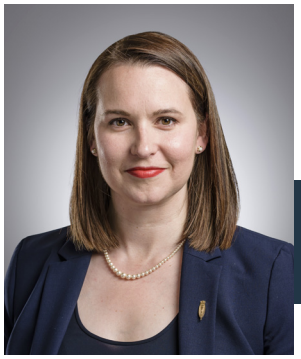
ANNUAL REPORT

2024-2025

Office of the Chief Information Officer

Newfoundland & Labrador



MESSAGE FROM THE MINISTER

As Minister Responsible for the Office of the Chief Information Officer (OCIO), I am pleased to present the 2024-2025 Annual Report. The report, covering the period of April 1, 2024, to March 31, 2025, has been prepared in accordance with the **Transparency and Accountability Act**. As Minister, I am accountable for the reported results.

The OCIO continues to make progress on a series of ambitious multi-year technology initiatives, reshaping how government interacts with residents and businesses in Newfoundland and Labrador.

With over 400,000 registered users, the OCIO continues to build on the success of MyGovNL, the province's digital front door. MyGovNL supports services like MyHealthNL, the Early Learning Gateway, the Crown Lands Application Portal, the Medical Care Plan (MCP), and Motor Registration. The next version of MyGovNL will advance the technology even further, introducing functionality that will allow users to interact as business entities. This expansion will unlock a new suite of online services, specifically tailored to the needs of small businesses, entrepreneurs, organizations and industry stakeholders.

Led by the OCIO, a full redesign of the Provincial Government's website is also underway, featuring enhanced accessibility and a service-centric design that puts user needs first. Part of this redesign includes the launch of a new AI-powered chatbot on the website. This virtual assistant will help people navigate government services more easily, offering 24/7 support and intuitive guidance to help users find information quickly.

A cornerstone of the OCIO's work is the full replacement of key legacy computer systems. Modernizing this technology will enable and support more flexible service delivery across multiple departments who provide valuable services to residents and businesses such as Student Aid, MCP, Motor Registration and Fines Administration.

As artificial intelligence (AI) technology reshapes how services are delivered and how residents and businesses engage with governments, Newfoundland and Labrador is emerging as a public sector leader in the responsible adoption of AI technology. Province-wide training and awareness for public sector employees is underway, supported by a formal policy on the responsible use of AI.

The Provincial Government is committed to safe and secure digital services today and into the future – services built on strong partnerships and real-time collaboration. The OCIO, through the Cyber Security Office, is working closely with all levels of government to protect essential digital government services people rely on every day to modernize our information technology systems and responsibly adopt new and emerging technologies, like AI.

In today's evolving landscape where cyber threats are increasingly sophisticated and persistent, collaboration isn't optional - it's essential. We have established robust measures to strengthen our province's ability to share real-time intelligence, tools, and resources - ensuring we can respond quickly and effectively. We're laying the foundation for a digital government that's responsive, resilient and built for today and the future, doing so with a strong focus on protecting personal data and digital systems.

Hon. Sarah Stoodley
Minister of Government Modernization and Service Delivery
Minister Responsible for the Office of the Chief Information Officer

