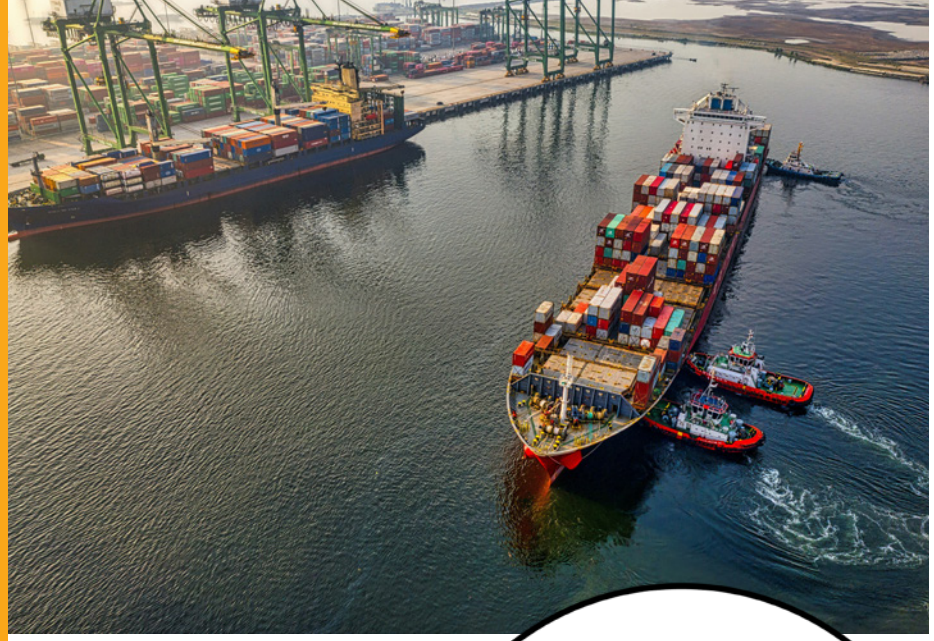


NATIONAL CYBERSECURITY CONSORTIUM

CONSORTIUM NATIONAL POUR LA CYBERSÉCURITÉ

2024 - 2025 Annual Report

A Message from the

Chair of the Board

Dr. Charmaine Dean

Cybersecurity continues to be a critical topic in everyday life in Canada. The National Cybersecurity Consortium (NCC) was created to advance Canada's cybersecurity ecosystem, and to support world class initiatives to keep Canadians safe. Each day, the NCC supports our community and the projects we have funded in our commitment to improve cybersecurity in Canada.

The NCC and the demand for its funding support has grown significantly in our second full year of operation. In 2024, we received more than 90 requests for funding and supported 37 significant Canadian cybersecurity projects with more than $22m in funding. The need for well-funded, far-reaching cybersecurity research, development, training, and commercialization is being well demonstrated.

The NCC and its team have worked diligently to become recognized as one of Canada's most active and vital cybersecurity ecosystem entities. Under the direction of our Scientific Director, Ken Barker, our dedicated team works hard to deliver effective and efficient programs, and to build a pan-Canadian, interconnected membership of cybersecurity experts. Along with our partners at the Cyber Security Innovation Network of the Ministry of Innovation, Science and Economic Development Canada, the NCC has provided a much-needed touch point for the development of programs in cybersecurity across research, educational, and commercialization activities. We see 2024-2025 as a year of further building our community and expanding the scope of our impact for an ever-expanding group of Canadian cybersecurity entities in academia and in the private sector.

I want to thank my fellow NCC Board members, and the entire NCC team for their service to such a game-changing environment. Your dedication and creativity have been vital to the NCC's success in this past year, and it has been my honour to work with you.

Sincerely,

Charmaine Dean

NCC Board of Directors

Amir Belkhelladi
Partner and National Leader,
Cyber Risk Services, Deloitte

Dr. Effrosyni Diamantoudi
Dean of Graduate Studies
Concordia University

Dr. William Ghali
Vice President Research
University of Calgary

Elaine Hum
Director, Cybersecurity Partnerships,
Scotiabank

Dr. Emily Laidlaw
Associate Professor and Canada,
Research Chair in Cybersecurity Law,
Faculty of Law, University of Calgary

Dr. Steven N. Liss
Vice President, Research and
Innovation Toronto Metropolitan
University

Dr. David MaGee
Vice President, Research
University of New Brunswick

Greg Murray
SVP Cyber Security, Privacy & Network,
Loblaw Companies Ltd.

A Message from the Scientific Director,

National Cybersecurity Consortium

Dr. Ken Barker

The NCC has had a very exciting and productive year! We have moved from being a "vision" to a "reality" that is impacting the Canadian cybersecurity ecosystem.

This has been our first fully operational year, which included the delivery of first round of funding from the Cybersecurity Security Innovation Network (CSIN) and the roll out of our Call 2024 to identify meritorious cybersecurity/privacy initiatives to support Canada and to help protect Canadians.

The NCC has now put in place a full staff complement to support its activities. The group provides our stakeholders with the highest quality of service to ensure they enable our project leaders to deliver on their goals including training programs, research and development initiatives, and commercialization of innovative ideas. Our team has adopted an internal mantra of "Upholding research … not holding it up!"

