



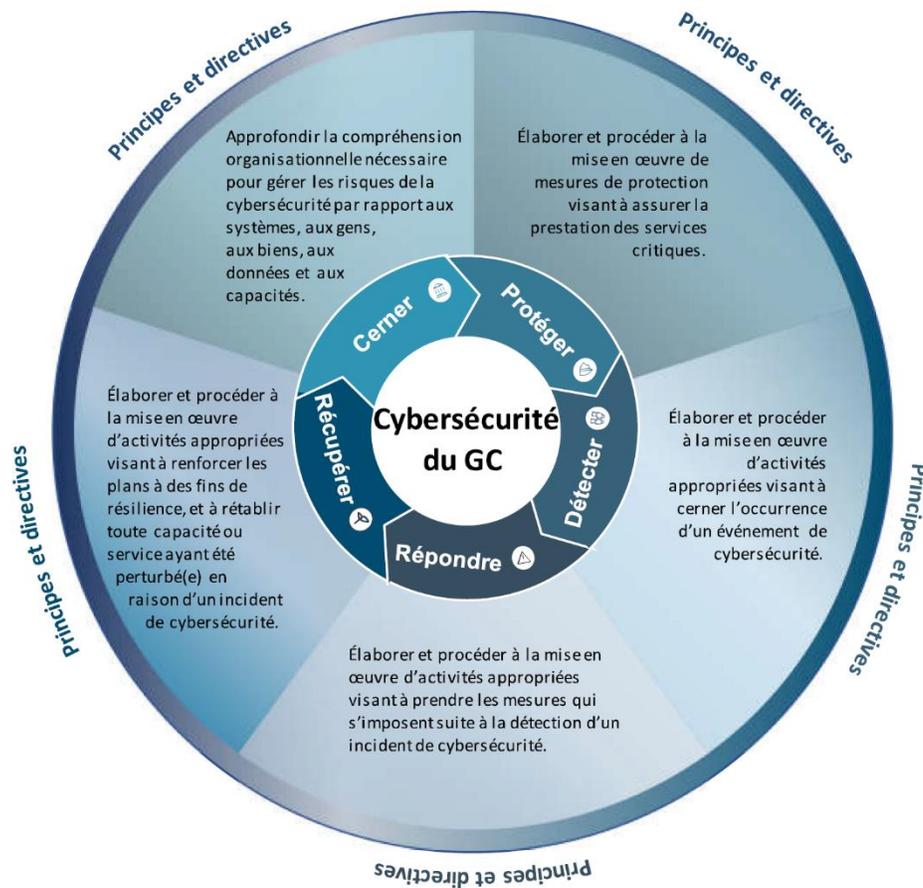
Guide pour l'Outil d'auto-évaluation de la cybermaturité (OACM)



Contexte

¹ Comme le précise la section 4.4.4.1 de la [Directive sur les services et le numérique](#), l'agent désigné pour la cybersécurité (ADC) doit « veiller à ce que les exigences en matière de cybersécurité et les mesures adéquates axées sur les risques soient appliquées systématiquement suivant une approche de type **identification, protection, détection, réponse et rétablissement** pour protéger les systèmes et services d'information ».

C'est pourquoi un ensemble de [Lignes directrices sur la gestion de la cybersécurité au gouvernement du Canada \(GC\)](#) a été établi pour aider l'ADC à satisfaire à cette exigence.



Il est prévu que l'ADC collabore² avec le dirigeant principal de l'information ministériel et le dirigeant principal de la sécurité dans l'application de ces principes et lignes directrices, dans le but d'améliorer la posture de cybersécurité au sein d'un ministère ou d'un organisme.

¹ Conformément à la mise à jour à la Directive sur les services et le numérique qui doit être publiée au début de 2022.

² Conformément à la section 4.4.4 de la Directive sur les services et le numérique.

