Office of the Auditor General of Ontario

Value-for-Money Audit:
Office of the Corporate Chief Information Officer

November 2022

Ministry of Public and Business Service Delivery (MPBSD)

Office of the Corporate Chief Information Officer

1.0 Summary

The Ontario Public Service (OPS) uses a vast array of information technology (IT) systems to deliver government programs and services, from issuing health cards and drivers' licences to providing family support programs and COVID-19 grants. IT systems have become crucial for Ontarians. In 1998, the Government of Ontario established the Office of the Corporate Chief Information Officer (CCIO) to provide IT support to all its provincial ministries as well as to Cabinet Office and the Premier's Office.

The CCIO is directly responsible for IT needs that exist across the OPS. For instance, the CCIO establishes and maintains IT strategic planning, policies, standards and best practices such as the information security, application development, and database management standards. On behalf of the ministries, it also procures and maintains hardware such as laptops and mobile phones for all OPS employees, and is responsible for securing the overall OPS' IT network from cyberattacks. As well, the CCIO manages two data centres, located in Guelph and Kingston, that house the servers and host the databases associated with 1,200 IT systems storing Ontarians' data.

Ministry-specific IT needs are directly addressed by eight IT service "clusters", so called because they are responsible for providing IT services and support unique to a specified cluster, or group, of ministries. For example, one IT cluster is the Health Services Cluster, which groups together the Ministry of Health and Ministry of Long-Term Care and operates many IT systems unique to the health-care sector, like the Client Registration System for storing patient data and contact information. The eight IT clusters are managed by the ministries and report to deputy ministers. The CCIO provides services and consultation to these cluster employees, who in turn manage and make decisions about the IT systems used by the Ontario public. The CCIO reports into the Ministry of Public and Business Service Delivery (Ministry) with a mandate to ensure the provincial government's IT services are effectively and efficiently delivered. Our audit found that a consequence of the reporting structure—whereby IT clusters report to their respective deputy ministers and not the CCIO—is that the CCIO does not have oversight, accountability, and authority for day-to-day IT operations and decision-making at the eight IT clusters. Without such oversight, the CCIO is unable to fulfill its mandate and ensure that IT services such as procurement, vendor performance, and cybersecurity are in fact delivered effectively and with due regard for economy.

We determined that cybersecurity practices at the OPS need improvement. Ontarians' personal and sensitive data stored within IT systems that we reviewed were not protected using cybersecurity controls such as encryption. We reviewed controls related to cybersecurity assessments. Due to the nature of cybersecurity, and so as to minimize the risk of exposure for the OPS, we provided relevant details of our findings and recommendations directly to the CCIO. The CCIO agreed with the recommendation and committed to safeguarding the data entrusted to the government by the people and businesses of Ontario. We also found that half of the IT systems that are critical for continuous and reliable operations of government programs do not have a

disaster recovery plan in case of a significant outage or a disaster.

We also found that Ontario's highest-rated data centre, used by the CCIO to host servers and databases for all 1,200 OPS IT systems, has been significantly underutilized since it opened 10 years ago, and that usage has even declined over the last five years. Although the data centre was built in March 2011 with the intention of servicing the OPS, a business case was submitted to the Treasury Board Secretariat in 2012 to leverage the data centre for use by the broader public sector outside of the OPS. Despite having the capacity, there is currently minimal use from the broader public sector and Crown agencies. As a result of the limited utilization of the centre, the CCIO who is the custodian of the data centre has incurred approximately $31 million in additional operating expenses (in the past five years) for power, cooling, maintenance and physical security for the unoccupied space. This cost could have been offset by filling the unutilized space with other government entities, such as Crown agencies and the broader public sector that would share in the costs.

The following are some of our significant audit findings:

Governance

- **The CCIO has weak IT oversight of operations at the eight IT clusters.** The CCIO is unable to meet its mandate of ensuring that government's IT services are managed and delivered effectively since it does not have oversight and accountability for IT operations performed by the eight IT clusters. Clusters report to their respective deputy ministers, not to the CCIO. As a result, the CCIO is not always aware of key IT decisions about procurement under $2 million or the safeguarding of Ontarians' data as collected by the clusters, nor can it measure performance outcomes for cluster IT systems.
- **The CCIO has not identified the Enterprise IT risks and mitigating strategies impacting OPS operations.** Currently, IT risks are not being identified within the CCIO and the CCIO does not have an overarching strategy for the OPS to identify IT risks and implement mitigating and remediation strategies. We noted that the CCIO relied on ministries and clusters to identify elements of IT risk which impact a specific ministry or cluster. Upon our review of these identified risks, we noted that the CCIO has not identified major IT risks that would impact the OPS, or any risks commonly identified by industry best practice.
- **Ontario's primary data centre is significantly underutilized.** The data centre has been awarded a Tier IV rating, the highest rating available for a data centre to indicate that IT systems are able to withstand any type of failure. At the time of our audit, Guelph Data Centre was being utilized at 30% of its capacity with a total annual cost of $9 million. Two main factors in the low utilization are:
  - the standard charge rate for using the data centre is $75 per square foot (converted to power drawn for comparison is $1.33 kWh) which is more than double compared to other private Tier IV data centre operators that charge $0.59 kWh in other countries such as the United States, the United Kingdom, and Australia; and
  - the lack of an outreach marketing strategy to promote the data centre outside of the OPS to Crown agencies and the broader public sector.

Disaster Recovery

- **Almost half of all critical IT systems within the OPS do not have a disaster recovery plan.** We found that almost half (44%) of all critical IT systems, those crucial for continuity of government services such as health, education, and drivers' licensing, do not have a disaster recovery plan. Disaster recovery plans outline detailed procedures for recovering and restoring an IT system from a disaster such as a prolonged Internet outage or a major cyberattack. In particular, we noted that the CCIO does not have

a redundant secondary network provider for some of its critical operations, such as 44 contact centres, that it could rely on during an outage to maintain functionality for its critical IT systems. As a result, the nation-wide Rogers Communications outage on July 8, 2022 impacted the OPS such that it was unable to provide Ontarians services through contact centres such as Service Ontario, COVID-19 Vaccination Patient, and social assistance payments websites.

Cybersecurity

- **Personal and sensitive data is not consistently secured through encryption in accordance with the CCIO's security standard.** In a sample selection of five key IT systems used by the Ministry of Health, Ministry of the Solicitor General, Ministry of Community Safety and Correctional Services, and the Ministry of Public and Business Service Delivery, we discovered that sensitive and personal information was not being encrypted in any of them as required by the security standard.
- **There is no cybersecurity oversight over Ontarians' data when stored by IT vendors.** The CCIO does not oversee cybersecurity-related risks for 140 OPS IT systems that are managed by external vendors to the OPS, as the CCIO does not obtain or review third-party assurance reports.
- **Cybersecurity awareness training in the OPS can be strengthened.** The CCIO is responsible for developing and implementing cybersecurity-related training for OPS staff. We noted that only 11,000 of 40,000 OPS staff completed the mandatory cybersecurity awareness course in 2021. Although employees' managers are responsible for ensuring this training is completed, the CCIO does not track or ensure that the course is attended by all staff. In addition, the cybersecurity awareness training is not required for about 7,000 contract employees, nor is it provided annually to all OPS employees even though it is regarded as a best practice.

Procurement of Consultants

- **There is insufficient due diligence when hiring IT consultants.** Prior to hiring contract staff, the CCIO does not assess whether it already has the internal resources to complete the work, or whether it should hire a full-time permanent employee or hire a consultant. From our analysis, the CCIO paid double the amount of salary to consultants as it would have spent hiring full-time staff for the same positions. In addition, from April 1, 2021 to May 31, 2022, 25 consultants from a total of 244 were paid an average of $86 above the daily rate recommended by the Treasury Board Secretariat. The highest overpayment was $232 above the daily rate as set without any justification provided.

IT Incident Resolution

- **IT incident resolution targets missed.** In 2016, the CCIO established a compliance target of 90% for the resolution of IT incidents as per the established service level agreements. This target has not been re-evaluated since. CCIO data indicated an average compliance of 95% for all IT incidents in the past five years. When we recalculated the resolution compliance rate we found that the average resolution rate was 85%. This 10% discrepancy is due to the fact that CCIO calculates the compliance rate using the elapsed time, which is the time spent by the technician to resolve the incident ticket, whereas for our calculation, we compared the time when the incident ticket was created against the time when it was closed. Further, we noted that the compliance rate for IT incidents with the most significant impact ("critical") was 66%.

Overall Conclusion

Our audit concluded that the Office of the Corporate Chief Information Officer (CCIO) does not exercise thorough oversight of information technology (IT) operations and the delivery of IT services across the Ontario Public Service (OPS). Due to the current

reporting structure—in which "cluster" ministries report to their respective deputy ministers rather than to the CCIO—the CCIO is often unaware of key decisions on IT procurement and data security and cannot monitor or measure performance outcomes of most of the critical IT systems in use by the OPS. Although the CCIO bears overall responsibility for these IT systems as per its mandate, the current reporting structure presents a significant obstacle to the CCIO achieving its mandate, namely, to deliver value-for-money on the technology infrastructure that powers all of government and to ensure the privacy, security, availability, and integrity of critical government information, operations, networks, and systems.

Further, we found that OPS' Guelph Data Centre, which has the world's highest data centre rating and is used by ministries and several other government agencies to host their IT systems, has been significantly underutilized since it became operational 10 years ago. Although the data centre was built in March 2011 with the intention of servicing the OPS, a business case was submitted to the Treasury Board Secretariat in 2012 to leverage the data centre for use by the broader public sector outside of the OPS. Despite having the capacity, there is currently minimal use from the broader public sector and Crown agencies. Usage has even declined over the past five years, during which time an additional $31 million, a direct loss in operating costs was spent on power, cooling, maintenance and physical security for the unoccupied space. One reason for low utilization of the data centre is its high cost to clients, which is more than double the amount charged by other Tier IV data centres. As well, the CCIO does not have an outreach strategy to onboard other government entities.

We also noted that the CCIO does not have disaster recovery plans for almost half of the critical IT systems in the OPS. Disaster recovery plans support the continuous and reliable operation of government programs should an unexpected event affect its IT systems. In addition, the CCIO has not developed an overarching disaster recovery strategy and has not performed comprehensive disaster recovery testing for all the critical IT systems in the OPS.

With respect to Ontarians' personal and sensitive information, we found that this information is not being fully protected in accordance with the security standard (e.g., through data encryption). We reviewed controls related to cybersecurity assessments. Due to the nature of cybersecurity, and so as to minimize the risk of exposure for the OPS, we provided relevant details of our findings and recommendations directly to the CCIO. The CCIO agreed with the recommendation and committed to safeguarding the data entrusted to the government by the people and businesses of Ontario.