Newfoundland & Labrador

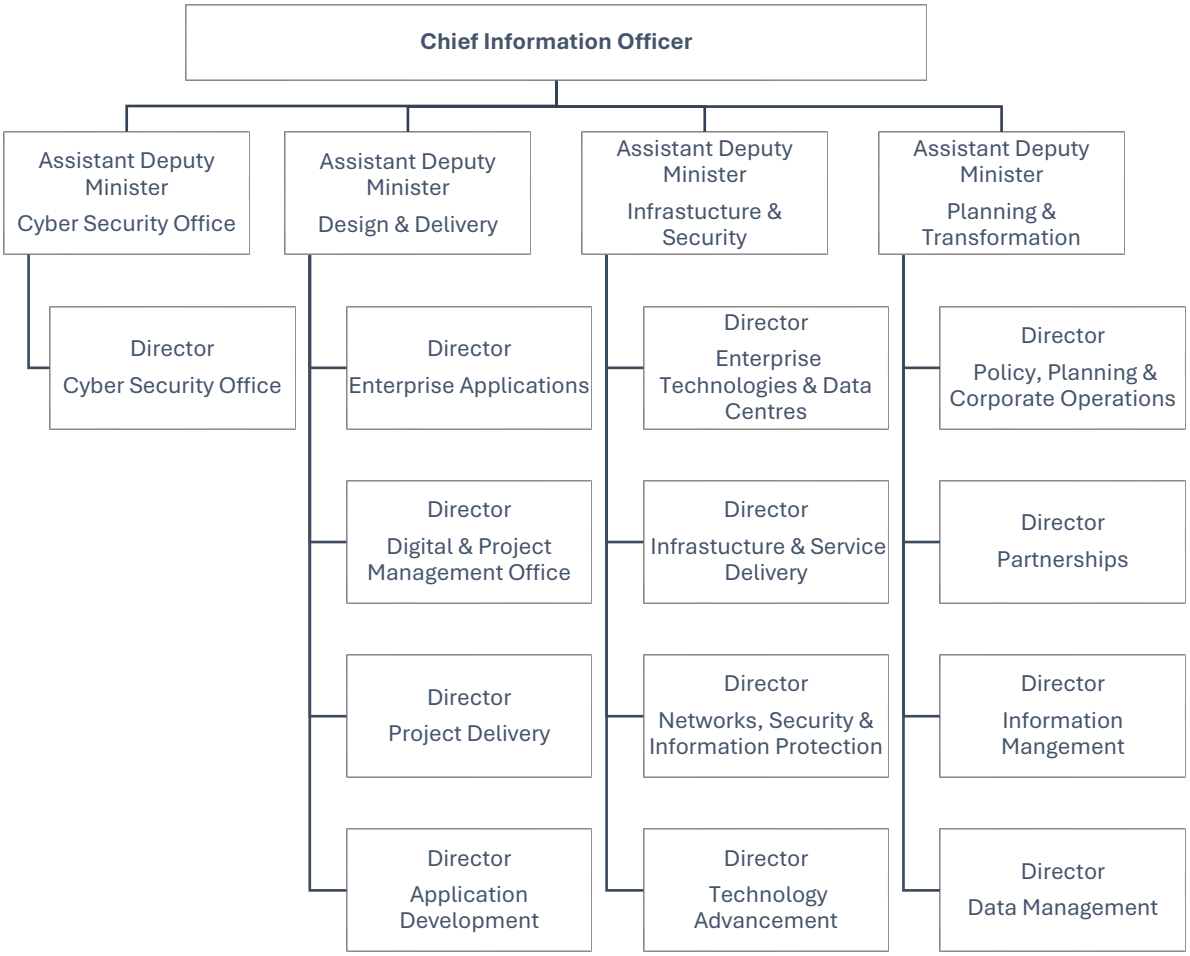
Table of Contents

Departmental Overview

The Office of the Chief Information Officer (OCIO) provides professional information technology and information management capability to support the business of government and the residents of Newfoundland and Labrador.

Organizational Structure

The OCIO is structured into four main branches: Cyber Security Office, Design and Delivery, Infrastructure and Security, and Planning and Transformation.



Cyber Security Office

The Cyber Security Office is leading cyber security initiatives within government departments and public bodies in Newfoundland and Labrador. The Office is committed to protecting government assets and the integrity and confidentiality of data throughout the province and works collaboratively with provincial public bodies, other provincial/territorial cyber security offices, and federal partners, such as the Canadian Centre for Cyber Security, to fulfill its mandate.

The Office's cyber security initiatives emphasize delivering innovative cyber programming and guidance for awareness aligned with government objectives and priorities.

The Office aims to prevent and address cyber security attacks proactively with standards, best practices, guidelines, and directives, including cyber training, phishing campaigns, social engineering, monitoring, audit, and compliance.

The Office provides business continuity and disaster recovery capability guidance including incident response planning services and incident response support.

