Public Services and Procurement Canada
Services publics et Approvisionnement Canada
Canada

Évaluation du Programme canadien de certification en cybersécurité : Rapport final et plan d'action de la direction

Catalogue nº : P4-176/2026E-PDF

ISBN : 978-0-660-78674-2

Services publics et Approvisionnement Canada

Place du Portage III, 11, rue Laurier, Phase III, Gatineau (Québec) K1A 0S5

Also available in English

Table des matières

Introduction

Le Programme canadien de certification en cybersécurité (PCCC) est une initiative du gouvernement du Canada (GC) visant à renforcer la cybersécurité pour les fournisseurs des contrats de défense fédéraux. Les chaînes d'approvisionnement du GC sont visées par des activités cybernétiques fréquentes, sophistiquées et malveillantes, les auteurs des menaces ciblant de plus en plus les grandes organisations de façon indirecte en exploitant les vulnérabilités au sein de leurs chaînes d'approvisionnement élargies. Face à cette situation, le GC a créé le PCCC afin de renforcer la protection de la chaîne d'approvisionnement de la défense canadienne et de mieux protéger l'information contractuelle du GC.

L'approvisionnement en matière de défense au sein du GC est effectué par SPAC, conformément au mandat inscrit dans la *Loi sur le ministère des Travaux publics et des Services gouvernementaux*, qui exige que SPAC fournisse des services d'approvisionnement aux ministères et organismes fédéraux. Dans le cadre de ce mandat, SPAC gère l'approvisionnement en biens et services pour le GC et fournit un soutien administratif et des outils aux organisations fédérales, les aidant ainsi à offrir des programmes et des services à la population canadienne.

Aperçu du PCCC

À l'automne 2023, le Conseil du Trésor (CT) a approuvé le PCCC dans le but d'établir des exigences obligatoires en matière de cybersécurité pour les fournisseurs qui soumissionnent ou travaillent pour des contrats de défense du GC.

Les objectifs (résultats) du PCCC sont les suivants :

- Protéger les renseignements contractuels fédéraux non classifiés sur les systèmes, réseaux et applications des entrepreneurs.
- Maintenir l'accès de l'industrie canadienne aux occasions d'approvisionnement international assorties d'exigences de certification en cybersécurité comparables.
- Renforcer le niveau de base de la cybersécurité pour l'industrie de la défense du Canada.
- S'assurer que les systèmes des fournisseurs demeurent solides et fiables pour les capacités et la préparation des Forces armées canadiennes (FAC).
- Accroître la participation de l'industrie canadienne au programme de certification en cybersécurité.

Le PCCC est dirigé par la Direction générale de l'approvisionnement maritime et de défense (DGAMD) de SPAC et, plus précisément, par le secrétariat du PCCC, qui est responsable de la conception et de la mise en œuvre de l'initiative. La DGAMD est soutenue par la Direction générale de la surveillance (DGS) du Ministère, qui agit à titre d'autorité technique et de propriétaire fonctionnel pour appuyer la réalisation des projets de la DGAMD tout en dirigeant l'élaboration des futures exigences de conception. La Direction générale des approvisionnements soutient le système de répertoire de données. D'autres contributions et soutiens sont fournis par une équipe pluriministérielle qui rassemble le ministère de la Défense nationale (MDN) en sa qualité de client, le Conseil canadien des normes (CCN) qui est l'organisme d'accréditation, le Centre canadien pour la cybersécurité (CCC) du Centre de la

sécurité des télécommunications (CST) qui fournit l'expertise technique en matière de cybersécurité, et le Secrétariat du Conseil du Trésor du Canada (SCT) qui donne des orientations et des mises à jour sur les politiques. La supervision est assurée par le Comité directeur de la direction générale (DG) de la certification en cybersécurité. Le budget fédéral de 2023 a alloué 25 million$ (dont 13 million$ en nouveaux fonds) pour la conception et la mise en œuvre du PCCC au cours de la période allant de 2023 à 2024 à 2025 à 2026.

Niveaux de certification du PCCC

Une fois la mise en œuvre achevée, les fournisseurs souhaitant soumissionner ou travailler pour certains contrats de défense du GC pourront se voir exiger une certification en vertu du PCCC. Les niveaux de certification requis pour les fournisseurs de la défense seront déterminés pour chaque contrat et seront clairement définis dans les demandes de propositions et dans les clauses contractuelles. Les exigences de l'initiative en matière de certification de la cybersécurité comporteront trois niveaux :

- Niveau 1 : exige une auto-évaluation annuelle de la cybersécurité.
- Niveau 2 : exige une évaluation externe quadrimestrielle de la cybersécurité dirigée par un organisme d'évaluation tiers certifié et une confirmation annuelle de conformité.
- Niveau 3 : exige une évaluation quadrimestrielle de la cybersécurité menée par le MDN et une confirmation annuelle de conformité.

La création du PCCC fait suite à l'annonce de la création du programme de certification du modèle de maturité de la cybersécurité (Cybersecurity Maturity Model Certification, CMMC) aux États-Unis, qui vise à protéger l'information contractuelle fédérale américaine et l'information non classifiée contrôlée américaine qui sont communiquées aux entrepreneurs du Département de la Défense (DoD) des États-Unis. Le PCCC vise à consolider la protection des données mises en commun avec les entrepreneurs et les sous-traitants du MDN au Canada, en appliquant une version canadienne des contrôles cybernétiques définie dans les directives du CCC énoncées dans la publication en matière de sécurité des technologies de l'information (ITSP) 10.171 / 172.

Activités de conception et de mise en œuvre du PCCC

Des activités pour soutenir la conception du PCCC ont été entreprises durant les exercices 2023 à 2024 et 2024 à 2025. Un « prélancement » du PCCC a été effectué en mars 2025; il s'agissait de la première phase d'un processus de mise en œuvre en quatre phases. Les principaux objectifs de la phase de mise en œuvre 1 (prélancement) sont les suivants :

- mettre à l'essai l'utilisation fonctionnelle d'un dépôt de données relatives aux entrepreneurs, comprenant les certifications et l'outil d'auto-évaluation que les entrepreneurs doivent utiliser;
- tester les exigences fonctionnelles des responsables des achats du MDN et de SPAC qui doivent valider l'achèvement de la certification avant l'attribution du contrat;
- perfectionner les capacités et les connaissances des intervenants, notamment les entreprises canadiennes, à l'égard du PCCC;

- publier la norme canadienne sur la cybersécurité industrielle, fondée sur la norme du National Institute for Standards and Technology[1] (NIST) des États-Unis.

Les plans de mise en œuvre du PCCC tablent sur une exécution des trois phases supplémentaires étalée entre l'automne 2025 et 2027[2]. Au cours de cette mise en œuvre, les trois niveaux de certification en cybersécurité seront intégrés dans les contrats de défense applicables.

À propos de cette évaluation

L'évaluation du PCCC a été réalisée par la Direction des services d'évaluation de SPAC entre avril et juin 2025, sous l'autorité du chef de l'évaluation de SPAC.

Cette évaluation obligatoire fait partie du Plan d'évaluation ministériel de SPAC pour la période allant de 2024-2025 à 2026-2030.

