Office of the Chief Information Officer

Business Plan

2020 - 2023

Newfoundland Labrador

MESSAGE FROM THE MINISTER

As Minister responsible for the Office of the Chief Information Officer, I am pleased to submit this business plan for the Office of the Chief Information Officer covering April 1, 2020 to March 31, 2023. The goals and objectives set out in this document will guide the Office of the Chief Information Officer as it continues to provide secure information technology, information protection, and information management services and support to government departments, agencies, boards and commissions under its mandate.

In carrying out this mandate, the Office of the Chief Information Officer will also offer innovative information technology solutions that will enhance the business of government by improving the delivery of public services, maximizing investment in technology, and responding more effectively to changing public needs and expectations.

Building on the Digital by Design roadmap framework enables multi-channel service delivery, which will improve the efficiency of the public sector and improve service to residents. This outcome supports the strategic directions of government, which have been considered in the development of this plan.

The Office of the Chief Information Officer has identified the following strategic issues which will guide its work over the next three years: Value, Service and Cyber Security. I look forward to working with the Office to advance these initiatives.

My signature below is indicative of my accountability for the preparation of this plan and the achievement of the identified goals and objectives which were developed with consideration of Government's strategic directions.

Hon. Sarah Stoodley
Minister Responsible for the
Office of the Chief Information Officer

Table of Contents

Overview

The Office of the Chief Information Officer (OCIO) was established under the **Executive Council Act**. It is a category two entity under the **Transparency and Accountability Act** and is responsible for providing information technology (IT) support, developing information management (IM) and information protection (IP) policies and standards, and providing IT and IM/IP advisory/consulting services to government departments and other primary clients under its mandate.

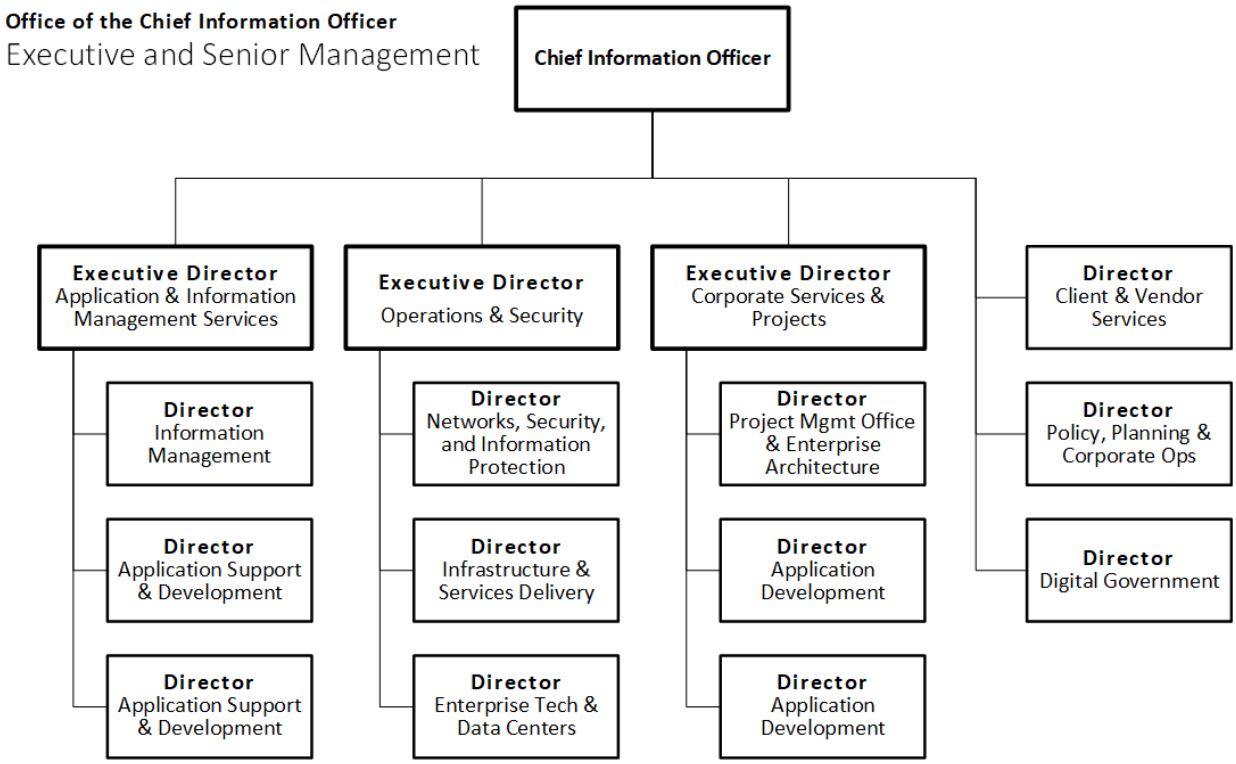
The OCIO supports in excess of 9,000 computers, approximately 630 applications and 150 websites which service the business of government. These applications and websites reside on over 1,760 servers. Government also owns significant network infrastructure and supports a comprehensive province-wide area network. This varied and complex environment requires security frameworks, preventative maintenance, disaster recovery plans, capacity planning, and software license monitoring and management.