Design and Delivery Branch

The Design and Delivery Branch is responsible for the Project Management Office (PMO), project delivery, application development and support, the MyGovNL program, and the Enterprise Application Team.

The PMO manages the framework and methodology for project delivery, portfolio management, and reporting. The PMO works very closely with the Project Delivery Division which is responsible for ensuring projects are delivered to stakeholders and support the adoption of the technology they deliver.

The Application Development Team is responsible for software development activities, which includes developing new solutions and supporting and enhancing existing applications.

The MyGovNL Team is responsible for the entirety of the MyGovNL program, which includes development, support, integration, and service roadmaps.

The Enterprise Application Team supports enterprise applications used across government in the areas of finance, budgeting, human resources, and database technologies. The Team works in collaboration with Government Modernization and Service Delivery to define the overall digital strategy for government.

Infrastructure and Security Branch

The Infrastructure and Security Branch provides day-to-day, front-line support to ensure OCIO clients have what they need to deliver government programs and services, back-end technology support and maintenance, cyber security services to ensure the integrity and availability of government's assets including computers, mobile devices, networking, storage, data backup, server infrastructure, enterprise data centre, enterprise infrastructure applications and related technologies. It also provides an Information Protection (IP) program and related advisory services to government.

Planning and Transformation Branch

The Planning and Transformation Branch consists of four divisions: Information Management, Policy, Planning and Corporate Operations, Partnerships, and Data Management.

The Information Management (IM) Division administers the **Management of Information Act,** develops information management directives, standards, procedures,

and guidelines, and provides information management advisory services and guidance to government departments and other public bodies.

The Policy, Planning, and Corporate Operations Division manages OCIO's operations, fiscal management (including budget preparation and monitoring), vendor contract management, human resource planning, IT procurement, cabinet support, facilities management, and occupational health and safety.

The Partnerships Division is responsible for cultivating strong client relationships and ensuring the strategic direction of the OCIO aligns with the priorities of government departments, agencies, boards, and commissions. It also leads digital transformation and training initiatives, supporting clients in adopting and integrating modern technologies by preparing them for changes in business processes.

The Data Management Division is a new division, established in 2024-2025. This Division is responsible for providing data management services to government departments, incorporating department data needs into digital solutions, and implementing a governance framework to ensure appropriate data use and data sharing for service delivery and decision-making.

Staff and Budget

The OCIO's head office is located at 40 Higgins Line in St. John's. There are six regional offices in Clarenville, Corner Brook, Gander, Grand Falls-Windsor, Happy Valley-Goose Bay, and Stephenville.

The breakdown of staff and budget by division for fiscal year 2024-2025 is detailed below.

Branch	# of Employees	Budget
Cyber Security Office	7	$ 839,400
Design and Delivery	165	$ 29,542,000
Infrastructure and Security	140	$ 28,631,500
Planning and Transformation	37	$ 3,453,200
Total	**349**	**$62,466,100**

Vision

To enable the business of government by establishing an inclusive, modern workforce providing industry class daily support, modern technology, and information management services to the public service and the residents of Newfoundland and Labrador.

Mandate

The OCIO operates as an entity within Executive Council, governed by the **Executive Council Act,** and is responsible for:

- Information technology and information management coordination, planning, budgeting and policy development.
- Daily customer support to departments.
- Cyber security protection of government's technology assets.
- Developing and operating computer systems and infrastructure for government departments, agencies, boards, and commissions that are directly supported by the administrative support services of departments.
- Expenditure and procurement of information technology goods and services.
- Administering the **Management of Information Act**.

- Managing information technology-related agreements and contracts.
- Providing consultative services, particularly in information management.
- Working collaboratively with the private information technology sector to maximize business opportunities while meeting the information technology and information management needs of government.

Lines of Business

The OCIO has aligned its organizational structure with its primary business lines to meet client needs more effectively.

- Cyber Security Office
- Design and Delivery
- Infrastructure and Security
- Planning and Transformation

Highlights and Partnerships

Highlights

During 2024-2025, the OCIO was responsible for managing a large portfolio of technology projects and initiatives for departments and supporting public bodies.