We would very much like to thank the many private and public sector participants in the NCC including our cohort of post-secondary stakeholders. In addition, the NCC is very thankful for the strong support received from the federal government, who has helped ensure we are meeting our goals and assisted time and again in finding ways to get things done. In addition, I would like to thank the wider community of cyber experts from all sectors for their contributions to the NCC including providing advice, reviews of projects, applications for funding, and moral support as we have set up the NCC.

I want to thank our Board for their unwavering commitment to the NCC, its goals and vision, and our staff as they continue to work hard to establish a truly visionary approach to meeting a core need for Canada. Your vision, commitment, and expertise will allow the NCC to thrive and diversify its value proposition to its members as we move into the third full year of our operations.

Emerging opportunities around AI and Quantum are being integrated into our thinking about cybersecurity/privacy in Canada in several ways that can be categorized into two dimensions: First, these technologies can be used as tools to enhance security and ensure privacy by using the techniques being developed; and secondly, the threat posed by the emergence and maturation of these technologies present new challenges that need to be addressed as they are deployed. The NCC believes it should take the leadership role in both dimensions by drawing upon our deep expertise in cybersecurity/privacy to ensure that AI/Quantum is applied most effectively to the challenges/opportunities that exist in Canada's digital activities. Significant investments are being made to develop AI and Quantum in Canada, and it is necessary to make corresponding investments in understanding the threats and opportunities they present through the expertise reflected across the NCC. This will ultimately require investment in cyber from public and private sources.

Sincerely,

Ken Barker

2024

Call for Proposals

In our second call for proposals, the NCC committed $21.4 million toward 36 individual projects, which mobilized financial and technical contributions from organizations across Canada. This brings the total project investment in Canadian cybersecurity to over $56 million.

The NCC's annual funding program exists to stimulate a strong national cybersecurity ecosystem and position Canada as a global leader in cybersecurity. Since 2023, the NCC has funded cybersecurity projects in three funding categories: **Commercialization, Research and Development, and Training**. These projects represent a diverse range of activity, from building a cyber-resilient secure 5G network using AI, to offering a master's program in cybersecurity.

2024 Funded Projects

Research & Development - Spearhead

Privacy Assurance for Canadian Children: A Safe and Secure Framework for Large Language Models

Recipient: Carleton University, Ottawa, ON

Committed Funds: $88,800

Enterprise-Scale Zero Trust Platform for Privacy-Enhancing Smart Metering Services

Recipient: University of New Brunswick, Fredericton, NB

Committed Funds: $90,390

Securing the Metaverse with Multimodal Access Control and Authentication Methods

Recipient: Institut national de la recherche scientifique, Quebec City, QC

Collaborators: In Virtuo, Beam Me Up, Kaptics, MYND Therapeutics, University of Waterloo, ColAB Numerique, Digital Trust

Committed Funds: $500,000

Enhancing Electric Vehicle Charging Infrastructure Cybersecurity Through Autonomous and Sustainable AI

Recipient: University of Ontario Institute of Technology, Oshawa, ON

Collaborators: University of Western Ontario

Committed Funds: $175,294.10

Ostrich Accounting: Dotting I's and Crossing t's with your Head in the Sand

Recipient: University of Calgary, Calgary, AB

Committed Funds: $500,000

Fully Automated End-to-end Vulnerability Discovery and Repair with LLMs

Recipient: Simon Fraser University, Burnaby, BC

Committed Funds: $500,000

Boosting the Cyber-Resilience of Microgrids within Future Energy Critical Infrastructures

Recipient: Concordia University, Montreal, QC

Collaborators: RMDS Innovation Inc., University of New Brunswick

Committed Funds: $352,940

Adaptive Decision Defense System: A Proactive Approach to Detecting and Mitigating Dual Denial of Decision Attacks in Critical Infrastructure

Recipient: University of Calgary, Calgary, AB

Collaborators: University of Guelph, Laval University, CyberPatterns Inc., Waterfall Security Solutions

Committed Funds: $496,800

ICS Security in the Age of Industry 4.0

Recipient: University of British Columbia, Vancouver, BC

Committed Funds: $500,000

Protecting Democracy from Cyber Threats

Recipient: University of Calgary, Calgary, AB

Committed Funds: $500,000

Preserving Relationship Privacy in Large Networks

Recipient: Simon Fraser University, Burnaby, BC

Committed Funds: $500,000

Novel Methods for Quantifying and Improving Privacy in Machine Learning

Recipient: University of British Columbia, Vancouver, BC

Committed Funds: $495,000

Fortifying Cybersecurity: Early Ransomware Detection and Mitigation Methods

Recipient: University of New Brunswick, Fredericton, NB

Collaborators: University of Ottawa, Bell Canada, EzSec

Committed Funds: $79,500

Combatting Cyber Influence Operations in Online Social Media

Recipient: Université Laval, Quebec City, QC

Collaborators: McGill University, University of Manitoba

Committed Funds: $485,875

Adaptive AI Firewall Specializing in the Protection of AI Models, Critical Infrastructure, Systems, and Agents

Recipient: University of Western Ontario, London, ON

Collaborators: Syngen AI Lab, University of Waterloo

Committed Funds: $500,000

Security Awareness Training through Online Social Learning - "From Phishing through Smishing to Vishing"

Recipient: University of Ottawa, Ottawa, ON

Collaborators: Royal Canadian Mounted Police

Committed Funds: $373,500

Ensuring Mission-Critical Security: Coordination of Autonomous Drone Groups with Security-Aware Decision Making