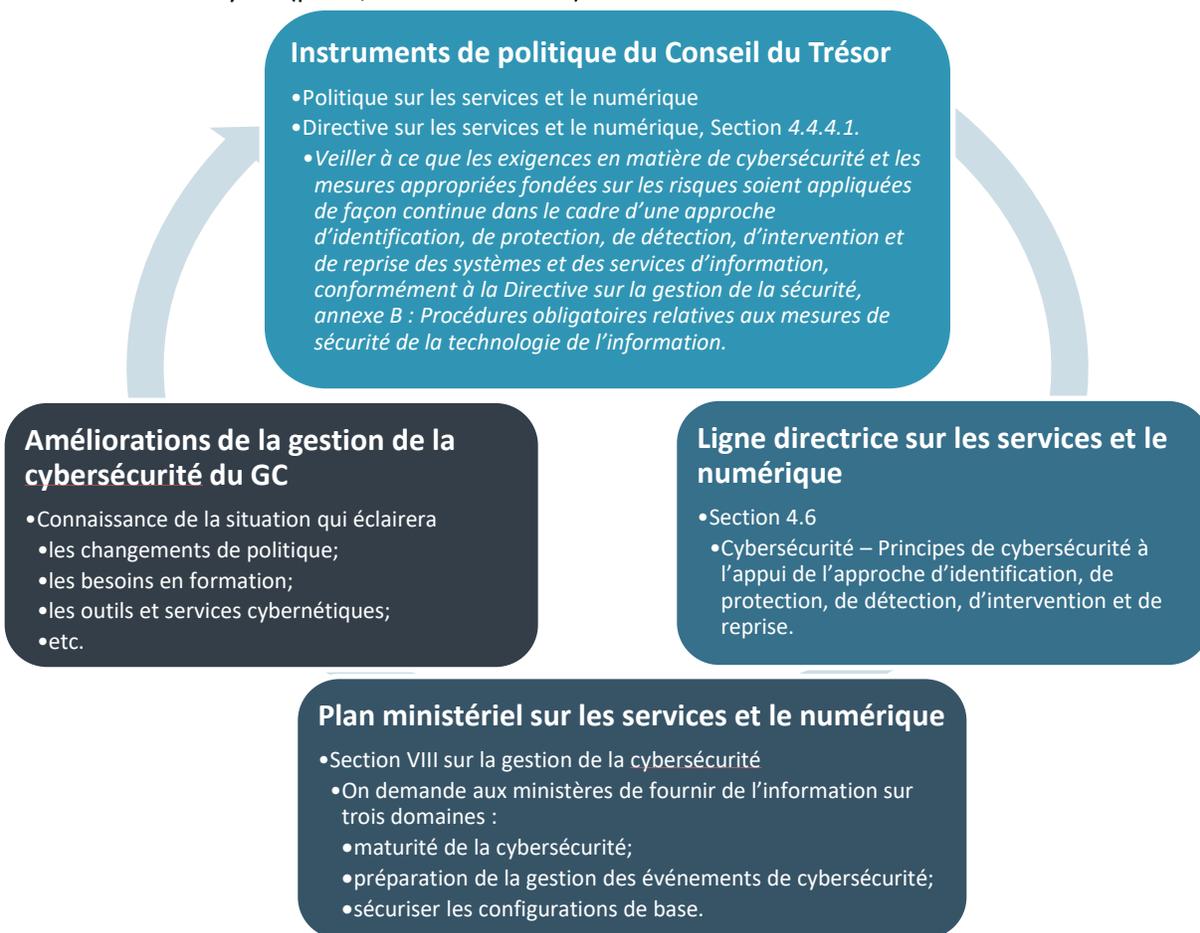


Évaluation de la cybermaturité

Pour comprendre la posture de maturité en matière de cybersécurité dans l'ensemble du gouvernement du Canada (GC), une méthodologie visant à faciliter, dans toutes les institutions du GC, l'évaluation de leur maturité en matière de cybersécurité par rapport aux pratiques exemplaires reconnues a été établie.

L'[Outil d'auto-évaluation de la cybermaturité](#) (OACM) s'harmonise avec les [Lignes directrices sur la gestion de la cybersécurité au GC](#), tel qu'illustré ci-dessous. Les buts de l'Outil sont les suivants :

- veiller à ce que les cyberrisques de l'organisation sont gérés de manière adéquate et à cerner les secteurs à améliorer;
- augmenter la vitesse de réaction aux risques éventuels en s'assurant qu'une infrastructure intégrée sécurisée et solide permette l'exécution des programmes et la prestation des services digne de confiance;
- réduire le coût et le temps consacrés à l'évaluation de la maturité de la cybersécurité par d'autres moyens (p. ex., tiers évaluateurs).





Comment accéder à l'OACM

L'[OACM](#) est hébergé dans le **Portail des applications de cybersécurité** du **Portail d'applications du Secrétariat du Conseil du Trésor (SCT) (PAS)**. Seuls les utilisateurs qui sont authentifiés au moyen de GCpass (ouverture de séance MaClé) et à qui un rôle est attribué au sein du Portail d'applications de cybersécurité sont autorisés à accéder à l'Outil.

Rôles

Il y a deux rôles qui sont attribués au sein de l'OACM :

1. **Agent désigné pour la cybersécurité (ADC);**
2. **Répondeur ministériel.**

L'ADC et le répondeur ministériel ont un accès équivalent à l'Outil où ils peuvent : accéder au rapport de l'OACM pour leur organisation, le créer et le modifier.

Bien que le répondeur ministériel soit principalement responsable d'intervenir à l'OACM, l'ADC aura accès à l'information sur l'intervention afin de l'examiner et d'approuver l'évaluation de l'organisation du GC.