From April 1, 2024 to March 31, 2025, the OCIO successfully met all its 2024-2025 objectives outlined in the 2023-2026 Business Plan, advancing modernization across workforce development, business processes, and essential government technologies.

The OCIO modernized technology by deploying M365 across government and launching new MyGovNL services like the Early Learning Gateway, off-road vehicle operator safety training, vehicle ownership transfers, and written tests for commercial class of driver’s license (Class 1,2,3,4) and for an airbrake endorsement. Digital service use increased, reaching 408,000 MyGovNL registered account users, 1.3 million online vehicle renewals, and over 125,000 Personal Health Record users.

The Design and Delivery branch led and advanced several projects and initiatives which included:

- Substantial completion of phase one of the four-stage legacy mainframe replacement.
- Launching emergency funding application portals for the Labrador West wildfires, supporting both businesses and employees affected by those emergencies.

The Infrastructure and Security Branch had many accomplishments in 2024-2025, which included:

- Upgrading Wide Area Network (WAN) link speeds on existing sites.
- Implementing high-speed satellite connectivity in locations where network availability was not present, or build costs were previously prohibitive.
- Continuing modernization of network, storage, and enterprise application technologies with security, monitoring, and feature enhancements.

The Planning and Transformation Branch led key initiatives in 2024-2025 such as:

- Developing and implementing a Responsible Use of Artificial Intelligence (AI) Policy and Guiding Principles for government employees.
- Continued review of information management policy, directives, standards, and guidance materials in support of the recent implementation of M365 and a full policy modernization initiative.
- Supporting employee mental and physical wellness initiatives through the OCIO’s Wellness Program.

The Cyber Security Office made continued progress, highlighted by the following achievements:

- Strengthened relationships with international and Canadian vendors to receive threat advisories.
- Strengthened relationships with federal, provincial, and territorial governments, as well as local peers, to receive threat intelligence.
- Built its cyber practice playbooks and updated its cyber security framework.
- Introduced multiple communication channels to reach, educate, and train government audiences.

Partnerships

The OCIO engaged with information technology partners and vendors to address several key areas:

- Continued Federal-Provincial-Territorial (FPT) collaboration, including the hosting of the September 2024 Annual Meeting of FPT Ministers for discussions on Digital Trust and Cyber Security Priorities.
- Established collaborative working groups across the public sector, including technology leaders from the various public service entities.
- Facilitated opportunities for 17 registered private sector information technology vendors via the government's Managed Service Provider.
- Collaborated with the Centre for Learning and Development to develop a public service artificial intelligence (AI) training campaign and an AI Basics and Responsible Use course for public servants.

Report on Performance

In accordance with the **Transparency and Accountability Act**, this section is an account of the OCIO's progress in meeting the 2024-2025 objectives and accompanying indicators as outlined in the 2023-2026 Business Plan. Indicators for

plan objectives outlined below were developed by senior management and identify activities to address planned results.

Issue One: Modernize

Information technology is constantly evolving and creating new opportunities for innovation. As previously announced in Budget 2023-2024 - Modernizing Government's Information Technology Assets with a $50 million investment - the OCIO is continuing its journey to modernize government's information technology assets, associated policies, and staff skills to spur innovation, operational improvements, and connectivity with the province's citizen and business stakeholders securely.

Goal

By March 31, 2026, the OCIO will have modernized its workforce, its processes (e.g., operational and service delivery frameworks), and government's foundational technologies.

2024-2025 Objective

By March 31, 2025, the OCIO will have implemented the second phase of the modernization plan.

Indicators and Accomplishments

Indicator (Planned)	Accomplishments (Actual)
Continued engagement with departments for modernization of technology, enhancement of M365, and upgrading of public facing services.	• Completion of a modernized network design and procurement phase to replace network infrastructure, increasing resilience and availability of networking services.