Le plan d'action de la direction de SPAC en réponse aux constatations de la présente évaluation est présenté à l'annexe 1: Plan d'action de la direction de ce présent rapport.

Objectif de l'évaluation

L'objectif de l'évaluation était de réaliser une évaluation formative du PCCC afin de soutenir la prise de décision concernant l'avenir de cette initiative. L'évaluation a permis d'évaluer les activités de SPAC en soutien au PCCC avec la contribution des autres ministères et organismes du GC qui ont soutenu ses activités de mise en œuvre.

Approche de l'évaluation

On a effectué l'évaluation grâce à des examens ciblés de la pertinence, de l'efficacité et de l'exécution du PCCC.

Pertinence : L'évaluation comprenait un examen des programmes nationaux et internationaux; on a examiné l'importance de la reconnaissance de la certification canadienne par les États-Unis et étudié d'autres mécanismes possibles pouvant être envisagés pour atteindre les objectifs du PCCC.

Efficacité : L'évaluation portait sur la compréhension de la mesure dans laquelle les principales activités de conception, de planification et de mise en œuvre du PCCC avaient été entreprises comme prévu jusqu'à présent.

---

[1] Il s'agit d'une agence gouvernementale américaine du département du Commerce. Sa mission est de promouvoir l'innovation et la compétitivité industrielle des États-Unis en faisant progresser la science, les normes et la technologie de la mesure.

[2] *Le PCCC a reçu trois ans de financement pour ses activités de conception et de mise en œuvre (pour la période allant de 2023-2024 à 2025-2026). Les activités prévues au-delà de cette période n'étaient pas financées au moment de cette évaluation.*

Exécution : L’évaluation portait sur la consultation des intervenants et sur leur contribution à la mise en œuvre du PCCC, sur la mesure dans laquelle les pratiques de gestion des risques étaient employées, ainsi que sur l’établissement de la priorité des activités et des ressources disponibles.

On a mené l’évaluation en utilisant les sources de données suivantes :

- **examen des documents** : documentation de planification du programme, documents de gouvernance (dont les procès-verbaux des réunions de comités), documents de recherche en cybersécurité, renseignements budgétaires et documents sur la consultation des intervenants de l’industrie.
- **entrevues** : entrevues avec neuf intervenants du PCCC provenant de la direction de programme de SPAC (DGS et DGAMD), du niveau opérationnel de SPAC (DGS et DGAMD) et du SCT (direction de programme).
- **sondages** : deux sondages distincts auprès des intervenants du PCCC – un sondage pour le niveau opérationnel et un autre au niveau de la direction de programme – de SPAC, du MDN, du CCN, du SCT, du CCC du CST, de la Corporation commerciale canadienne et de Sécurité publique.

Les limites attribuables aux méthodes de collecte des données ont été atténuées dans la mesure du possible du fait que les constatations sont issues de plusieurs sources de données. Une discussion portant sur les limites particulières qui ont eu une incidence sur l’évaluation et des mesures d’atténuation prises pour y remédier se trouve à l’annexe 2: Méthodologie d’évaluation.

Portée de l’évaluation

L’évaluation a consisté à examiner les activités du PCCC entre avril 2023 et juin 2025. Il s’agissait d’examiner les activités et les résultats des étapes de consultation, de préparation et de mise en œuvre de la phase 1 du PCCC. Par conséquent, afin de garantir la disponibilité d’un rapport d’évaluation final pour appuyer la prise de décision sur l’orientation future du PCCC, les neuf derniers mois de fonctionnement du PCCC dans le cadre de son financement initial n’ont pas été couverts.

Principales constatations

Nous avons articulé la présentation des constatations de cette évaluation autour des enjeux de pertinence, d’efficacité et d’exécution.

Enjeu 1 : pertinence

Sommaire

L'évaluation a permis de constater que le PCCC était pertinent pour les besoins continus du GC dans le cadre de son objectif de protéger l'accès, la transmission et le stockage des renseignements contractuels fédéraux non classifiés, mais considérés comme étant de nature délicate.

L'évaluation a permis de remarquer que d'autres pays ont aussi des programmes nationaux de cybersécurité avec des objectifs comparables à ceux du programme canadien, notamment le programme de CMMC aux États-Unis. L'examen des programmes internationaux a fourni des exemples de mécanismes de renforcement du soutien à l'entrée initiale dans le programme de certification.

En ce qui concerne le programme américain, l'évaluation a conclu que, même si la réciprocité entre la CMMC et le PCCC pourrait potentiellement améliorer l'efficacité du programme canadien et apporter des avantages à son industrie, il demeure nécessaire que le PCCC appuie ses autres objectifs tout aussi importants que sont la protection des renseignements fédéraux de nature délicate, le renforcement de la cybersécurité de l'industrie de la défense canadienne et le maintien de l'intégrité du système d'approvisionnement des FAC.

Lorsqu'on a demandé quels étaient les autres mécanismes potentiels pour atteindre les objectifs fixés par le PCCC, l'intégration du PCCC dans d'autres programmes existants de SPAC tels que le Programme de sécurité des contrats (PSC) et le Programme des marchandises contrôlées (PMC) était la proposition la plus fréquente.

1.1 Comparaison avec les programmes nationaux et internationaux

1.1a Programmes du gouvernement du Canada

Le GC dispose de nombreux programmes de sécurité et d'approvisionnement, en plus de plusieurs programmes visant à renforcer la cybersécurité des entreprises et entrepreneurs canadiens. L'évaluation a permis de mener une analyse des programmes fédéraux actuels liés à l'approvisionnement et à la cybersécurité afin de détecter d'éventuels recoupements des services avec le PCCC. L'évaluation a permis de relever des similitudes entre les programmes, mais sans trouver de preuves de services faisant double emploi avec le PCCC. Il s'avère que le PCCC est unique, car il est axé précisément sur le renforcement de la cybersécurité pour les fournisseurs de la défense, ce qui le distingue des autres programmes qui ont des objectifs en matière de développement économique plus large, d'innovation ou propres à des secteurs en particulier.

L'évaluation a révélé que CyberSécuritaire Canada (CSC) – un programme d'Innovation, Sciences et Développement économique Canada – était le programme qui présentait la plus grande similarité avec le PCCC. Bien que CSC soit destiné aux petites et moyennes entreprises (PME) de tous les secteurs de l'économie canadienne, les deux programmes visaient à renforcer la cybersécurité des entreprises canadiennes en offrant des certifications, de la formation et des conseils. À l'arrêt de CSC le 31 mars 2023, son pouvoir d'agrément des organisations de certification des PME a été transféré à Services partagés Canada. Cette interruption souligne le rôle crucial du PCCC dans le maintien et le relèvement du niveau de cybersécurité de base au sein de l'industrie canadienne. Au cours des entrevues, plusieurs personnes ont cité CSC

comme une source majeure de leçons apprises pour l'élaboration du PCCC, notamment le fait qu'une approche d'évaluations de cybersécurité volontaires n'était pas efficace.

