AdmA ORDRE DES ADMINISTRATEURS AGRÉÉS
GESTIONNAIRE PROFESSIONNEL

Bienvenue

1

La protection de l'information, un enjeu de gouvernance !

Cette formation a été développée dans le cadre du Congrès Gestion 2021.
Elle a cependant été conçue pour pouvoir être écoutée de façon indépendante.

DÉVELOPPEMENT PROFESSIONNEL

AdmA ORDRE DES ADMINISTRATEURS AGRÉÉS GESTIONNAIRE PROFESSIONNEL

2

Chantale Pineault, Adm.A., C.M.C., CRISC

Consultante et Spécialiste en Gouvernance, Risques et Conformité en sécurité de l'information

La protection de l'information, un enjeu de gouvernance !

DÉVELOPPEMENT PROFESSIONNEL

AdmA ORDRE DES ADMINISTRATEURS AGRÉÉS GESTIONNAIRE PROFESSIONNEL

3

Contexte

Les informations sont des actifs précieux pour les entreprises. Leur protection devient donc un incontournable si on veut assurer la pérennité de l'organisation.

- Dès lors, comment identifier les informations qui sont critiques et les distinguer de celles qui sont accessoires ?
- Quelles valeurs leur attribuer pour démontrer ces différences et surtout quels moyens devons-nous mettre en place pour en assurer la protection ?

Pour bien comprendre la nature des mesures de protection à mettre en place, il importe au préalable de bien comprendre les enjeux de gouvernance de notre industrie, notre marché et notre sphère d'activités au regard des informations.

4

Implication de la haute direction

Le plus haut dirigeant de l'organisation est le premier responsable de la gouvernance et de la mise en œuvre de la sécurité

5

Implication de la haute direction et du CA

Dans les organisations de grande taille, **le groupe d'intervenants comprend généralement** :

- le conseil d'administration; l'équipe de direction ;
- L'officier de sécurité, le responsable de la PRP, les détenteurs ;
- le personnel d'exploitation et le personnel des services fonctionnels ;
- les responsables de la gestion des risques et de la conformité, notamment les responsables de l'audit interne et les conseillers juridiques à l'interne ;
- les experts externes, notamment les auditeurs, les cabinets d'avocats et les conseillers externes ;
- d'autres parties prenantes, le cas échéant.

Source : Institut Canadien des Comptable Agréés

6

Enjeux de gouvernance

À titre de dirigeant principal il doit **s'assurer de la mise en place des activités critiques** de gouvernance soit **:**

- S'assurer du respect des lois et des règles de sécurité de l'information (incluant la cyber) ;
- Assurer la mise en place des bonnes pratiques en sécurité de l'information ;
- S'assurer de la mise en place d'un comité chargé de la sécurité de l'information ;
- Avoir un cadre de gestion de la sécurité de l'information ;
- Nommer un responsable de la sécurité de l'information et de la cyber ;
- Mettre en œuvre une politique de sécurité de l'information et la faire adopter ;
- Identifier les actifs informationnels caractérisant l'organisation ;

7

Enjeux de gouvernance

Suite de la mise en place des principales activités de gouvernance soit :

- S'assurer de la mise en place de la gestion des risques des actifs informationnels afin d'assurer la protection adéquate et suffisante des informations ;
- S'assurer de la mise en place des mesures liées aux menaces et les impacts sur la sécurité de l'information ;
- S'assurer de la prise en charge des exigences de sécurité de l'information lors de la réalisation de projets de développement ou de l'acquisition de systèmes d'information ;
- S'assurer que la catégorisation des actifs informationnels est effectuée et qu'une révision est faite annuellement ;
- S'assurer de l'élaboration et de la mise en œuvre d'un programme formel de formation et de sensibilisation en matière de sécurité de l'information ; Etc…

8

Définition des actifs

Notion d'actifs informationnels

- Les actifs informationnels sont **intangibles** et **comprennent l'ensemble des informations portées par un support** (électronique, papier ou autre) dans le but d'offrir des services, de prendre des décisions d'affaires, de partager et transmettre des connaissances dans le cadre des activités de l'organisation ;
- Les actifs incluent les applications, les logiciels, les systèmes d'information, les traitements informatiques, les progiciels et les données traitées électroniquement ;
- Un **actif informationnel est constitué d'information de différents types, appelés « familles ou groupes d'information »**. Dans le but de simplifier les façons de faire lors de l'établissement des valeurs, un regroupement des informations doit être fait.

9

Les familles d'actifs (des exemples)

Famille	Description	Exemple
1 - Renseignements personnels	Tout renseignement concernant une personne et qui permet de l'identifier	Données sur le personnel : nom, prénom, adresse du domicile, # assurance sociale, données sur la santé, renseignements de nature financière, etc.
2 - Renseignements financiers sur les entités commerciales	Tout renseignement de nature financière concernant un client corporatif ou une entité commerciale	Dossier de crédit, informations bancaires, données de carte de crédit d'une entité commerciale, etc.
3 - Informations financières corporatives	Toute information financière d'entreprise concernant la gestion des finances	États financiers, rapports, plan budgétaire, activités de trésorerie, etc.
4 - Informations stratégiques corporatives	Toute information d'entreprise concernant des dossiers stratégiques	Projet d'acquisition, d'impartition, etc.

