ;
  - à la planification commune du conseil et du comité de direction et aux visites aux pairs et aux leaders de la meilleure pratique en matière de cyber-sécurité ;
  - aux séances d'information relatives à la sécurité sur l'environnement des menaces ; et
  - aux échanges au niveau du conseil des informations sur la gouvernance et les rapports.
- ☐ **Indiquez clairement à la direction qu'elle a la responsabilité de signaler une évaluation quantifiée et compréhensible des cyber-risques, menaces et événements comme un élément permanent à l'ordre du jour lors des réunions du conseil d'administration.**
- ☐ **Vérifiez régulièrement auprès de la direction et des autres membres du personnel concernés, les développements liés aux problèmes systémiques constants, tels que les vulnérabilités de la chaîne d'approvisionnement, les dépendances courantes et les écarts dans le partage des informations.**

DONNER LE TON

- ☐ **Assurez-vous que les membres du personnel, à tous les niveaux, reconnaissent qu'ils ont chacun des responsabilités importantes pour garantir la cyber-résilience de votre organisation.**
- ☐ **Supervisez le rôle de la direction dans la promotion et le maintien de la culture du risque de votre organisation. Évaluez régulièrement l'efficacité de la culture du risque de votre organisation, en tenant compte de l'impact de la culture sur la sécurité et la solidité, et en apportant des changements si nécessaire.**
- ☐ **Indiquez clairement que vous attendez de tout le personnel qu'il agisse avec intégrité et qu'il fasse remonter rapidement le non-respect observé au sein ou à l'extérieur de votre organisation.**

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP
SWIFT INSTITUTE
FS-ISAC
Standard Chartered
CYBER READINESS INSTITUTE
GLOBAL CYBER ALLIANCE
ICBA Independent Community Bankers of America®