This report contains 13 recommendations, with 40 action items, to address our audit findings.

OVERALL MINISTRY RESPONSE

The Ministry of Public and Business Service Delivery (Ministry) thanks the Auditor General and her team for this value-for-money report on the Office of the Chief Corporate Information Office (CCIO).

The CCIO within the Ministry is committed to safeguarding the data entrusted to the government by the people and businesses of Ontario. The Ministry utilizes a defense in depth approach to cybersecurity, which includes multiple layers of security controls, to identify inherent cybersecurity weaknesses within OPS IT systems. The Ministry recognizes there is room for improvement and is committed to continuously evolving and enhancing current cyber practices. This includes strengthening the management of vendor performance by centralizing the management of key IT vendors along with ensuring effective performance management and monitoring. Over the past several years, the Ministry has made advances in cybersecurity maturity practices and as the Ministry embarks on the next iteration of the cybersecurity strategy (2023–26), the focus will be on strengthening the OPS' cybersecurity posture, while empowering the broader public sector (BPS) and extending support to key sectors (health, education).

To support the government's digital journey, over the past decade the Ministry has consolidated 22 regional data centres into two data centres at

Guelph and Kingston, reducing the government's data centre footprint, in addition to work underway to decommission the Kingston Data Centre over the next two years. As the government continues to reduce its footprint, it is adopting innovative technologies to increase operational efficiency, reliability, availability, and value-for-money. As the government continues to adopt innovative technologies, the Ministry is committed to adhering to key principles to ensure the ongoing protection, security, and privacy of Ontarians' personal information. Working with ministry and cluster partners, the Ministry will embed cybersecurity by design into all applications to strengthen reliability and efficiency, and enable more strategic and effective use of IT assets and resources.

The Ministry also recognizes that more can be done to address enterprise IT risk. In addition to identifying enterprise IT risks, the Ministry is committed to continue working with the Office of the Chief Risk Officer to mature practices in risk management, to better monitor and manage risks at an enterprise level.

The Ministry commits to taking all the necessary steps and using the recommendations in this report to continuously improve the service delivery of the government's IT systems.

2.0 Background

2.1 Overview

The mandate of the Office of the Corporate Chief Information Officer (CCIO) is to ensure that the Ontario government's IT systems are managed and delivered efficiently and effectively. It needs to do this by supporting all provincial ministries in their IT initiatives and investments. The CCIO is directly responsible for OPS-wide IT needs such as procuring assets, maintaining cybersecurity, developing IT policies and standards such as the information security, application development, and database management standards, and overseeing the day-to-day operations of the OPS's two data centres located in Guelph and Kingston. Ministry-specific IT needs are separately addressed by eight service "clusters" who are responsible for providing IT services unique to a specified group of ministries (as discussed in **Section 2.2**).

The CCIO is part of the Ministry of Public and Business Service Delivery (Ministry) and is comprised of four divisions, namely: Infrastructure Technology Services (ITS), Cyber Security Division (CSD), Enterprise Technology Delivery (ETD) and Enterprise Technology Strategy (ETS). **Figure 1** summarizes the roles and responsibilities of each enterprise division. In total, the CCIO has about 1,250 IT employees. Over 1,000 of these staff work within the ITS division. Refer to **Appendix 1** for a glossary of acronyms used in this report.

2.1.1 CCIO's Four Enterprise Divisions

Infrastructure Technology Services

Infrastructure Technology Services (ITS) is responsible for providing hardware such as laptops, cell phones and printers, as well as enterprise-wide software applications like Microsoft Office, to about 60,000 OPS staff in office locations across Ontario. ITS manages daily operational activities at its two data centres that store about 1,200 IT systems used internally by ministries and with the public. To deliver government programs and critical services to Ontarians, the Guelph Data Centre is to ensure that the data is secure and available with minimal disruption. There is a 24-hour OPS Service Call Centre hotline which provides telephone, remote and in-person technical support for requests such as password resets and general IT troubleshooting for all OPS staff.

ITS equips OPS staff and its two data centres with appropriate IT assets such as laptops, desktop computers, peripherals, and servers. IT clusters are responsible for engaging the ITS to request assets such as laptops, printers, telephone devices on behalf of the ministries within the cluster. As of January 2022, ITS managed over 90,000 laptop and desktop computers, 45,000 mobile devices, and 10,000 servers on behalf of ministries. Three categories of assets are managed by ITS (see **Section 2.5**).

Figure 1: Office of the Corporate Chief Information Officer (CCIO) Enterprise Divisions

Prepared by the Office of the Auditor General of Ontario

In addition, ITS provides the infrastructure that supports critical ministry and agency IT systems.

Cyber Security

The CCIO's Cyber Security Division (CSD), which is responsible for setting cybersecurity requirements for the OPS through policies and standards, consistently performs vulnerability scans for critical IT systems to identify potential vulnerabilities. In addition, CSD recommends safeguards and compensating controls through point-in-time cybersecurity assessments such as penetration tests and Threat Risk Assessments. Implementation and operationalization of these recommendations is the responsibility of system owners. The CSD is also responsible for information-security-related activities for all ministries and clusters across the OPS. The division focuses on increasing cyber awareness and education among Ontario government staff and addressing high cyber risk areas. It also provides services such as: monitoring for cyberattacks; performing Threat Risk Assessments; providing security advice; reviewing IT network architecture; and advising on security-related procurement. The division maintains various cybersecurity policies, standards and guidelines that hold across the OPS. The division has also established a cybersecurity standard for clusters and ministries that requires them to safeguard sensitive information by using security controls such as encryption.

The Cyber Security Division also operates the Cyber Security Operations Centre, available to OPS employees 24 hours a day. The operations centre performs incident identification, notification, response, prevention and web filtering. CSD's Secure Solution Design Unit provides advice and guidance on configuration of information systems and solutions to address security requirements based on security assessments. Within CSD's Vulnerability Management Unit, the staff performs vulnerability assessments, penetration tests, and Threat Risk Assessments.

In 2019, the CCIO established a Cyber Security Centre of Excellence, led by the Cyber Security Division. The centre provides seminars, workshops and an online cybersecurity awareness program to broader

public sector employees to increase their awareness of cybersecurity risks. It also runs monthly campaigns and advises client ministries and agencies on cybersecurity best practices and relevant industry standards. The Cyber Security Centre of Excellence is also responsible for developing and delivering a cybersecurity-related training and awareness course through the LearnON IT system, accessible to all OPS employees.

Enterprise Technology Delivery

The Enterprise Technology Delivery division is responsible for managing a significant portion of government authentication systems that manage access to government IT systems. The division also runs a document management IT system called OPSdocs that has significant integration with several OPS leading IT systems, providing document hosting, search and records management functions. The Enterprise Technology Delivery division also runs a technology platform that hosts several mission critical IT systems and provides integrations services between systems so they can exchange data and complete transactions that support business processes.

Enterprise Technology Strategy

The Enterprise Technology Strategy (ETS) division was recently established, on April 1, 2021. It is responsible for developing and maintaining IT standards, policies, and procedures and for the development of an overall IT strategy and vision across the OPS. ETS works in collaboration with IT clusters and their ministries. ETS has established a strategy called Technology Roadmap and Investment Plan that outlines the plan of technology investments, identifies and prioritizes common technologies within OPS that could be leveraged by ministries, and uses IT resources in the most efficient way.

The Enterprise Technology Strategy division governs the design of projects that are high-risk or cost $2 million or more. This includes chairing the Corporate Architecture Review Board (ARB) which oversees OPS' Enterprise Architecture practice; co-ordinates the security, privacy, and accessibility; and records management reviews.

2.1.2 CCIO Funding

In fiscal year 2021/22, the CCIO's total operating expense was $144 million and $9.2 million in capital expenses. Notably, ITS is the organization's largest division by far; salaries and wages in 2021/22 for this division were $99.8 million.

In 2020/21, expenditures were $117 million in operating costs and $9.6 million in capital expenses.

2.2 The Eight IT Clusters

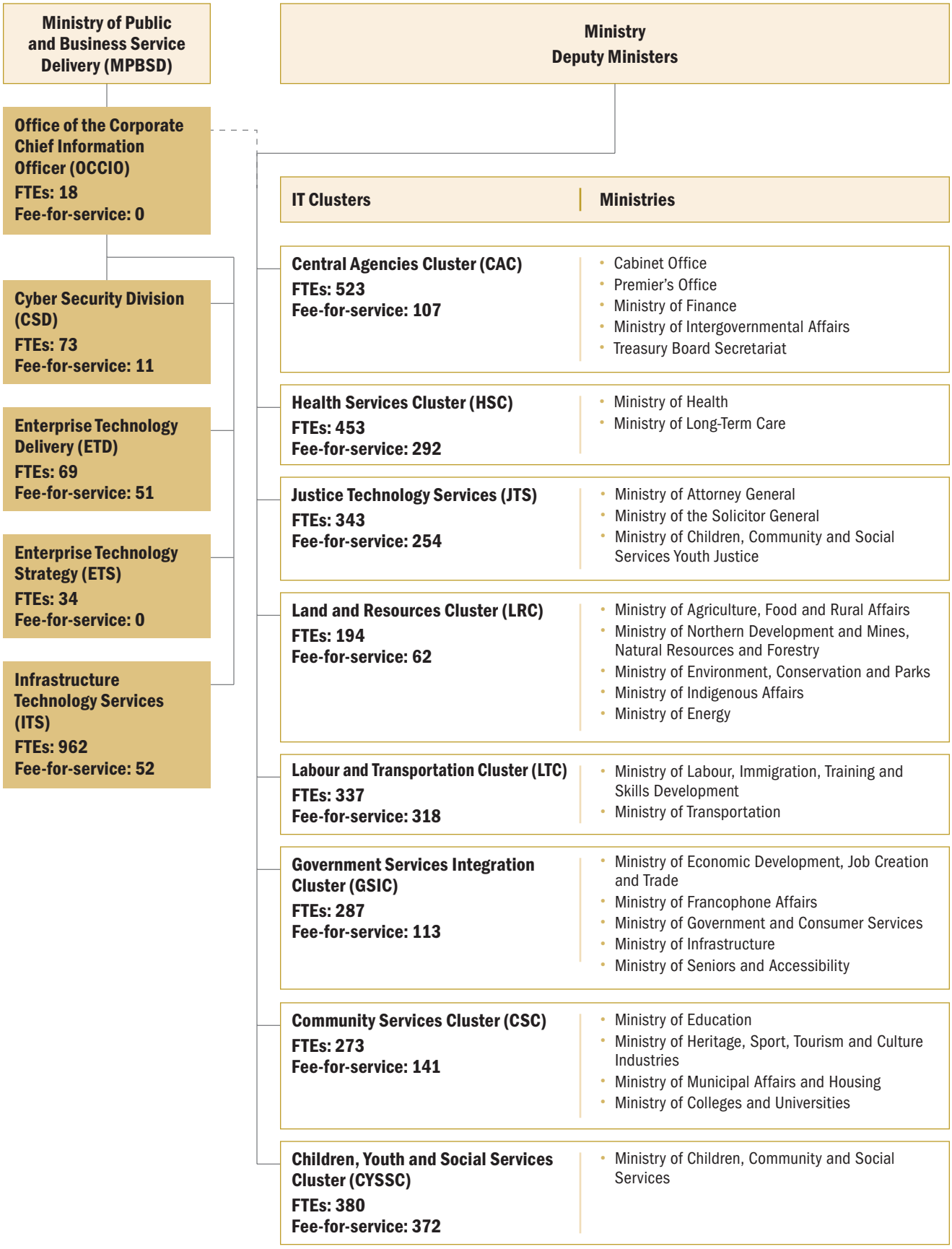
While the CCIO's four enterprise divisions address OPS-wide needs, initiatives and projects such as email and phone service, there are also eight IT "clusters" (with a total of roughly 2,400 employees) that each have their own Chief Information Officer (CIO) and manage IT needs considered particular to a grouping, or cluster, of ministries. These clusters are not part of the CCIO; cluster employees are employees of the ministries, reporting to a deputy minister. **Appendix 2** records the individuals who oversee each of the IT clusters, as of September 2022.