Recipient: University of Ottawa, Ottawa, ON

Collaborators: Quanser, Concordia University

Committed Funds: $499,100

Cybersecurity assessment of industrial system predeployment models

Recipient: University of Sherbrooke, Sherbrooke, QC

Collaborators: Centris Technologies, Neverhack, Productique Québec

Committed Funds: $480,000

Secure Genomic Data Processing: Unleashing the Potential of Personalized Medicine

Recipient: University of Waterloo, Waterloo, ON

Collaborators: Independent genomics researcher identified

Committed Funds: $129,900

Adaptive Defense Strategies for Advanced Driver-Assistance Systems: A Game-Theoretic Approach

Recipient: University of Waterloo, Waterloo, ON

Committed Funds: $164,622.50

Transformative Adversaries: Leveraging Generative Pretrained Transformers for the Development of Next-Generation Metamorphic Malware Engines

Recipient: University of Ontario Institute of Technology, Oshawa, ON

Committed Funds: $382,352.94

End-to-End Cyber-Security Solution for the Power Grid

Recipient: York University, Toronto, ON

Collaborators: Cistel Technology, Siemens Inc., IESO, Dalhousie University, Carleton University

Committed Funds: $300,000

Research & Development - Standard

Enabling Secure Outsourcing of Sensitive Data

Recipient: University of Waterloo, Waterloo, ON

Collaborators: Amazon AWS, Royal Bank of Canada, Airbus

Committed Funds: $295,000

Authentication for Quantum-Enabled Secure Communication

Recipient: Quantized Technologies Inc., Calgary, AB

Collaborators: University of Calgary

Committed Funds: $940,000

IntruderInsight: Elevating Cyber Attribution with AI Insights

Recipient: ENFOCOM International Corporation, Calgary, AB

Collaborators: University of Calgary – CPSC, Field Effect Software Inc., Raytheon Canada, Cybera, Royal Canadian Mounted Police, Calgary Police Services, Edmonton Police Services, IBM Canada, Université du Québec en Outaouais, Intlabs, Check Point Software Technologies, InceptionU Educational Foundation Ltd., Raytheon Canada, University of New Brunswick, Toronto Metropolitan University – Rogers Cybersecure Catalyst

Committed Funds: $2,000,000

Toward a Secure User-Centric Green Credit Management System

Recipient: University of Calgary, Calgary, AB

Collaborators: Toronto Metropolitan University, University of Alberta, Telus, GuildOne

Committed Funds: $561,000

Revolutionizing Personal Cyber Security with AI-driven Insights

Recipient: Protexxa Inc., Aurora, ON

Collaborators: Toronto Metropolitan University, Core Centre Inc, Mila Montreal

Committed Funds: $1,701,280

SCMS: Securing Critical Marine Systems

Recipient: Memorial University of Newfoundland, St. John's, NL

Collaborators: Dalhousie University, Defense Research and Development Canada Marine Institute, Transport Canada

Committed Funds: $759,073.18

Commercialization

CyberGuardian: Bridging the Cybersecurity Enforcement Training Gap

Recipient: ENFOCOM International Corporation, Calgary, AB

Collaborators: Raytheon Canada, University of Calgary, Royal Canadian Mounted Police, Calgary Police Service, Edmonton Police Service, Check Point Software Technologies, InceptionU Educational Foundation Ltd., University of Ottawa, Field Effect Software Inc., IBM Canada

Committed Funds: $1,000,000

C1R3 Commercialization

Recipient: Portage CyberTech Inc., Gatineau, QC

Collaborators: Converge, Centre for Research and Experimental Development in Informatics Libre, Université de Québec en Outaouais, McGill University, Zu, Flex Groups

Committed Funds: $1,000,000

Training

IncidentSync: Bridging IT and Law Enforcement

Recipient: ENFOCOM International Corporation, Calgary, AB

Collaborators: Field Effect Software Inc., Toronto Metropolitan University - Rogers Cybersecure Catalyst, Royal Canadian Mounted Police, Calgary Police Services, Edmonton Police Services, University of Calgary - Cont. Ed., InceptionU Educational Foundation Ltd., Intlabs, Université du Québec en Outaouais, Savvy Knowledge Corporation, Raytheon Canada, IBM Canada, Check Point Software Technologies

Committed Funds: $1,000,000

Accelerating Efforts to Secure Canada in an Era of Quantum

Recipient: Quantum Algorithms Institute, Surrey, BC

Collaborators: Field Effect, Information and Communications Technology Council, Canadian Information Processing Society, Beauceron Security, Quantum Algorithms Institute, Durham College

Committed Funds: $1,000,000

Human-Centric Immersive Cybersecurity Training: Socio-Technical and Legal Implications of an Attack

Recipient: University of Ottawa, Ottawa, ON

Collaborators: Université de Montréal, University of Calgary, ENFOCOM, Field Effect, IBM, Desjardin, BNC (to be confirmed)

Committed Funds: $961,400

CRAFT: Cybersecure Robotics and Future Talent

Recipient: University of Waterloo, Waterloo, ON

Collaborators: Cobionics, Labforge, Canadian Nuclear Labs, BTQ, Palitronica, Quanser, Alectra, Milton Hydro, Real Life Robotics

Committed Funds: $1,000,000

MCT: Marine Cybersecurity Training

Recipient: Memorial University of Newfoundland, St. John's, NL

Collaborators: Thales

Committed Funds: $1,000,000

Training for proactive interdisciplinary cybersecurity in the workplace

Recipient: University of Sherbrooke, Sherbrooke, QC

Collaborators: Cybereco, Intact corporation financière

Committed Funds: $580,679

2025
Call for Proposals

In our third call for proposals, the NCC will commit over $20 million toward cybersecurity and privacy projects in Canada.

