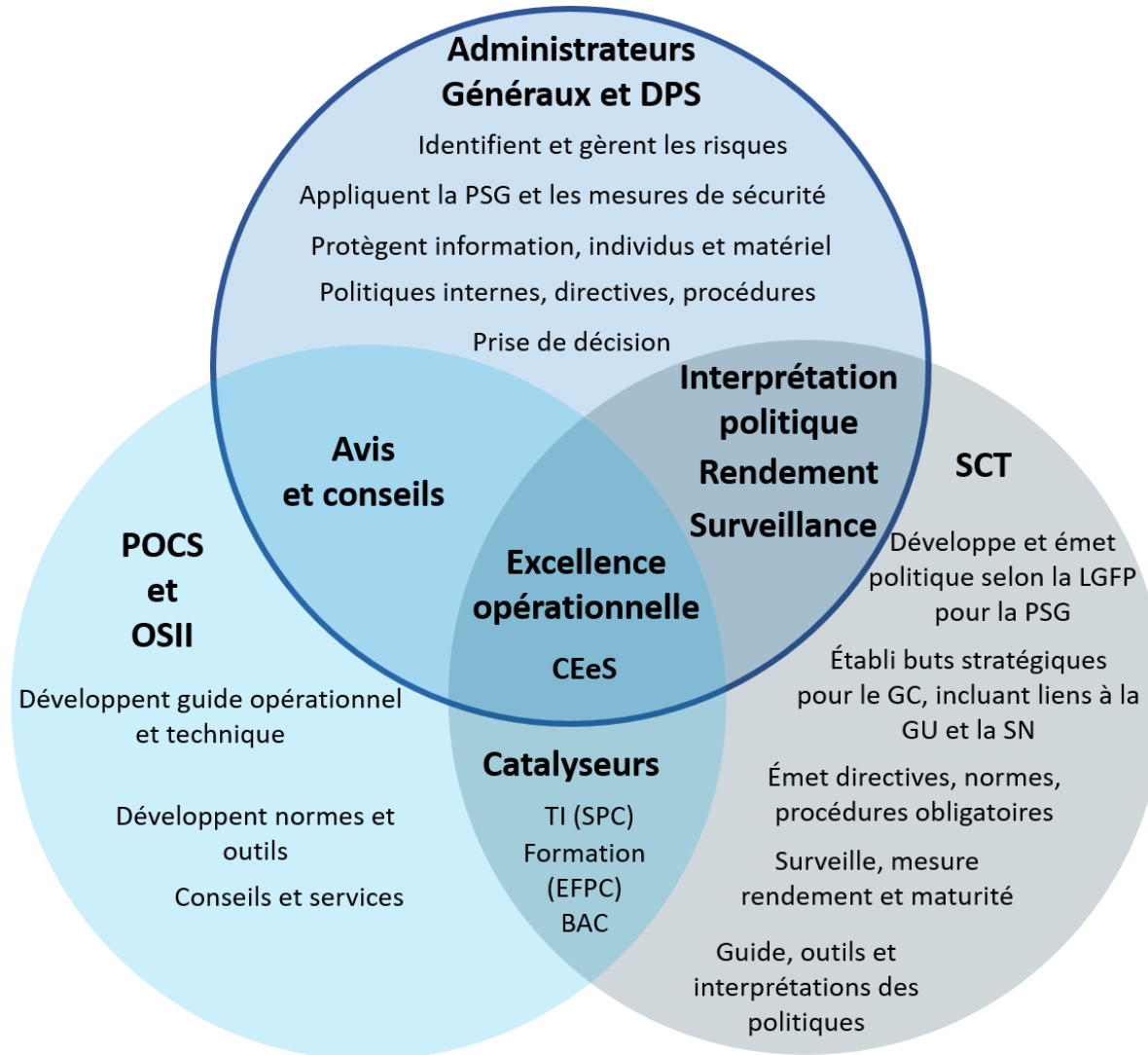


Rôle du Centre d'excellence en sécurité

Historique et contexte

- Le CEES, anciennement connu comme étant le Centre de perfectionnement (CdP) des ASM, est en opération depuis 2012
- Son mandat fut renouvelé en 2022 par le Conseiller à la sécurité nationale et au renseignement (CSNR) auprès du Premier ministre pour cinq années additionnelles
- Mission : Diriger le développement d'une communauté de la sécurité informée, résiliente et intégrée à travers l'ensemble du gouvernement du Canada (GC)
- Hébergé au BCP, le CEES soutient :
 - Les dirigeants principaux de la sécurité (DPS) du GC et une communauté d'environ 3 500 spécialistes de la sécurité
 - Le rôle du CSNR en tant que champion de la sécurité du gouvernement
 - Le mandat des POCS dans l'apport d'orientations opérationnelles agiles et la prestation d'événements d'apprentissage/de réseautage, incluant le rôle du BCP en tant que POCS en matière de préparation à travers la conception et la facilitation de divers exercices
 - Un plus grand partage de l'information en lien avec la sécurité et le renseignement et les objectifs d'intervention du GC

Les forces du CEES



- Situé au cœur de la communauté, le CEES agit au nom des ministères en tant que catalyseur et capacité d'intensification pour répondre à leurs besoins opérationnels
- En tant que leader fonctionnel, il met à profit toutes les ressources disponibles pour développer des outils et des solutions innovantes qui ont été approuvées par les POCS et le SCT
- Étant hébergé par le BCP, le CEES offre une perspective unique en matière de défis liés à la sécurité
- Une forte gouvernance est en place, lui permettant d'atteindre des résultats et y ajoutant de la valeur
- Il est visionnaire, allant au-delà des politiques existantes
- Il est agile et a démontré sa capacité à fournir un travail significatif en de courts lapses de temps