L'analyse a également noté des similitudes entre le PCCC et deux autres programmes dirigés par SPAC, à savoir le PSC et le PMC, tous deux gérés par la DGS. L'évaluation a révélé que ces deux programmes sont actuellement complémentaires l'un de l'autre et avec le PCCC, et qu'il n'y a pas de recoupement des services.

Les similitudes du PSC et du PMC avec le PCCC concernent les garanties et la protection de la conformité au domaine. Par exemple, le PMC comme le PCCC exigent que les organisations mettent en œuvre des mesures de sécurité pour protéger les marchandises contrôlées et les données techniques telles qu'elles sont définies dans le *Règlement sur les marchandises contrôlées*, ainsi que l'information connexe dans le cadre des processus de passation de marchés du gouvernement, le tout en menant des inspections de conformité et des évaluations de sécurité. Le PSC et le PCCC ont quant à eux des objectifs communs et des garanties de protection qui reposent sur des mesures de conformité ainsi que sur une série de contrôles appliqués aux habilitations des organisations et aux employés des entrepreneurs au moyen du filtrage de sécurité du personnel. Ces deux programmes soutiennent également l'élaboration des clauses de sécurité dans les contrats et offrent de la formation, des conseils et des outils pour améliorer la sécurité de l'information. Enfin, les trois programmes exigent une consultation et une liaison constantes avec le même consommateur cible : l'industrie. Chaque programme nécessite un soutien de première ligne, de la sensibilisation et de la formation. Ces programmes servent également à rationaliser le processus de réception des demandes de l'industrie visant à obtenir la confirmation de la conformité aux exigences de sécurité précontractuelles. Cependant, ces programmes sont gérés de façons différentes. Le PSC est géré dans le cadre des autorités désignées en matière de sécurité décrites dans la Politique sur la sécurité du gouvernement et il n'est pas obligatoire pour les organisations clientes du GC. Le PMC est quant à lui régi par la *Loi sur la production de défense* et par le *Règlement sur les marchandises contrôlées*; il est obligatoire pour toutes les entités canadiennes (à l'exception des organisations fédérales) qui souhaitent posséder des marchandises contrôlées telles qu'elles sont définies par le Règlement ou accéder à ces marchandises. En revanche, le prélancement du PCCC serait géré en vertu de la Politique sur la sécurité du gouvernement et défini selon les normes publication en matière de sécurité des technologies de l'information (ITSP) 10.171 et ITSP10.172 promulguées par le Centre de la sécurité des télécommunications (CSTC), dont l'objectif principal demeure la protection des renseignements non classifiés, mais jugés de nature délicate dans les contrats du GC.

1.1b Programmes internationaux

En raison de la fréquence et de la sophistication croissantes des cybermenaces, les pays sont en train de renforcer rapidement leurs mesures de cybersécurité nationales. Pour évaluer l'harmonisation du PCCC avec d'autres programmes nationaux de cybersécurité et pour déterminer d'éventuelles pratiques exemplaires, l'évaluation a procédé à l'examen des programmes du « Groupe des cinq », un rassemblement d'organismes de renseignement dont le Canada fait partie. On a évalué les programmes suivants :

- États-Unis : Certification du modèle de maturité en matière de cybersécurité (Cyber Maturity Model Certification [CMMC])

- Royaume-Uni : Modèle de cybersécurité (Cyber Security Model [CSM])
- Australie : Programme de sécurité de l’industrie de la défense (Defense Industry Security Program [AU DISP])
- Nouvelle-Zélande : Programme de sécurité de l’industrie de la défense (Defense Industry Security Program [NZ DISP])

L’évaluation a permis de constater que ces quatre programmes avaient un but principal en commun, à savoir la protection des renseignements fédéraux obtenus au moyen de contrats, alors que les programmes de la Nouvelle-Zélande et de l’Australie étaient également axés sur l’industrie de la défense. De plus, les buts des quatre programmes comprenaient l’augmentation du niveau de base en matière de cybersécurité des industries nationales ainsi que le maintien de l’intégrité du système d’approvisionnement. Contrairement au Canada, le maintien de l’accès de l’industrie aux marchés publics externes n’est pas un but explicite des quatre programmes examinés.

L’évaluation a également révélé que le coût pour l’industrie est une préoccupation majeure pour tous les programmes de cybersécurité examinés. Dans le cas du Canada, la consultation de l’industrie menée par le secrétariat du PCCC en mai 2024 indiquait que 46 % des sous-traitants s’attendaient à investir moins de 50 000 $, tandis que 29 % des consultants prévoyaient des coûts compris entre 150 000 $ et 175 000 $. Sur tous les répondants, 68 % veulent un soutien complet – aide financière, orientation et ressources – afin de se préparer à l’évaluation du PCCC. L’évaluation a révélé que chaque programme international comportait également des coûts associés pour la certification, la mise en œuvre et la maintenance, et que ces coûts peuvent être importants, en particulier pour les PME. L’Australie comme le Royaume-Uni cherchent à soutenir leurs industries de cybersécurité par l’intermédiaire de leurs programmes, en accordant des prêts et des fonds de développement régional (Australie), et en atténuant les coûts grâce aux auto-évaluations et à des exigences minimales de contrôle (Royaume-Uni).

1.2 Réciprocité avec le programme américain

Le PCCC a l’intention de maintenir l’accès de l’industrie canadienne aux occasions d’approvisionnement international dont les exigences en matière de certification en cybersécurité sont comparables, ce qui comprend la CMMC des États-Unis. Actuellement, la règle du programme final de CMMC n’autorise pas les programmes bilatéraux de certifications réciproques entre et le Département de la Défense (DoD) des États-Unis et un autre pays. La Division de la sécurité industrielle de la DGS poursuit ses négociations avec la Defense Technology Security Administration (DTSA) des États-Unis afin de mettre à jour le protocole d’entente bilatéral sur la sécurité industrielle existant entre le Canada et les États-Unis.

L’évaluation a permis d’examiner l’importance du maintien de l’accès de l’industrie canadienne aux occasions d’approvisionnement international avec des exigences de certification en cybersécurité comparables. Les personnes interrogées au cours de l’évaluation (entrevues et sondages) ont noté que l’absence d’accord de réciprocité représentait un risque pour la pertinence et pour la valeur du programme. Plusieurs d’entre elles ont fait remarquer que les conséquences les plus graves seraient une diminution de l’intérêt et de la satisfaction de l’industrie à l’égard du PCCC, en raison du possible dédoublement des coûts et des efforts pour les entrepreneurs devant obtenir à la fois les certifications du PCCC et celles du programme de CMMC. Les réponses aux entrevues et aux sondages soulignent également que ce fardeau

pèserait tout particulièrement sur les PME, car elles ont généralement moins de ressources à consacrer à ces coûts supplémentaires. Lors des entrevues au niveau opérationnel, plusieurs personnes ont suggéré que le PCCC devrait envisager d'intensifier les activités de consultation de l'industrie pour accroître la sensibilisation et l'adhésion au PCCC, surtout compte tenu des derniers développements concernant l'absence d'accord de réciprocité. Les entrevues ont également permis de souligner qu'une demande plus faible de l'industrie pourrait diminuer la nécessité d'avoir recours à des organismes d'évaluation tiers certifiés, et aux services d'accréditation du CCN, ce qui pourrait nuire au modèle de recouvrement des coûts du CCN, qui dépend d'une demande constante pour ses services.