	• Completion of M365 rollout, supported by training with departments to promote active engagement of the new tools. • Substantial progress completed on Student Aid mainframe modernization. • Planning phase completed for core government Enterprise Resourcing Planning technology completed. • Completed analysis phase of Quarry Management System (QMS) modernization project. • Initiated the modernization of the Fisheries Aquaculture Licensing System (FALS). • Continued work on replacing and modernizing legacy Apprenticeship and Certification Management System (ACMS).
Continued delivery of a case management strategy.	The OCIO advanced its case management strategy of leveraging the Microsoft Power Platform to streamline workflows and improve service delivery by partnering with departments to complete projects/initiatives, including: • Fisheries, Forestry and Agriculture (Animal Health) • Environment and Climate Change (Hazardous Waste) • Government Modernization and Service Delivery (French Services, Occupational Health and Safety Inspections)

Continued modernization of internal policies and processes for IT and IM delivery.	• The OCIO has consolidated and established a plan for modernizing all policies, standards, and associated processes to align with the technology modernization work.
Analysis of policy development related to digital service delivery and artificial intelligence.	• The OCIO developed and implemented a Responsible Use of AI Policy and Guiding Principles for government users.
Continued deployment of client services to departments.	The OCIO continued to work with departments to modernize and enhance citizen-facing services, including: • Crown Lands Permits and Licenses (Fisheries, Forestry and Agriculture) • Companies and Deeds Online (Government Modernization and Service Delivery) • Launch of an online portal in support of the Business Navigator program for entrepreneurs and business owners.

Discussion of Results

Between April 1, 2024 and March 31, 2025, the OCIO made strong progress in the second year of its three-year modernization plan.

The OCIO reviewed and updated policies and guidelines, especially those related to Microsoft 365. New guides and quick references were shared to help employees use these tools responsibly.

The OCIO continued to strengthen reliable network access across government buildings by modernizing foundational network infrastructure components.

The OCIO's launch of the Responsible Use of Artificial Intelligence (AI) Policy and Guiding Principles along with several trials, was recognized as a key achievement, enabling safe, fair, ethical, and transparent government use of AI, and established the OCIO and government as a leader in the public sector in this area.

Objective 2025-2026

By March 31, 2026, the OCIO will have implemented the operational sustainment phase of the modernization plan.

Indicators

The OCIO will continue to modernize IT assets in 2025-2026 evidenced by the following key indicators:

- Completed infrastructure modernization and upgrades for identified departments and physical office spaces.
- Implemented replacement of key legacy technologies.
- Initiated remaining phases of the mainframe modernization project.
- Delivered modern policies and processes related to modern technology.
- Delivered enhanced modern Information Management programming.

Issue Two: Enable

The OCIO will enable government's departmental visions and goals through enhanced operational support, modern technology, and partner advisory services.

Goal

By March 31, 2026, the OCIO will have:

- Expanded evidence-based decision-making technologies for government departments.
- Implemented more online services to improve resident and business interactions with government.
- Enhanced departmental partnerships to maximize the potential and value of government's technology investment.
- Enhanced service to departments.

2024-2025 Objective

By March 31, 2025, the OCIO will have:

- Continued online service expansion.
- Continued implementing modern functionality (with associated training) to departments.

Indicators and Accomplishments

Indicator (Planned)	Accomplishments (Actual)
Implementation of additional online digital services functionality within MyGovNL.	• Citizens used the MyGovNL online portal to complete over 525,000 transactions in 2024-2025. This included activities such as renewals, purchasing permits, and completing driving exams. • Implemented Early Learning Gateway for Department of Education and Early Childhood Development. • The OCIO has signed a Memorandum of Understanding with Service Canada to complete analysis on the future use of the MyGovNL to access Federal services.

