

Rapport annuel 2023 - 2024



www.ncc-cnc.ca

TABLE DES MATIÈRES

Message de la présidente	1
Conseil d'administration	2
Message du directeur scientifique	3
Appel à propositions 2023	4
Appel à propositions 2024	8
Diffusion et mobilisation	9
Nos membres 2023/24	11
Mise à jour des finances	12
États financiers	13

Message de la Présidente



Dre Charmaine Dean

L'importance de la cybersécurité au Canada se manifeste tous les jours.

La mission du Consortium national pour la cybersécurité (CNC) est de développer l'écosystème de la cybersécurité au Canada et d'assurer la sécurité des Canadiens en finançant des projets de calibre mondial. Le CNC soutient quotidiennement ses membres et leurs projets dans le cadre de son engagement à améliorer la cybersécurité au Canada.

L'année qui vient de passer fut à la fois exigeante et valorisante pour le CNC. Nos activités ont pris leur envol en 2023 avec l'attribution de plus de 11 millions de dollars en financement et une augmentation considérable des propositions de projets en 2024.

Le CNC et son équipe se sont rapidement taillé une réputation comme étant un organisme essentiel et engagé dans l'écosystème de la cybersécurité au Canada. Notre équipe, sous la direction du directeur scientifique Ken Barker, ne ménage aucun effort pour concevoir des programmes efficaces et développer un réseau pancanadien de membres spécialisés en cybersécurité.

En association avec nos partenaires du Réseau d'innovation pour la cybersécurité d'Innovation, Sciences et Développement économique Canada, le CNC est devenu le point de contact pour le développement de programmes en cybersécurité dans les secteurs de la recherche, de la formation et de la commercialisation. C'est aussi en 2023-2024 que nous avons mis en place notre infrastructure pour bâtir notre communauté et élargir notre portée future à partir d'une base solide.

Je tiens à remercier mes collègues du conseil d'administration et toute l'équipe du CNC pour leur apport envers ce secteur révolutionnaire. Votre dévouement et votre innovation sont à la source de la réussite de CNC au cours de la dernière année. C'est un honneur pour moi de travailler avec vous.

Cordialement,

Charmaine Dean

Membres du conseil



Dominique Bérubé, Ph. D.
Vice-rectrice à la recherche et aux
études supérieures
Université Concordia



William Ghali, Ph. D.
Vice-président, Recherche
Université de Calgary



Steven N. Liss, Ph. D.
Vice-président, Recherche et
innovation
Université métropolitaine de Toronto



David MaGee, Ph. D.
Vice-président, Recherche
Université du
Nouveau-Brunswick

Message du directeur scientifique, Consortium national pour la cybersécurité



Ken Barker, Ph. D

Ce fut une année productive et passionnante pour le Consortium national pour la cybersécurité! Notre idée s'est transformée en influence de taille envers l'écosystème de la cybersécurité au Canada.

Nous avons octroyé une première phase de financement dans le cadre du programme du Réseau d'innovation pour la cybersécurité (RIC) et avons lancé un deuxième appel à propositions en 2024 pour repérer des initiatives intéressantes en matière de cybersécurité et de protection de la vie privée des Canadiens. Tout cela dès notre première année d'activités.

Notre directrice générale, Mary Henricksen, a procédé à l'embauche d'employés à temps plein exceptionnellement qualifiés. Ce petit groupe d'experts consacre tous ses efforts à soutenir nos bénéficiaires ultimes dans l'atteinte de leurs objectifs, que ce soit des programmes de formation, des initiatives de recherche et de développement ou des idées innovantes dans le secteur de la commercialisation. L'équipe a même développé une devise : respecter la recherche... et non la retenir!

Nous tenons à remercier les nombreux intervenants des secteurs public et privé, ainsi que notre cohorte d'intervenants du milieu de l'enseignement postsecondaire qui participent au CNC. Le CNC est également très reconnaissant du soutien d'Innovation, Sciences et Développement économique Canada qui veille à l'atteinte de nos objectifs et nous aide à trouver des solutions pour aller encore plus loin. Un grand merci à la communauté élargie d'experts en informatique de tous les secteurs pour leur contribution sous forme de conseils, d'analyses et de soumission de projets, et de soutien moral lors du démarrage du CNC.