The eight IT clusters provide customized IT services based on a ministry's unique needs, whether those be day-to-day or longer-term in scope. This includes implementing new IT projects and overseeing the development, testing and implementation of IT systems, IT resource management and IT consulting services. For example, the Community Services Cluster manages IT support for the Ministries of Education; Colleges and Universities; Municipal Affairs and Housing; and Heritage, Sport, Tourism and Culture Industries. The cluster developed and maintained the IT systems needed to provide COVID-19 reporting in schools and an Internet modernization program for schools.

Figure 2 presents the organizational/reporting structure of the CCIO in relation to the eight IT clusters, while **Appendix 3** lists the responsibilities of the CCIO as compared to the clusters.

Figure 2: IT Reporting Structure in the Ontario Public Sector, as at August 19, 2022

Prepared by the Office of the Auditor General of Ontario



2.2.1 Governance Committees

The CCIO is governed by the IT Governance Boards and Committees to review CCIO's IT operation service delivery, policies and value of services delivered. The following governance committees/boards have been established to provide oversight for IT operations.

Information Technology Executive Roadmap Committee

The mandate of the Information Technology Executive Roadmap Committee is to provide functional level leadership and governance for the IT organization, by promoting a broader understanding of IT directions and partnerships between the business and IT communities. The committee also provides support for the development of IT professionals within the Ontario Public Service and the effective functioning of the IT organization. It is also responsible for development and implementation of enterprise IT standards and solutions where appropriate.

Technology Roadmap and Investment Plan (TRIP) Program Governance Committee

The purpose of the TRIP Program Governance Committee is to provide comprehensive strategic support for the ongoing evolution, oversight, and direction-setting of the government's Technology Roadmap and Investment Plan. The committee shares information and updates to senior management and clarifies and communicates accountabilities for technology enablement and investments. It also monitors, approves, and endorses major initiatives.

2.3 Guelph and Kingston Data Centres

Guelph Data Centre (data centre) is a physical facility used by the OPS to host servers and databases for about 1,200 IT systems. These include critical IT systems that are used to ensure continuity and effective delivery of government services. In addition, some broader public sector and Crown agencies use the data centre to store their data, including the Liquor Control Board of Ontario, Ontario Health, Technical Standards and Safety Authority, Wellington-Dufferin-Guelph Public Health, Metrolinx and Financial Services Regulatory Authority of Ontario. The data centre was built in 2011 because the current data centre at the time, the Toronto Data Centre, had reached its end of life and could not meet the capacity and availability demands of the OPS' IT systems. The OPS also makes use of a smaller, secondary physical facility, the Kingston Data Centre, which hosts about 260 IT systems. The CCIO is currently in the process of moving the existing IT systems at Kingston to the data centre in Guelph as well as to a cloud service provider. By May 2025, the Kingston Data Centre is expected to be fully phased out.

2.3.1 Disaster Recovery Management

A Disaster Recovery (DR) strategy, one component of IT risk management, is used to evaluate whether an IT system can be restored or made functional during various disaster scenarios, such as power outages, cyberattacks and earthquakes. DR strategies are prepared by each ministry to determine priorities and map a timeline for recovery. Once a DR strategy is finalized, a DR plan is created to document a step-by-step process to recover and resume critical operations and services following a disaster scenario. It is best practice for a DR plan to be reviewed, tested and updated on an annual basis, at minimum.

2.4 Risk Management in the OPS

The Office of the Chief Risk Officer (Chief Risk Officer) for the Province of Ontario has established an Enterprise Risk Management (ERM) process by which IT clusters, the CCIO, and ministries identify and report risks. The Chief Risk Officer was established in April 2021 and reports into the Office of the Comptroller General, within the Treasury Board Secretariat. As part of the ERM process, the CCIO has initiated work in collaboration with the Chief Risk Officer to identify various IT risks related to cybersecurity and management of IT assets. Each IT risk documented in the risk register is assigned a risk owner responsible

for monitoring that risk until it has been remediated or mitigated.

ERM identifies the processes that are in place for key control areas in an organization to ensure that risks have been adequately identified, treated or mitigated and addressed, including risks relating to IT operations and cybersecurity. ERM is holistic, and includes consideration for risk aspects of IT investments, responsibilities for risk management, risk analysis methodology, strategies for addressing risks and continuous monitoring of threats, occurrence, and impact.

Ontario's Chief Risk Officer is responsible for:

- overseeing the OPS enterprise risk management process, including reviewing and advising on ministry risk information and risk management practices;
- providing guidance and training, and being a centre of expertise in support of the Enterprise Risk Management Directive and OPS Enterprise Risk Management Framework;
- providing advice and guidance when the other program areas may be addressing risk in new or existing corporate directives and policies;
- advising the Secretary of Treasury Board/Management Board of Cabinet on requirements for ministries and provincial agencies to report risk information to central agencies; and
- working in co-operation with ministries and central agencies to ensure that risk information is available to the Treasury Board/Management Board of Cabinet, and other key decision-makers as required to inform decision-making.

2.5 IT Asset Management in the OPS

Asset management involves the monitoring and administration of the resources needed to provide infrastructure and IT system-related services. This includes the lifecycle management of hardware and the utilization of tools to manage and enable asset reporting.

There are three categories of assets managed by the CCIO's ITS division:

- **End user computing assets** are devices used by OPS staff such as laptops, desktops, mobile devices, and tablets. These assets are tracked and stored in the Configuration Management Database (CMDB), a central repository which stores the information related to IT assets.
- **Data centre operation assets** include servers, storage devices, back-up hardware and software devices that are used at the two data centres. The CCIO tracks these assets in the CMDB.
- **Telecom assets** include network and voice services such as remote access services, telephone systems, and satellite phones.

2.6 IT Consultants

The CCIO uses the company Flextrack to source fee-for-service IT consultants. The contract with Flextrack is valued at $600 million over five years. Flextrack began to provide contract IT consultants in October 2020, in conjunction with the Vendor of Record at the time.

At the CCIO, when IT consultants are needed, a request for services is sent to Flextrack using the Vendor Management System (VMS), an IT system used for processing and maintaining vendor-related documents. The VMS is owned by Flextrack and employs a Salesforce-based software. The requesting manager submits a requisition on the platform. The request is automatically received by Flextrack via the VMS, after checking the existing pool of IT consultants within the IT system first. Flextrack has a list of 359 firms, called IT qualified firms, who are allowed to submit candidates for the contract requisition. Flextrack then performs an initial review of resumes to arrive at a shortlist of candidates based on their fit for role. This shortlist is then sent to the requesting manager and interview evaluators for assessment.

The subsequent evaluation consists of a review of the candidate's resume. The candidate must score a minimum of 70% on their resume in order to proceed to an interview. The interview is then performed by at least three full-time equivalent evaluators and they

each assign an interview score. The candidate with the highest combined score of their interview and daily rate of pay is awarded the contract and undergoes the applicable security clearance and background check. **Figure 3** depicts a flowchart of the fee-for-service intake process.

2.6.1 Rate of Pay and Payment

The hiring manager determines a per diem rate for the hire in accordance with the per diem maximum rates, per role, developed by the Treasury Board Secretariat. (See the chart in **Appendix 4**.) To complete the procurement process the Treasury Board Secretariat, CAC, and the requesting ministry are notified of the award and its finance team submits payment invoices to Flextrack.

Payments made are in accordance with the consultant's timesheets. The CAC performs a reconciliation of hours submitted by the contract employee against the payment made to Flextrack on a monthly basis. OPS then issues payment to Flextrack, and Flextrack in turn issues a payment to the IT qualified firm, who then pays the consultant.