Strategy development and implementation of modern technology for government departments.	The Partnerships Division developed a new framework in consultation with all departments to improve communication, engagement, and the prioritization of requests. Implementation of this new framework is anticipated next fiscal.
Continued enhancements to a tier one service help desk.	• The Infrastructure & Security division conducted multiple focus group sessions to build a IT service modernization plan. • The Design & Delivery team and Infrastructure & Security team collaborated to modernize the OCIO internal IT Help Site.
Provision of information management advisory services, training, and awareness.	• The Information Management Division conducted training which included both general and specific IM training, covering a wide range of departments and audiences through in-person sessions, webinars, and collaborative events. Topics covered included: IM Best Practices, IM Sessions for M365 Deployment, and Transitory Records.
Expansion of training to end users of OCIO technologies.	• The Partnerships Division's Digital Transformation Specialists led M365 on-site engagement sessions with key departmental stakeholders to introduce M365 functionality and increase user adoption.

Introduction of a data services function.	• The OCIO established a Data Management Division, including hiring staff and establishing a data management services departmental delivery strategy.

Discussion of Results

Between April 1, 2024 and March 31, 2025, the OCIO continued to expand and improve digital services for both the public and government departments.
To better support government staff, the OCIO launched a pilot of Microsoft Copilot, introducing new tools to help public service employees work more efficiently and collaboratively.

The OCIO partnered with departments to deliver key technology solutions that support important public services, including the successful completion of upgrades to the MRD Dealer Web and Customer Engagement Centre. Work also continued to modernize aging systems such as Mainframe, VB6, Access, and Oracle Cloud, and to develop a government-wide Case Management Program.

Objective 2025-2026

By March 31, 2026, the OCIO will have:

- Continued online service expansion;
- Continued implementing modern functionality with associated training to line departments; and
- Enabled modern mobile technology.

Indicators

The OCIO will continue to enable government business in 2025-2026, evidenced by the following key indicators:

- Continued project delivery on departmental requests.

- Expansion of awareness programming to the public service in the areas of AI, IM, technology usage, cyber as well as general core technology competencies. Implemented the data services division to enable line departments.

Issue Three: Protect

Cyber security threats against government assets are evolving and increasing. Residents and businesses must be reassured that the government is providing services and keeping their assets safe from unauthorized access and usage. The OCIO will continue to evolve its cyber security programming to protect the province against dynamic security threats to sustain asset availability, integrity, and confidentiality.

Goal

By March 31, 2026, the OCIO will have:

- Implemented a Cyber Security Office.
- Fostered cyber security resources and culture within government's public service.
- Modernized the cyber security framework including partnerships with subject matter experts.
- Proactively strengthened government's cyber security posture in response to evolving technology and constant security risks.

Objective 2024-2025

By March 31, 2025, the OCIO will have continuous awareness of the cyber threat landscape and adjusted required operational frameworks, procedures, and continued to expand cyber security education and awareness across government.

Indicators and Accomplishments

Indicator (Planned)	Accomplishments (Actual)
Establishment of a Cyber Security Office Community of Action to support departments, agencies, boards, and commissions.	• The OCIO hosted several Community of Action events and implemented a registration process for accepting new members.
Continued leveraging of the investment in M365 by deploying enhanced security tools and features.	• The OCIO transitioned its client protection solution to modern tools for better visibility, detection, and response to client-based threats. • The OCIO incorporated modern email threat detection for inbound and outbound emails transiting GNL's email technologies. • The OCIO continued to update several defense technologies.
Continued development of an internal assessment and audit program.	• The OCIO continued to develop an internal assessment and audit program, based on its cyber security framework.
Continued enhancements to internal security frameworks.	• The OCIO refined its cyber security posture by updating its framework and continuously adapting operational playbooks to align with evolving threat landscapes and best practices.
Continued enhancements to vulnerability management programs.	• The OCIO developed a modern continuous vulnerability management program plan which includes risk-based exposure management in application

	development, back-end technologies, and high-risk targets. Modern tools were procured and continue to be integrated into a development security operations and infrastructure security operations structure.
Expansion of cyber security education and awareness through courses and campaigns.	• The OCIO increased the breadth of educational offerings by acquiring additional cyber security training content, thereby supporting broader awareness and capacity-building across departments. • The OCIO improved the reach and effectiveness of its awareness and training efforts by introducing multiple delivery channels, including digital platforms and in-person sessions, to educate and train public service employees

Discussion of Results

Since the Cyber Security Office launched in September 2023, the OCIO has made progress in enhancing cyber security across government. It broadened its threat intelligence capabilities by partnering with international, national, and local organizations, and introduced a continuous data feed to support faster, more proactive threat detection.