Je remercie notre conseil d'administration pour son engagement absolu envers la vision, les objectifs et le personnel du CNC qui travaille sans relâche pour établir une approche visionnaire en réponse à un besoin essentiel au Canada. Votre détermination et votre expertise permettront au CNC de réussir et de diversifier la valeur qu'il offre à ses membres alors que nous entamons notre deuxième année d'activités.

Cordialement,

Ken Barker

Appel à propositions 2023

Le CNC a octroyé **11,2 millions de dollars** pour 20 projets dans le cadre du premier appel à propositions en 2023.

L'appel à propositions annuel du CNC vise à favoriser un écosystème de cybersécurité solide et à positionner le Canada en tant que chef de file mondial en matière de cybersécurité. Les 20 projets retenus lors de l'appel à propositions 2023 dans les catégories **Commercialisation, Recherche et développement et Formation** couvrent un large éventail d'activités, de la création d'un réseau 5G sécurisé cyberrésilient avec l'aide de l'intelligence artificielle (IA) à un programme de maîtrise hybride en analyse de la cybersécurité. L'investissement représentent une valeur équivalente à 39,2 millions de dollars.

Projets 2023 retenus

Recherche et développement

ATLAS

Bénéficiaire : Deloitte

Collaborateurs : Université Concordia (Que.), Prompt (Que.), Desjardins (Que.), Cybereco (Que.), Pinq2 (Que.)

Fonds engagés : 1 000 000 \$

Conception d'un système de sauvegarde confidentiel, évolutif et performant

Bénéficiaire : Université du Waterloo

Collaborateurs : École Polytechnique de Montréal (Que.), Acronis

Fonds engagés : 370 036 \$

Construire des réseaux 5G cyber-résilients et sécurisés grâce à l'automatisation et à l'IA

Bénéficiaire : Université Concordia

Collaborateurs : Ericsson (Que.), University of Waterloo (Ont.), University of Manitoba (Man.)

Fonds engagés : 1 000 000 \$

Gestion des vulnérabilités grâce à l'IA

Bénéficiaire : Université du Nouveau-Brunswick

Collaborateurs : Rogers (Ont.), CIC (N.-B.)

Fonds engagés : 240 750 \$

Recherche et développement (cont.)

Nouvelle génération d'empreintes digitales pour la détection et la prédiction de la fraude

Bénéficiaire : Université du Waterloo

Collaborateurs : Mastercard (C.-B.), Université du Nouveau-Brunswick (N.-B.)

Fonds engagés : 288 099 \$

« Transfer Fuzzing » pour les appareils sans micrologiciel

Bénéficiaire : Université du Waterloo

Collaborateurs : Blackberry (Ont.), Rational Minds Innovation (Que.)

Fonds engagés : 270 470 \$

Atténuer les impacts sur la sécurité, la vie privée et l'éthique dans les systèmes de pointe d'aide à la conduite

Bénéficiaire : Université du Queens

Collaborateurs : Irdeto (Ont.), Université Western (Ont.), Collège militaire royal (Ont.)

Fonds engagés : 300 000 \$

La sécurité d'exécution du système d'info-divertissement automobile Android

Bénéficiaire : Université du Saskatchewan

Collaborateurs : Blackberry (Ont.), Amazon (Ont.), McGill University (Que.)

Fonds engagés : 420 619,61 \$

Projet de recherche sur la migration des modules de sécurité matériels (HSM) post-Quantum

Bénéficiaire : Université du Nouveau-Brunswick

Collaborateurs : Scotiabank (Ont.)

Fonds engagés : 286 000 \$

Cybersécurité de l'identité numérique

Bénéficiaire : Université du Québec en Outaouais

Collaborateurs : Portage Cybertech (Que.), Université Laval (Que.), Concordia University (Que.)