Excellence en sécurité : #Prêt et Préparé

Objectifs stratégiques

Effectif

Investir dans le capital humain par l'éducation, les exercices, la formation et le mentorat, et maintenir ainsi que perfectionner un effectif de sécurité compétent capable d'atténuer les risques connus et émergents;



Communauté

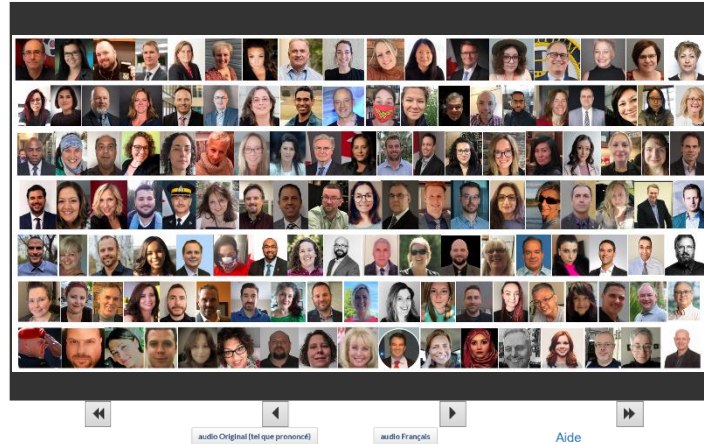
Établir un « centre communautaire » où les praticiens de la sécurité peuvent bâtir ou élargir leurs réseaux en échangeant de l'information ou en collaborant pour soutenir la préparation en matière de sécurité dans l'ensemble du gouvernement;

Connaissances

Tirer parti de la compréhension collective du contexte de la sécurité au Canada pour soutenir et améliorer la résilience à l'échelle du gouvernement.

Plus fort ensemble En connectant la communauté

Government of Canada Virtual Security Summit 2020



audio Original (tel que prononcé) audio Français Aide



Government of Canada / Gouvernement du Canada

GCcollab

Home Communities The Wire Groups Members Career More

Groups

Security Centre of Excellence / Centre d'excellence en sécurité

Security Centre of Excellence / Centre d'excellence en sécurité

Activity Discussion Files Events More

Description

On this space you will find the latest information of interest to the security community, as well as tips, tips, and critical information to support and strengthen the security function across government. Here, security functional specialists can connect, engage, and share best practices with each other in a dynamic and collaborative forum open ONLY to the GC security community.

User Guide About Us Services Security Knowledge Sharing Contact

Welcome to the Security Centre of Excellence, your Centre for Development.

As your Centre for Development, the SCOE is pleased to support our security colleagues with this space on GCcollab. It is part of our ongoing commitment to you, the security community, and to a robust security-positive government-wide. We are bringing together, and future such as to help facilitate the sharing of information, ideas, and solutions to resolve those vital links.

Join the SCOE mailing list to be informed about hot topics in security, upcoming training and networking events, and the latest tools that empower GC security functional specialists.

What's New? / Quoi de neuf?

NEW: The SCOE has recently developed and published a new group on GCcollab: Security Scoping Tools. Your CISO/CSSP can help us the names and email addresses of their respective officials regarding access at SCOE.

NOUVEAU: Le CSES a récemment développé et publié un nouveau groupe sur GCcollab: L'Élaboration de l'état de sécurité. Votre CISO/CSSP peut nous faire parvenir les noms et adresses des fonctionnaires des services de sécurité en matière d'accès au CSES.

Security Centre of Excellence / Centre d'excellence en sécurité

SCOE-CEES

Security Community Bulletin

Welcome to the third edition of the Security Centre of Excellence (SCOE) Security Community Bulletin. Our goal is to inform CSOs and security functional specialists of the latest tools, events, and topics of interest. We dedicate this edition to the unyielding efforts of the GC security community in response to COVID-19.

For quick access to knowledge sharing by subscribing

Security Centre of Excellence / Centre d'excellence en sécurité

SCOE-CEES

Security Community Bulletin

The global GC security support col throughout training to work from These are t

Welcome to the January 2021 edition of the Security Community Bulletin! The team at the Security Centre of Excellence (SCOE) wants to wish all of you a very Happy New Year. Here's to a safe and secure 2021!

For quick access to the full content of each initiative, join the SCOE group on GCcollab, our knowledge sharing and community networking hub. Stay in the know with future bulletins by subscribing here.

- PSI
- HC
- CC
- GA

Upcoming Events

Public Sector Network – Disaster Management and Recovery – Virtual Event – January 22, 2021 (ENGLISH only)

A CSIS Virtual Expert Briefing – Big Data Surveillance and Security Intelligence: current and future challenges – January 28, 2021 (GC employees only)

Learning Hub – Canadian Centre for Cyber Security

You can now access three of the most popular pre-recorded courses on cyber security.

- Course 107 – Cyber Security in the GC for non-IT Employees
- Course 110 – Cyber Security in the GC and Online Exposure
- Course 111 – Cyber Security in the GC for Home and Telework

GC Virtual Security Summit 2021 scheduled for the week of May 17, 2021!

What's New? / Quoi de neuf?

NEW: The SCOE has recently developed and published a new group on GCcollab: Security Scoping Tools. Your CISO/CSSP can help us the names and email addresses of their respective officials regarding access at SCOE.