For the 2025 Call for Proposals, the NCC implemented three new categories to accommodate different types of projects within the Canadian cybersecurity and privacy ecosystem. The new funding Categories include:

Category 1, Accelerated Projects: Intended to make impactful progress on highly targeted, larger budget projects;

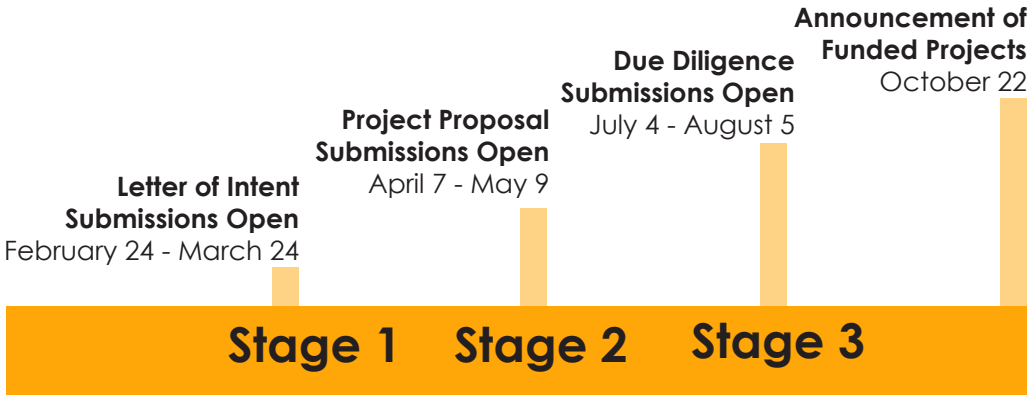
Category 2, New 2025 Projects: An open call for cybersecurity and privacy-related projects; and

Category 3, Top-ups to 2023/2024 Projects: Intended to increase the impact of projects already vetted and approved by the NCC by allowing them to incorporate nascent insights or cover gaps that emerged through the work to date.

Categories 1 and 2 follow a three-stage application and assessment process where submissions are reviewed for eligibility, merit and feasibility by both internal staff and external subject matter experts. Projects that have successfully passed through all three stages will be announced in October during Cybersecurity Awareness Month.

Category 3 projects have an abbreviated application and review process with successful projects announced in January 2026.

2025 Call for Proposals Timeline



Category 1 & 2

Category 3

2025
Call for Proposals Information Sessions

To support applicants throughout the various stages and categories of the Call for Proposals, we hosted a series of Information Sessions held on Zoom in both English and French.

Sessions were well attended with over 250 participants having joined, representing organizations from across Canada. The sessions covered topics including general information, stream and category-specific details, and a breakdown of the requirements during different stages of the Call. The sessions also provided a platform for applicants to directly raise questions with an opportunity to learn how to optimize their applications.

Outreach & Engagement

Throughout 2024-2025 fiscal year, the NCC engaged in many events that cultivated collaboration and capacity-building within the Canadian cybersecurity and privacy ecosystem, a few of which included:

CARA Conference, May 14, 2024, Calgary, AB - Dr. Ken Barker, NCC Scientific Director conducted a presentation entitled, "Upholding Research – Not Holding it Up" at the Canadian Association of Research Administrators Conference.

ORION Think Conference, October 16 and 17, 2024, Blue Mountains, ON – Dr. Charmaine Dean, NCC Chair of the Board and Dr. Steven Liss, NCC Board Director, sat on a panel entitled, "The Intersection of Education and Cybersecurity".

Canada 157: The Canadian National Conference on Innovation, November 7 - 8, 2024, Université du Québec en Outaouais, Gatineau-Ottawa, QC - Dr. Ken Barker, NCC Scientific Director conducted a presentation entitled, "On Advancing the Canadian Cybersecurity Ecosystem".

NCC Conferences & Events

Scientific & Ecosystem Advisory Committee

The NCC has now established an advisory committee called the Scientific & Ecosystem Advisory Committee (SEAC) to advance its goals by providing strategic insights about current trends, challenges, and potential directions that will allow the NCC to impact most effectively cybersecurity in Canada. SEAC is composed of key cybersecurity and privacy experts and leaders drawn from academia, the private sector, not-for-profits, and governments. SEAC will provide advice about where the most pressing needs are across the Canadian cybersecurity ecosystem and how those needs are situated within the larger international setting. SEAC will provide the NCC with insight regarding the changing scope of cybersecurity research, activity, and delivery across its various activities.

SEAC provides advice to the NCC's Scientific Director in identifying strategic scientific and ecosystem imperatives for further research and direction by providing input on a strategic vision and identifying priorities to best serve Canada's cybersecurity needs. It will review, identify, and recommend ways and means for the NCC to deal with scientific strategic and ecosystem objectives for cybersecurity initiatives in Canada. It will provide advice about how to identify potential funding sources for commercialization, training, research & development, and industry collaboration. SEAC will help us promote strong linkages between the NCC and various sectors such as government, public institutions, the security intelligence and law enforcement community, and the private sector. It will help identify potential focused calls-for-proposal and identify sector-based strategic opportunities for the NCC as opportunities present themselves. Members may also play a role in evaluating grant applications based on individual expertise and interests.

