2023 - 2024
Annual Report

www.ncc-cnc.ca

TABLE OF CONTENTS

A Message from the Chair of the Board	1
Board of Directors	2
A Message from the Scientific Director	3
2023 Call for Proposals	4
2024 Call for Proposals	8
Outreach & Engagement	9
2023/24 Members	11
Finance Update	12
Financial Statements	13

A Message from the

Chair of the Board

Dr. Charmaine Dean

It isn't hard to see the importance of cybersecurity each day 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 members and their projects in our commitment to improve cybersecurity in Canada.

The past year has been a challenging and gratifying one for the NCC. We've seen our operations come together, with over $11m in grants awarded in 2023, and experiencing overwhelming growth in grant applications in 2024.

It hasn't taken long for the NCC and its team 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 2023-2024 as a year of establishing our operational infrastructure to allow us to build our community and expand the scope of our impact from a solid foundation in future years.

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

Board of Directors

Dr. Dominique Bérubé
Vice-President,
Research and Graduate Studies
Concordia University

Dr. William Ghali
Vice-President Research,
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

A Message from the

Scientific Director,

National Cybersecurity Consortium

Dr. Ken Barker

The National Cybersecurity Consortium 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 second Call 2024 to identify worthy cybersecurity/privacy initiatives to support Canada and to help protect Canadians.

The past year has also seen the hiring of an exceptionally strong group of full time staff members led by our Executive Director, Mary Henricksen. This small but powerful group is dedicating to the providing our members with the highest quality of service to ensure they are enabling 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 they receive from the Ministry of Innovation, Science and Economic Development Canada, 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 sector 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 its staff as we've worked 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 second full year of our operations.

Sincerely,

Ken Barker

2023 Call for Proposals

In our first call for proposals, the NCC committed $11.2 million toward 20 individual projects

The NCC's annual funding program exists to stimulate a strong national cybersecurity ecosystem and position Canada as a global leader in cybersecurity. With a total project investment value of $39.2 million, the 2023 Call for Proposals funded 20 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 hybrid master's program in cybersecurity analytics.

2023 Funded Projects

Research & Development

ATLAS

Recipient: Deloitte

Collaborators: Concordia University (QC), Prompt (QC), Groupe Desjardins (QC), Cybereco (QC), Pinq2 (QC)

Committed Funds: $1,000,000

Designing a Scalable and Performant Confidential Backup System

Recipient: University of Waterloo

Collaborators: École Polytechnique de Montréal (QC), Acronis

Committed Funds: $370,036

Building Cyber Resilient and Secure 5G Networks Through Automation and AI

Recipient: Concordia University

Collaborators: Ericsson (QC), University of Waterloo (ON), University of Manitoba (MB)

Committed Funds: $1,000,000

AI-Enabled Vulnerability Management

Recipient: University of New Brunswick

Collaborators: Rogers (ON), CIC (NB)

Committed Funds: $240,750

Research & Development (cont.)

Next Generation User Fingerprinting for Fraud Detection and Prediction

Recipient: University of Waterloo

Collaborators: Mastercard (BC), University of New Brunswick (NB)

Committed Funds: $288,099

Transfer Fuzzing for Devices Without Firmware

Recipient: University of Waterloo

Collaborators: Blackberry (ON), Rational Minds Innovation (QC)

Committed Funds: $270,470

Mitigating security, privacy, and ethical impacts in advanced driver assistance systems

Recipient: Queen's University

Collaborators: Irdeto (ON), Western University (ON), Royal Military College (ON)

Committed Funds: $300,000

The Run-Time Security of Android Automotive infotainment system

Recipient: University of Saskatchewan

Collaborators: Blackberry (ON), Amazon (ON), McGill University (QC)

Committed Funds: $420,619.61

Post-Quantum Hardware Security Module (HSM) Migration Research Project

Recipient: University of New Brunswick

Collaborators: Scotiabank (ON)

Committed Funds: $286,000

Cybersécurité de l'identité numérique

Recipient: Université du Québec en Outaouais

Collaborators: Portage Cybertech (QC), Laval University (QC), Concordia University (QC)

Committed Funds: $90,000

Research & Development (cont.)