L'examen des documents des consultations de l'industrie réalisé par le secrétariat du PCCC (avant la décision américaine d'interdire les accords bilatéraux de réciprocité avec d'autres pays) allait dans le même sens que ces réponses aux sondages et entrevues. La majorité des entrepreneurs de l'industrie ont exprimé une forte préférence pour le PCCC s'il y avait une réciprocité complète avec la CMMC américaine. Les personnes interrogées disaient s'attendre à ce qu'un PCCC soutenu par un accord de réciprocité avec les États-Unis ait une incidence majeure sur leur capacité à remporter des contrats de défense américains et à être jugées conformes pour accéder aux marchés et aux chaînes d'approvisionnement de la défense des États-Unis.

Si les répondants aux sondages et aux entrevues ont reconnu les conséquences potentielles d'une absence d'accord de réciprocité en matière de certification en cybersécurité sur la valeur et la pertinence du PCCC, ils étaient généralement d'accord pour dire que l'initiative demeurait pertinente. Lors des entrevues, la majorité des personnes interrogées au sein de la direction du programme ont souligné que le PCCC continuait de répondre à la nécessité de protéger les renseignements sensibles figurant dans les contrats, d'améliorer l'hygiène en matière de cybersécurité au sein de l'industrie et de satisfaire au besoin d'un programme national. L'examen des documents de politique pertinents a confirmé que le PCCC était harmonisé avec les approches du GC en matière de cybersécurité telles qu'elles sont énoncées dans la Stratégie intégrée de cybersécurité du gouvernement du Canada (2024), la Stratégie nationale de cybersécurité du Canada (2022) et le projet de loi C-8 qui, collectivement, visent à renforcer la cyberrésilience du Canada.

Lors des entrevues aux niveaux opérationnel et de la gestion du programme, plusieurs personnes ont défendu l'idée qu'il faudrait chercher à établir une réciprocité des certifications en cybersécurité avec d'autres programmes nationaux de cybersécurité – par exemple avec les autres partenaires du « Groupe des cinq » (Royaume-Uni, Australie et Nouvelle-Zélande) et avec l'Union européenne (UE) – tandis que d'autres répondants ont exprimé des inquiétudes quant au fait que les différences significatives entre ces programmes pourraient créer des obstacles majeurs à la réciprocité des certifications.

1.3 Autres mécanismes

Le PCCC a introduit un partenariat pluriministériel pour entamer l'introduction de protocoles de cybersécurité pour les fournisseurs et leur intégration dans les exigences contractuelles. Il a également lancé une approche innovante de l'exécution, conçue pour être transversale entre les différentes directions générales de SPAC. Le modèle de gestion actuel du PCCC, tel qu'il est administré par la DGAMD, avait été conçu pour être temporaire et prévoyait une réévaluation

et un transfert de la gestion à une autre entité à l'issue de la mise en œuvre du programme. Dans le cadre de l'évaluation, nous avons mené une analyse d'autres mécanismes ou processus pouvant être envisagés pour atteindre trois des cinq objectifs du PCCC (protection des renseignements fédéraux, renforcement de la cybersécurité de l'industrie de la défense canadienne et maintien de l'intégrité du système d'approvisionnement des FAC).

On a consulté les intervenants du PCCC lors de la mise en œuvre du PCCC pour savoir s'ils connaissaient d'autres mécanismes possibles pour atteindre ces résultats. Si certaines personnes interrogées lors des entrevues ont souligné la possibilité d'intégrer le PCCC au sein de l'organisme d'approvisionnement de la défense dont la création vient d'être annoncée, plusieurs répondants, tant au niveau opérationnel que de la gestion du programme, ont suggéré que le PCCC – actuellement administré par la DGAMD de SPAC – pourrait potentiellement bien s'intégrer à d'autres programmes existants de passation de marchés axés sur la sécurité de l'information et dirigés par SPAC, notamment le PSC ou le PMC qui relèvent de la DGS de SPAC. Il a été noté que le PSC est un programme fondé sur des politiques et donc plus souple, ce qui facilitait son intégration, comparativement au PMC qui est régi par la législation. Les répondants ont indiqué que, à l'heure actuelle, ces autres programmes ne suivaient pas de manière distincte la façon dont les mesures actuelles d'assurance de la conformité s'harmonisaient avec les contrôles de cybersécurité ITSP 10.171. Ils ont en outre noté qu'une harmonisation et une restructuration d'ampleur pourraient s'avérer nécessaires pour intégrer le PCCC dans l'un de ces deux autres programmes. Les personnes interrogées ont précisé qu'une restructuration pourrait devoir passer par des mesures visant à accroître les connaissances et l'expertise en matière d'évaluation de la cybersécurité afin d'améliorer la mise en œuvre et l'intégration des contrôles de cybersécurité supplémentaires dans les secteurs d'activités existants des programmes de sécurité lors de la transition du PCCC vers un nouveau propriétaire.

Bon nombre de personnes interrogées lors des entrevues au sein de la direction du programme ont indiqué que les exigences en matière de cybersécurité pourraient être inscrites dans la loi ou dans les règlements, et ce pour tous les contrats de défense. Cela pourrait éliminer le besoin d'un programme de certification, qui serait remplacé par l'établissement de règles, l'assurance de la conformité étant alors réalisée grâce aux audits et à la supervision du gouvernement. Parallèlement, les répondants au sondage étaient divisés quant à la question de savoir si d'autres mécanismes pouvaient atteindre les buts du PCCC, certaines personnes interrogées signalant qu'aucun autre mécanisme n'était activement envisagé au moment où elles répondaient au sondage.

L'évaluation des programmes internationaux a également permis de cerner d'autres mécanismes potentiels que le Canada pourrait envisager pour améliorer l'efficacité et l'efficience du programme. Il s'agit notamment d'un modèle (britannique) pour les fournisseurs non conformes dans lequel les fournisseurs qui n'obtiennent pas la certification du PCCC devraient présenter un plan de mise en œuvre de la cybersécurité, décrivant les étapes à suivre pour se conformer aux normes de cybersécurité. Ce modèle prévoit en outre un niveau d'entrée de base (niveau 0) de la certification du PCCC de niveau 1 avec seulement des contrôles très basiques mais nécessaires, représentant un très faible niveau d'évaluation du risque de cybersécurité, le but étant d'améliorer le processus afin d'atteindre le niveau 1. Plusieurs personnes interrogées au cours des entrevues ont suggéré que le PCCC pourrait envisager de fournir aux participants un soutien financier et technique, comparable aux soutiens offerts aux participants des

programmes nationaux de cybersécurité au Royaume-Uni et en Australie. L’évaluation a permis de noter que le programme australien comprenait des prêts et des financements pour le développement régional, tandis que le programme britannique visait à atténuer les coûts par des auto-évaluations et des exigences minimales de contrôle.