Fonds engagés : 90 000 \$

Recherche et développement (cont.)

Cadre fiable basé sur l'intelligence artificielle pour les technologies d'essaimage de drones autonomes

Bénéficiaire : Ontario Tech Institute

Fonds engagés : 89 987,50 \$

Formation

CyberLab

Bénéficiaire : Field Effect Software

Collaborateurs : Cyberquebec (Que.), Algonquin College (Ont.), Université du Calgary (Alb.)

Fonds engagés : 900 000 \$

Programme de maîtrise hybride en analyse de la cybersécurité (anciennement le certificat d'études supérieures en ligne du SIS en cybersécurité)

Bénéficiaire : Université du McGill

Collaborateurs : Blackberry (Ont.), Ericsson (Que.), Samsung (Que.)

Fonds engagés : 1 000 000 \$

De la formation à la cyberstart-up innovante

Bénéficiaire : École Polytechnique de Montréal

Collaborateurs : Desjardins (Que.), Cybereco (Que.), HEC Montréal (Que.), Université de Montréal (Que.)

Fonds engagés : 999 900 \$

Formation multidisciplinaire et exhaustive en cybersécurité

Bénéficiaire : Université du Waterloo

Collaborateurs : Université du Brandon (Man.), Université d'Alberta (Alb.), eSentire (Ont.)

Fonds engagés : 402 691,43 \$

Formation (cont.)

Façonner la réglementation en matière de cybersécurité au Canada

Bénéficiaire : Université du Calgary

Fonds engagés : 915 838,15 \$

Maîtrise en gestion de la cybersécurité

Bénéficiaire : Université du Nouveau-Brunswick

Fonds engagés : 998 538 \$

Programme de formation en sécurité infonuagique (microcertification)

Bénéficiaire : Université du McGill

Collaborateurs : FX Innovation (Que.)

Fonds engagés : 666 941 \$

Commercialisation

PASCAL

Bénéficiaire : Palitronica Inc.

Collaborateurs : Arcfield (Alb.), Continental (Ont.), Sera4 (Ont.), Université du Waterloo (Ont.)

Fonds engagés : 1 000 000 \$

Appel à propositions 2024

Le CNC a octroyé plus de **20 millions de dollars** pour des projets de cybersécurité au Canada dans le cadre du deuxième appel à propositions.

Le CNC a tiré profit du succès du premier appel et amélioré le processus de demande de financement pour le simplifier et le rendre plus efficace, suite aux commentaires des participants.

Le deuxième appel à propositions, tenu en 2024, comportait trois volets de financement : la commercialisation, la recherche et le développement, et la formation. Le volet de la recherche et du développement comportait, quant à lui, deux sous-volets : les projets standards et les projets de pointe. Autre nouveauté : les propositions sont maintenant déposées sur une plateforme en ligne, le portail Adsigno, selon trois phases.

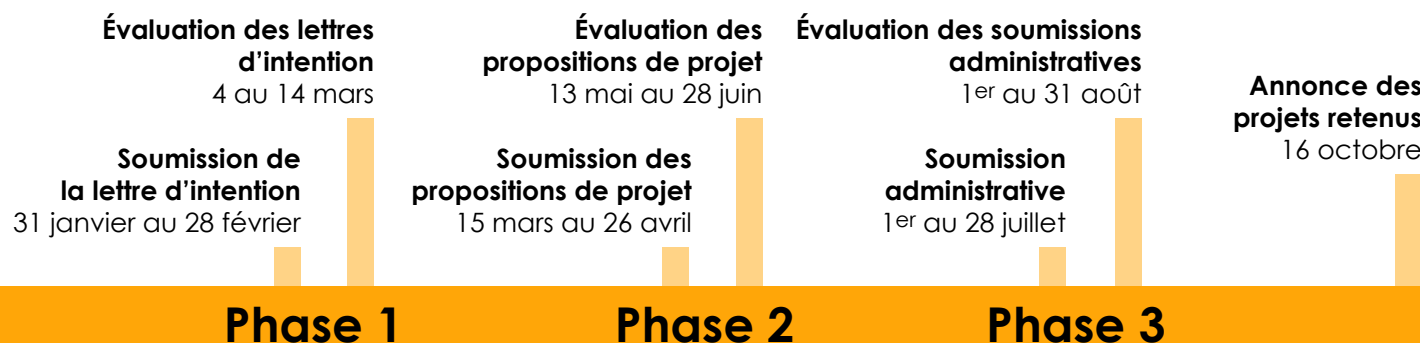
Phase 1 : lettre d'intention. Les organisations intéressées étaient invitées à soumettre une courte lettre d'intention afin de donner un aperçu du projet proposé et des sources de contributions de contrepartie, le cas échéant. Le CNC a évalué ces lettres d'intention pour en vérifier l'admissibilité selon les paramètres de l'appel à propositions. Nous avons reçu trois fois plus de demandes qu'au premier appel et avons invité 90 % des demandeurs à soumettre une proposition de projet, soit la phase 2.