2.6.2 Timesheets and Performance Evaluation

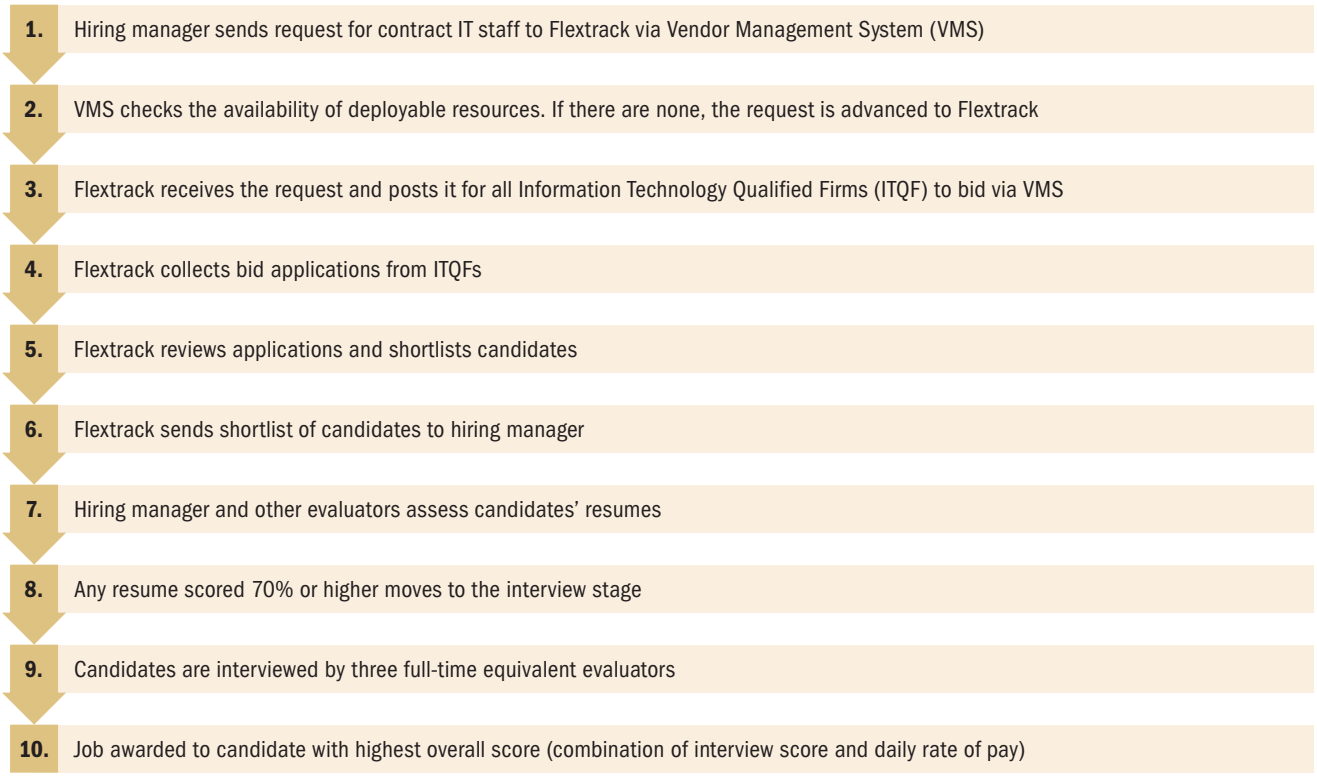
Planview, a Treasury Board Secretariat-managed system, is the IT system currently used for capturing, managing and maintaining the timesheets of contract employees and IT OPS employees in ministries. At the end of an employee's work term a survey is to be performed by the reporting manager to evaluate their performance. The survey results are shared by Flextrack with the CAC.

2.6.3 IT System for Procurement and Evaluation

The candidate's evaluation status is shown in the VMS and when a candidate is selected the offer is submitted via the VMS. Approvals of statement of work and contract awards are captured and stored within the VMS as well. Signatures for these documents are

Figure 3: IT Consultant Hiring Process

Prepared by the Office of the Auditor General of Ontario



carried out via the electronic signature DocuSign function in an automatic workflow.

2.7 Monitoring of Service Delivery

IT systems are critical for continuous operation of the services and programs delivered by government. Any disruption to operations and/or outages with key IT systems can have a significant impact in availability and effective delivery of OPS operations on Ontarians. So, it is important that services are delivered and any IT incidents are resolved as per the expected service level agreements, which should be in line with industry best practices.

Service delivery is established and enforced through several agreements between the CCIO, clusters, and ministries. These agreements establish the roles and responsibilities of the work that is expected to be delivered by the CCIO.

The CCIO has established a compliance target of 90% for all service delivery tickets relating to IT incidents such as password resets, restoration after system outages, installing IT software and user account-related administration.

3.0 Audit Objective and Scope

Our audit objective was to assess whether the Office of the Corporate Chief Information Officer (CCIO) has effective processes and procedures in place to ensure:

- A governance framework is in place that encompasses an overall IT strategy that demonstrates effective oversight of IT functions to deliver IT services to the Ontario Public Service and Ontarians efficiently and effectively.
- IT operations and systems are effectively monitored in accordance with established performance metrics and corrective actions are taken upon review.
- Ontarians' data and IT assets including hardware and software are secure, reliable and protected against cyberattacks.
- IT resources including IT contract employees are procured in accordance with legislative, regulatory and contractual requirements and with due regard for economy.

In planning for our work, we identified the criteria we would use to address our audit objective (see **Appendix 5**). These criteria were established based on a review of applicable legislation, policies and procedures, internal and external studies, and best practices. Senior management at the CCIO reviewed and agreed with the suitability of our audit objective and related criteria.

We conducted our audit between January 2022 and September 2022. We obtained written representation from management that, effective November 23, 2022, they had provided us with all the information they were aware of that could significantly affect the findings or the conclusion of this report.

We interviewed senior management staff at the CCIO under the Ministry of Public and Business Service Delivery to review their roles and responsibilities related to oversight and administration of day-to-day IT activities at OPS and effective delivery of government programs. We interviewed the Chief Information Security Officer to assess if policies and processes are in place to protect the security and privacy of confidential data. We interviewed senior management staff of the Cyber Security Division of the CCIO to assess if adequate cybersecurity scans and assessments are being performed to identify and remediate IT risk within the Ontario government's IT system portfolio. We interviewed stakeholders who are responsible for management of IT assets in OPS to assess if IT asset inventory is being maintained to support the identification of risk and support investment decisions into critical assets.

We also interviewed senior management staff at the clusters and Treasury Board Secretariat to obtain an understanding of the contingent employee procurement process and to assess if the CCIO procured IT contract employees with due regard for economy. We selected a sample of 30 IT contract employees and reviewed the practices involved in hiring them,

including but not limited to shortlisting of candidates, interview notes, candidate selection criteria and performance evaluations.

We conducted a survey of 51 IT executives working within the eight IT clusters in order to understand the existing operating model and potential improvement opportunities with respect to IT operations and services being performed by the CCIO. We also wanted to understand stakeholders' perspectives on the CCIO's overall strategy, cybersecurity practices, oversight over IT vendors and procurement of IT systems. We invited cluster CIOs, directors and management process leads to participate and received a response rate of 76% (39 out of 51).

We visited Guelph Data Centre, which stores Ontarians' financial and confidential data, to assess physical security, environmental controls, safety and emergency procedures along with IT incident response procedures. We did not visit the Kingston Data Centre since it is in the process of being decommissioned.

Over the next two years we plan to audit the eight IT clusters to assess if IT systems and operations are being managed effectively and efficiently and with due regard for economy. **Figure 4** depicts our Office's planned audit coverage of IT in the OPS.

4.0 Detailed Audit Observations

4.1 Reporting Structure Prevents the CCIO from Ensuring Clusters Have Effective and Efficient Delivery of IT Systems

According to the CCIO's mandate, it is responsible for ensuring the provincial government's IT systems are working efficiently and effectively, by supporting all ministries in their IT initiatives and projects. Within this broad mandate, the CCIO is directly responsible for OPS-wide IT needs such as procuring IT assets, cybersecurity, and developing IT policies and standards. Specifically, its mandate is to deliver value-for-money on the technology infrastructure that powers all of government and to ensure the privacy, security, and integrity of critical government information, operations, networks, and systems. The CCIO also oversees day-to-day operations of the OPS's two data centres.

The CCIO develops OPS IT policies and standards such as for information security, application development, and database management standards, and provides them to the eight IT clusters. Ministry goals

Figure 4: Audit Coverage of Internet Technology Across the Ontario Public Service

Prepared by the Office of the Auditor General of Ontario

2021–22	2022–23	2023–24 (Tentative)
Audit Topic: IT Governance of the CCIO	**Audit Topic: Governance of IT Systems and Operations – PART 1**	**Audit Topic: Governance of IT Systems and Operations – PART 2**
1. Cyber Security Division 2. Enterprise Technology Delivery 3. Enterprise Technology Strategy 4. Infrastructure Technology Services	1. Central Agencies Cluster 2. Community Services Cluster 3. Children, Youth and Social Services Cluster 4. Government Services and Integration Cluster	1. Health Services Cluster 2. Justice Technology Services 3. Land and Resources Cluster 4. Labour and Transportation Cluster

Audit Coverage of IT Across OPS

and priorities, staffing and funding, however, are under the purview of the deputy ministers associated with each cluster. Consequently, the CCIO is unable to measure the performance outcomes of cluster-specific IT systems. Further, key decisions about IT that are made in the clusters—such as about safeguarding Ontarians' data, or IT procurement under $2 million as per its policy which outlines requirements to manage IT projects' lifecycle, set by the Treasury Board Secretariat are not overseen by the CCIO, and therefore, it cannot hold clusters accountable for them. IT projects valued at $2 million and above are required to seek IT project approval from Treasury Board/Management Board of Cabinet and may be subject to quarterly reporting on their status and risk.

The current reporting structure, in which the clusters report to their respective deputy ministers and the CCIO reports to the Ministry of Public and Business Service Delivery, does not allow for the oversight necessary to mitigate overarching risks associated with day-to-day IT operations in the OPS. As a result, the CCIO is unable to fulfil its mandate. Our survey of cluster employees found that 92% of respondents believed that the CCIO's overall strategy provides an appropriate vision for the future. However, 43% of respondents were not satisfied with their relationship with the CCIO, and indicated that although the strategy is a work-in-progress, they would like to be more engaged and integrated in that vision.

When we inquired whether there were any services the CCIO did not currently provide that would be helpful in daily operations, 18 (46%) of the 39 respondents suggested cross-cluster collaboration and centralized IT procurement would be better for managing IT projects and capacity. Only 13 (33%) of the 39 respondents reported they had always involved the CCIO in procurement decisions over the past five years.

Given the current reporting structure of IT clusters—reporting to their respective deputy ministers instead of to the CCIO—we noted a number of constraints that prevented the CCIO from ensuring that clusters are effectively and efficiently delivering IT systems. Some key examples are:

Cybersecurity Standards to Secure Sensitive Data Are Not Enforced

The CCIO has established a security standard that requires ministries and IT clusters to encrypt sensitive government and Ontarians' data. However, we noted that the CCIO cannot monitor whether the clusters secure the data as required by the standard. During our audit we identified IT systems that were supposed to encrypt confidential information that was not encrypted. Refer to **Section 4.6.1** for details on that finding.

No Workforce Strategy Exists to Efficiently Share Internal IT Resources

Because the clusters report into their respective deputy ministers, their respective IT staff are siloed within their designated cluster. As a result of the siloed approach, an OPS-wide IT workforce strategy has not been developed. Given the CCIO's mandate, such a strategy would allow IT staff with similar skillsets to be shared amongst the CCIO and the eight IT clusters. Results from our IT survey showed that 90% of respondents believed they did not have sufficient IT resources; respondents highlighted cross-cluster collaboration and sharing of IT staff as one of the services the CCIO could provide.