Enjeu 2 : efficacité

Sommaire

Le PCCC a connu une mise en œuvre plus lente que ce qui était prévu à l’origine en raison de facteurs tels que la nécessité de réélaborer le programme, début 2025, en le concentrant uniquement sur le Canada. Les principaux jalons franchis à ce jour concernent des activités de consultation et de sensibilisation des intervenants externes, ainsi que la publication de la norme canadienne sur la cybersécurité industrielle.

2.1 État de la mise en œuvre

Le PCCC a reçu son financement et l’autorisation de procéder à la mise en œuvre initiale du programme en mars 2023. L’évaluation s’est faite en procédant à un examen de l’étendue des activités clés du PCCC déjà menées ainsi que des résultats déjà obtenus par l’initiative.

Les préparatifs pour le prélancement du PCCC ont commencé à l’été 2024. Les activités comprenaient la consultation de l’industrie, par exemple avec des webinaires présentant de façon détaillée le PCCC et les exigences applicables aux fournisseurs, ainsi qu’une demande de renseignements adressée à l’industrie canadienne, c’est-à-dire aux entrepreneurs de la défense, aux sous-traitants, aux consultants en cybersécurité/technologie de l’information ainsi qu’aux fournisseurs de services de technologie de l’information.

Le prélancement du PCCC, initialement prévu pour s’étaler de janvier à juin 2025, a été décalé au mois de mars 2025 (avec une estimation actuelle d’achèvement en décembre 2025). Ce retard s’explique par les conséquences de l’incapacité à établir une voie de réciprocité avec le programme américain lors du démarrage du PCCC. Le PCCC avait besoin de temps pour délibérer sur le passage à un modèle exclusivement canadien et pour opérer une refonte avant son lancement.

À ce jour, bien que certains produits livrables clés aient été atteints, de nombreux autres jalons de mise en œuvre ont été reportés à l’automne 2025 et à l’hiver 2026, dont des produits livrables fondamentaux tels que l’application des exigences de niveau 1 (auto-évaluation) du PCCC aux contrats pilotes, qui serviraient de cas d’essais importants pour les nouvelles exigences du PCCC.

Parmi les produits livrables du prélancement qui sont achevés, les intervenants du PCCC interrogés dans les sondages et les entrevues aux niveaux opérationnel et de la gestion du programme ont approuvé les principales réalisations à ce jour, citant la publication de la norme canadienne sur la cybersécurité industrielle ainsi que les activités de consultation et de

sensibilisation des intervenants internes/externes, notamment la consultation des fournisseurs et les présentations à l'industrie.

Tableau 1 : État d'avancement des produits livrables du PCCC[3]

Terminé à temps	Terminé en retard	Arrivé à échéance – en retard	Pas arrivé à échéance
5 sur 26 (19 %)	2 sur 26 (8 %)	9 sur 26 (35 %)	10 sur 26 (38 %)

Les personnes interrogées, tant au niveau opérationnel qu'au niveau de la gestion du programme, ont généralement noté que la mise en œuvre du PCCC était plus lente que ce qui était prévu initialement, certains répondants faisant remarquer que les retards s'expliquent par l'incapacité à parvenir à un accord de réciprocité avec les États-Unis – ce qui était inattendu – ainsi que par les répercussions des négociations bilatérales en cours entre le Canada et les États-Unis sur la sécurité industrielle visant à mettre à jour les équivalences qui existent déjà dans le protocole d'entente entre les deux pays. Lors des entrevues, les personnes interrogées ont souligné que les retards étaient principalement dus à l'interdépendance des activités de l'initiative, les produits livrables du prélancement ayant été reportés dans certains cas parce que les conditions préalables n'étaient pas encore réunies, et donc les produits livrables connexes pas encore achevés. Les personnes interrogées lors des entrevues ont également souligné la complexité associée à la nature horizontale de la mise en œuvre du PCCC qui touche divers ministères, tout en exprimant leur perception d'une capacité ou d'une responsabilité insuffisante en matière de personnel, d'expertise et de ressources au sein du PCCC. L'examen des documents effectué dans le cadre de l'évaluation a permis de noter que la plupart des activités de prélancement du PCCC qui avaient été retardées sont au moins en partie attribuables à une interdépendance avec une ou plusieurs activités de mise en œuvre, appuyant la justification fournie par les répondants.

Enjeu 3 : exécution

Sommaire

Avec la mise en place d'une structure de gouvernance formelle pour le PCCC, les répondants à l'évaluation déclarent qu'ils sont globalement satisfaits du soutien en matière de secrétariat fourni par SPAC tout en mentionnant la nécessité de clarifier davantage les rôles et responsabilités dans l'administration du PCCC.

L'évaluation a permis de noter que certains outils clés de gestion de projet ne sont pas encore terminés et qu'il y a des occasions de renforcer, entre autres, les produits de gestion des risques.

[3] *L'évaluation a suivi 26 produits livrables au total. Parmi ceux-ci, 16 devaient être livrés avant ou en juin 2025, tandis que la date de livraison des 10 autres n'est pas encore passée.*

Les intervenants ont souligné qu'il serait important d'examiner l'établissement de la priorité des ressources, et indiqué les domaines opérationnels qui n'ont pas reçu de financement direct dans le cadre des autorités du PCCC.

3.1 Rôles et responsabilités

Les relations et la coordination avec les intervenants jouent un rôle clé dans le PCCC, puisque pas moins de cinq ministères du GC ont la responsabilité de contribuer à la mise en œuvre du programme. L'évaluation s'est faite en procédant à un examen des contributions des intervenants (internes à SPAC et externes à SPAC) à la mise en œuvre efficace du PCCC.

On a effectué un examen des documents de gestion afin de mieux comprendre la détermination des rôles et responsabilités. L'évaluation a permis de constater que le PCCC s'appuie sur une structure de gouvernance clairement définie composée de comités de cybersécurité. Il s'agit d'un comité au niveau des sous-ministres adjoints qui supervise plus largement les politiques et les opérations de cybersécurité du GC, ainsi que de plusieurs comités au niveau du directeur général et de l'équipe spéciale, qui sont directement responsables de la mise en œuvre du PCCC. Le programme est également rendu possible grâce aux comités de la Stratégie d'approvisionnement en matière de défense au niveau des sous-ministres et des sous-ministres adjoints. On a constaté que les comités offraient une plateforme pour fournir des séances d'information et recevoir la supervision et les décisions de haut niveau concernant l'orientation du PCCC.

On a également constaté que les rôles et responsabilités des contributeurs du PCCC étaient définis dans plusieurs documents tels qu'une charte[4] et un cadre de gestion; cependant, ces documents sont en cours d'élaboration et n'ont pas encore été approuvés. L'évaluation a permis de cerner des aspects où les rôles et responsabilités pourraient être plus clairs dans ces documents, notamment les activités de transition et les activités prévues au calendrier, les activités de transfert des connaissances, la communication et la gestion des risques.