NOUVEAU: Le CSES a récemment développé et publié un nouveau groupe sur GCcollab: L'Élaboration de l'état de sécurité. Votre CISO/CSSP peut nous faire parvenir les noms et adresses des fonctionnaires des services de sécurité en matière d'accès au CSES.

From the onset of the pandemic in March 2020, the focus on BCM has increased across the Government of Canada. There are two main concepts that deserve to be highlighted here:

Tips on Business Continuity Management (BCM) and Emergency Management in light of the pandemic

- First, BCM is, in the current circumstances and possibly in future other type of events, a prioritization exercise that is continuous and goes beyond the critical services. With resources and technology supporting remote work, organizations will need to continue to balance the delivery of other priorities and programs while ensuring critical services remain available.
- Second, BCM is about fluidity and flexibility and should move away from a strict procedural manual that is dusted off in the case of an unpredictable event.

Lessons learned from the Pandemic will be used to inform a BCM program reveal strategy including establishing a lifecycle management framework to ensure data on BCM and critical services remain evergreen. More details on the strategy will be available in the coming months.

Prioritization:

- Establish continuous communication between Security and Senior Management
- Establish continuous communication between Security and Senior Management
- Ensure that critical services are functioning well—if not, provide surge capacity to assist
- Prioritize all other services of the organization based on resource availability and management priority

Flexibility:

- Conduct periodic review

Excellence opérationnelle

Le BCP est responsable de la supervision des **activités administratives et des dépenses** du CEES

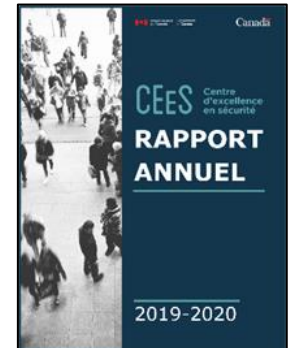
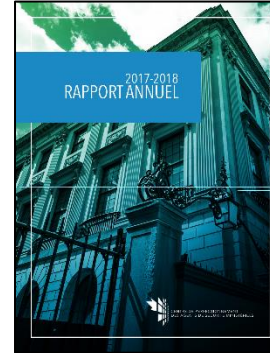
Une gouvernance via un Conseil de gestion comprenant six représentants des DPS qui approuvent les priorités, les plans de travail et les rapports annuels, ainsi qu'un Conseil de direction comprenant quatre représentants des POCS qui fournissent une direction stratégique

Un budget d'approximativement 1,5M\$/AF via PE

- 30K pour les grandes organisations (plus de 5 000 employés)
- 20K pour les organisations moyennes (1 000 à 5 000 employés)
- 10K pour les petites organisations (100 à 1 000 employés)
- 5K pour les micro organisations (moins de 100 employés)

Une organisation tournée vers les résultats où la performance est mesurée régulièrement et des objectifs sont fixés. La communauté est très satisfaite des services, de l'optimisation des ressources et du retour sur investissement. Il y a eu une croissance significative de tous les services.

Un fonctionnement à l'aide de **stratégies de gestion des ressources humaines** (postes indéterminés, affectations et employés à terme) pour s'assurer que l'organisation demeure relativement petite et s'adapte aux changements dans les priorités en matière de sécurité tout en restant dans les limites du financement offert par la communauté



Pour l'ensemble de la communauté



Recrues

- Révision du curriculum
- Coopération avec CFP
- Création de lieux de rencontre (réseautage rapide, foire de l'emploi, etc.)

JPS

- Réseautage
- Activités d'apprentissage
- Présentation de leur travail

Leaders en sécurité

- Apprentissage continu
- Des outils à portée de main
- Offre de conseils

DPS

- Session d'orientation
- Guide des opérations de sécurité du DPS
- Offre de conseils

Soutien aux opérations avec les avis et l'orientation

Équiper la communauté de connaissances

Processus de demande

Les demandes sont soumises au Centre

- ▶ Les demandes sont reçues via diverses sources:
 - ▶ Courriels
 - ▶ Appels téléphoniques
 - ▶ Rencontres en personne (Diffusion, activités, etc.)
- ▶ Les demandes sont consignées dans un document de suivi avec des métadonnées:
 - ▶ Nom du demandeur
 - ▶ Nom de l'organisation
 - ▶ Date de réception
 - ▶ Résumé de la demande
 - ▶ Mesure de sécurité en cause ou autre
 - ▶ Nom du répondant au CEES
 - ▶ Besoin d'un suivi O/N

Processus de validation

Les demandes sont validées pour s'assurer que leur portée et leur nature soient bien comprises

- ▶ Les demandeurs sont contactés afin de valider leurs besoins et attentes
- ▶ Les critères de portée et de nature appuient le Processus de recherche et d'analyse:
 - ▶ Taille de l'organisation
 - ▶ Secteur d'activités de l'organisation
 - ▶ Échéanciers et priorités
 - ▶ Composantes nationales v. organisationnelles
 - ▶ Nature (partage de matériel existant v. développement de nouveau matériel)
- ▶ Les demandes hors du mandat du CEES sont transférées aux autorités concernées (CDTE, POCS, etc.)
- ▶ Entente sur les prochaines étapes est conclue avec le demandeur (si nécessaire)

Processus de recherche et d'analyse

Une recherche et une analyse est effectuée pour collecter et partager des renseignements pertinents et à jour