Phase 2 : proposition de projet. proposition de projet. Les demandeurs invités devaient remplir un formulaire en ligne afin de définir davantage leur projet, et d'en démontrer le bien-fondé et la faisabilité. Un groupe d'experts a procédé à l'évaluation des propositions soumises et leur a attribué une note en fonction des critères d'évaluation fournis aux demandeurs dans le *Guide de l'appel à propositions 2024*. Les organisations dont les propositions ont été retenues étaient invitées à passer à la phase 3.

Phase 3 : soumission administrative. L'objectif de la phase 3 est d'effectuer des vérifications concernant des erreurs ou des risques, et de valider les documents justificatifs lors d'une demande d'informations supplémentaires.

Les projets ayant complété les trois phases avec succès ont été annoncés le 16 octobre, à l'occasion du Mois de la sensibilisation à la cybersécurité.

2024 Calendrier de l'appel à propositions



Diffusion et mobilisation

Développer la collaboration et les compétences au sein de l'écosystème canadien de la cybersécurité

Conférence annuelle du Cybersecurity and Privacy Institute en 2023 Université de Waterloo



Dr Ken Barker, directeur scientifique du CNC, lors de la conférence annuelle du Cybersecurity and Privacy Institute tenue à l'Université de Waterloo en 2023.

[Visionner la présentation du Dr Barker](#)

Équité, diversité, inclusion et accessibilité

Le CNC estime qu'un groupe talentueux et diversifié de personnes ayant des points de vue, de l'expérience et des antécédents variés est mieux équipé pour réaliser sa vision et sa mission.

L'année 2023-2024 fut une année de croissance remarquable pour le CNC, et nous en avons profité pour intégrer les principes d'équité, de diversité, d'inclusion et d'accessibilité à nos politiques et notre culture dès le début. Nous avons même atteint les objectifs fixés par le Défi 50-30 du gouvernement du Canada au sein de notre personnel et de notre conseil d'administration. Nous incorporons également les concepts de l'équité, de la diversité et de l'inclusion dans la structure de soumission des appels à propositions et nous redoublons d'efforts pour élaborer des communications qui respectent les meilleures pratiques en matière d'accessibilité.

Diffusion et mobilisation

Séances d'information relatives à l'appel à propositions 2024

Pour aider les demandeurs à bien se préparer aux phases 1 et 2 de l'appel à propositions, nous avons offert une série de 10 séances d'information sur Zoom, en anglais et en français.

Plus de 300 personnes représentant des organisations d'un bout à l'autre du Canada ont participé à ces séances afin de mieux comprendre le processus complexe de l'appel et ses multiples étapes. Chaque séance abordait un sujet précis, y compris les renseignements généraux, les explications concernant les différents volets ainsi qu'une liste des éléments exigés pour chacune des phases. Les webinaires permettaient aux participants de poser des questions afin d'optimiser leurs candidatures.