Trustworthy AI-based Framework for Self-aware Drone-based Swarm Technologies

Recipient: Ontario Tech Institute

Committed Funds: $89,987.50

Training

CyberLab

Recipient: Field Effect Software

Collaborators: Cyberquebec (QC), Algonquin College (ON), University of Calgary (AB)

Committed Funds: $900,000

From Training to Innovative Cyber Start-Up

Recipient: École Polytechnique de Montréal

Collaborators: Desjardins (QC), Cybereco (QC), HEC Montréal (QC), Université de Montréal (QC)

Committed Funds: $999,900

Hybrid Master's Program in Cybersecurity Analytics (formerly SIS Online Graduate Certificate in Cybersecurity)

Recipient: McGill University

Collaborators: Blackberry (ON), Ericsson (QC), Samsung (QC)

Committed Funds: $1,000,000

CMD-CT: Comprehensive MultiDisciplinary Cybersecurity Training

Recipient: University of Waterloo

Collaborators: Brandon University (MB), University of Alberta (AB), eSentire (ON)

Committed Funds: $402,691.43

Training (cont.)

Mobilizing Cybersecurity Regulation for Canada

Recipient: University of Calgary

Committed Funds: $915,838.15

Masters In Cybersecurity Management

Recipient: University of New Brunswick

Committed Funds: $998,538

Cloud Security Training Program (micro-credential)

Recipient: McGill University

Collaborators: FX Innovation (QC)

Committed Funds: $666,941

Commercialization

PASCAL

Recipient: Palitronica Inc.

Collaborators: Arcfield (AB), Continental (ON), Sera4 (ON), University of Waterloo (ON)

Committed Funds: $1,000,000

2024 Call for Proposals

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

For the 2024 Call for Proposals, the NCC's second funding call, we were determined to build on our successes, and make improvements based on feedback from participants to develop a more streamlined, open, and efficient process to apply for funding.

This year's funding call included three streams: Commercialization, Training and Research and Development. The Research and Development stream was further divided into two sub-steams: Standard, and Spearhead Projects. Also new this year, intake is being administered through an online platform, the Adsigno Portal, and is being executed in three stages:

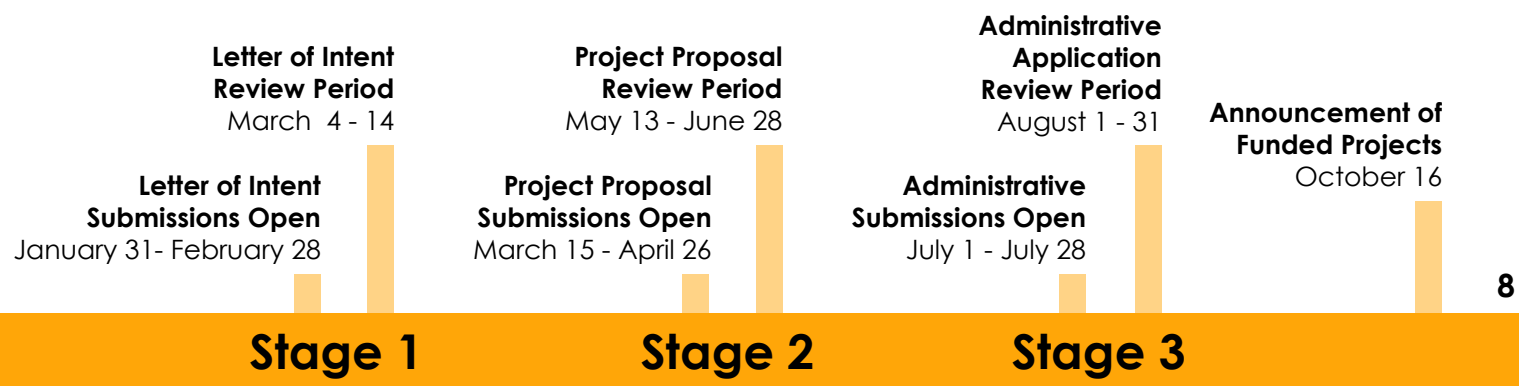
Stage 1 - Letter of Intent (LOI): Interested applicants were encouraged to submit a short LOI to summarize their project and identify matching sources of contributions as applicable. These submissions were internally assessed for eligibility as identified in the call parameters. The NCC received approximately three times the applications assessed in the previous call, of which 90% were invited to submit a project proposal in Stage 2.

Stage 2 - Project Proposal: Invited applicants had access to the project proposal application where they could further elaborate on their project to be assessed for merit and feasibility. Projects will be subject to a peer-review process using a scoring matrix that was provided to applicants as part of the *2024 Call for Proposals Guide*. Applications recommended for funding by the evaluation committee will be invited to proceed to Stage 3.