To stay aligned with best practices and evolving risks, the OCIO updated its cyber security framework and adapted its operational playbooks to strengthen cyber risk management. Efforts to engage a wider government audience were supported through

new communication and training channels that expanded awareness and built cyber capacity across departments.

Targeted initiatives including phishing simulations, audits, and awareness campaigns were delivered to promote a stronger culture of cyber readiness across the public service.

These accomplishments reflect OCIO's ongoing commitment to a secure and informed digital government that protects both public services and the personal information of all Newfoundlanders and Labradorians.

Objective 2025-2026

By March 31, 2026, the OCIO will have continued to evolve government's cyber security program and provided additional cyber security education and awareness to public service.

Indicators

The OCIO will continue to protect government in 2025-2026 evidenced by the following key indicators:

- Increase sources for and frequency of threat intelligence.
- Continue to expand cyber security education content, awareness, and training available to government and other public bodies.
- Implement modernized security and cyber practices, including program enhancements related to governance, risk and compliance.
- Increase government's security posture to protect citizens' data.

Opportunities and Challenges

During 2024-2025, the OCIO worked to meet the objectives in its 2023-2026 Business Plan and provided information technology, information management and information

protection support to departments as an increased number of online services were delivered to Newfoundlanders and Labradorians.

Opportunities

As technology continues to evolve, the OCIO is embracing new opportunities to build a more connected, secure, and responsive government.

Technology Modernization
Modernizing core systems, including legacy platforms, will make government services more efficient and deliver faster, simpler digital experiences for the public.

Data Management and Artificial Intelligence (AI)
The increasing adoption of artificial intelligence and data-driven technologies offers significant potential to enhance government operations. Through the implementation of robust data governance frameworks and the responsible adoption of AI, government can deliver more efficient services, such as expedited processing and tailored support, while safeguarding privacy and ensuring transparency.

Cybersecurity
Cybersecurity continues to be a top priority, with ongoing investments in security tools aimed at enhancing the province's ability to safeguard critical systems and information against changing threats. Additionally, through a whole-of-government approach, services are being made more consistent and coordinated, providing users with standardized interactions across ministries and agencies.

Challenges

Keeping Pace with Rapid Technological Change
Technology is evolving rapidly, and keeping pace requires continuous investment in updated tools, platforms, and skills. Governments face the task of adopting new

technologies in ways that prioritize security, efficiency, and alignment with public requirements. Maintaining adaptable systems over time supports the provision of consistent digital services.

Attracting and Retaining Digital Talent

With the increasing need for skilled technology professionals in various sectors, recruiting and retaining digital talent is a continuing challenge. The public sector competes with the private industry to hire specialists in fields such as cybersecurity, cloud computing, and artificial intelligence.

Building Public Trust in Digital Services

As government implements more advanced digital tools, such as artificial intelligence and data analytics, considerations around personal information protection and transparency increase in importance. Maintaining public trust is addressed through safeguards, clear communication, and technology practices that prioritize privacy and fairness.

Financial Information

The expenditure and revenue figures included in this document are unaudited and based on public information provided in the Report on the Program Expenditures and Revenues of the Consolidated Revenue Fund for the Year Ended March 31, 2025. Audited financial statements are a requirement at the government level and made public through the Public Accounts process; however, the OCIO is not required to provide a separate audited financial statement.