**Regarder les
séances d'information**

Lancement du programme d'adhésion au CNC

Lancé en janvier 2024, le nouveau programme d'adhésion au CNC soutient notre objectif de développer un réseau pancanadien pour faire avancer la cybersécurité.

Ce programme permet aux membres de collaborer, d'innover et d'apprendre les uns des autres. Il offre plusieurs opportunités, dont les appels à propositions et des événements de réseautage, qui favorisent et stimulent la recherche et la croissance économique et améliore la cybersécurité au Canada. Nous sommes enthousiastes à l'idée de développer plusieurs autres avantages pour nos membres, de continuer à privilégier les liens intersectoriels et de stimuler la croissance dans l'ensemble de l'écosystème.

Le CNC comptait 21 organisations membres à la fin de l'exercice financier 2023-2024, provenant du milieu universitaire et des secteurs privé et à but non lucratif.

En savoir plus sur l'adhésion

Membres 2023-2024

Membres du monde académique



Membres du secteur privé



Membres à but non lucratif

Information And Communications
Technology Council of Canada Inc.



MISE À JOUR DES FINANCES 2023-2024

Suite à la mise en place du CNC par des consultants externes, l'exercice financier 2023-2024 représente la première année d'activités du Consortium avec du personnel à temps plein. Le Consortium a reçu 2 560 898 \$ cette année de la part d'Innovation, Sciences et Développement économique Canada (ISDE). De ce montant, 1 485 318 \$ de dépenses admissibles ont été affectés aux activités de démarrage et à l'évaluation de notre premier appel à propositions. L'ISDE a donné son accord pour un report des sommes non dépensées en 2023-2024 à l'exercice 2024-2025.

Le Consortium a investi 11 269 871 \$ dans 20 projets, avec des contributions de contrepartie d'environ 35 738 030 \$, pour un investissement total de 47 007 901 \$ dans l'écosystème de la cybersécurité.

Quant aux frais d'adhésion, 33 585 \$ ont été comptabilisés en tant que revenus sur un total de 199 250 \$ perçus au cours de l'année.

Le Consortium fait l'objet d'un audit financier annuel réalisé par des auditeurs indépendants, autorisé par le conseil d'administration et supervisé par le comité de vérification et des finances. BDO Canada LLP a terminé l'audit pour l'exercice financier 2023-2024 en juin 2024 avec une opinion sans réserve. Les états financiers vérifiés sont présentés à la page 10.

En outre, le Consortium se conforme à toutes les exigences réglementaires et prévues par la loi en matière de déclaration et de paiement. Notre engagement en matière de transparence et de respect des obligations réaffirme notre volonté de maintenir des normes élevées en matière de responsabilité et de gouvernance.

Consortium national pour la cybersécurité

États financiers

Pour l'exercice terminé le 31 mars 2024

Table des matières

Rapport de l'auditeur indépendant	2 - 4
États financiers	
État de la situation financière	5
État de l'évolution de l'actif net (insuffisance)	6
État des résultats	7
État des flux de trésorerie	8
Notes complémentaires	9 - 11



Rapport de l'auditeur indépendant

Aux membres du Consortium national pour la cybersécurité

Opinion

Nous avons effectué l'audit des états financiers du Consortium national pour la cybersécurité (le « consortium »), qui comprennent l'état de la situation financière au 31 mars 2024, et les états des résultats, de l'évolution de l'actif net (insuffisance) et des flux de trésorerie pour l'exercice terminé à cette date, ainsi que les notes, y compris le résumé des principales méthodes comptables.

À notre avis, les états financiers ci-joints donnent, dans tous leurs aspects significatifs, une image fidèle de la situation financière du consortium au 31 mars 2024, ainsi que de sa performance financière et de ses flux de trésorerie pour l'exercice terminé à cette date, conformément aux Normes comptables canadiennes pour les organismes sans but lucratif.