As of March 31, 2020, the OCIO has 299 employees. The majority of its employees are located in offices throughout St. John's. There are 16 employees distributed among the OCIO's regional offices in Happy Valley-Goose Bay, Stephenville, Corner Brook, Grand Falls-Windsor, Gander and Clarenville.

The OCIO employs approximately 71 percent male and 29 percent female employees in total; 75 percent male and 25 percent female in non-management positions, and 48 percent male and 52 percent female employees in management-level positions.

Organizational Structure Chart

The OCIO is structured into three branches: Application and Information Management Services, Operations and Security, and Corporate Services and Projects.



Application and Information Management Services Branch: provides overall leadership and vision for the support, enhancement, maintenance, protection and database administration of government's portfolio of applications. The branch also develops information management directives, standards, procedures and guidelines, and provides advisory services and support to government departments and other supported public bodies. In addition, the branch is responsible for the administration of the **Management of Information Act**, providing government-wide advice and guidance on IM activities and initiatives.

Operations and Security Branch: provides support, maintenance, and security services to ensure the integrity and availability of government's Information Technology infrastructure. This includes computers, mobile devices, networking, storage, data backup, servers, enterprise data centre, enterprise applications and related

technologies. In addition, the branch is responsible for OCIO-wide change management and the OCIO's Information Protection (IP) program and related advisory services that support government-wide IP initiatives.

Corporate Services and Projects Branch: comprised of four divisions: Corporate Services, Client and Vendor Services, Projects, and Digital Government.

> **Corporate Services Division** is responsible for business operations, financial management (budget preparation and monitoring), contract management, human resource planning, IT procurement oversight, cabinet support, and Occupational Health and Safety.
>
> **Client and Vendor Services Division** is primarily responsible for engaging and collaborating with departments to set strategic IT direction, assisting in the prioritization of departmental IT spend, managing the interests of client departments and supported agencies, acting as a liaison with the local IT industry, and managing vendor relationships. The division has additional responsibility for planning, monitoring and reporting for the OCIO.
>
> **Projects Division** is responsible for the delivery of IT solutions to government departments and supported entities using project management best practices and standards and striving to reduce technology complexity by promoting integration of systems and data, reducing duplication, and supporting standardization of processes and systems.
>
> **Digital Government Division** is responsible for leading, defining, and delivering the overall government-wide digital strategy and digital channel in support of a more efficient public sector and government-wide service delivery change for residents and businesses.

The 2020-21 budget for the OCIO is $48,886,500.

Branch	Budget
Application and Information Management Services	$10,160,400
Corporate Services and Projects	$16,130,400
Operations and Security	$22,595,700

Mandate

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

- IT and IM/IP coordination, planning, budgeting, and policy development;
- Developing, operating, and securing computer systems and infrastructure for government departments, agencies, boards and commissions which are directly supported by the administrative support services of departments;
- Procurement of IT goods and services;
- Administering the **Management of Information Act**;
- Managing IT-related agreements, contracts and vendor relationships;
- Providing consultative services, particularly in the areas of IM and IP; and,
- Collaborating with industry to maximize business opportunities for the IT sector, while meeting the IT and IM/IP needs of government.

Lines of Business

In delivering its mandate, the OCIO provides the following lines of business to its clients:

- IT Projects/Solution Delivery
- Application Support and Maintenance

- Information Management Services
- Infrastructure Operations and Security

Primary Clients

Primary clients of the OCIO are all government departments, the Courts, the Royal Newfoundland Constabulary, and the House of Assembly and its Statutory Offices. The OCIO also supports agencies, boards and commissions, which receive administrative support services from their respective government departments.

For day-to-day operational IT support, staff of government departments and supported agencies, boards and commissions can contact the OCIO Service Desk during regular government business hours by phone or e-mail. For strategic, planning and budgetary discussions as well as service escalations requiring immediate action, OCIO Client Services is available to management/executive of government departments and supported agencies, boards and commissions by phone and e-mail.