	Actual $	Estimates Amended $	Original $
OFFICE OF THE CHIEF INFORMATION OFFICER			
CURRENT			
4.1.01. PLANNING AND TRANSFORMATION			
01. Salaries	**3,126,203**	3,129,400	3,044,500
Operating Accounts:			
Employee Benefits	**12,820**	12,900	11,800
Transportation and Communications	**186,600**	202,900	204,000
Supplies	**60,669**	72,300	72,300
Professional Services	**-**	-	-
Purchased Services	**69,156**	77,400	87,400
Property, Furnishings and Equipment	**30,659**	33,200	33,200
02. Operating Accounts	**359,903**	398,700	408,700
Total: Planning and Transformation	**3,486,107**	3,528,100	3,453,200
4.2.01. DESIGN AND DELIVERY			
01. Salaries	**10,892,365**	10,901,800	11,501,800
Operating Accounts:			
Employee Benefits	**1,443**	3,300	3,300
Transportation and Communications	**6,171**	12,000	12,000
Supplies	**2,149,949**	2,150,000	736,000
Professional Services	**1,838,258**	2,240,300	7,274,300
Purchased Services	**43,185**	62,400	62,400
Property, Furnishings and Equipment	**2,295,958**	2,296,000	6,000
02. Operating Accounts	**6,334,964**	6,764,000	8,094,000
	17,227,328	17,665,800	19,595,800
02. Revenue - Provincial	**(7,600)**	(27,000)	(27,000)
Total: Design & Delivery	**17,219,728**	17,638,800	19,568,800
CAPITAL			
4.2.02. DESIGN AND DELIVERY			
01. Salaries	**2,524,267**	2,629,600	2,500,000
Operating Accounts:			
Supplies	**257,216**	430,000	180,000
Professional Services	**6,017,599**	6,016,900	7,293,200
Property, Furnishings and Equipment	**6,653**	6,700	-
02. Operating Accounts	**6,281,468**	6,453,600	7,473,200
Total: Design & Delivery	**8,805,735**	9,083,200	9,973,200
CURRENT			
4.3.01. INFRASTRUCTURE AND SECURITY			
01. Salaries	**8,906,338**	8,913,700	9,069,600
Operating Accounts:			
Employee Benefits	**525**	4,000	4,000
Transportation and Communications	**1,339,258**	1,349,000	1,551,000
Supplies	**16,514,361**	16,508,300	12,603,100
Professional Services	**363,818**	363,900	247,700
Purchased Services	**3,787,962**	3,839,700	4,149,700
Property, Furnishings and Equipment	**582,338**	585,700	791,900
02. Operating Accounts	**22,588,260**	22,650,600	19,347,400
	31,494,598	31,564,300	28,417,000
02. Revenue - Provincial	**(301,791)**	(343,500)	(343,500)
Total: Infrastructure and Security	**31,192,807**	31,220,800	28,073,500

	Actual $	Estimates Amended $	Original $
OFFICE OF THE CHIEF INFORMATION OFFICER			
CAPITAL			
4.3.02. INFRASTRUCTURE AND SECURITY			
Operating Accounts:			
Property, Furnishings and Equipment			
02. Operating Accounts	**283,459**	283,500	557,900
Total: Infrastructure and Security	**283,459**	283,500	557,900
CURRENT			
4.4.01. CYBER SECURITY OFFICE			
01. Salaries	**409,585**	409,600	474,400
Operating Accounts:			
Employee Benefits	**942**	1,000	1,000
Transportation and Communications	**13,887**	14,000	8,000
Supplies	**7,495**	44,000	5,000
Professional Services	**377,664**	377,700	250,000
Purchased Services	**151,493**	152,000	1,000
Property, Furnishings and Equipment	**13,871**	14,000	100,000
02. Operating Accounts	**565,351**	602,700	365,000
Total: Cyber Security Office	**974,937**	1,012,300	839,400
CAPITAL			
4.4.02. CYBER SECURITY OFFICE			
Operating Accounts:			
Property, Furnishings and Equipment	-	100	100
02. Operating Accounts	-	100	100
Total: Cyber Security Office	-	100	100

The expenditure and revenue figures included in this document are unaudited and based on public information provided in the Report on the Program Expenditures and Revenues of the Consolidated Revenue Fund for the Year Ended March 31, 2025.

These amounts were as of May 2, 2025, and Public Accounts changes may be applied if required.