Nouveaux documents de gouvernance : Survol

Groupe de travail sur la gouvernance et les politiques
Automne 2022

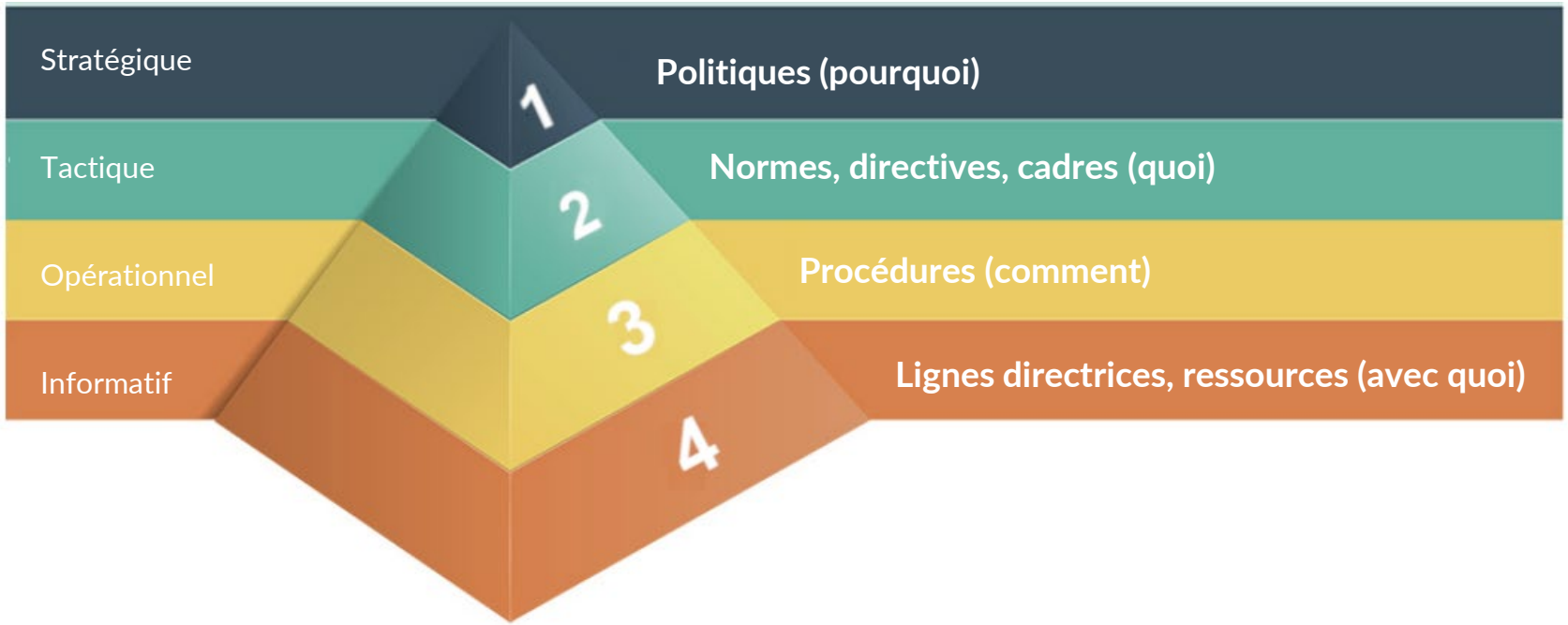
Ordre du jour

- Raison de notre rencontre
- Hiérarchie des documents et processus d’élaboration
- Mise en œuvre des politiques et des normes
- Aperçu des politiques et des normes qui ont été approuvées et documents connexes
- À venir : Politiques et normes en cours d’élaboration
- Rappels et prochaines étapes

Raison de notre rencontre

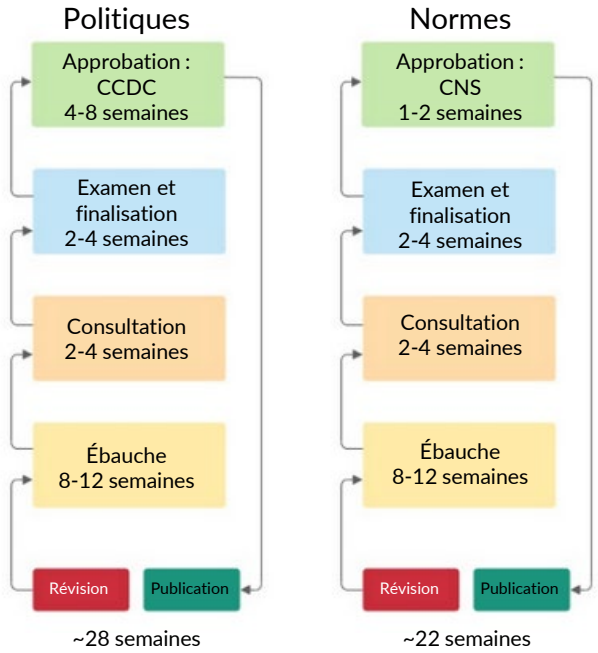
- Nous souhaitons expliquer comment les documents sont créés et l'endroit où ils sont publiés une fois approuvés.
- Pour être efficace, le programme de sécurité doit comprendre des activités de communication et de sensibilisation.
- Nous voulons établir des attentes communes à toutes les parties, y compris les utilisateur(-trice)s, notamment en ce qui concerne le processus et les contrôles techniques.
    - Puisque ces politiques auront des répercussions sur vous et votre travail, vous devez en connaître les points clés.
- Nous n'avons pas organisé de réunion entre les membres du personnel depuis longtemps.