Stage 3 - Administrative Details Review: The purpose of Stage 3 is to complete due diligence on the Project Proposal by reviewing the submission for any risks and discrepancies, and to validate supporting documentation.

Projects that have successfully passed through all three stages will be announced on October 16th during Cybersecurity Awareness Month.

2024 Call for Proposals Timeline



Outreach & Engagement

Cultivating collaboration and capacity-building within the Canadian cybersecurity ecosystem

2023 Cybersecurity and Privacy Institute Annual Conference

University of Waterloo

Photo: Harminder Phull, University of Waterloo

NCC Scientific Director, Dr. Ken Barker speaking at the 2023 Cybersecurity and Privacy Institute Annual Conference at the University of Waterloo.

Watch Dr. Barker's Presentation

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.

2023-2024 has been a landmark year of growth for the NCC, and with this growth came an opportunity to embed Equity, Diversity, Inclusion, and Accessibility principles into the policies and culture of the organization from the start. We have achieved goals set by the Government of Canada's 50 – 30 Challenge within our staff and board. We 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.

Outreach & Engagement

2024 Call for Proposals Information Sesions

Preparing a submission for the NCC's Call for Proposals is an involved, multi-step process. To support applicants throughout Stage 1 and 2 of the call, we hosted a series of 10 Information Sessions held on Zoom in both English and French.

Sessions were well attended with over 300 participants having joined, representing organizations from across Canada. Each session covered a topic, including general information, stream-specific details, and a breakdown of the requirements during different stages of the call. The webinars also provided a platform for applicants to directly raise questions with an opportunity to discuss ways in which to optimize their applications.

Learn More About the Information Sessions

Launch of the NCC's Membership Program

January 2024 saw the launch of the NCC's new Membership program – an important milestone that supports our mission to grow a pan-Canadian network to advance cybersecurity.

The program offers a platform where members benefit from collaboration, innovation, and learning from each other. Opportunities, including our annual funding call and networking events, foster an environment that stimulates research, drives economic growth, and ultimately, improves cybersecurity in Canada. Looking forward, we are eager to continue developing our membership benefits, cultivating cross-sectoral connections, and stimulating growth across the ecosystem.

At the close of the 2023-2024 fiscal year, the NCC's membership base includes 21 organizations from industry, academia, and the not-for-profit sector.

Learn More About Membership

2023 - 2024 Members

Academic Members

Université Concordia University

INRS Institut national de la recherche scientifique

McGill

Polytechnique Montréal

Toronto Metropolitan University

Queen's University

UNB Est. 1785 University of New Brunswick

University of Calgary

University of Guelph

uOttawa

University of Waterloo

York U

Industry Members

Field Effect

INETCO Every transaction tells a story®

Magnificus Software Inc.

Palitronica

QOHASH

SATUS/AI

valencia Ready for anything.

Not-for-Profit Members

Information And Communications Technology Council of Canada Inc.

QAI Quantum Algorithms Institute

2023-2024 Finance Update

The 2023-24 fiscal year marked the first year of operation for the Consortium with full-time staff, following its initial setup by external consultants. During this year, the Consortium received $2,560,898 in funding from Innovation, Science, and Economic Development Canada (ISED). This contribution was allocated to start-up operations and the evaluation of our first call for proposals, which resulted in eligible costs amounting to $1,485,318. With the agreement of ISED, any unspent contributions from 2023-24 were carried forward to 2024-25.

During the year, the Consortium invested in 20 projects amounting to $11,269,871 million, with matching contributions of approximately $35,738,030 million, bringing the total investment in the cybersecurity ecosystem to $47,007,901 million.

Membership fees collected during the year totaled $199,250, of which $33,585 was recognized as revenue.

The Consortium undergoes an annual financial audit conducted by independent auditors, approved annually by the Board of Directors, and overseen by the Board's Finance & Audit Committee. The financial audit for 2023-24 was completed in June 2024 by BDO Canada LLP with a clean audit opinion. The audited financial statements are presented on Page 10.

Additionally, the Consortium complies with all regulatory and statutory filing and payment requirements. Our commitment to transparency and adherence to these requirements underscores our dedication to maintaining high accountability and governance standards.