Le groupe de travail de l'équipe spéciale a été créé en 2022 à 2023 pour appuyer une demande du Cabinet et il a continué de soutenir le PCCC par l'entremise de membres de longue date. Un sondage auprès de l'équipe spéciale a révélé que ses membres avaient une compréhension claire de la raison d'être de leur groupe de travail ainsi que de leurs rôles et responsabilités individuels. Les répondants ont également affirmé que leurs rôles et responsabilités individuels au sein du groupe de travail étaient appropriés. Dans l'ensemble, les membres du groupe de travail de l'équipe spéciale d'autres ministères ont fait part de leur satisfaction quant au soutien fourni par SPAC en matière de secrétariat tout en exprimant la nécessité de clarifier davantage les rôles et responsabilités des différentes organisations afin de mieux soutenir les activités au niveau opérationnel ainsi que l'initiative dans son ensemble. De plus, la majorité des personnes interrogées au cours des entrevues au niveau opérationnel ont noté que le PCCC pourrait accroître son efficacité et son efficience en améliorant ses activités de communication et de consultation auprès des intervenants organisationnels du programme. Ces personnes ont

[4] *Bien que le PCCC ne soit pas un projet officiel soumis à la Directive sur la gestion de projets et programmes du Conseil du Trésor, le PCCC a mis en œuvre des outils clés de gestion pour soutenir sa mise en œuvre initiale, tels que ceux mentionnés dans ce rapport.*

également indiqué que les outils de l'initiative pourraient être mieux entretenus et mieux diffusés parmi les intervenants par le secrétariat du PCCC.

Il y avait un consensus parmi les répondants au niveau opérationnel et de la gestion du programme pour dire que les rôles et responsabilités du PCCC sont généralement clairs, certains soulignant une amélioration de cette clarté avec le temps. Les personnes interrogées lors des entrevues ont exprimé l'idée qu'on pourrait renforcer l'efficacité de l'exécution du PCCC en clarifiant mieux les rôles et responsabilités entre les différents ministères du GC qui interviennent dans le programme, ce qui appuierait sa mise en œuvre. L'examen des documents effectué dans le cadre de l'évaluation a permis de constater que certaines mesures ont été prises à ce jour dans ce domaine. Ainsi, la DGS a dirigé deux exercices de simulation, en avril et en juillet 2025, avec les ministères intervenants dans le but de mieux définir les rôles et responsabilités dans le cadre des différentes activités liées au PCCC.

Au sein de SPAC, la DGAMD supervise actuellement la conception et l'exécution du PCCC pendant toute la durée du prélancement. Le modèle temporaire introduit pour lancer l'exécution du PCCC est innovant et a nécessité que la DGAMD et la DGS travaillent en étroite collaboration sur les activités de mise en œuvre. En ce qui concerne la mise en œuvre de cette approche, l'évaluation a permis de constater que la majorité des personnes interrogées lors des entrevues au niveau opérationnel signalaient que la DGAMD – qui a un rôle d'approvisionnement en matière de défense et d'élaboration et de mise en œuvre des politiques – disposait d'une expertise limitée en matière de cybersécurité au moment de la création du PCCC et exprimaient des inquiétudes quant à la possibilité que cela puisse nuire à la capacité de la DGAMD à soutenir ses activités de mise en œuvre. Les personnes interrogées lors des entrevues au niveau de la gestion du programme ont insisté sur la nécessité de définir clairement les rôles et responsabilités avant de décider de l'avenir du PCCC, notamment en ce qui a trait à la possibilité d'un transfert de gestion. La gestion du programme a également souligné l'importance d'une transition bien planifiée au moment de transférer la gestion du PCCC de la DGAMD vers une autre organisation.

Les entrevues aux niveaux opérationnel et de la gestion du programme ont indiqué que, bien que les rôles des intervenants soient généralement appropriés, il n'y a pas assez de personnel et d'expertise technique en cybersécurité au sein des ministères qui interviennent dans le PCCC, et que cela pourrait limiter les résultats de mise en œuvre à ce jour. Il a été signalé que le manque d'expertise en cybersécurité concernait l'ensemble du GC. Plusieurs personnes interrogées au cours des entrevues ont reconnu le CCC du CST comme la principale source d'expertise technique en matière de cybersécurité pour le PCCC et souligné que son implication était limitée à ce jour, expliquant que le manque de financement et de capacité constituait un obstacle. L'évaluation a permis de faire remarquer l'absence d'un rôle clairement défini dans les documents de base concernant la participation du CCC du CST.

Si les rôles et responsabilités actuels ne sont pas mis à jour pour tenir compte des lacunes cernées, renforcer la responsabilité des intervenants et se préparer à un possible changement d'emplacement du programme, alors il y a un risque que la mise en œuvre du PCCC prenne davantage de retard, ce qui nuirait à la réalisation rapide et efficace de ses produits livrables.

Recommandation 1 : On recommande que SPAC clarifie les rôles et responsabilités des intervenants dans la documentation du programme afin d'améliorer l'efficacité et l'efficience du

PCCC à court terme (pendant qu'il est géré par la DGAMD) et à long terme (une fois que les décisions concernant la gestion du PCCC auront été prises).

3.2 Gestion des risques

Comprendre et atténuer les risques est essentiel pour atteindre les résultats escomptés. L'évaluation a consisté à mener un examen des outils de gestion des risques du PCCC et à consulter les intervenants afin de comprendre la mesure dans laquelle les pratiques de gestion des risques sont mises en œuvre de manière efficace.

Un examen des documents a permis de constater que l'information sur la gestion des risques est décrite dans plusieurs produits différents du PCCC, comme le plan de gestion, le registre des risques et la charte; elle fait en outre l'objet d'autres références dans les documents d'autorisation. Bon nombre de ces documents étaient encore en cours d'élaboration et pas encore terminés au moment de l'évaluation, le secrétariat du PCCC reconnaissant qu'il restait du travail à faire. L'examen des documents a porté sur une liste des lacunes compilée par la DGS, qui a été communiquée à tous les membres du PCCC à des fins d'examen et de rétroaction. Cette liste avait pour but de déterminer et suivre les lacunes dans les pratiques de gestion des risques au sein du PCCC afin de mieux réaliser les activités d'atténuation. L'évaluation a permis de souligner des occasions de renforcer la compréhension et l'atténuation des risques dans les documents. Cela comprenait l'amélioration de l'exhaustivité, car de nombreuses déclarations de risque manquaient souvent de détails sur les déclencheurs d'événements à risque ainsi que sur leurs effets possibles s'ils se concrétisaient. Cela comprenait aussi l'amélioration des évaluations de la probabilité et de l'incidence (quantitative ou qualitative) ainsi que l'évaluation ou la hiérarchisation des risques, des éléments qui n'étaient souvent pas disponibles. L'examen a permis de noter un manque de couverture systématique, ne trouvant aucune preuve de l'utilisation d'une taxonomie des risques pour appuyer leur détermination exhaustive. De plus, on a noté que des risques stratégiques plus vastes pour la réussite à long terme de l'initiative avaient été pris en considération au lieu d'une évaluation des risques liés à la mise en œuvre initiale. L'examen des documents a permis de constater que les rôles et responsabilités liés à la surveillance des risques avaient été établis, mais que la partie responsable de l'activité n'était pas indiquée. Enfin, l'examen des documents a relevé des activités de gestion des risques non achevées, comme les activités de surveillance et de contrôle des risques, les plans d'urgence et d'intervention ou encore la déclaration des risques.