Collaboration between clusters and the CCIO could allow for efficiencies and the ability to meet increased demand for IT resources. For example, the CCIO led a cross-jurisdictional team across various clusters to identify 30 OPS IT employees to provide temporary assistance in the Health Services Cluster, in support of the COVID-19 vaccination program, systems support, training, and communications functions.

No Oversight for IT Vendors Procured by Clusters for Contracts Under $2 Million

Projects within clusters that have an estimated cost of $2 million or more are reviewed by the CCIO as per its policy set by the Treasury Board Secretariat, a policy that outlines requirements to manage IT projects' lifecycle. However, below the $2 million threshold, there is no requirement for cluster staff to obtain input or

approval from the CCIO. Consequently, the CCIO is often unaware of which IT vendors were procured, whether their performance history was taken into account during the selection, and whether procurement complied with the OPS Procurement Directive. Without any awareness of these IT-related decisions, the CCIO cannot hold clusters accountable for them.

Our audit found that from April 1, 2017 to March 31, 2022, 34 IT vendors provided duplicate or similar IT services to the CCIO and the eight clusters. We noted that there was no verification of past performance prior to procurement, nor any leveraging of existing contracts.

Our audit also confirmed that the CCIO does not perform an evaluation of vendor performance for the procurements in which it is involved. In contrast, the majority (64%) of our survey respondents working in the clusters told us they did in fact evaluate vendor performance. These respondents also indicated (74%) that they did not share their evaluations with the CCIO or any other cluster. There is no central repository that records how a vendor performed which could be referenced and used by the clusters or the CCIO to determine whether that vendor should be hired again.

RECOMMENDATION 1

To ensure there is a clear alignment of operations amongst the IT clusters and so that the Office of the Corporate Chief Information Officer (CCIO) can appropriately oversee and enforce accountability of day-to-day IT operations to ensure the IT clusters effectively and efficiently deliver IT systems, we recommend that the Treasury Board Secretariat:

- work with the IT clusters and their respective ministries so that the right level of governance, oversight, and accountability is in place; and
- re-evaluate the criteria to review IT systems based on impact and risk rather than the current financial threshold of $2 million.

MINISTRY RESPONSE

The Ministry and the Treasury Board Secretariat accept the Auditor General's recommendation and are committed to ensure the right governance is in place to ensure value for money. In this regard, the Treasury Board Secretariat and Ministry will:

- work together with Clusters to review the governance structures and reporting relationship of Cluster CIOs within the context of other operational, structural and leadership considerations and take necessary action to ensure the right governance and accountability is in place; and
- re-evaluate the criteria to review IT systems based on impact and risk rather than the current financial threshold of $2 million and include this in the new Integrated Digital and IT Governance model that is being established that would govern high-risk information technology and digital solutions in the Ontario Public Service.

4.2 The CCIO Does Not Compile a List of IT Risks Across the Ontario Public Service, Nor Do They Identify IT Risks within the CCIO

As part of the risk identification process, ministries, IT clusters, and the CCIO are responsible for identifying IT-related risks for their own portfolio and reporting them quarterly to the Office of the Chief Risk Officer (Chief Risk Officer). As of August 2022, the Chief Risk Officer maintained a risk register which included 38 IT-related risks such as cybersecurity, data privacy, and aging IT systems that have been identified by the ministries and clusters. Each risk is categorized as either high, medium-high, medium or low.

We met with Ontario's Chief Risk Officer to review the IT-related risks they track for the OPS and learned that the CCIO had not identified or assessed any IT risks within its own area of operations. Also, the CCIO relied on ministries and clusters to identify IT risks. Upon review, we found that the only IT risk on the registry rated as high was a cybersecurity risk identified by our Office's 2018 audit School Boards—IT Systems and Technology in the Classroom.

In addition, we noted that clusters and ministries do not share or inform the CCIO of their respective IT risks.

Even though the CCIO has the overall responsibility for IT in the OPS (as per their mandate), it does not identify, document and communicate systemic IT risks and mitigating factors to the OPS, nor does it perform an independent assessment of these IT risks or evaluate the impact holistically on the entire OPS.

We also compared the IT risks listed in the OPS' risk register against industry standard IT risks and noted that none of the key expected risks were identified. For example, Open Web Application Security Project (OWASP), a leading non-profit foundation, publishes top cybersecurity risks that affect industries globally; none of OWASP's top 10 cybersecurity risks such as security misconfiguration, lack of encryption, and insecure design, were present on the OPS IT risk register. We noted that other key IT risks associated with aging IT systems, data security, lack of disaster recovery plans and risks associated with third-party vendors were also missing. Refer to **Sections 4.4**, **4.6**, and **4.7** for our findings on disaster recovery, cybersecurity, and IT asset management, respectively.

At the CCIO, the current risk management process is immature and lacks a formal strategy for identifying and managing IT risk. At the time of our audit, the CCIO was in the process of establishing a new framework and strategy to work with the Chief Risk Officer to identify, document and communicate IT risks to the OPS through the Enterprise Risk Management process.

RECOMMENDATION 2

To ensure IT-related risks for the Ontario Public Service (OPS) are identified, reported and mitigated appropriately, we recommend that the Office of the Corporate Chief Information Officer work with the Office of the Chief Risk Officer to:

- develop and implement an overarching strategy that encompasses all IT risks impacting the OPS;
- put in place actions to mitigate IT risks that impact OPS-wide operations; and
- periodically compare its risk register to industry standards to ensure the risks listed are relevant and up-to-date.

MINISTRY RESPONSE

The Ministry agrees with this recommendation and acknowledges the importance of identifying, reporting and mitigation of IT-related risks at an enterprise level.

In this regard, the Ministry is committed to:

- maturing its risk reporting process and working with the Office of the Chief Risk Officer to establish a new framework aligned to the IT strategy that encompasses enterprise IT risks and risks reported by the IT clusters to the CCIO;
- ensuring that the CCIO tracks all IT risks and that actions are in place to mitigate the IT risks. IT Clusters will continue to play a role in identifying and mitigating their own IT project-specific risks in support of ministries; and
- reviewing industry standards to help inform the enterprise IT risks in the risk register are relevant and up-to-date.

4.3 Ontario's Highest Rated Data Centre is Significantly Underutilized

The government's Guelph Data Centre was built with a total budget of $352 million and has been operational since March 31, 2011. It costs an average of $9 million annually to operate and is owned by the Ministry of Public and Business Service Delivery. The CCIO's ITS division is responsible for daily operations and supervision of the data centre, such as granting access to the server rooms and monitoring server capacity (storage) and availability (outages). The facility is about 250,000 square feet and the server storage area is 30,000 square feet.

The data centre was awarded a Tier IV rating—the highest standard rating for a data centre—by an independent international organization, Uptime Institute. The Tier IV rating indicates that the IT systems hosted at the certified data centre are able to withstand any type of failure: hardware, HVAC, or environmental crises such as earthquakes or fire. Guelph Data Centre

is the only data centre in all of Canada, and only one of four in North America, to receive this rating.

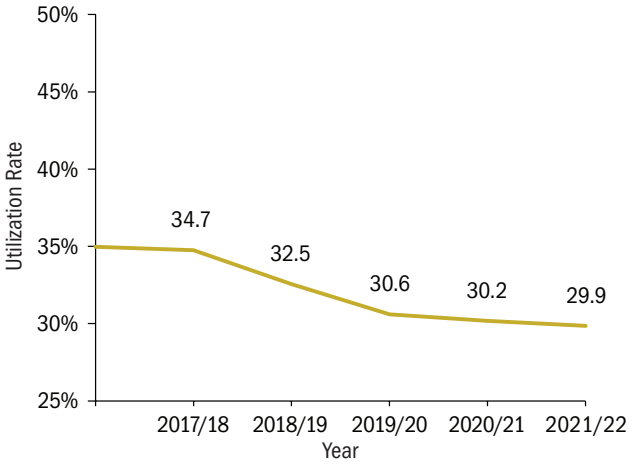
Our audit revealed that the data centre is significantly underutilized. We examined utilization reports for the last five years and noted that it has been operating at an average of only 32% of its capacity for hosting servers and databases. Utilization declined over this time frame, as shown in **Figure 5a**, and as of August 2022, the data centre was utilizing only 30% of available space. We calculated that as a direct result of underutilization, the CCIO incurred an additional $31 million, a direct loss in operating costs over five years for power, cooling, maintenance and physical security for the unoccupied space. These operating costs could have been offset by occupying the unutilized space with other government clients that would have shared in the costs. **Figure 5b** represents operating expenses for utilized and unutilized space at the data centre.

Although the data centre was built in March 2011 with the intention of only servicing the OPS, and has this capacity, there is currently minimal use from the broader public sector and Crown agencies. We noted the CCIO submitted a business case in 2012 to the Treasury Board Secretariat with the intention to leverage the new data centre for use by public sector organizations outside of the OPS by establishing a co-location service to be used by the broader public sector. However, the CCIO has not established a marketing strategy or engaged in any outreach to showcase the data centre's capabilities. At present, taxpayers are incurring costs to operate the data centre along with incurring the additional costs Crown agencies pay to private sector companies for the same services that the data centre could provide. By comparison, the government of British Columbia has mandated the use of its provincial data centre for its broader public sector, including health agencies.

We compared the data centre pricing with private sector data centres and discovered that the data centre generally charges significantly more than its private sector competitors. The standard data centre charge is approximately $75 per square foot (converted to power drawn for comparison purposes is or $1.33 kWh) usage for facility cost and resource cost which includes floor space, heating, cooling, electrical, physical security and other needs to run the facility based on their allocated space. Private sector data centres' cost structure is calculated by electricity usage based on kilowatt hour (kWh), not square foot usage. The CCIO engaged an external consulting firm, Ernst & Young, to assess the data centre's operations. The consultant determined

Figure 5a: Utilization Rate (%) of Guelph Data Centre, 2017/18 to 2021/22*

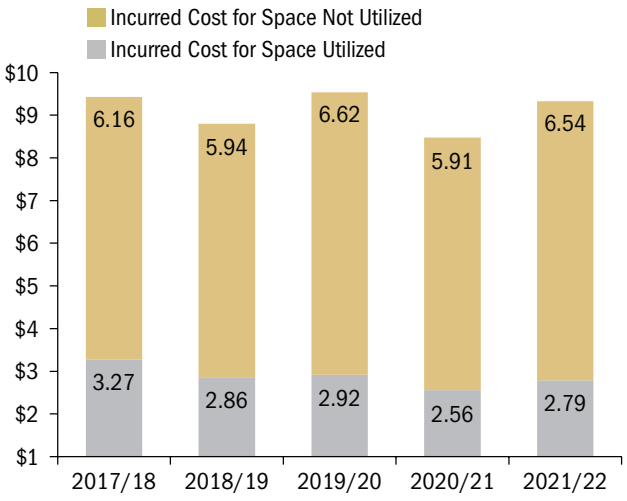
Prepared by the Office of the Auditor General of Ontario



* Utilization rate is based on the average of power (kWatt), cooling (tonnes), and physical server space.