- ▶ La recherche démarre à l'interne en usant de sources diverses:
 - ▶ Document de suivi du CEES
 - ▶ Disques partagés du CEES
 - ▶ InfoXpress du BCP, GCdocs, InfoNet
 - ▶ Bibliothèque du BCP
 - ▶ OutilsGC (GCconnex, GCcollab, GCpédia, GCintranet...)
- ▶ La recherche démarre à l'externe en usant de sources diverses:
 - ▶ Sources ouvertes
 - ▶ Ressources partagées par le GC
 - ▶ Autres sites/collections hors du GC (Conférence Board du Canada, etc.)
- ▶ La communication et l'échange de renseignements avec les intervenants sont lancés:
 - ▶ POCS
 - ▶ OSII
 - ▶ Facilitateurs
 - ▶ Autres experts en la matière
- ▶ Le matériel assemblé est révisé et analysé pour s'assurer que des liens soient faits avec la demande et que les attentes soient remplies
- ▶ Le matériel pertinent et à utiliser est isolé
 - ▶ Conception d'une proposition de réponse et révision à l'interne
 - ▶ Une révision à l'externe est effectuée (si nécessaire)

Processus de réponse

Le demandeur reçoit une réponse à sa/ses demande(s)

- ▶ La réponse est envoyée au demandeur par courriel
- ▶ D'autres personnes sont copiées ou informées de la réponse
- ▶ Si nécessaire:
 - ▶ Une plus ample révision ou recherche auprès de différentes autorités peut être faite et est offerte au demandeur
 - ▶ L'information peut devoir être partagée avec d'autres intervenants
- ▶ La réponse est jointe au document de suivi du CEES
- ▶ Un processus de rétroaction est disponible afin d'obtenir des commentaires du demandeur

Processus de rapport

Des statistiques et tendances sont disponibles et utilisés pour orienter les futurs projets et événements d'apprentissage

- ▶ Des graphiques & des rapports
 - ▶ Sont créés en fonction du document de suivi du CEES
 - ▶ Sont partagés avec le Conseil de gestion
- ▶ Les graphiques sommaires sont partagés dans le Rapport annuel du CEES et distribués à la communauté de la sécurité du GC
- ▶ Les statistiques et les tendances sont notés dans le plan de travail du CEES et utilisés pour discuter de futurs événements et projets, en fonction du Plan stratégique du CEES

Sommet sur la sécurité du GC

- Événement annuel phare et sans frais pour à l'apprentissage des membres de la communauté de la sécurité du GC
- Devenu une expérience entièrement virtuelle depuis le début de la pandémie



2021 GC VIRTUAL SECURITY SUMMIT

Security: Going the Distance

May 17 – 20, 2021

**Sommet virtuel sur la sécurité
du GC de 2021**

La sécurité : le cœur à l'ouvrage

Du 17 au 20 mai 2021

Série de conférences

- Sans frais pour les membres du Centre d'excellence en sécurité
- Conférence sur un sujet opportune par des experts dans leur champ d'intérêt respectif
- Trois fois par année

Les impacts de la COVID-19 sur le milieu de la sécurité, un regard à travers les futurs



Bureau du Conseil privé



Reprise et préparation pour le « nouveau normal »

- Assouplissement des restrictions en milieu de travail – Un succès sur le plan de la sécurité
- Comprendre et gérer les risques à la sécurité des outils de collaboration virtuelle
- Reprise et préparation pour le « nouveau normal » - Considérations clés et priorités pour la communauté de la sécurité
- La fraude - Une perspective pour la communauté de la sécurité

Exercice Chaos dans la métropole



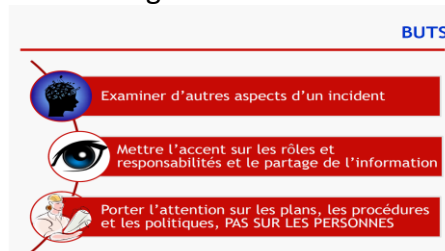
- A conçu et facilité un exercice sur table dans l'ensemble du GC, y faisant participer simultanément 45 organisations et 500 employés
- A testé les connaissances du PCA et la réponse à des événements importants affectant le GC
- A testé le Protocole d'échange d'information sur les incidents marquants
- Un scénario impliquant un tremblement de terre

Autres exercices

Chaos dans la ville



Branle-bas au gouvernement



Prêt et préparé?



Exercice du COSM



Jeunes professionnels de la sécurité



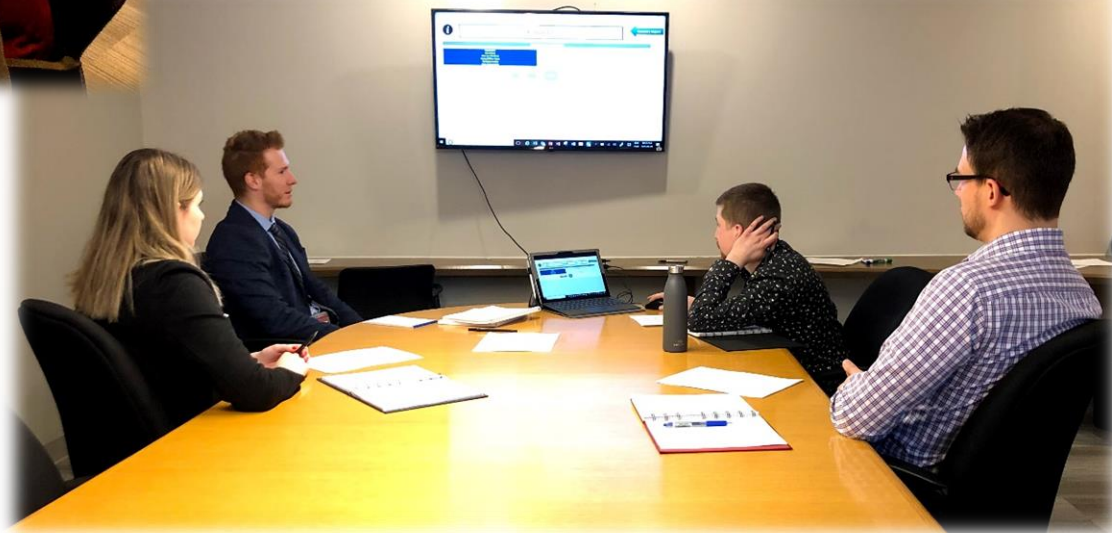
- Un réseau de jeunes professionnels de la sécurité
- Présidé par le CEES
- Trois activités par année