Hiérarchie des documents



Processus d'élaboration des documents de gouvernance

- Groupes de travail thématiques ou axés sur la politique (avec des expert[e]s en la matière de l'externe)
- Examen effectué par le Conseil national de la sécurité (CNS) et la communauté avant l'approbation
- Approbation : Conseil consultatif et directeur sur la cybersécurité (CCDC) pour les politiques; CNS pour les normes
- Tenue de registres des changements et commentaires



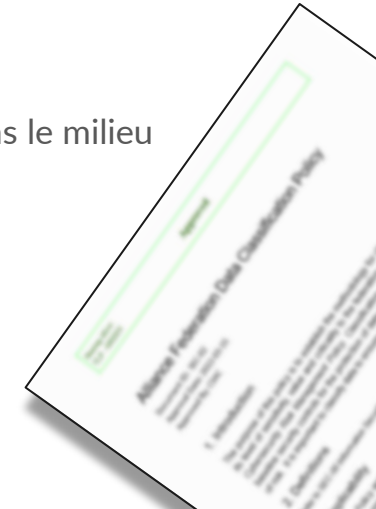
Mise en œuvre des politiques et des normes

- Vous pouvez commencer dès maintenant! (exemples : nouveaux projets et services)
- Le cadre suppose que tous les services nationaux satisferont à ces exigences
- Il faudra du temps pour mettre en œuvre certaines politiques et normes (les attentes sont établies pour chacune), et des efforts spécifiques pour ce faire seront déployés en temps et lieu

SEC-00 Glossaire de la sécurité de l'information

Statut : Document approuvé et en vigueur

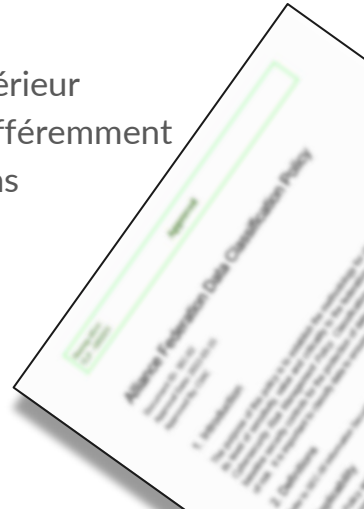
- Une source fiable pour les définitions
- Sera modifié souvent à mesure que d'autres politiques et normes seront élaborées
- Les définitions sont complexes et importantes
- Nous avons évité de redéfinir les termes « du dictionnaire » couramment utilisés dans le milieu
- Évite de définir un terme ayant un sens afin de lui en donner un autre



SEC-02 Politique de classification des données

Statut : Document approuvé et en vigueur

- Quatre niveaux de classification reposant sur l'importance ou la sensibilité relative
- Les exemples fournis pour chaque niveau de classification ne sont pas exhaustifs
- Le propriétaire des données peut classer celles-ci à un niveau supérieur, mais pas inférieur
- La classification nous permet de savoir comment traiter les catégories de données différemment
- Le propriétaire des données *nous indiquera* sa classification, de sorte que nous saurons comment traiter les données



SEC-03 Norme de gestion des données

Statut : Document approuvé et en vigueur – Première année de la période de transition

- Comprend une zone réservée aux renseignements sur les politiques et normes qui n'existent pas encore
- Ainsi, certaines sections sont plus générales, tandis que d'autres (p. ex., transmission des données) sont plus détaillées
- Sera lié à d'autres documents à mesure qu'ils seront disponibles; ce document sera modifié

SEC-05 Politique de gestion des risques liés à la cybersécurité

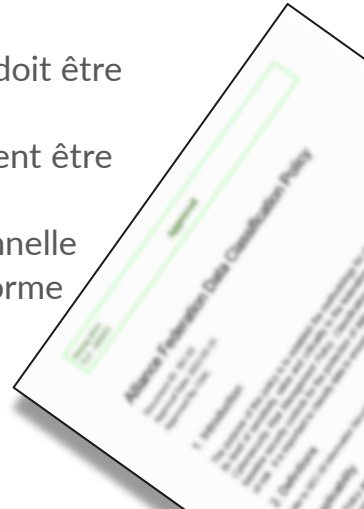
Statut : Document approuvé – Mise en œuvre en cours

- Normalise l'identification des risques et le désir de les traiter – y compris la documentation (registre)
- Au bout du compte, permettra d'améliorer la posture de cybersécurité
- Début du projet d'évaluation des risques – le CNS communiquera avec les expert(e)s en la matière pour lancer le projet
- (Le document sur la procédure d'évaluation des risques est disponible)

SEC-04 Norme de gestion des vulnérabilités

Statut : Document approuvé et en vigueur – Première année de la période de transition

- Cycle de vie de la gestion des vulnérabilités : analyse -> traitement des résultats -> mesures correctives -> reddition de compte
- Généralement, plus une vulnérabilité est grave, plus elle présente un risque élevé et doit être traitée rapidement
- Les vulnérabilités non traitées posent des risques pour l'organisation, lesquels devraient être consignés conformément à la politique de gestion des risques
- Des éléments clés tels que le Conseil consultatif et directeur sur la sécurité opérationnelle et le registre des risques n'existent pas encore et devront être définis avant que la norme entre en vigueur



Politiques et normes en cours d'élaboration

- Politique de cybersécurité
- Norme de surveillance des événements systèmes et de la sécurité
- Norme de gestion des biens

Rappels et prochaines étapes

- Toutes les politiques et normes seront disponibles ici : **https://alliancecan.ca/fr/politiques**
- Nous nous attendons à ce que le personnel hautement qualifié de la Fédération de l'Alliance se familiarise avec ces documents
- Nous suggérons aux utilisateur(-trice)s d'en faire autant
- Les commentaires sont toujours les bienvenus – courriel : security@tech.alliancecan.ca