10

Les familles d'actifs

Famille	Description	Exemple
5 - Données d'authentification	Toute information liée à l'authentification des clients ou usagers	Mots de passe, NIP, données biométriques, questions secrètes, etc.
6 - Informations juridiques et contractuelles	Toute information représentant un engagement légal ou contractuel entre l'organisation et un tiers	Contrat ou entente contractuelle, etc.
7 - Données transactionnelles	Donnée décrivant une séquence d'échange d'information dans un système	Détail concernant une transaction financière, etc.
8 - Données informationnelles	Donnée qui définit l'ensemble des valeurs admissibles à utiliser par d'autres champs de données. Considérée comme un sous-ensemble des données maîtresses.	Détail concernant une transaction financière, nbre de clients par lignes de produits etc.

11

Quoi faire pour identifier les actifs informationnels?

Identification des actifs

- **À partir des processus d'affaires de l'organisation**, il suffit d'identifier les données, applications et systèmes (actifs informationnels) qui les supportent.
  - ✓ Dans les façons de faire, les technologies de l'Information et des Communications (TIC) sont des éléments essentiels dans toutes organisations et facilitent la création, le traitement, le stockage, la transmission, la protection et la destruction de l'information.

12

3 aspects à préserver

Disponibilité

Propriété d'une information d'être accessible en temps voulu et de la façon requise par une personne autorisée ;

Intégrité

Propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni détruite sans autorisation ;

Confidentialité

Propriété d'une information de n'être accessible qu'aux personnes autorisées.

13

L'importance des actifs: catégorisation

La catégorisation est un processus d'assignation d'une valeur à certaines caractéristiques d'une information. **La valeur caractérise le degré de sensibilité de cette information** et, conséquemment, **la protection à lui accorder.**

L'échelle des valeurs est souvent constituée de 4 niveaux soit :

- ✓ 1 - Bas
- ✓ 2 - Moyen
- ✓ 3 - Élevé
- ✓ 4 - Très élevé

14

Exemple : Échelle de valeurs

Niveau	DISPONIBILITÉ	INTÉGRITÉ	CONFIDENTIALITÉ
1 Bas	**Tolérance** au délai d'interruption du système **de quelques semaines**	**Information peut être compromise; Sans répercussion** sur les activités de l'administration	**Information ou renseignement** à caractère public
2 Moyen	**Tolérance** au délai d'interruption du système **de quelques jours**	Information peut être compromise; sans répercussion sur les **activités administratives ou d'affaires.** Requis d'**identifier** les éventuelles **pertes d'intégrité**	Information **non assujettie** à une obligation de **confidentialité**
3 Élevé	**Tolérance** au délai d'interruption du système **de quelques heures**	Information critique peut être compromise; Peut en découler des **conséquences médicales et/ou juridiques graves.** Requis d'identifier et de corriger les causes	Information **confidentielle** à préserver (s'assurer que les accès sont contrôlés entre autre)
4 Très élevé	**Tolérance** au délai d'interruption du système **de quelques secondes**	Information critique pouvant affecter la vie ou la santé. **Conséquences** médicales et/ou juridiques **graves**	Information **confidentielle** (régime juridique) et **très sensible** à une divulgation. (Barrière à l'accès doit exister)

15

Évaluation de la criticité

L'évaluation de la criticité permet d'identifier les actifs critiques, soit ceux qui sont considérés comme ayant le plus de valeurs pour l'organisation et qui requièrent d'être protégés en conséquence.

Le niveau de criticité d'un actif informationnel est équivalent au niveau d'impact potentiel le plus élevé pour chaque objectif de sécurité. Ainsi, un actif informationnel dont la catégorisation a été évaluée à 3, se verra attribuer un niveau de criticité de « 3 – Élevé).

Un actif dont le niveau de criticité est « 4- Très élevé » sera considéré comme un « actif critique ».

16

Gouvernance efficace

La catégorisation des actifs informationnels fait partie intégrante des grandes activités de la gouvernance de la sécurité de l'information, il est impératif :

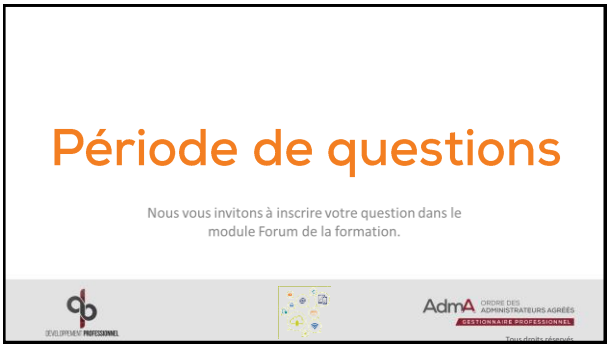
- d'analyser les besoins spécifiques en sécurité de l'information propres à votre organisation;
- d'évaluer et de proposer des solutions personnalisées en conformité avec les standards et les normes reconnus dans le domaine ;
- de créer, documenter et appliquer les processus liés à la gouvernance de la sécurité de l'information à des situations réelles ;

Plus on tarde à réaliser les travaux décrits, plus l'organisation s'expose à des pertes de services et des pertes d'information qui pourraient avoir des conséquences désastreuses sur la continuité des activités et la santé financière.

17

Merci !

18


Période de questions
Nous vous invitons à inscrire votre question dans le module Forum de la formation.
AdmA
ORDRE DES ADMINISTRATEURS AGRÉÉS
GESTIONNAIRE PROFESSIONNEL

19