Figure 5b: Guelph Data Centre Operating Expenses ($ million), 2017/18 to 2021/22

Prepared by the Office of the Auditor General of Ontario



that the data centre charges approximately $1.33 kWh, more than double the amount charged by other private Tier IV data centre operators. The average charge is about $0.59 kWh in other countries such as the United States, the United Kingdom, and Australia. This analysis also determined that if the data centre was operating at 100% capacity, the cost would reduce to $0.67 kWh compared to the current fee of $1.33 kWh.

In 2019, Elections Ontario moved its data hosting from Guelph Data Centre to a cloud-based data centre owned by Microsoft. We reviewed management meeting minutes and noted that the decision was made based on lower cost, flexibility to increase IT infrastructure capacity during election cycles, and the faster provisioning time to con**figure s**ervers offered by cloud providers. At present, the data centre does not have the above-mentioned capabilities.

We also noted that the Kingston data centre will be decommissioned by May 2025 and the IT systems hosted there are in the process of being moved to the Guelph data centre as well as to a third-party cloud service provider. Not all IT systems are being moved to the Guelph data centre because the CCIO wants to ensure that IT systems are able to scale capacity and disaster recovery capabilities quickly. Other challenges include a lack of standardization of IT systems in the OPS and technical skillsets. The CCIO has acknowledged these shortcomings of the data centre and is currently working on a plan to address them and increase usage of the data centre. Refer to **Section 4.3.1** for details.

4.3.1 Future of The Guelph Data Centre

Recognizing underutilization of the data centre, the CCIO engaged an external consulting firm, Ernst & Young (E&Y), in April 2021 to perform a review of the data centre's current operating model. The purpose of the review was to understand costing in data centre operations, identify any gaps, compare similar data centres that were available in the market, and provide recommendations for a future operating model that would increase utilization and generate more revenue. Three different operating models were proposed with the intent of increasing its utilization while reducing operating costs. The three options were:

- **Option 1:** Maintain status quo and continue to operate the data centre as it operates today. Develop a strategy to increase the utilization of the data centre within this operating model.
- **Option 2:** Partner with Infrastructure Ontario and the private sector to operate and manage the data centre. Explore lease or lease-sharing arrangements where the OPS would sublease 100% of the space for a fixed fee, then pay for its own usage.
- **Option 3:** Terminate the lease and sell the data centre to a vendor. The OPS would become one of the tenants of the vendor-owned data centre.

At the time of our audit, the CCIO was in the process of performing its own analysis of the three options proposed by E&Y. The analysis to determine which of the proposed options it intends to move forward with is expected to be completed by December 2022. We were informed that once its analysis is complete, the CCIO will prepare a business case that takes input from various stakeholders such as Infrastructure Ontario, Supply Ontario, Labour Relations, digital, and private consultations to assess the future operating model and will submit the business case to the Treasury Board Secretariat for review and approval of funding (depending upon the option they select) as part of its 2023/24 multi-year planning process.

4.3.2 The CCIO Does Not Have a Process to Revoke Terminated Users' Access to Guelph Data Centre for Non-OPS Employees

In our review of the data centre, we noticed that the CCIO has not established a user access review process to ensure that employees with access to the data centre have their access revoked in a timely manner upon departure from their job. The data centre and the CCIO obtain periodic attestations from those within the OPS but not from Crown agencies or those in the broader public sector. In these cases, the CCIO depends solely on Crown agencies and the broader public sector to inform them of any employee terminations.

As a result, one employee from the Liquor Control Board of Ontario who was terminated in February 2022 continued to have access to the data centre until the physical access card's expiration date in July 2022. The data centre has not established a user removal process to ensure terminated users are actively removed within 24 hours of employment termination, which is a significant process breakdown for a Tier IV data centre.

RECOMMENDATION 3

To increase Guelph Data Centre's utilization and strengthen its existing user access controls, we recommend that the Office of the Corporate Chief Information Officer:

- determine the cost recovery rate per square foot or by kWh to then perform a cost/benefit analysis of the most optimal charge out rate in order to attract and onboard more government entities;
- assess if it is feasible to mandate that the broader public sector and Crown agencies move their data centre operations to the data centre at its cost recovery rate;
- implement an outreach strategy to broader public sector and provincial agencies to increase the data centre adoption;
- review all proposed options for the future operating model of Guelph Data Centre so that the decision made is in due regard for economy and data security; and
- similar to obtaining an attestation from those in the OPS, the data centre should establish a user access review process across all agencies to ensure that user access to the data centre is removed within 24 hours of an employee's termination.

MINISTRY RESPONSE

The Ministry agrees with this recommendation to increase Guelph Data Centre's utilization and strengthen its existing user access controls and will:

- perform a cost/benefit analysis that incorporates the cost recovery rate to attract and onboard additional entities to the data centre;
- assess the feasibility to mandate broader public sector (BPS) and Crown agencies to increase the data centre's adoption;
- develop an outreach strategy for the BPS and provincial agencies to increase the data centre's adoption;
- determine a future operating model for the Guelph Data Centre with due regard for economy and data security; and
- develop an attestation process for agencies and vendors to ensure user access is removed within 24 hours of an employee termination.

4.4 Half of All Critical IT Systems Used by the OPS Do Not Have a Disaster Recovery Strategy

A Disaster Recovery (DR) strategy is an organization's plan to identify and restore critical IT systems that are essential for its operation, in the case of a disaster or interruption to services. Given the IT systems in use in the OPS, a disaster could impact public safety (in the case of emergency 911 IT systems, for example) or critical services such as health-care operations. Having a DR strategy can help to restore IT systems as soon as possible if a disaster occurs.

Our audit found that the CCIO has not developed an enterprise-wide DR strategy or policy for IT systems in the OPS. Nor has it tested its capability to restore IT operations in an event of a major outage, similar to the Rogers' outage that incurred in July 2022, discussed in **Section 4.5**. Instead, each IT cluster is responsible for developing and testing its own DR strategy, without testing the dependencies its IT systems may have on other IT systems or on the network services managed by the CCIO.

Specifically, we noted that:

- 63 of 142 (or 44%) of all mission critical systems do not have a disaster recovery plan;

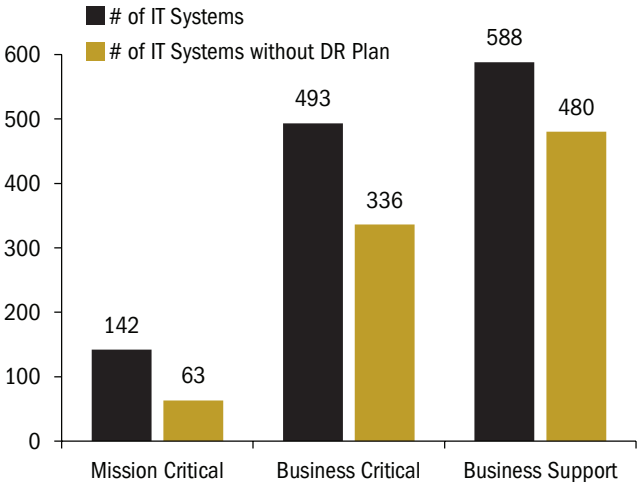
- 336 of 493 (or 68%) of all business critical systems do not have a disaster recovery plan; and
- 480 of 588 (or 82%) of all business support systems do not have a disaster recovery plan.

Refer to **Figure 6** for a breakdown of IT systems without a DR plan as of August 2022. We noted that some of these IT systems have experienced significant incidents in the past five years resulting in unplanned outages that could have been prevented had a DR strategy been in place and tested to ensure minimal disruption to IT systems. For example:

- **Emergency Health Services IT system** is used by OPS contact centres for emergency 911 services involving ambulances, hospitals and patient transfers. We noted there were 13 critical IT incidents where numerous 911 telephone lines across Ontario were impacted due to both IT hardware and software issues such as faulty network cables, power supply failures and IT equipment performance issues. This resulted in the loss of connection between the 911 systems and several Central Ambulance Communication Centres, causing delays in ambulance dispatch. On average, these incidents were resolved in 8 hours. The longest resolution time was 24 hours, whereas the target resolution time is 4.5 hours.
- **COVID-19 Patient Viewer** and **COVID-19 Vaccination Patient Portal** websites are used by Ontarians to register for the COVID-19 vaccine appointments and to view COVID-19 test results. These websites encountered 18 critical IT incidents during the pandemic, during which Ontarians were unable to make vaccine appointments or view their test results. The IT outages occurred because maintenance patches were not applied on time. On average, these incidents were resolved in 17 hours, with the longest resolution being 48 hours. The required resolution time is set at 4.5 hours.
- **Laboratory Information System** is a healthcare software used by Public Health Laboratories to maintain, process, and retain patient information associated with lab procedures and test results. We noted six critical incidents occurred due to database connectivity issues and performance issues resulting in delays to retrieve patient information. On an average these incidents were resolved in 36.5 hours compared to the required resolution time of 4.5 hours.
- **GO Secure** is used by OPS employees and contractors to access OPS IT systems securely. We found 10 critical IT incidents such as unexpected server restart and database issues prevented OPS employees and contractors from accessing OPS IT systems for an extended period of time. On an average these incidents were resolved in 12.5 hours whereas the required resolution time is 4.5 hours.

Figure 6: IT Systems Without a Disaster Recovery Plan, as of August 2022

Prepared by the Office of the Auditor General of Ontario



RECOMMENDATION 4

In order to minimize any interruptions to operations, we recommend that the Office of the Corporate Chief Information Officer:

- work with the IT clusters to develop an OPS-wide Disaster Recovery (DR) strategy and verify that all critical IT systems have a DR plan developed and in place;
- assess whether all IT systems require a disaster recovery plan on an ongoing basis;

- review and assess clusters' compliance with the DR plans on an annual basis, at minimum, and whenever there is a significant change to the OPS IT environment; and
- periodically test its ability to ensure IT systems can recover on a timely basis in a disaster scenario.

MINISTRY RESPONSE

The Ministry agrees with this recommendation and is committed to ensuring IT systems are resilient and available, minimizing any interruptions to operations, with a Disaster Recovery (DR) plan.