Fondement de l'opinion

Nous avons effectué notre audit conformément aux normes d'audit généralement reconnues du Canada. Les responsabilités qui nous incombent en vertu de ces normes sont plus amplement décrites dans la section *Responsabilités de l'auditeur à l'égard de l'audit des états financiers* du présent rapport. Nous sommes indépendants du consortium conformément aux règles de déontologie qui s'appliquent à notre audit des états financiers au Canada et nous nous sommes acquittés des autres responsabilités déontologiques qui nous incombent selon ces règles. Nous estimons que les éléments probants que nous avons obtenus sont suffisants et appropriés pour fonder notre opinion d'audit.

Responsabilités de la direction et des responsables de la gouvernance à l'égard des états financiers

La direction est responsable de la préparation et de la présentation fidèle des états financiers conformément aux Normes comptables canadiennes pour les organismes sans but lucratif, ainsi que du contrôle interne qu'elle considère comme nécessaire pour permettre la préparation d'états financiers exempts d'anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs.

Lors de la préparation des états financiers, c'est à la direction qu'il incombe d'évaluer la capacité du consortium à poursuivre son exploitation, de communiquer, le cas échéant, les questions relatives à la continuité de l'exploitation et d'appliquer le principe comptable de continuité d'exploitation, sauf si la direction a l'intention de liquider le consortium ou de cesser son activité ou si aucune solution réaliste ne s'offre à elle.

Il incombe aux responsables de la gouvernance de surveiller le processus d'information financière du consortium.

Responsabilités de l'auditeur à l'égard de l'audit des états financiers

Nos objectifs sont d'obtenir l'assurance raisonnable que les états financiers pris dans leur ensemble sont exempts d'anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs, et de délivrer un rapport de l'auditeur contenant notre opinion. L'assurance raisonnable correspond à un niveau élevé d'assurance, qui ne garantit toutefois pas qu'un audit réalisé conformément aux normes d'audit généralement reconnues du Canada permettra toujours de détecter toute anomalie significative qui pourrait exister. Les anomalies peuvent résulter de fraudes ou d'erreurs et elles sont considérées comme significatives lorsqu'il est raisonnable de s'attendre à ce que, individuellement ou collectivement, elles puissent influencer sur les décisions économiques que les utilisateurs des états financiers prennent en se fondant sur ceux-ci.

Dans le cadre d'un audit réalisé conformément aux normes d'audit généralement reconnues du Canada, nous exerçons notre jugement professionnel et faisons preuve d'esprit critique tout au long de cet audit. En outre :

- Nous identifions et évaluons les risques que les états financiers comportent des anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs, concevons et mettons en œuvre des procédures d'audit en réponse à ces risques, et réunissons des éléments probants suffisants et appropriés pour fonder notre opinion. Le risque de non-détection d'une anomalie significative résultant d'une fraude est plus élevé que celui d'une anomalie significative résultant d'une erreur, car la fraude peut impliquer la collusion, la falsification, les omissions volontaires, les fausses déclarations ou le contournement du contrôle interne;
- Nous acquérons une compréhension des éléments du contrôle interne pertinents pour l'audit afin de concevoir des procédures d'audit appropriées aux circonstances, et non dans le but d'exprimer une opinion sur l'efficacité du contrôle interne du consortium;
- nous apprécions le caractère approprié des méthodes comptables retenues et le caractère raisonnable des estimations comptables faites par la direction, de même que des informations y afférentes fournies par cette dernière;
- Nous tirons une conclusion quant au caractère approprié de l'utilisation par la direction du principe comptable de continuité d'exploitation et, selon les éléments probants obtenus, quant à l'existence ou non d'une incertitude significative liée à des événements ou situations susceptibles de jeter un doute important sur la capacité du consortium à poursuivre son exploitation. Si nous concluons à l'existence d'une incertitude significative, nous sommes tenus d'attirer l'attention des lecteurs de notre rapport sur les informations fournies dans les états financiers au sujet de cette incertitude ou, si ces informations ne sont pas adéquates, d'exprimer une opinion modifiée. Nos conclusions s'appuient sur les éléments probants obtenus jusqu'à la date de notre rapport. Des événements ou situations futurs pourraient par ailleurs amener le consortium à cesser son exploitation;
- Nous évaluons la présentation d'ensemble, la structure et le contenu des états financiers, y compris les informations fournies dans les notes, et apprécions si les états financiers représentent les opérations et événements sous-jacents d'une manière propre à donner une image fidèle.