SEAC will be a key strategic asset for the NCC and members will be engaged in wider ecosystem to both collect emerging challenges and provide direction for how to address them. We highly value those who have agreed to serve on the initial SEAC committee and will expand upon it over the upcoming year to maximize its value to the NCC and wider ecosystem.

Equity, Diversity, Inclusion & Accessibility

The NCC believes that it can best achieve its mission and vision when it draws on the skills, talents, and perspectives of a diverse group of people with a variety of viewpoints, experiences, and backgrounds.

Since its inception, the NCC has prioritized implementing principles of Equity, Diversity, Inclusion, and Accessibility into the policies and culture of the organization. Throughout 2024-2025, we continue to uphold goals achieved by the Government of Canada's 50 – 30 Challenge within our staff and board. We also continue to integrate EDI considerations into the Call for Proposals submission framework and always strive to develop communications in a way that adheres to accessibility best practices.

Intellectual Property & Partnerships Report

As part of the NCC's staff, the Intellectual Property and Partnership (IP&P) team have been focused on catalysing collaboration across Canada's cybersecurity innovation ecosystem. The team links the NCC to Canadian cybersecurity activities and key regional, sectoral, and institutional stakeholders critical to building Canada's cyber resilience.

The IP&P team's central goal is strengthening the NCC's ecosystem intelligence by translating engagements into initiatives that align public and private leadership and addressing emerging cybersecurity challenges. The team has connected with private sources of capital to acknowledge their catalytic role in the commercialization of cyber technologies. Engagement with potential investors and industry accelerators has brought to the NCC's attention the acute lack of cybersecurity 'accelerator' capabilities in Canada, and inspired workshop topics at the upcoming NCC's 2025 Conference in Banff.

The IP&P team further sought alignment with several industries on data governance, talent development, and the challenges facing CISO and CIOs with intense pressure to 'innovate' in the face of emergent quantum technologies, and broader national innovation policies. In attending the Canadian Science Policy Conference in November in Ottawa, the NCC sees the need for better alignment with industrial policy relating to cybersecurity. It also highlighted possible opportunities in the innovation policy sector relating to the economic importance of cybersecurity for securing economic infrastructure.

In 2025, the IP&P team is working closely with the NCC's Scientific and Ecosystem Advisory Committee (SEAC) to enable the expertise and networks to spur new initiatives with the Canadian cybersecurity and privacy ecosystem.

Membership

The NCC is continually grateful for our members. NCC base membership is open to Canadian organizations from academia, private industry, and the not-for profit sector; and in the past year we saw significant growth in the member complement. Beginning with the founding members from the founding universities that have been NCC members since inception, membership expanded to 54 members for the 2024-25 membership year.

The significant growth of the membership complement helps to uplift an essential goal of the NCC. This network of cybersecurity and privacy leaders and experts from NCC member organizations across Canada supports the NCC in its core directive to strengthen cybersecurity in Canada.

We are deeply appreciative of the important organizations that supported the NCC in the 2024-25 membership year:

2313090 Alberta Ltd.
Actua
Carleton University
Ciptor IT-SAFE Canada Inc.
Concordia University (Founding Member)
Concordia University of Edmonton
CyberSci Cyber Security Challenge Canada
Dalhousie University
DarkCheck
Deloitte
Durham College Of Applied Arts & Technology
École Polytechnique de Montréal
ENFOCOM International Corporation
EnStream LP
Ericsson Canada Inc.
ezSec Inc
Field Effect Software
Fields Institute for Research in the Mathematical Sciences
Humber College Institute of Technology and Advanced Learning
INETCO Systems Limited
Information And Communications Technology Council of Canada Inc.
Institut national de la recherche scientifique
Laboratoire de confiance numérique du Canada - Digital Trust Laboratory of Canada
Lethbridge College
Magnificus Software Inc.
Manitoba Research Network
McGill University
Memorial University of Newfoundland
Palitronica
Portage Cybertech Inc.
Private AI Inc.
Protexxa Inc.
Qohash Inc.
Quantized Technologies Inc.
Quantum Algorithms Institute
Queen's University
RESTIV Technology Inc.
Le Réseau d'Informations Scientifiques du Québec
Saskatchewan Polytechnic
Simon Fraser University
Southern Alberta Institute of Technology
TerraHub Technologies Inc.
Toronto Metropolitan University (Founding Member)
Université Laval
Université de Sherbrooke
University of British Columbia
University of Calgary
University of Guelph
University of New Brunswick
University of Ontario Institute of Technology
University Ottawa
University Quebec Outaouais
University of Saskatchewan
University of Waterloo
University of Western Ontario
Valencia IIP Advisors Limited
VanWyn Inc.
York University


The right people, having
the right conversations at
the right time.