Découvrir de nouveaux talents

Agrandir son réseau

Partager des connaissances

Innover et apprendre



Activités de recrutement

- Rassembler les gestionnaires d'embauche de la sécurité et les étudiants en un endroit
- Soutenir la croissance de la communauté de la sécurité du GC
- Faciliter la découverte de nouveaux talents



Les gestionnaires y découvrent un grand nombre de nouveaux talents pour beaucoup moins de temps et d'énergie

Guide des opérations de sécurité du DPS

- A complété la révision du Guide de l'agent de sécurité ministérielle conçu en 2015 afin qu'il s'aligne avec la nouvelle Politique sur la sécurité du gouvernement
- A réalisé des entrevues avec des DPS débutants et chevronnés pour obtenir des conseils
- A consulté les POCS et les OSII à propos du contenu
- Le texte dans les deux langues officielles a été finalisé en mars 2021 et sa publication est attendue pour Q1 2021-22
- La promotion de cet outil de référence se fera sur diverses plateformes
- Une proposition pour des sessions d'orientation et de mentorat pour DPS est à l'étude



Développer des initiatives importantes pour la communauté en collaboration avec les partenaires



Engagement

Identifier les tendances et les besoins de la communauté de la sécurité du GC en se basant sur des statistiques, des enquêtes, des sondages et les priorités du GC



Planification

Créer un plan (activités & échéanciers) et conceptualiser le matériel nécessaire, aligné avec toutes les politiques et lignes directrices du GC pertinentes



Exécution

Organiser des groupes de travail ou des projets pilotes, produire le matériel, conduire des révisions avec des experts en la matière de la communauté de la sécurité du GC et consulter les Principaux organismes chargés de la sécurité



Contrôle

Suivre la progression du projet et le niveau d'efforts, s'assurer du respect des échéanciers et que les étapes clés sont atteintes



Conclusion

Promouvoir le matériel créé auprès de comités, durant des événements et sur les OutilsGC, garder à jour le matériel et répondre aux questions de la communauté de la sécurité du GC

ANNEXES

Exemples d'outils

Trousse de formation du GC sur les intrus armés

- Dans les six mois suivant la demande, fournir une trousse de formation complète incluant le matériel de breffages pour la haute gestion et les employés ainsi que la vidéo canadienne du GC
- Plan présenté au CEPASM, la communauté a accepté d'utiliser une terminologie commune
- Lancée au Sommet sur la sécurité du GC de 2018 par la CSNR, un an avant que la nouvelle EUEI du SCT ne demande des exercices annuels
- Inclue dans le cours de sensibilisation à la sécurité de l'ÉFPC pour tous les employés du GC
- Non disponible au public mais partagée avec d'autres niveaux de gouvernement et les universités, sur demande (Provinces/Municipalités/Universités)
- Partenaires clés: GRC, BDPRH, IRCC, AMC, ARC et Justice

Il n'y aura peut-être jamais d'intrusion armée dans votre milieu de travail... Mais si l'impensable se produit.

SAVEZ-VOUS QUOI FAIRE?

SE SAUVER
Votre première option est de vous sauver.

SE DÉFENDRE
Vous devriez choisir cette option uniquement si votre vie est en danger immédiat.

SE CACHER
Trouvez un endroit où vous êtes bien caché et protégez-vous des coups de feu.

Familiarisez-vous avec votre environnement – établissez un plan!

Consultez la page Intrusion armée sur **GCcampus** ou contactez votre équipe de sécurité pour plus de renseignements
myschool-monecole.gc.ca

Canada

INTRUSION ARMÉE

Savez-vous quoi faire?
Regardez autour de vous. Comment pourriez-vous vous enflammer? Ou pourriez-vous vous cacher? Que pourriez-vous faire pour survivre? Même si le risque qu'un agresseur armé s'introduise dans votre lieu de travail est faible, vous pouvez être prêt à faire face.

Congniez votre environnement, établissez un plan!
Le plus important c'est d'agir immédiatement

SE SAUVER

Votre première option est de vous sauver.

- Si vous entendez des coups de feu ou des cris, fuyez.
- Ne prenez rien avec vous, partez sans tarder.
- Avertissez ceux que vous croisez de la menace.
- Partez, même si certains ne vous suivent pas.
- Appelez le 911 lorsque vous pouvez le faire en toute sécurité.

SE CACHER

Trouvez un endroit où vous êtes bien caché et protégez-vous des coups de feu.