Nous communiquons aux responsables de la gouvernance notamment l'étendue et le calendrier prévus des travaux d'audit et nos constatations importantes, y compris toute déficience importante du contrôle interne que nous aurions relevée au cours de notre audit.

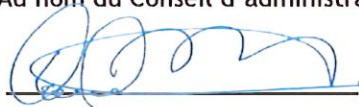
BDO Canada S.R.L./LLP

Comptables professionnels agréés, experts-comptables autorisés
Ottawa (Ontario)
Le 10 juin 2024

Consortium national pour la cybersécurité État de la situation financière

31 mars	2024	2023
Actif		
Court terme		
Encaisse	1 520 299 \$	501 089 \$
Comptes à recevoir	140 823	-
Autres créances	46 200	23 778
Frais payés d'avance	26 346	10 515
Actif total	1 733 668 \$	535 382 \$
Passif et actif net (insuffisance)		
Court terme		
Créditeurs et frais courus	127 487 \$	164 346 \$
Subventions et adhésions reportées (Note 2)	1 513 992	200 719
Dû aux membres fondateurs	112 500	150 000
	1 753 979	515 065
Actif net (insuffisance)		
Non affecté	(20 311)	20 317
Total du passif et de l'actif net	1 733 668 \$	535 382 \$

Au nom du Conseil d'administration :

 Directeur

 Directeur

Consortium national pour la cybersécurité
État de l'évolution de l'actif net (insuffisance)

Pour l'exercice terminé le 31 mars 2024	2024	2023
Solde, début de l'exercice	20 317 \$	57 601 \$
Insuffisance des produits sur les charges	(40 628)	(37 284)
Solde, fin de l'exercice	(20 311)\$	20 317 \$

Consortium national pour la cybersécurité

État des résultats

Pour l'exercice terminé le 31 mars	2024	2023
Produits		
Subventions (Note 2)	1 445 318 \$	544 048 \$
Adhésions (Note 2)	33 585	-
	<u>1 478 903</u>	<u>544 048</u>
Charges		
Développement, prestation et administration du programme	1 485 318	568 415
TVH non réclamable	34 213	12 917
	<u>1 519 531</u>	<u>581 332</u>
Charges totales		
	<u>1 519 531</u>	<u>581 332</u>
Insuffisance des produits sur les charges	<u>(40 628)\$</u>	<u>(37 284)\$</u>

Consortium national pour la cybersécurité

État des flux de trésorerie

Pour l'exercice terminé le 31 mars	2024	2023
Flux de trésorerie liés aux activités de fonctionnement		
Insuffisance des produits sur les charges	(40 628)\$	(37 284)\$
Variations des éléments hors caisse du fonds de roulement:		
Comptes à recevoir	(140 823)	-
Autres créances	(22 422)	(23 778)
Frais payés d'avance	(15 831)	(10 515)
Créditeurs et frais courus	(36 859)	164 346
Subventions et adhésions reportées	1 313 273	200 719
	1 056 710	293 488
Flux de trésorerie liés aux activités d'investissement		
Dû aux membres fondateurs	(37 500)	150 000
Augmentation nette de la trésorerie	1 019 210	443 488
Encaisse, début de l'exercice	501 089	57 601
Encaisse, fin de l'exercice	1 520 299 \$	501 089 \$

Consortium national pour la cybersécurité

Notes complémentaires

31 mars 2024

1. Méthodes comptables

Statut et objectif de l'organisme

Consortium national pour la cybersécurité (le « consortium ») est un organisme sans but lucratif constitué sans capital-actions en vertu de la Loi canadienne sur les organisations sans but lucratif le 3 mars 2020, en tant qu'organisation fondée par les membres avec une entente entre Innovation, Sciences et Développement économique Canada (ISDE) et le Consortium national pour la cybersécurité. Le consortium est un organisme sans but lucratif au sens de la Loi de l'impôt sur le revenu et, à ce titre, il est exonéré d'impôt.