The DR plans are based on ministry-specific Service Level Agreements (SLA) and, as such, the Ministry is committed to:

- incorporating the IT cluster-specific DR plans into an overarching OPS-wide Disaster Recovery Strategy;
- working with ministry partners to confirm IT systems requiring a DR plan, taking into account ministry business continuity of operations plans, and ensuring that those that require a DR plan have one developed through established SLAs; and
- working with ministry partners to review clusters' compliance with DR plans and test them annually or in the event of a significant change to the OPS IT environment to recover critical IT systems on a timely basis.

4.5 The OPS Has No Backup Network Provider to Ensure Continuity of Operations for Some Critical Services

Rogers Communications (Rogers) is one of the largest telecommunications providers for the OPS and the sole network service provider for about 128 office locations, as well as telephone connectivity for 44 contact/call centres and the 56,000 cell phones used by all OPS employees. On July, 8 2022, Rogers experienced a major nation-wide outage which affected thousands of Canadians across various provinces. Rogers customers, including the OPS, were left without phone and Internet service for more than 15 hours. The outage was caused by a coding error with its network equipment, according to the company.

Since Rogers is the sole service provider of some network services for key critical OPS operations such as contact centres and mobile phones, the nation-wide outage significantly impacted these operations such that it was unable to provide Ontarians services through contact centres such as Service Ontario, COVID-19 Vaccination Patient, and social assistance payments websites. Although the majority of OPS office locations were not impacted by the outage, OPS employees who were using Rogers home Internet were unable to access the Internet to perform their day-to-day activities. The CCIO has estimated a direct loss of $500,000 in productivity as a result of these employees being unable to work. The CCIO developed a business position on what the estimated compensation could potentially be based on the impact to government business.

In addition, affected components included 11 critical IT systems, 44 contact centres, 29 ministry IT systems, 128 physical ministry locations and 56,000 cell phones used by OPS employees. Five out of the 11 critical IT systems provide emergency services such as the 911 call centre, ambulance, fire notification and critical payments to Ontarians.

Some examples of IT systems impacted by the outage were:

- Automatic Vehicle Location and mobile Computer Aided Dispatch systems are used to collect and share ambulance locations, dispatch ambulance to the emergency and transfer 911 incidents to Ambulance Dispatch Centres. These IT systems were solely dependent on Rogers services in four cities: Mississauga, Cambridge, Georgian and London. Due to the outage, ambulance dispatch centres were unable to share ambulance locations and paramedic services were unable to make operational decisions. As a work-around, dispatch centres manually tracked the ambulances using radios.

- Automated Fire Notification system is used by 911 call centres to notify fire stations in the event of an emergency. Due to the Rogers outage, fire stations were not able to receive automated fire notifications from dispatch centres. As a work-around, fire stations were contacted by telephone.
- Social Assistance Management System used by the Province to deliver social assistance payments was not able to process payments.

Forty-four call centres across the province were also disrupted. For example, Public Health Ontario and the Provincial Vaccine Contact Centre were unable to function during this time frame. Ontarians also faced issues while contacting Service Ontario customer care, as communications were down. **Appendix 6** provides a list of other OPS services impacted by the Rogers outage.

Typically, organizations would initiate their business continuity and disaster recovery plans in the case of a network outage, to ensure that critical operations are delivered with minimal interruption. Since OPS was uniquely dependent on a sole network service provider for its contact centres and mobile phones, and it did not have a backup service provider, it was therefore unable to restore operations even for those IT systems where business continuity and disaster recovery plans existed.

4.5.1 Fines Imposed for Rogers Outage Do Not Reflect the Losses Incurred by OPS

According to the existing service level agreement between the CCIO and Rogers, performance targets such as 99.9% availability of Internet connection should be maintained. This agreement has penalty clauses which stipulate fines if Rogers fails to provide the agreed-upon service levels.

The CCIO conducted an evaluation to determine the appropriate fines that it can impose on Rogers. Based on the penalty clauses in the agreement, the CCIO calculated it can impose a fine of $38,000 on Rogers. In addition, the CCIO will receive five days' worth of service credits, approximately $200,000, which Rogers has announced for all its customers. However, the CCIO has estimated a direct loss of $500,000 in productivity as a result of this outage since OPS employees were unable to work. The CCIO developed a business position on what the estimated compensation could potentially be based on the impact to government business.

Considering the financial impact to OPS as a direct result from Rogers outage, the fines imposed by the CCIO do not make up for the loss it incurred. Our audit found that the contract between the CCIO and Rogers was created in 2014 and has never been updated. The existing contract does not provide the CCIO with the ability to impose fines related to an overall network outage.

RECOMMENDATION 5

To ensure continuous operations of critical IT systems in OPS, we recommend that the Office of the Corporate Chief Information Officer:

- perform a cost/benefit analysis for acquiring a secondary, back-up network provider for its critical operations; and
- amend the existing contracts for all vendors to include a comprehensive penalty clause that could be imposed in the event that service level agreement performance targets are missed.

MINISTRY RESPONSE

The Ministry agrees with this recommendation. In response to the Auditor General's recommendations, the Ministry is committed to:

- acquiring a secondary, back-up network redundancy for Ministry-identified critical operations, including contact centres, mobility services and IT systems; and
- reflecting penalty clauses for upcoming new network contracts and renewals of existing contracts.

4.6 OPS Cybersecurity Practices Need Improvement

The CCIO's Cyber Security Division (CSD) is responsible for providing cybersecurity services to all 29 ministries

of the Ontario government. These services include monitoring for cyberattacks, performing cybersecurity assessments and scans, delivering cybersecurity training, and providing IT security-related procurement advice for cybersecurity services for the government. While the OPS has made progress in its overall cybersecurity posture, we noted it requires further strengthening to secure Ontarian's data with minimum impact to its integrity, security, and availability.

We reviewed controls related to cybersecurity assessments. Due to the nature of cybersecurity, and so as to minimize the risk of exposure for the OPS, we provided relevant details of our findings and recommendations directly to the CCIO. The CCIO agreed with the recommendation and committed to safeguarding the data entrusted to the government by the people and businesses of Ontario.

4.6.1 Sensitive Data Is Not Secured Using Encryption as Required

The CCIO has established a security standard that outlines the requirements for safely storing Ontarians' personal and sensitive information. As per the standard, any personal information collected must be retained, transferred and disposed of in a secure manner so as to protect that information against theft, loss or unauthorized use or disclosure. If personal information collected digitally is not secured through, for example, encryption, it could result in a violation of the *Freedom of Information and Protection of Privacy Act*.

We selected five IT systems used by the Ministry of Public and Business Service Delivery, the Ministry of the Solicitor General, the Ministry of Health, and the Ministry of Community Safety and Correctional Services that store sensitive and personal data of Ontarians to see if the data was being stored according to the required data security standard. We discovered that none of the five IT systems we sampled had data security controls such as encryption.

The CCIO relies on the ministries to enforce the data security requirements for the clusters and does not itself monitor compliance with them. Further, due to the existing reporting structure of clusters to their respective ministries (rather than to the CCIO), the CCIO does not enforce and monitor data security requirements on the clusters.

As part of 2021/22 Public Accounts audit conducted by the Office of the Auditor General of Ontario, we identified data security weaknesses with respect to IT general controls such as user access administration, change management and IT operations for IT systems managed by IT clusters.

RECOMMENDATION 6

To help ensure Ontarians' confidential and sensitive personal information is protected from unauthorized and accidental disclosure we recommend that the Office of the Corporate Chief Information Officer:

- enforce clusters to follow the required security standard of applying robust cybersecurity controls such as encryption; and
- monitor compliance with the security standard requiring encryption of sensitive data.

MINISTRY RESPONSE

The Ministry would like to thank the Auditor General and her staff for their recommendations to improve upon the cybersecurity program's depth in defense practices and in this regard, is committed to working with ministry partners and clusters to review and implement approaches to monitor and enforce cluster compliance with security standards including the encryption of sensitive data.

4.6.2 Insufficient Cybersecurity Awareness among OPS Staff

4.6.2.1 Majority of OPS Staff Are Not Trained on Latest Cybersecurity Practices

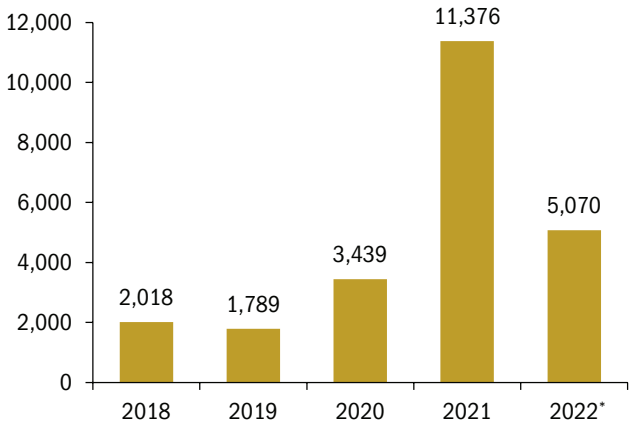
Human error is one of the largest threats to an organization's cybersecurity. According to Gartner Inc., an industry-leading research and consulting firm, in an article from April 2022, human error continues to be one of the top five security risks globally. Basic

cybersecurity awareness training is therefore crucial for employees to be able to understand and avoid exposing the data they work with to potential hackers. In 2020, the CCIO's Cyber Security Division, through its Cyber Security Centre of Excellence, developed an introductory cybersecurity course for all OPS staff to keep them informed about the risk of cybersecurity-related attacks. All full-time staff have access to an IT system called LearnON where they can take training courses designed for Ontario government employees. As of April 2022, the CCIO's mandatory "Cyber Security Basics" course, hosted on LearnON, provided an understanding of data classification and best practices such as appropriate email use, downloading external attachments or programs, and phishing avoidance. We noted:

- Based on the attendance report for "Cyber Security Basics" from 2018–2022, only 11,000 (or less than 30%) of the approximately 40,000 staff in the OPS completed the cybersecurity basics course in 2021. However, since its launch in 2020, there has been an increase in the number of OPS staff that have attended the mandatory cybersecurity training. Refer to **Figure 7** for a five-year trend of cybersecurity course attendance for all OPS staff from 2018 to 2022.
- From 2017–2022, the Cyber Security Division reported a total of 33 cybersecurity attacks, as shown in **Figure 8**. Of these 33 cybersecurity attacks, 27 were related to a phishing event, namely, an OPS employee clicked on a malicious weblink and provided their username and password. The remaining six incidents were impersonation attacks, in which an email with a malicious attachment was sent and an employee opened the attachment.
- Completion of mandatory courses is tracked by employees' managers. If an employee does not complete a mandatory course, it is their manager's responsibility to follow up to ensure they take it. We determined that the CCIO does not review any training completion reports or have awareness of course completion rates amongst OPS employees.
- The cybersecurity mandatory course provided to OPS employees does not have a due date by which the employees have to complete the training, and is also not provided on a regular basis, such as annually in accordance with industry best practices.