- Si vous ne pouvez pas fuir, cachez-vous.
- Restez silencieux et immobiles pour éviter qu'on vous détecte.
- Verrouillez ou barricadez les portes, fermez les stores, éteignez les lumières et vos téléphones.
- Ne laissez personne entrer dans votre zone sécurisée.
- Appelez le 911 lorsque vous pouvez le faire en toute sécurité, plus attendez la police.

SOUVEZ-VOUS

Il y a trois options possibles si un agresseur armé s'introduit dans votre lieu de travail!

SE SAUVER
Sauvez-vous!

SE CACHER
Évitez de vous faire voir!

SE DÉFENDRE
Comme dernier recours, soyez déterminé et combatif!

Il ne s'agit pas d'une série d'étapes progressives. Le premier choix que vous faites peut avoir à changer en fonction de la situation et de l'endroit où vous êtes.

POUR EN SAVOIR PLUS ⓘ

Apprenez à connaître les meilleures stratégies pour répondre à ce type de situation. Contactez les responsables de la sécurité de votre institution pour demander plus de renseignements.

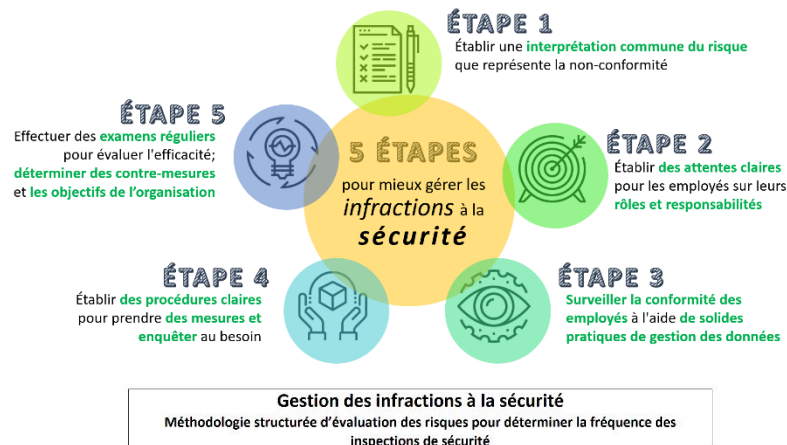
Canada

SENSIBILISATION ACCRUE : VIDÉO SUR L'INTRUSION ARMÉE



Guide sur la gestion des infractions à la sécurité

- Délégué par le Greffier de développer un approche cohérente pour le GC
- Révisé les pratiques de la GC et présenté les résultats clés au CEPASM
- Offert une trousse complète comprenant comment établir/changer la culture de sécurité et engager les employés à tous les niveaux au sujet des risques, de l'accueil jusqu'aux mesures correctives
- Développé un outil pour déterminer la fréquence des inspections basée sur un facteur de risque
- Assuré un financement par RDDC afin de développer les exigences d'un SGC de la TI
- Éléments inclus dans la stratégie de protection de l'information présentée aux sous-ministres et à l'équipe spéciale sur la science et la sécurité nationale
- Partenaires clés: MDN, SCRS, BDPRH, GRC, SCT, AMC, ISDE



Voir rapport sommaire

Faire l'évaluation de risque

Trousse du filtrage de sécurité

- La communauté a demandé un gabarit uniforme, adaptable et facile d'utilisation qu'elle pourrait utiliser afin de prendre des décisions en matière de risques
- Financée par le Ministère de Patrimoine Canada (25K)
- Contient plus de 50 documents opérationnels d'appui, gabarits, guides, PON, questionnaires
- Comprend une matrice du risque en format Excel afin de soutenir la prise de décision et générer une approche cohérente à travers la communauté
- L'approche et les outils permettent de terminer rapidement les dossiers à faibles risques, de concentrer les efforts sur ceux à hauts risques et de soutenir un processus d'embauche rapide en maintenant un niveau de risque acceptable
- Révisée par la communauté de pratique et présentée au CSPGC
- Partagée avec l'ÉFPC pour le développement de cours
- Partenaires clés: BCP, CFP, EFPC, SCRS, GRC, SCT

Phase 1 - Indicateurs sur les formulaires de sécurité

INDICATEURS ADMINISTRATIFS

Type de dossier	Non	Autre
Niveau de risque	Non	Cote de fiabilité
Informations diffusées ou divulguées	Non	
Type de poste	Administratif	
Accès à un véhicule	Non	
Accès aux armes à feu	Non	
Recommandation de poste	Non	Recommandé

INDICATEURS DES FORMULAIRES

Pays de naissance	Couche	
Statut au Canada	Non	Citoyen canadien
Filtrage préalable de gouvernement	Non	
Développements d'activités criminelles	Non	
Emplois multiples	Non	
Emploi concurrent	Non	
Emploi dans le passé	Non	
Type de contrat	Non	
Emploi à l'étranger	Non	
Voyageurs à l'étranger	Non	
Niveau à l'étranger	Non	
Statut militaire	Non	

INDICATEURS FINANCIERS

Ratio de dette	Ratio élevé (0,68)	
Évaluation de crédit	Non	
Comptes	Non	
Évaluation de crédit	Évaluation à hauts risques	
Montant de la dette	Non	
Factures	Non	
Propriété de biens	Non	
Prêt sur salaire	Non	
Requêtes	Non	
Comptes en collection	Non	
Écart de crédit	Non	
Fluctuation de crédit	Non	
Montant de la dette	Non	
Montant de la dette	Non	