Le mandat du Consortium est de faire progresser l'écosystème de la cybersécurité du Canada par la recherche et le développement, la commercialisation et la formation.

Référentiel comptable

Le consortium applique les Normes comptables canadiennes pour les organismes sans but lucratif.

Utilisation d'estimations

La préparation des états financiers exige que la direction procède à des estimations et pose des hypothèses qui ont une incidence sur les montants présentés au titre des actifs et des passifs et sur les montants comptabilisés au titre des produits et des charges pour l'exercice visé.

Comptabilisation des produits

Le consortium applique la méthode du report pour comptabiliser les apports. Les apports affectés sont comptabilisés à titre de produits de l'exercice au cours duquel les charges connexes sont engagées. Les apports non affectés sont comptabilisés à titre de produits lorsqu'ils sont reçus ou à recevoir si le montant à recevoir peut faire l'objet d'une estimation raisonnable et que sa réception est raisonnablement assurée.

Les adhésions sont comptabilisées à titre de produits au prorata dans l'exercice auquel elles se rapportent.

Instruments financiers

Évaluation initiale et ultérieure

Le consortium évalue initialement ses actifs financiers et passifs financiers à la juste valeur. Il évalue ultérieurement tous ses actifs financiers et passifs financiers au coût après amortissement.

Dépréciation

Les actifs financiers évalués au coût après amortissement sont soumis à un test de dépréciation s'il existe des indications d'une possible dépréciation.

Consortium national pour la cybersécurité

Notes complémentaires

31 mars 2024

1. Méthodes comptables (suite)

Instruments financiers (suite) Coûts de transaction

Les coûts de transaction relatifs à des instruments financiers évalués ultérieurement au coût après amortissement sont comptabilisés au coût initial de l'actif ou du passif financier et comptabilisés aux résultats sur la durée de l'instrument selon la méthode de l'amortissement linéaire.

2. Subventions et adhésions reportées

Les subventions et adhésions reportées représentent les montants restreints reçus d'ISDE et des adhésions liées aux années ultérieures ou pour lesquels les charges associées n'ont pas encore été encourues. Le solde se compose des éléments suivants:

	2024	2023
Subventions d'ISED reportées	1 310 827 \$	200 719 \$
Adhésions reportées	203 165	-
Solde, à la fin de l'exercice	1 513 992 \$	200 719 \$

Les variations du solde au cours de l'année sont les suivantes:

	2024	2023
Solde, au début de l'exercice	200 719 \$	- \$
Plus: subventions d'ISED reçues pendant l'année	2 555 426	744 767
Plus: adhésions reçues pendant l'année	236 750	-
Moins: subventions d'ISED constatées à titre de produits de l'exercice	(1 445 318)	(544 048)
Moins: adhésions constatées à titre de produits de l'exercice	(33 585)	-
Solde, à la fin de l'exercice	1 513 992 \$	200 719 \$

3. Dépendance économique

Le consortium a reçu 98% (2023 - 100%) de ses produits d'ISED. Si ce financement ne continue pas ou si le consortium ne peut pas le remplacer, le consortium ne pourrait pas continuer ses opérations au niveau actuel.

Consortium national pour la cybersécurité

Notes complémentaires

31 mars 2024

4. Instruments financiers

Risque de crédit

Le consortium est exposé au risque de crédit puisque tous ses comptes bancaires sont détenus auprès d'une seule institution financière. Il n'y a pas eu de variation dans le risque comparativement à l'année précédente.

5. Chiffres comparatifs

Certains chiffres de l'exercice précédent ont été reclassés afin de rendre leur présentation identique à celle de l'exercice courant.



www.ncc-cnc.ca



[Suivez-nous sur LinkedIn](#)



[Inscrivez-vous à notre liste d'envoi](#)

Funded by the Government of Canada
Financé par le gouvernement du Canada

Canada 