Seul le SCT a le pouvoir d'attribuer un rôle à des utilisateurs dans le **Portail d'applications de cybersécurité**. Veuillez communiquer avec la [boîte aux lettres](#) des ADC de la Cybersécurité du SCT pour identifier ou modifier les rôles des ADC ou de répondeur ministériel pour veiller à ce que les représentants aient accès à l'Outil.



Étapes à suivre pour accéder à l'Outil d'auto-évaluation de la cybermaturité et le remplir

Étape 1 :

Accédez au Portail d'applications du SCT à <https://portal-portal.tbs-sct.gc.ca/home-eng.aspx>

Sélectionnez le **Portail des applications de cybersécurité** pour accéder à l'OACM.

The screenshot shows the 'Portail des applications du SCT (PAS)' interface. At the top, there are navigation links for 'Page d'accueil du PAS', 'Applications', and 'Aide'. Below this, a message states: 'ENVIRONNEMENT D'ESSAI : Ceci est l'environnement d'essai pour le Portail des applications du SCT. Voici un lien vers le Portail des applications du SCT en direct : <https://portal-portal.tbs-sct.gc.ca/home-fra.aspx>'. A yellow banner below reads: 'Nous comprenons que de nombreux employés tentent d'accéder au SSAV-GC. Nous vous demandons d'être patients pour y accéder et soumettre votre attestation. Il n'est pas nécessaire de contacter votre bureau d'aide à la TI.' The main section, 'Mes applications', contains a grid of application tiles. The 'PACS' tile, 'Version bêta - Portail des applications de cybersécurité', is highlighted with a red circle. Other visible tiles include SSAV-GC, GRFP, CRG, SCREL, CALIBRAGE, SGTCs, SIPC, RPEE, IRG, AVDRH, and SIRE.



Étape 2 :

Une fois à la page d'accueil du Portail des applications de cybersécurité, sélectionnez « **Access (Accès)** » pour accéder au questionnaire de l'OACM de votre organisation.

Portail des applications de cybersécurité

GCconnex GCpedia GCdirectory GCcollab English

Autoévaluation de la cybersécurité

[Accueil](#)

Connecté en tant que [redacted] de SCT avec le rôle de Répondeur ministériel [Quitter le PACS](#)

Bienvenue au portail des applications de cybersécurité

On entend par cybersécurité la protection de l'information numérique et l'intégrité de l'infrastructure qui héberge et transmet l'information numérique.

Autoévaluation de la cybermaturité (AECM)

Accédez au questionnaire d'évaluation pour mesurer la cybermaturité de votre ministère en fonction de pratiques exemplaires reconnues.

[Accéder](#)

Version : 1.0.0



Étape 3 :

Vous aboutirez à la page de l'OACM de votre ministère, qui indiquera les évaluations achevées ou en cours pour votre organisation.

Pour commencer une nouvelle évaluation, sélectionnez « **Commencer une nouvelle évaluation** ».

Il n'est pas nécessaire de réaliser une évaluation au complet en un temps. Vous pouvez enregistrer vos travaux au fur et à mesure, et modifier une évaluation existante en tout temps.

Portail des applications de cybersécurité [GCconnex](#) [GCpedia](#) [GCdirectory](#) [GCcollab](#) English

Autoévaluation de la cybersécurité

[Accueil](#)

Connecté en tant que [redacted] de [SCT](#) avec le rôle de **Répondeur ministériel** [Quitter le PACS](#)

Autoévaluation de la cybersécurité

[Aide](#)

Secrétariat du Conseil du Trésor du Canada : Autoévaluations de la cybermaturité

Commencer une nouvelle évaluation

Filtrer les articles Affiche 1 à 1 de 1 entrées | Afficher 10 entrées

Date de la dernière modification (AAAA-MM-JJ) ↑↓	Modifié par ↑↓	État ↑↓	Cote de maturité ↑↓	Actions
				👁 ✎

1



Étape 4 :

Lorsqu'une nouvelle évaluation a été lancée (ou si vous souhaitez modifier une évaluation en cours), vous serez acheminé à un sondage qui se divise en cinq onglets correspondant aux **principes de gestion de la cybersécurité** : 1) **Identification**; 2) **Protection**; 3) **Détection**; 4) **Réponse** et 5) **Rétablissement**.

- *Si vous souhaitez obtenir de plus amples renseignements et d'orientation sur les principes de gestion de la cybersécurité du GC, nous vous invitons à consulter les [Lignes directrices sur la gestion de la cybersécurité du GC](#) à partir de GCpédia.*

Les répondeur ministériel doivent répondre au sondage en répondant à **toutes** les questions sous chacun des onglets correspondant aux principes de gestion de la cybersécurité.