National Cybersecurity Consortium
Consortium national pour la cybersécurité

Financial Statements

For the year ended March 31 2024

Contents

Independent Auditor's Report 2 - 3

Financial Statements

Statement of Financial Position 4

Statement of Changes in Net Assets (Deficiency) 5

Statement of Operations 6

Statement of Cash Flows 7

Notes to Financial Statements 8 - 9

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 2024, 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 2024, 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, Licensed Public Accountants
Ottawa, Ontario
June 10, 2024

National Cybersecurity Consortium
Statement of Financial Position

March 31	2024	2023
Assets		
Current		
Cash	$1,520,299	$ 501,089
Accounts receivable	140,823	-
Other receivables	46,200	23,778
Prepaid expenses	26,346	10,515
Total Assets	$1,733,668	$ 535,382
Liabilities and Net Assets (Deficiency)		
Current		
Accounts payable and accrued liabilities	$ 127,487	$ 164,346
Deferred grants and memberships (Note 2)	1,513,992	200,719
Due to founding members	112,500	150,000
	1,753,979	515,065
Net Assets (Deficiency)		
Unrestricted	(20,311)	20,317
Total Liabilities and Net Assets	$1,733,668	$ 535,382

On behalf of the Board:

Director

Director

The 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	2024	2023
Balance, beginning of the year	**$ 20,317**	$ 57,601
Deficiency of revenues over expenses	**(40,628)**	(37,284)
Balance, end of the year	**$ (20,311)**	$ 20,317

The notes are an integral part of these financial statements.

National Cybersecurity Consortium
Statement of Operations

For the year ended March 31	2024	2023
Revenues		
Grants (Note 2)	**$ 1,445,318**	$ 544,048
Memberships (Note 2)	**33,585**	-
	1,478,903	544,048
Expenses		
Program development, delivery, and administration	**1,485,318**	568,415
Unclaimable HST	**34,213**	12,917
Total expenses	**1,519,531**	581,332
Deficiency of revenues over expenses	**$ (40,628)**	$ (37,284)

The 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	2024	2023
Cash flows from operating activities		
Deficiency of revenues over expenses	**$ (40,628)**	$ (37,284)
Changes in non-cash working capital:		
Accounts receivable	**(140,823)**	-
Other receivables	**(22,422)**	(23,778)
Prepaid expenses	**(15,831)**	(10,515)
Accounts payable and accrued liabilities	**(36,859)**	164,346
Deferred grants and memberships	**1,313,273**	200,719
	1,056,710	293,488
Cash flows from financing activities		
Change in due to founding members	**(37,500)**	150,000
Net increase in cash	**1,019,210**	443,488
Cash, beginning of the year	**501,089**	57,601
Cash, end of the year	**$ 1,520,299**	$ 501,089

The notes are an integral part of these financial statements.

March 31 2024

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 proportionately over the year to which they relate.

Financial Instruments

Initial and subsequent measurement
The Consortium initially measures its financial assets and liabilities at fair value. The Consortium subsequently measures all its financial assets and financial liabilities at amortized cost.

Impairment
Financial assets measured at amortized cost are tested for impairment when there are indications of possible impairment.

Transaction costs
Transaction costs related to financial instruments subsequently measured at amortized cost are included in the original cost of the asset or liability and recognized in the statement of operations over the life of the instrument using the straight-line method.

2. Deferred Grants and Memberships

Deferred grants and memberships reported represent restricted amounts received from ISED grants and memberships related to subsequent years or for which the related expenses have not yet been incurred. The balance consists of the following:

	2024	2023
Deferred ISED grants	**$ 1,310,827**	$ 200,719
Deferred memberships	**203,165**	-
Balance, end of year	**$ 1,513,992**	$ 200,719

The variations in the balance during the year are as follows:

	2024	2023
Balance, beginning of year	**$ 200,719**	$ -
Plus: ISED grants received in the current year	**2,555,426**	744,767
Plus: Memberships received in the current year	**236,750**	-
Less: ISED grants recognized as revenue in the year	**(1,445,318)**	(544,048)
Less: Memberships recognized as revenue in the year	**(33,585)**	-
Balance, end of year	**$ 1,513,992**	$ 200,719

3. Economic Dependence

The Consortium received 98% (2023 - 100%) 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.

4. Financial Instruments

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.

5. Comparative Figures

Certain figures for the previous year have been reclassified to conform to the presentation adopted in the current year.

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