CRIMINALITÉ

Précédents en matière d'activités criminelles	Non	
Précédents en matière de violence	Non	

Commentaires supplémentaires

Sommaire de l'évaluation

Bas

Rapport d'analyse du filtrage de sécurité

Nom et prénom du sujet:	
Titre du poste:	
DDN:	
Niveau de filtrage de sécurité requis:	Cote de fiabilité
Numéro du dossier:	
Nom de l'analyste de sécurité:	
Date de l'analyse:	

Évaluation du risque	Résultat	Commentaires
Indicateurs sur les formulaires de sécurité	BAS	
Indicateurs des vérifications de sécurité	BAS	
Évaluation du risque	Résultat	Commentaires
Vérification de crédit	Info défavorable	
Vérification d'antécédents criminels	Info défavorable	
SCRS	N/A	
Recommandation	Commentaires	
Octroyer		
Analyse supplémentaire requise		

Déroulement du processus et évaluation des risques

Réception	Filtrage pré-indicateurs	Processus d'évaluation des risques	Décision	Mesures de suivi
Réception de la demande de filtrage	Utilisation de la Matrice des risques pour déterminer les vulnérabilités du poste	Vérifications pour évaluer le risque posé par la personne	Décision éclairée, d'après le niveau de risque du poste et de la personne	Assurance permanente à l'égard de la fiabilité et de la loyauté d'une personne envers le Canada
Demande affectée à un agent de filtrage Attribution du niveau de priorité de la demande	Indicateurs utilisés pour déterminer le niveau de risque : - Types de cote/autorisation - Niveau de cote/autorisation - Précédente évaluation défavorable au dossier - Type de poste - Accès à la flotte - Accès à des armes à feu - Délais au sujet du poste	Indicateurs utilisés pour déterminer le niveau de risque : Indicateurs de filtrage (en fonction des formulaires) - Pays de naissance - Filtrage préalable de gouvernement - Divulgation des antécédents criminels Indicateurs de filtrage (en fonction des vérifications) - Finances - Ratio d'endettement - Cotes de crédit - Manquant des dettes - Faillites - Proposition de consommateur - Arrivé en matière de paiements - Jugements - Recouvrement - Criminalité - Condamnation - Activité avec intervention de la police - Autres sources - Incidents de sécurité antérieurs - Sources ouvertes - Filtrage - Loyauté	La cote/autorisation est accordée ou refusée après l'évaluation de tous les résultats des vérifications. On reporte la décision le temps d'évaluer tous les résultats des vérifications.	Activités de suivi post-cote/autorisation - séance d'information sur la sécurité - Comptes rendus - Processus de départ - Sensibilisation à la sécurité - Cycles de filtrage de sécurité - Changement de circonstances

Guide de numérisation du filtrage de sécurité

- Écologiser les opérations a été un point d'intérêt et une priorité du GC
- Initiative financée par ECCC (50K)
- Développer un guide en 5 phases pour soutenir les organisations lors de la numérisation de leurs dossiers de filtrage de sécurité
- Basé sur une approche utilisée à l'ASFC
- Guide appuyé par les conseils techniques du CEES en tant qu'EM
- Plusieurs organisations participantes permettant des économies significatives, un processus simplifié et une réduction de l'espace occupé
- Permet à la sécurité de numériser les opérations, d'éclater les préconceptions, de contribuer à réduire les arrérages et de faire la transition vers un travail à distance
- Les organisations ont constaté les avantages de la numérisation durant la pandémie
- Partenaires clés: ASFC, SPAC

COUP D'OEIL SUR LA NUMÉRISATION DE DOSSIER

Uniformité
Technologie et processus de pointe assurant le rendement et l'uniformité

Conformité
Respect des lignes directrices et exigences du SCT (sécurité, protection des renseignements personnels, GI-TI)

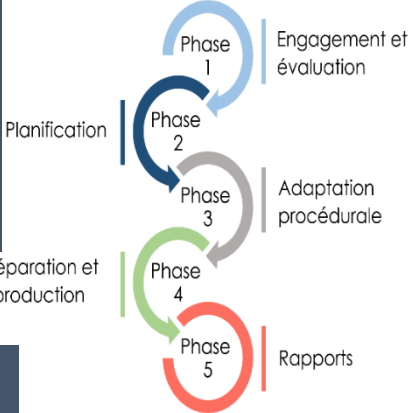
Opérationnalisation
Processus intégré harmonisé avec les plans et priorités du gouvernement du Canada

Fiable **Sécuritaire** **Écologique**

Approche solide à l'appui des organisations pour réduire le risque de compromission de l'information sensible, accroître l'efficacité des programmes et contribuer aux priorités gouvernementales

- ✓ **Assurer une base de confiance**
Adoption de pratiques exemplaires et de mécanismes efficaces pour accroître la productivité et réduire les coûts
- ✓ **Intégrité**
Respecte les normes d'intégrité les plus élevées et améliore la sécurité du point de vue de la protection des documents et des sinistres
- ✓ **Écono et éco**
Fait partie de notre processus de réduction de l'empreinte écologique et de notre initiative de transformation numérique

Planification



NUMÉRISATION - VALEUR AJOUTÉE

- ✓ Atténue le risque d'utilisation abusive grâce à des pistes de vérification solides et des mécanismes de secours.
- ✓ Permet l'accès aux dossiers en fonction du besoin de savoir et des profils des utilisateurs de GCdocs
- ✓ Permet l'accès 24 heures sur 24 et 7 jours sur 7 aux utilisateurs sur place ou à distance
- ✓ Met fin au fardeau du transfert des fichiers papier. Les dossiers peuvent être transférés rapidement par courriel aux autres ministères et aux intervenants.