Le répondeur ministériel peut choisir « **Hors du champ de compétence du ministère** » si la responsabilité décrite dans le questionnaire du sondage relève d'une autre organisation. Si vous le sélectionnez, une boîte de commentaire s'affichera et vous demandera de nommer l'organisation responsable.

Après avoir répondu au sondage, sélectionnez « **Sauvegarder** » dans la partie inférieure de la page Web, puis sélectionnez l'onglet « **Résultats** ».

Portail des applications de cybersécurité GCconnex GCpédia GCdirectory GCcollab English

Autoévaluation de la cybersécurité

Accueil → Autoévaluation de la cybersécurité

Connecté en tant que [redacted] de S.C.T avec le rôle de Répondeur ministériel Quitter le PACS

Autoévaluation de la cybersécurité

► Aide

Identification 3,0 Protection 3,4 Détection 3,3 Réponse 3,3 Rétablissement 3,8 Résultats 3,3

Gestion des biens

ID.AM-1 * Les appareils et les systèmes physiques au sein du ministère sont répertoriés.
À quel point le processus pour répertorier les appareils et les systèmes physiques est-il complet? (obligatoire)

- 0 - Aucun processus d'inventaire n'existe pour les appareils et les systèmes physiques.
- 1 - Les appareils et les systèmes physiques sont cernés et répertoriés de façon ponctuelle.
- 2 - Certains des appareils et des systèmes physiques ont été cernés et un inventaire de ces biens a été documenté.
- 3 - Les appareils et les systèmes physiques ont été cernés et un inventaire de ces biens est maintenu de façon régulière, en fonction d'une politique.
- 4 - Les appareils et les systèmes physiques font l'objet d'un cycle de gestion défini des biens (création, traitement, entrepôt, transmission, suppression et destruction).
- Hors du champ de compétence du ministère

ID.AM-2 * Les plateformes de logiciel et les applications au sein du ministère sont répertoriées.
À quel point le processus de répertoire des logiciels et des applications est-il complet? (obligatoire)

- 0 - Les logiciels et les applications ne sont pas cernés et répertoriés.
- 1 - Les logiciels et les applications sont cernés et répertoriés de façon ponctuelle.
- 2 - Certains logiciels et certaines applications ont été cernés et un inventaire de ces biens a été documenté. Toutefois, il n'existe aucun processus défini pour la création de l'inventaire.
- 3 - Les logiciels et les applications sont cernés et un inventaire de ces biens est maintenu de manière régulière, en fonction d'une politique ou d'un processus défini.
- 4 - Le logiciel et les applications sont sujets à un cycle de vie défini de gestion des biens (création, traitement, stockage, transmission, suppression et destruction).



Étape 5 :

Selon les réponses au sondage, l'onglet « **Résultats** » résumera le niveau de cybermaturité de l'organisation.

Votre organisation recevra une cote générale entre 0 et 4, ainsi que des notes réparties selon les cinq principes de gestion de la cybersécurité (c.-à-d., identification, protection, détection, réponse et rétablissement).





Après avoir rempli l'OACM, l'historique de l'évaluation s'affichera à la page de l'OACM avec les options suivantes :

- **visualiser une évaluation** en choisissant l'icône de l'œil;
- **modifier ou remplir une évaluation** en sélectionnant l'icône du stylo;
- **exporter l'évaluation en format Excel** en sélectionnant « **Exporter vers Excel** ».

Portail des applications de cybersécurité [GCconnex](#) [GCpedia](#) [GCdirectory](#) [GCcollab](#) [English](#)

Autoévaluation de la cybersécurité

[Accueil](#)

Connecté en tant que [redacted] de [SCT](#) avec le rôle de **Répondeur ministériel** [Quitter le PACS](#)

Autoévaluation de la cybersécurité

[Aide](#)

Secrétariat du Conseil du Trésor du Canada : Autoévaluations de la cybermaturité

[Exporter vers Excel](#)

Filtrer les articles Affiche 1 à 1 de 1 entrées | Afficher entrées

Date de la dernière modification (AAAA-MM-JJ) <input type="text" value="↑↓"/>	Modifié par <input type="text" value="↑↓"/>	État <input type="text" value="↑↓"/>	Cote de maturité <input type="text" value="↑↓"/>	Actions
2021-10-27	[redacted]	Ébauche (100% complété)	3,3	<input type="checkbox"/> <input type="checkbox"/>

1

Version : 1.0.0



Coordonnées

Si vous éprouvez des difficultés techniques avec l’Outil, veuillez communiquer avec nous à l’adresse électronique suivante :

- DOCS/ADCS DOCS-ADCS@tbs-sct.gc.ca

Si vous avez des questions d’ordre général ou souhaitez obtenir de plus amples renseignements, veuillez communiquer avec nous à l’adresse électronique suivante :

- Cyber-SCT zbtbscybers@tbs-sct.gc.ca