La majorité des répondants aux sondages (aux niveaux opérationnel et de la gestion du programme) ont confirmé que des discussions sur les risques avaient eu lieu, du moins dans une certaine mesure. Toutefois, lorsqu'on leur a demandé si des outils de gestion des risques avaient été utilisés pour aider à orienter la planification et la mise en œuvre du PCCC, les répondants étaient divisés quant à la mesure dans laquelle la gestion des risques avait été intégrée à leur travail. La majorité des répondants ont également indiqué qu'il existait des risques passés, actuels ou émergents, qui pourraient ne pas être entièrement traités. La liste suivante comprend les risques que les personnes interrogées lors des sondages et des entrevues, aux niveaux opérationnel et de la gestion du programme, ont signalé comme n'étant pas entièrement pris en compte au moment où on leur a posé la question :

- Les PME qui peinent à gérer les exigences financières et techniques liées aux normes de mise en œuvre et d’audit du PCCC.
- L’évolution du paysage géopolitique et des enjeux liés à l’établissement de la réciprocité.
- Le manque d’expertise du personnel, de la gestion de projet et technique en matière de cybersécurité au sein des ministères intervenants du PCCC.
- L’incohérence des priorités, de la coordination et de la consultation des intervenants (notée par la direction du programme, et non par le niveau opérationnel).
- L’absence de mise à l’essai du PCCC**,** car le MDN n’a pas encore déterminé de contrat.
- Le manque de clarté des plans pour transférer la gestion du PCCC après la mise en œuvre de l’initiative.

Il existe un risque que, à mesure que les risques du PCCC arriveront à maturité, de nouveaux enjeux continueront d’émerger, ce qui exigera du programme qu’il adopte une approche systématique et rigoureuse pour le suivi, la surveillance et la déclaration des risques et des stratégies d’atténuation, ainsi que pour la manière dont il les traite.

Recommandation 2 : On recommande que SPAC examine, renforce et termine les outils de gestion des risques utilisés par le PCCC.

3.3 Établissement des priorités en matière de ressources

L’établissement des priorités en matière de ressources est un élément majeur de la gestion de projet, car elle permet de concentrer des ressources limitées sur les tâches les plus importantes. L’évaluation a permis d’examiner comment les activités du PCCC étaient classées par ordre de priorité compte tenu des ressources disponibles et de la complexité de l’initiative.

SPAC a dépensé 85 % du budget prévu pour le PCCC au cours de ses deux premiers exercices de fonctionnement (2023 à 2024 et 2024 à 2025). La DGAMD a dépensé 70 % de son budget prévu pour l’exercice 2023 à 2024 et 84 % pour 2024 à 2025. La DGAMD a dépensé 0 % de son budget prévu pour l’exercice 2023 à 2024 (puisque les activités de la DGAMD n’avaient pas encore commencé) et a dépensé 97 % de son budget prévu pour l’exercice 2024 à 2025.

Au niveau opérationnel, les répondants aux entrevues et au sondage ont cité l’attribution et la priorité des ressources comme des facteurs clés influençant la coordination des intervenants et la mise en œuvre de l’initiative, soulignant l’existence d’un déséquilibre puisque certains intervenants avaient reçu du financement tandis que d’autres non. L’évaluation a permis de noter que SPAC et le CCN étaient les ministères intervenants destinataires des fonds visant à aider la mise en œuvre du PCCC. Bien que le MDN, le SCT et le CCC du CST soient responsables de plusieurs activités de mise en œuvre, ils n’ont pas reçu de financement. En réponse au sondage comme lors des entrevues, les répondants du niveau opérationnel ont cité nommément le CCC du CST comme un acteur pour lequel un manque de ressources pouvait nuire à sa capacité à contribuer à la mise en œuvre du PCCC. Beaucoup de répondants, tant au niveau opérationnel que de la gestion du programme, ont aussi indiqué qu’il était probablement nécessaire de rééquilibrer les ressources.

Les intervenants du PCCC de divers ministères, tant au niveau opérationnel que de la gestion du programme, ont formulé différentes idées sur ce qu’on devrait juger prioritaire à mesure que la mise en œuvre du PCCC touche à sa fin. Cela comprenait l’intensification de la mise à l’essai des composantes du PCCC pour cerner et combler les lacunes, ainsi que l’utilisation accrue d’exercices de gestion de projet tels que la matrice RACI (Responsable, Agent comptable, Consulté, Informé) pour mieux clarifier les rôles et responsabilités des intervenants. De plus, les personnes interrogées ont suggéré d’approfondir la consultation de l’industrie pour accroître la sensibilisation et l’adhésion au PCCC, tout en notant cependant que le PCCC n’avait pas reçu de fonds pour la consultation de l’industrie ou la promotion du programme.

Sommaire de l’évaluation

Le PCCC est une initiative du GC visant à renforcer la cybersécurité pour les fournisseurs des contrats de défense fédéraux. Le PCCC est administré par SPAC avec le soutien des intervenants externes suivants : le MDN (en tant que client), le CCN, le CCC du CST et le SCT. Le budget fédéral de 2023 a alloué 25 million$ (dont 13 million$ en nouveaux fonds) pour le PCCC pour la période allant de 2023-2024 à 2025-2026. Au moment de la présente évaluation, le PCCC mettait en œuvre son « prélancement » avec l’intention d’établir ses éléments fondamentaux. À ce jour, on n’a repéré aucun contrat potentiel pour la mise à l’essai du PCCC.

L’évaluation a permis d’effectuer des examens ciblés de la pertinence, de l’efficacité et de l’exécution du PCCC sur la période allant d’avril 2023 à juin 2025.

L’évaluation a permis de constater que le PCCC était pertinent pour les besoins continus du GC dans le cadre de son objectif de protéger l’accès, la transmission et le stockage des renseignements contractuels fédéraux non classifiés, mais considérés comme étant de nature délicate.

L’évaluation a permis de remarquer que d’autres pays ont aussi des programmes nationaux de cybersécurité avec des buts comparables à ceux du programme canadien, notamment le programme de CMMC aux États-Unis. L’examen des programmes internationaux a fourni des exemples de mécanismes de renforcement du soutien à l’entrée initiale dans le programme de certification.

En ce qui concerne le programme américain, l’évaluation a conclu que, même si la réciprocité entre la CMMC et le PCCC pourrait potentiellement améliorer l’efficacité du programme canadien et apporter des avantages à son industrie, il demeure nécessaire que le PCCC appuie ses autres objectifs tout aussi importants que sont la protection des renseignements fédéraux de nature délicate, le renforcement de la cybersécurité de l’industrie de la défense canadienne et le maintien de l’intégrité du système d’approvisionnement des FAC.

Lorsqu’on a demandé quels étaient les autres mécanismes potentiels pour atteindre les objectifs fixés par le PCCC, l’intégration du PCCC dans d’autres programmes existants de SPAC tels que le PSC et le PMC était la possibilité la plus fréquemment citée.

Avec la mise en place d’une structure de gouvernance formelle pour le PCCC, les répondants à l’évaluation déclarent qu’ils sont globalement satisfaits du soutien en matière de secrétariat fourni par SPAC tout en mentionnant la nécessité de clarifier davantage les rôles et responsabilités dans l’administration du PCCC.