Vision

The vision of the Office of the Chief Information Officer is of a professional information technology and information management organization aligned to enable the business of government.

Strategic Issues

Strategic Issue 1 – Value

Information technology is constantly changing and evolving. New technologies offer opportunities for improved features, innovative services, and greater efficiencies. Old technologies gradually become obsolete.

To continue delivering business value, government's IT and IM/IP solutions and services must also evolve. The OCIO continuously monitors government's technology

landscape to identify and address key technology opportunities and upgrades deemed necessary during this planning period; and, to optimize the value invested in its technology platforms and software applications (through technology reuse, maximizing service life of key aging infrastructures, and providing IT and IM/IP advisory services to government).

Goal

By March 31, 2023, the OCIO will have enhanced the capability of key IT technologies and refreshed the IM policy framework used by government to continue supporting the needs of citizens and businesses.

Goal Indicators

- Upgraded core enterprise technologies.
- Expanded the technology reuse model.
- Updated the IM policy framework**.**
- Provided IM services to government departments and entities.

Objective 2020-2021

By March 31, 2021, the OCIO will have upgraded a core enterprise technology and refreshed the IM policy framework.

Indicators

- Identified key infrastructures requiring technology upgrades.
- Upgraded a key infrastructure platform.
- Updated IM policy framework**.**

Objective 2021-2022

By March 2022, the OCIO will have continued to modernize enterprise technology and provide IM/IP advisory services.

Objective 2022-2023

By March 2023, the OCIO will have improved core enterprise technology and continued to provide IM/IP and advisory services.

Strategic Issue 2 – Service

Newfoundlanders and Labradorians are adopting technology to communicate, conduct business, and consume services. From the way people work, to the services they use and the places in which they live, digital technologies are enabling new patterns of citizen behaviour and new opportunities for Government to extend the reach of its public sector services for greater efficiency and public convenience. Digital services are assisting with the development of a more efficient public sector and contributing to the Government's strategic direction to deliver Better Service. This provides unique challenges for some of the more remote communities in the province that do not have strong or consistent internet service, and a standardized approach will have to take these challenges into consideration.

Goal

By March 2023, the OCIO will have expanded and improved government's services delivered through digital channels.

Goal Indicators

- Expanded government's digital service delivery.
- Improved access to digital services.

- Increased adoption of digital services.
- Reduced manual paper-based transactions.

Objective 2020-2021

By March 31, 2021, the OCIO will have improved digital transaction verification, expanded online services and defined a standardized approach to delivering digital services.

Indicators

- Continued the implementation of a credential management solution.
- Implemented new online services to a key stakeholder group.
- Developed a Digital Service Standards and Playbook to guide government's approach to reusable digital service design and development.

Objective 2021-2022

By March 31, 2022, the OCIO will have continued to expand and improve digital services to key stakeholders.

Objective 2022-2023

By March 31, 2023, the OCIO will have continued to expand and improve digital services to key stakeholders.

Strategic Issue 3 – Cyber Security

Citizens and businesses trust government to protect their information, keep it secure, and prevent it from compromise by unauthorized or inappropriate access. As digital stakeholder engagement increases, continued focus on cyber security and information

protection is required to: implement solutions that augment the government infrastructure and data security; reduce exposure to ever-evolving security risks and cyber threats; and, increase awareness and understanding to proactively manage threats. As Government embarks on a process to harness the full potential of technology, and grow the number of services delivered online, strong IT security is necessary to achieve these goals, and can only happen efficiently and effectively if businesses and citizens continue to have confidence availing of these services.

Goal

By March 31, 2023, the OCIO will have strengthened government's cyber security posture in response to evolving technology and security risks.

Goal Indicators

- Augmented solutions that protect government technology networks and data against security threats.
- Continued threat identification and protection of critical endpoints.
- Conducted IP education and awareness activities that promote cyber security best practices across government.

Objective 2020-2021

By March 31, 2021, the OCIO will have continued to evolve government's cyber security service with improved secure remote access and cyber security education and awareness for government staff.

Indicators

- Improved government network remote access, security, capacity and supportability.
- Continued cyber security education and awareness across government with focus on key cyber security risks.

Objective 2021-2022

By March 2022, the OCIO will have continued to evolve government's cyber security service and provided additional cyber security education and awareness to government staff.

Objective 2022-2023

By March 2023, the OCIO will have continued to evolve government's cyber security service and provided additional cyber security education and awareness to government staff.


Newfoundland
Labrador