NATIONAL CYBERSECURITY CONSORTIUM

CONSORTIUM NATIONAL POUR LA CYBERSÉCURITÉ

www.ncc-cnc.ca

Follow us on LinkedIn

Sign-up for our mailing list

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

Canada

Consortium national pour la cybersécurité
États financiers
Pour l'exercice terminé le 31 mars 2025

Table des matières

Tél./Tel: 613-237-9331
Téléc./Fax: 613-237-9779
www.bdo.ca

BDO Canada s.r.l./S.E.N.C.R.L./LLP
180 Kent Street
Suite 1700
Ottawa ON K1P 0B6 Canada

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 2025, 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 2025, 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 influer 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
Ottawa (Ontario)
Le 26 juin 2025

Consortium national pour la cybersécurité
État de la situation financière

31 mars	2025	2024
Actif		
Court terme		
Encaisse	1 516 381 $	1 520 299 $
Comptes à recevoir	191 492	140 823
Autres créances	76 710	46 200
Frais payés d'avance	100 375	26 346
Avances de projets	3 994 276	-
Actif total	5 879 234 $	1 733 668 $
Passif et actif net (insuffisance)		
Court terme		
Créditeurs et frais courus (Note 2)	292 149 $	127 487 $
Subventions à payer - remboursements	1 303 926	-
Subventions à payer - bénéficiaires finaux	952 266	-
Subventions et adhésions reportées (Note 3)	2 999 526	1 513 992
Dû aux membres fondateurs	115 000	112 500
	5 662 867	1 753 979
	5 662 867	1 753 979
Actif net (insuffisance)		
Non affecté	216 367	(20 311)
	216 367	(20 311)
Total du passif et de l'actif net	5 879 234 $	1 733 668 $

Au nom du Conseil d'administration :

Signed by: Charmaine B. Dean
41D0855C03A4474...
Directeur

Signed by: David MacGee
9C036B809005435...
Directeur

Les notes complémentaires font partie intégrante des états financiers.

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

Pour l'exercice terminé le 31 mars 2025	2025	2024
Solde, début de l'exercice	(20 311)$	20 317 $
Excédent (insuffisance) des produits sur les charges	236 678	(40 628)
Solde, fin de l'exercice	216 367 $	(20 311)$

Les notes complémentaires font partie intégrante des états financiers.

Consortium national pour la cybersécurité
État des résultats

Pour l'exercice terminé le 31 mars	2025	2024
Produits		
Subventions (Note 2)	5 010 800 $	1 445 318 $
Adhésions (Note 2)	309 862	33 585
Intérêts et autres revenus	24 434	-
	5 345 096	1 478 903
Charges		
Programmes	2 573 147	-
Développement, prestation et administration de programmes	2 524 935	1 485 318
TVH non réclamable	10 336	34 213
Charges totales	5 108 418	1 519 531
Excédent (insuffisance) des produits sur les charges	236 678 $	(40 628)$

Les notes complémentaires font partie intégrante des états financiers.

Consortium national pour la cybersécurité
État des flux de trésorerie

Pour l'exercice terminé le 31 mars	2025	2024
Flux de trésorerie liés aux activités de fonctionnement		
Excédent (insuffisance) des produits sur les charges	236 678 $	(40 628)$
Variations des éléments hors caisse du fonds de roulement:		
Comptes à recevoir	(117 410)	(140 823)
Autres créances	46 200	(22 422)
Frais payés d'avance	(74 029)	(15 830)
Créditeurs et frais courus	154 693	(83 061)
Subventions et adhésions reportées	1 485 534	1 313 273
Avances de projets	3 994 276	-
Subventions à payer – récipiendaires finaux	952 266	-
Subventions à payer – remboursements	1 303 926	-
	(6 418)	1 010 509
Flux de trésorerie liés aux activités d'investissement		
Changement au dû aux membres fondateurs	2 500	(37 500)
(Diminution) augmentation nette de la trésorerie	(3 918)	1 019 210
Encaisse, début de l'exercice	1 520 299	501 089
Encaisse, fin de l'exercice	1 516 381 $	1 520 299 $

Les notes complémentaires font partie intégrante des états financiers.

Consortium national pour la cybersécurité
Notes complémentaires

31 mars 2025

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.

1. Méthodes comptables (suite)

Instruments financiers	Les instruments financiers dans des conditions de pleine concurrence sont comptabilisés à la juste valeur lors de la comptabilisation initiale. Les instruments financiers contractés entre apparentés cotés sur un marché actif ou pour lesquels des données d'entrée importantes pour la détermination de la juste valeur de l'instrument sont observables ou des contrats dérivés existent sont comptabilisés à la juste valeur lors de la comptabilisation initiale. Tous les autres instruments financiers contractés entre apparentés sont comptabilisés au coût lors de la comptabilisation initiale. Les actifs financiers font l'objet d'un test de dépréciation lorsqu'il y a des indicateurs d'une perte de valeur. Lorsqu'un changement important dans le calendrier ou les flux de trésorerie futurs de l'actif financier est identifié, la valeur comptable de cet actif est réduite et le montant est constaté à titre de dépréciation dans le résultat net. La moins-value déjà comptabilisée peut faire l'objet d'une reprise dans la mesure de l'amélioration, pourvu qu'elle ne dépasse pas le montant qui aurait été constaté à la date de la reprise si la moins-value n'avait jamais été comptabilisée, et le montant de la reprise de valeur est comptabilisé en résultat net.

2. Créditeurs et frais courus

Le poste créditeurs et frais courus comprend des sommes à remettre à l'État de 49 344 $ (2024 - nul).