L’évaluation a permis de noter que certains outils clés de gestion de projet ne sont pas encore terminés et qu’il y a des occasions de renforcer, entre autres, les produits de gestion des risques.

Les intervenants ont souligné qu’il serait important d’examiner l’établissement de la priorité des ressources, et indiqué les domaines opérationnels qui n’ont pas reçu de financement direct dans le cadre des autorités du PCCC.

L’évaluation a formulé les recommandations suivantes :

Recommandation 1 : On recommande que SPAC clarifie les rôles et responsabilités des intervenants dans la documentation du programme afin d’améliorer l’efficacité et l’efficience du PCCC à court terme (pendant qu’il est géré par la DGAMD) et à long terme (une fois que les décisions concernant l’emplacement définitif du PCCC auront été prises).

Recommandation 2 : On recommande que SPAC examine, renforce et termine les outils de gestion des risques utilisés par le PCCC.

Annexe 1 : Plan d’action de la direction

Recommandation	Réponse de la direction	Plan d’action de la direction	Produits livrables	Date de mise en œuvre visée	Bureau de responsabilité
1. On recommande que SPAC clarifie les rôles et responsabilités des intervenants dans la documentation du programme afin d’améliorer l’efficacité et l’efficience du Programme canadien de certification en cybersécurité (PCCC) à court terme (pendant qu’il est géré par la Direction générale de l’approvisionnement maritime et de défense [DGAMD]) et à long terme (une fois que les décisions concernant l’emplacement définitif	Recommandation acceptée. Clarifier les rôles permettra à la DGAMD de suivre l’état d’avancement des tâches et permettra aux futurs responsables du programme de déterminer des axes de changement afin d’améliorer l’efficacité. De plus, la mise à jour de la documentation apportera davantage de clarté et améliorera le suivi et l’établissement de rapports afin que les responsables ministériels soient informés et assument la responsabilité des engagements et des tâches.	• Cartographier tous les intervenants internes et externes ainsi que leurs rôles actuels. • Mettre à jour les activités du plan de travail, la matrice RACI, les BPR et leurs états. and • Communiquer et valider les rôles et responsabilités avec tous les intervenants.	• Plan de travail et matrice RACI à jour pour clarifier les rôles et responsabilités afin de diffuser l’information aux intervenants du programme. • Confirmation par le comité directeur de la DG des documents mis à jour.	Décembre 2025	DGAMD (jusqu’au 31 déc. 2025) Direction générale de la surveillance (DGS) (à partir du 1er janvier 2026)

Recommandation	Réponse de la direction	Plan d’action de la direction	Produits livrables	Date de mise en œuvre visée	Bureau de responsabilité
du PCCC auront été prises).					
2. On recommande que SPAC examine, renforce et termine les outils de gestion des risques utilisés par le PCCC.	Recommandation acceptée.	• Examiner le registre des risques existants et les stratégies d’atténuation, notamment l’intégration des risques cernés lors de l’analyse des lacunes effectuée à l’été 2025, afin de redéfinir les risques de base avant de commencer les phases initiales de la mise à l’essai et de la mise en œuvre. • Renforcer le registre des risques et les stratégies d’atténuation en déterminant un responsable des risques conformément au plan de travail révisé et à la matrice RACI (chaque propriétaire étant responsable de la mise à jour des risques et des	• Registre des risques mis à jour à distribuer aux intervenants du programme, conformément à l’analyse des lacunes du programme. Le registre des risques mis à jour reflétera l’état actuel, indiquera le responsable des risques afin de favoriser la clarification des rôles et responsabilités, puis comportera des évaluations actualisées de la probabilité et de l’impact. Le registre des risques mis à jour comprendra les risques liés au programme, à la mise en œuvre, aux intervenants, et aux systèmes existants, ainsi	Janvier 2026	DGS

Recommandation	Réponse de la direction	Plan d’action de la direction	Produits livrables	Date de mise en œuvre visée	Bureau de responsabilité
		stratégies d’atténuation à mesure de l’avancement du programme) et en incluant des évaluations actualisées de la probabilité et de l’impact pour tous les risques. and • Finaliser le registre des risques et les stratégies d’atténuation au moyen d’examens trimestriels avec les ministères et les organismes partenaires afin que les risques et les mesures d’atténuation demeurent conformes à la conception et à l’élaboration du programme. Présentation trimestrielle des principaux risques au comité directeur de la DG aux fins de discussion et d’examen.	que les risques financiers. • Confirmation par le comité directeur de la DG des documents mis à jour afin de démontrer l’acceptation et la responsabilité des risques révisés. • Examen du registre des risques avec les ministères et les organismes partenaires, ainsi qu’avec le comité directeur de la DG. L’examen de la DG comprendra un examen de la tolérance au risque.		

Annexe 2 : Méthodologie d'évaluation

Sources de données	Entrevues	Examen des documents	Sondages
MÉTHODOLOGIE	– **Entrevues avec neuf intervenants du PCCC** : ▪ Direction de programme de SPAC (DGS et DGAMD) : **5** ▪ Niveau opérationnel de SPAC (DGS et DGAMD) : **3** ▪ SCT (direction de programme) : **1**	– **Environ 150 documents** examinés : ▪ ~50 documents du PCCC relatifs à la planification de programme ▪ ~20 documents du PCCC relatifs à la gestion de projet ▪ ~50 documents du PCCC relatifs à la gouvernance, dont les procès-verbaux des réunions de divers comités ▪ ~15 documents de recherche en matière de cybersécurité ▪ ~10 documents budgétaires du PCCC ▪ ~5 documents sur la consultation des intervenants de l'industrie	– 33 questionnaires envoyés aux intervenants du PCCC sous la forme de deux sondages distincts (un pour le niveau opérationnel et un autre au niveau de la direction de programme)
LIMITES	– La collaboration étroite avec la DGS et la DGAMD a permis d'interroger la plupart des intervenants pertinents, ce qui n'a pas limité la collecte de données. – Nous n'avons pas pu interroger l'autorité cliente, à savoir le MDN.	– La collaboration étroite avec la DGS et la DGAMD a permis d'examiner toute la documentation disponible, ce qui n'a pas limité la collecte de données. – La documentation reçue était suffisante pour formuler des constatations.	– Taux de réponse au niveau opérationnel : **11 sur 21 (52 %)** – Taux de réponse au niveau de la gestion du programme : **5 sur 12** (**42 %)**
MESURES D'ATTÉNUATION	– Les constatations préliminaires de l'évaluation et l'ébauche de rapport final ont été remises au comité directeur de la DG du PCCC pour examen. Elles ont également été communiquées pour examen aux fonctions d'évaluation des ministères partenaires.	– Sans objet	– Lorsque, dans un sondage, une même question était posée au niveau opérationnel et au niveau de la gestion du programme, nous avons combiné les réponses afin d'intégrer les points de vue de la direction. – Les constatations préliminaires de l'évaluation et l'ébauche de rapport final ont été remises au comité directeur de la DG du PCCC pour examen. Elles ont également été communiquées pour examen aux fonctions d'évaluation des ministères partenaires.