- ✓ Accélère grandement les demandes et les divulgations d'AIPRP
- ✓ Améliore les plans de continuité des activités et réduit le risque de perte d'information en raison de catastrophes environnementales et accidentelles (inondations, séismes, incendies, etc.)
- ✓ Plus de dossiers perdus ou égarés Les fonctions de recherche dans GCdocs sont très précises
- ✓ Réduit le délai de traitement du processus de filtrage, ce qui accroît l'efficacité du programme

Préparation et production

Trousse d'évaluation de la menace et des risques

- Financée par Patrimoine (25K), testée au BCP. Inclut des documents de soutien opérationnel, des PON et un outil automatisé d'EMR facile d'utilisation
- Présentée à la communauté de pratique
- Partenaires clés: ASFC, PC, BCP + POCS (GRC & SPAC)

Outil automatisé

Vérifier le contenu de la Liste

Instructions générales

Ouvrez et fermez les sections en cliquant sur les boutons bleus.

Pour des trucs et astuces, [cliquez ici](#).

Évaluation

Résumé de la liste de vérification

Renseignements

Liste de vérification de l'EMR

Ouvrir/Fermer

Section 1 - Caractéristiques de l'immeuble (renseignements administratifs)

Ouvrir/Fermer

Section 2 - Contrôle de l'accès

Ouvrir/Fermer

Section 3 - Mesures de sécurité matérielle

Ouvrir/Fermer

Section 4 - Formation et sensibilisation à la sécurité

Ouvrir/Fermer

Section 5 - Sécurité de l'information

Ouvrir/Fermer

Section 6 - Gestion de la continuité des activités

Ouvrir/Fermer

Section 7 - Filtrage de sécurité

Ouvrir/Fermer

Section 8 - Incidents liés à la sécurité

Ouvrir/Fermer

Section 9 - Réponse en cas d'urgence

Ouvrir/Fermer

Section 10 - Autres questions

Outil d'évaluation de la menace et du risque (EMR)

L'Outil d'EMR comporte quatre sections différentes. Vous pouvez utiliser les boutons ci-dessous pour atteindre une page, ou simplement utiliser les Onglets Feuille au bas de ce document Excel.

- Liste de vérification de l'EMR

Cette section est utilisée pour suivre différents éléments nécessaires à l'EMR. Cette section contient de multiples questions séparées où vous pouvez répondre "Oui", "Non" ou "N/A". L'autre colonne permet à l'utilisateur d'indiquer si un élément est "Acceptable" ou non. Il y a aussi une zone "Commentaires" où vous pouvez écrire des notes, au besoin.
- Évaluation

Cette section est utilisée pour réaliser la partie "Évaluation du risque" de l'EMR, en y identifiant les Biens, les Menaces et les Vulnérabilités. Vous pouvez utiliser les listes descendantes pour choisir le niveau de risque approprié. Une fois que vous aurez identifié tous les facteurs de risque, l'Outil générera un Tableau résumé des risques et qui identifiera le Risque résiduel.
- Résumé de la liste de vérification

Cette section vous fournit un résumé de tous les éléments auxquels vous avez répondu "Non" dans la colonne "Acceptable?" de la Liste de vérification de l'EMR. En d'autres mots, elle vous fournit une liste de tous les éléments non acceptables et peut être utilisée pour identifier les vulnérabilités, ce qui pourra vous être utile pour appuyer les recommandations présentes dans votre Rapport d'EMR.
- Renseignements utiles

Cette section contient des renseignements pour vous aider dans à compléter les différentes sections définies dans la section Évaluation. Vous n'avez rien à écrire dans cette section, vous pouvez cliquer sur l'icone " " pour voir l'information contenue dans la feuille Renseignements utiles, ou vous pouvez simplement utiliser les onglets au bas de ce document Excel pour naviguer entre les différentes sections.

Pour toute question concernant cet outil, ses applications ou toute autre demande en lien avec la sécurité opérationnelle, vous pouvez joindre le Centre d'excellence en sécurité (CEES) à SCOt-CEES-info@pco-bcp.gc.ca.



Nom du bien	Valeur du bien	Probabilité de menace	Niveau de vulnérabilité	Risque résiduel	Risque résiduel (après la prise en charge des vulnérabilités)
1 Renseignements Protégés A et B	Moyenne	Moyenne	Moyen	Moyen	Bas
2 Matériel de bureau et biens	Élevée	Moyenne	Moyen	Élevé	Bas
3 Individus	Élevée	Moyenne	Moyen	Élevé	Bas

Risque résiduel pour l'ensemble des biens

Nombre de biens évalués	Risque résiduel	Risque résiduel (après la prise en charge des vulnérabilités)
3	Élevé	Bas

Trousse d'outils pour la planification d'exercices

- Soutient le développement d'exercices
- Répond aux défis clés du développement d'exercices :
 - Comment obtenir une approbation
 - Que faire si je manque d'expérience en matière d'exercices
 - Où puis-je trouver de l'expertise
 - Comment puis-je obtenir l'appui d'autres organisations du GC
 - Comment gérer mon temps pour répondre aux échéanciers de planification
 - Quel scénario m'est le plus approprié
 - Quelles sont les exigences de l'exercice en matière de sécurité
 - Pourquoi dois-je évaluer l'exercice