3. Subventions et adhésions reportées

	2025	2024
Subventions d'ISED reportées	2 740 844 $	1 310 827 $
Adhésions reportées	258 682	203 165
Solde, à la fin de l'exercice	2 999 526 $	1 513 992 $

	2025	2024
Solde, au début de l'exercice	1 513 992 $	200 719 $
Plus: subventions d'ISED reçues pendant l'année	6 435 345	2 756 146
Plus: adhésions reçues pendant l'année	367 880	236 750
Moins: subventions d'ISED constatées à titre de produits de l'exercice	(5 010 800)	(1 445 318)
Moins: adhésions constatées à titre de produits de l'exercice	(309 862)	(33 585)
Solde, à la fin de l'exercice	2 999 526 $	1 513 992 $

4. Dépendance économique

Le consortium a reçu 94% (2024 - 98%) 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.

5. Instruments financiers

Risque de liquidité
Le risque de liquidité est le risque que le Consortium puisse rencontrer des difficultés à respecter ses obligations financières à leur échéance. Cela inclut le risque que, en raison de contraintes de liquidité opérationnelle, le Consortium n'ait pas suffisamment de fonds pour régler les transactions à leurs dates d'échéance, soit contraint de vendre des actifs financiers à des prix défavorables, ou soit incapable de récupérer la pleine valeur des actifs financiers. Le Consortium est principalement exposé au risque de liquidité par ses créditeurs et charges à payer. Le risque n'a pas changé depuis l'année dernière

Risque de crédit
Le consortium est esposé 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.

National Cybersecurity Consortium
Consortium national pour la cybersécurité
Financial Statements
For the year ended March 31, 2025

Contents

Tél./Tel: 613-237-9331
Téléc./Fax: 613-237-9779
www.bdo.ca

BDO Canada s.r.l./S.E.N.C.R.L./LLP
180 Kent Street
Suite 1700
Ottawa ON K1P 0B6 Canada

Independent Auditor's Report

To the members of
National Cybersecurity Consortium

Opinion

We have audited the accompanying financial statements of National Cybersecurity Consortium (the "Consortium"), which comprise the statement of financial position as at March 31, 2025, and the statements of operations, changes in net assets (deficiency) and cash flows for the year then ended, and notes to the financial statements, including a summary of significant accounting policies.

In our opinion, the accompanying financial statements present fairly, in all material respects, the financial position of the Consortium as at March 31, 2025, and its results of operations and its cash flows for the year then ended in accordance with Canadian accounting standards for not-for-profit organizations.

Basis for Opinion

We conducted our audit in accordance with Canadian generally accepted auditing standards. Our responsibilities under those standards are further described in the *Auditor's Responsibilities for the Audit of the Financial Statements* section of our report. We are independent of the Consortium in accordance with the ethical requirements that are relevant to our audit of the financial statements in Canada, and we have fulfilled our other ethical responsibilities in accordance with these requirements. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Responsibilities of Management and Those Charged with Governance for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting standards for not-for-profit organizations, and for such internal control as management determines is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

In preparing the financial statements, management is responsible for assessing the Consortium's ability to continue as a going concern, disclosing, as applicable, matters related to going concern and using the going concern basis of accounting unless management either intends to liquidate the Consortium or to cease operations, or has no realistic alternative but to do so.

Those charged with governance are responsible for overseeing the Consortium's financial reporting process.

Auditor's Responsibilities for the Audit of the Financial Statements

Our objectives are to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion. Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance with Canadian generally accepted auditing standards will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of these financial statements.

As part of an audit in accordance with Canadian generally accepted auditing standards, we exercise professional judgment and maintain professional skepticism throughout the audit. We also:

- Identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for our opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.
- Obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Consortium's internal control.
- Evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by management.
- Conclude on the appropriateness of management's use of the going concern basis of accounting and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the Consortium's ability to continue as a going concern. If we conclude that a material uncertainty exists, we are required to draw attention in our auditor's report to the related disclosures in the financial statements or, if such disclosures are inadequate, to modify our opinion. Our conclusions are based on the audit evidence obtained up to the date of our auditor's report. However, future events or conditions may cause the Consortium to cease to continue as a going concern.
- Evaluate the overall presentation, structure and content of the financial statements, including the disclosures, and whether the financial statements represent the underlying transactions and events in a manner that achieves fair presentation.

We communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal control that we identify during our audit.

BDO Canada LLP

Chartered Professional Accountants
Ottawa, Ontario
June 26, 2025

National Cybersecurity Consortium
Statement of Financial Position

March 31	2025	2024
Assets		
Current		
Cash	$ 1,516,381	$ 1,520,299
Accounts receivable	191,492	140,823
Other receivables	76,710	46,200
Prepaid expenses	100,375	26,346
Project advances	3,994,276	-
	$ 5,879,234	$ 1,733,668
Liabilities and Net Assets (Deficiency)		
Current		
Accounts payable and accrued liabilities (Note 2)	$ 292,149	$ 127,487
Grants payable – reimbursements	1,303,926	-
Grants payable – ultimate recipients	952,266	-
Deferred grants and memberships (Note 3)	2,999,526	1,513,992
Due to founding members	115,000	112,500
	$ 5,662,867	1,753,979
Net Assets (Deficiency)		
Unrestricted	216,367	(20,311)
	$ 5,879,234	$ 1,733,668

On behalf of the Board:

Signed by:
Charmaine B. Dean
41D0855C03A4474...
Director

Signed by:
David MaGee
9C036B809005435...
Director

The accompanying notes are an integral part of these financial statements.

National Cybersecurity Consortium
Statement of Changes in Net Assets (Deficiency)

For the year ended March 31	2025	2024
Balance, beginning of the year	$ (20,311)	$ 20,317
Excess (deficiency) of revenues over expenses	236,678	(40,628)
Balance, end of the year	$ 216,367	$ (20,311)

The accompanying notes are an integral part of these financial statements.

National Cybersecurity Consortium
Statement of Operations

For the year ended March 31	2025	2024
Revenues		
Grants (Note 2)	$ 5,010,800	$ 1,445,318
Memberships (Note 2)	309,862	33,585
Interest and other income	24,434	-
	5,345,096	1,478,903
Expenses		
Programs	2,573,147	-
Program development, delivery, and administration	2,524,935	1,485,318
Unclaimable HST	10,336	34,213
	5,108,418	1,519,531
Excess (deficiency) of revenues over expenses	$ 236,678	$ (40,628)

The accompanying notes are an integral part of these financial statements.

National Cybersecurity Consortium
Consortium national pour la cybersécurité
Statement of Cash Flows

For the year ended March 31	2025	2024
Cash flows from operating activities		
Excess (deficiency) of revenues over expenses	$ 236,678	$ (40,628)
Changes in non-cash working capital:		
Accounts receivable	(117,410)	(140,823)
Other receivables	46,200	(22,422)
Prepaid expenses	(74,029)	(15,831)
Accounts payable and accrued liabilities	154,693	(36,859)
Deferred grants and memberships	1,485,534	1,313,273
Project advances	3,994,276	-
Grants payable – ultimate recipients	952,266	-
Grants payable – reimbursements	1,303,926	-
	(6,418)	1,056,710
Cash flows from financing activities		
Change in due to founding members	2,500	(37,500)
Net (decrease) increase in cash	(3,918)	1,019,210
Cash, beginning of the year	1,520,299	501,089
Cash, end of the year	$ 1,516,381	$ 1,520,299

The accompanying notes are an integral part of these financial statements.

1. Accounting Policies

Purpose of Consortium

National Cybersecurity Consortium (the "Consortium") is a not-for-profit organization incorporated without share capital under the *Canada Not-for-profit Corporations Act* on March 3, 2020, as a member-based organization with an agreement between Innovation, Science and Economic Development Canada ("ISED") and the National Cybersecurity Consortium. The Consortium qualifies as a non-profit organization as defined in the Income Tax Act and, as such, is exempt from income tax.

The Consortium's mandate is to advance Canada's cybersecurity ecosystem through research and development, commercialization, and training.

Basis of Accounting

The Consortium applies the Canadian accounting standards for not-for-profit organizations.

Use of Estimates

The preparation of financial statements requires management to make estimates and assumptions that affect the reported amounts of assets and liabilities and the reported amounts of revenues and expenses for the year covered.

Revenue Recognition

The Consortium follows the deferral method of accounting for contributions. Restricted grant contributions are recognized as revenue in the year in which the related expenses are incurred. Unrestricted grant contributions are recognized as revenue when they are received or receivable if the amount to be received can be reasonably estimated and collection is reasonably assured.

Membership fees are recognized as revenue on a pro rata basis over the fiscal year to which they pertain. Amounts received in advance of the applicable fiscal year are recorded as deferred revenue.

1. Accounting Policies (continued)

Financial Instrument	Arm's length financial instruments are recorded at fair value at initial recognition. All other financial instruments are reported at cost or amortized cost less impairment. Transaction costs on the acquisition, sale or issue of financial instruments are expensed for those items measured at fair value and charged to the financial instrument for those measured at amortized cost. Financial assets are tested for impairment when indicators of impairment exist. When a significant change in the expected timing or amount of the future cash flows of the financial asset is identified, the carrying amount of the financial asset is reduced and the amount of the write-down is recognized in net income. A previously recognized impairment loss may be reversed to the extent of the improvement, provided it is not greater than the amount that would have been reported at the date of the reversal had the impairment not been recognized previously, and the amount of the reversal is recognized in net income.

2. Accounts Payable and Accrued Liabilities

Included in accounts payable and accrued liabilities are government remittances payable of $49,344 (2024 - nil).

3. Deferred Grants and Memberships

	2025	2024
Deferred ISED grants	$ 2,740,844	$ 1,310,827
Deferred memberships	258,682	203,165
Balance, end of year	$ 2,999,526	$ 1,513,992

	2025	2024
Balance, beginning of year	$ 1,513,992	$ 200,719
Plus: ISED grants received in the current year	6,435,345	2,756,146
Plus: Memberships received in the current year	367,880	236,750
Less: ISED grants recognized as revenue in the year	(5,010,800)	(1,445,318)
Less: Memberships recognized as revenue in the year	(309,862)	(33,585)
Balance, end of year	$ 2,999,526	$ 1,513,992

4. Economic Dependence

The Consortium received 94% (2024 - 98%) of its revenues from ISED. Should this funding not be continued or be unable to be replaced, the Consortium wouldn't be able to continue its operations at the current level.

5. Financial Instruments

Liquidity risk

Liquidity risk is the risk that the Consortium may encounter difficulty in meeting its financial obligations as they come due. This includes the risk that, due to operational liquidity constraints, the Consortium may not have sufficient funds to settle transactions on their due dates, may be forced to sell financial assets at unfavorable prices, or may be unable to recover the full value of financial assets. The Consortium is primarily exposed to liquidity risk through its accounts payable and accrued liabilities. The risk has not changed since last year.

Credit risk

The Consortium's is exposed to the credit risk arising from all of its bank accounts held at a single financial institution. The risk has not changed since last year.