Figure 7: Cybersecurity Training Attended by OPS Staff, 2018 to 2022

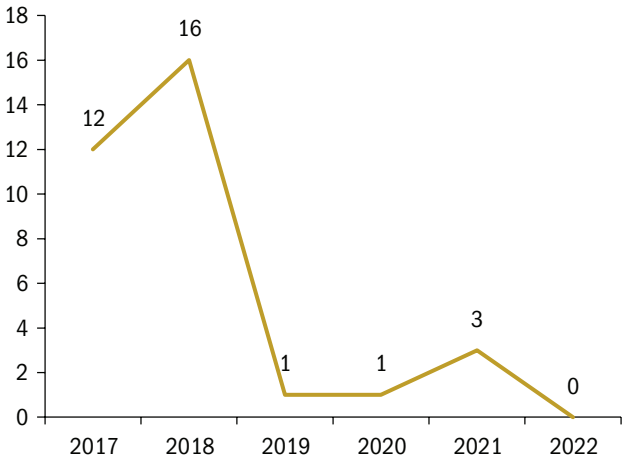
Prepared by the Office of the Auditor General of Ontario



* Data is as of July 2022.

Figure 8: Cybersecurity Attacks, January 2017 to January 2022

Prepared by the Office of the Auditor General of Ontario



4.6.2.2 Cybersecurity Training is Not Provided to OPS Contract Employees

- LearnON, the learning management system used to deliver online training to OPS employees, is accessible to full-time employees only. We noted that contract employees working for the OPS do not have access to LearnON, and as such cannot attend courses, including the "Cyber Security Basics" course.
- Yet contract employees make up a significant portion of the OPS workforce. There are about 7,000 contractors, as of January 2022, in long-term contract positions and many work in critical organizational roles such as in human resources and social services, or as health and safety consultants and correctional officers. These employees may have access to sensitive data, like their full-time counterparts. Not providing and requiring contract employees to take the Cyber Security Basics training increases the risk of cybersecurity incidents.
- The CCIO has established a cybersecurity standard, however, it did not assess risk or implement controls to protect confidential data when using personal devices. Industry best practices advise implementing controls such as prohibiting the use of personal devices. However, the CCIO is unable to identify or prevent OPS employees from using personal devices or storing confidential government data on them.
- We noted that both full-time and contract OPS employees can store OPS data on their personal USB devices (external storage). In addition, they are able to print confidential documents outside of the OPS IT network, such as at home.
- We also noted that, while the OPS has a mandatory automatic screensaver policy, about 1,000 users are exempted from this policy and either have no screensaver or have the ability to change the setting themselves. This increases the data security risk since confidential information could be viewed by an unauthorized person if the device was left unattended, a type of cyberattack known as shoulder-surfing.

RECOMMENDATION 7

To reduce the risk of human error when handling sensitive data and thereby reduce the exposure of the OPS to cybersecurity threats, we recommend that the Office of the Corporate Chief Information Officer:

- extend mandatory cybersecurity training courses to all OPS staff, including contract employees;
- review reports on mandatory course completion rates and create an escalation process for incomplete mandatory courses;
- provide cybersecurity training to all OPS staff at least on an annual basis;
- implement IT controls to restrict use of personal devices to prevent OPS employees who are working remotely from storing data on non-OPS devices; and
- enforce a screensaver policy for all users.

MINISTRY RESPONSE

The Ministry agrees with the recommendations of the Auditor General and continues to enhance its cybersecurity training and awareness program and is committed to:

- investigating the ability to extend mandatory cybersecurity training courses to contract employees;
- investigating mechanisms for ensuring completion of mandatory courses and implementing an escalation process for incomplete mandatory courses;
- implementing a policy requiring cybersecurity training to be completed by all OPS staff on an annual basis;
- reviewing and enhancing the existing IT controls to restrict the use of personal devices to prevent OPS employees who are working remotely from storing data on non-OPS devices by

documenting associated risks, and ensuring an appropriate risk treatment is in place; and

- reviewing the exemptions to the existing screensaver policy for all users by documenting associated risks, and ensuring an appropriate risk treatment is in place.

4.6.3 Ontarians' Data Used and Stored Within the Broader Public Sector Needs Better Oversight by the CCIO

Ontario's broader public sector refers to organizations that receive funding from the Ontario government but operate independently of it, such as regional school boards, hospitals, and universities. Broader public sector entities host a large amount of personal, health-related, and sensitive information, making their IT systems an attractive target for hackers. Personal and sensitive information contains data that can be used to identify an individual, such as a combination of their name, address, contact details or phone number.

Our Office reviewed publicly available news articles on cyberattacks on the Ontario government and the broader public sector from January 2018–July 2022. Over this period, there was increase in the number of cyberattacks on broader public sector agencies. There were 14 publicly available attacks, such as the ransomware attack on the Ontario Nurses' College, in which sensitive and personal data like names and financial records were compromised. A cyberattack on the Durham Region School Board IT network resulted in the Ontario Education Number, name, date of birth, address, and school location of students being stolen and leaked.

The Government of Ontario appointed a Cyber Security Expert Panel in October 2020. The panel's purpose was to identify challenges in the broader public sector and develop recommendations to improve cyber resilience across the province.

Our audit found that the CCIO does not track and is not aware of cyberattacks affecting the broader public sector; there is no centralized function to track cybersecurity incidents or breaches. This is a critical gap, since broader public sector entities such as school boards, colleges and hospitals store large amounts of Ontarians' data.

Currently, the Cyber Security Division's Centre of Excellence hosts monthly calls that are available for all individuals employed in the broader public sector, where they can learn about emerging cybersecurity trends and best practices. However, in the past five years, the Cyber Security Division has been engaged only 15 times by broader public sector entities for cybersecurity scanning and testing even though there are over 200 broader public sector organizations in the province.

RECOMMENDATION 8

To assist in responding to cyberattacks and increase engagement for preventative best practices for broader public sector entities that face cyberattacks, we recommend that the Office of the Corporate Chief Information Officer establish a Memorandum of Understanding with the broader public sector to share detailed reports of cybersecurity incidents and communicate about how to remediate any weaknesses.

MINISTRY RESPONSE

The Ministry agrees with the recommendations of the Auditor General and welcomes the opportunity to build upon its efforts to help modernize cybersecurity across the Ontario public sector. As part of the 2023–26 Cyber Security Strategy, the Ministry will be evaluating opportunities to strengthen broader public sector (BPS) partnership through the Strategy that includes establishing a framework to work with the BPS to share detailed reports of cybersecurity incidents and communicate about how to remediate any weaknesses as part of its go-forward cybersecurity strategy.

4.6.4 Cybersecurity Risks for Vendor IT Systems Are Not Assessed

As of August 2022, the CCIO used 140 IT vendors to manage IT services and systems on behalf of the OPS that are essential to the continuity of government programs and operations. We requested a list of the assurance reports being received and reviewed by the CCIO about these service providers. The CCIO was unable to provide us with any Service Organisation Control reports since it does not obtain and review third-party assurance reports to identify cybersecurity vulnerabilities and IT weaknesses. As a result, it is unable to assess the potential impact to its business operations and is unaware of the risks to which it is exposing Ontarians. Third-party assurance reporting is a crucial source of information for identifying any IT risks and weaknesses including cybersecurity risks.

In addition, we noted that the CCIO was not aware if any of the service providers contracted by the IT clusters were storing Ontarians' data outside of Canada, something which would violate provincial privacy and data security requirements related to the collection, retention, and disposal of sensitive information.

RECOMMENDATION 9

To identify any risks that Ontario government data may be exposed to, we recommend that the Office of the Corporate Chief Information Officer:

- establish a centralized process to mandate the receipt and review of third-party assurance reports from vendors that host or use OPS data;
- review IT weaknesses identified in third-party assurance reports to assess the impact to OPS operations and take corrective action where necessary; and
- work with IT clusters to identify any vendors that store data outside of Canada, assess the risk and take corrective action if that storage violates requirements related to the collection, retention, and disposal of sensitive information associated with storing data outside of Ontario.

MINISTRY RESPONSE

The Ministry agrees with the recommendations of the Auditor General and recognizes the importance of identifying risks that Ontario government data may be exposed to. Today, security assessments are conducted as part of OPS vendor procurement practices, where security terms and conditions are reflected in contracts to ensure ongoing protection of government data and any data residency requirements.

In this regard, the Ministry is developing a refreshed Cyber Security strategy where vendor management will be a component. The strategy will include a commitment to:

- establishing processes to mandate the receipt of third-party assurance reports;
- review any weaknesses identified in third-party assurance reports and their impact to OPS operations and take corrective actions to mitigate the risk; and
- working with the ministries and IT clusters to identify any vendors that store data outside of Canada and take corrective actions to mitigate the risk.

4.7 Ontario Government's IT System Inventory is Incomplete and Inaccurate

A current and complete IT asset inventory is important for any organization to ensure its IT assets are accounted for, maintained, and appropriately disposed of. Asset inventories also serve to identify aging IT and when IT security controls are needed.

As the CCIO is responsible for the purchasing of all Government of Ontario IT assets, it uses the Configuration Management Database (CMDB) to track and monitor all IT assets. The CMDB includes information for IT systems such as Transfer Payment Ontario and the Social Assistance Management System used by Ontarians to apply for and receive social assistance.

Figure 9: Critical Data Attributes Not Listed in Configuration Management Database

Prepared by the Office of the Auditor General of Ontario

Data Attribute	Description	# of IT Systems with Missing Data Attributes
Data storage technology	Location where the data is stored (OPS data centre or cloud)	179
Hosting costs	Annual hosting costs across all environments	145
Supports legislated function	Indicates whether the IT system supports any legislative or compliance function such as inspection, investigation, enforcement	141
Licensing cost	Licence fees or any non-hosting related costs	115
Privacy Impact Assessment completed	Indicates whether a Privacy Impact Assessment has been completed	51
Threat Risk Assessment completed	Indicates whether a Threat Risk Assessment has been completed	47

The CMDB typically includes details such as the IT system's name, criticality, owner (accountable person), the associated ministry (primary user) and the IT cluster responsible for servicing it.

We obtained a data extract from the CMDB for all IT systems. From a total of 1,212 IT systems being tracked and monitored, we noted that, although the inventory is being tracked, the database is incomplete. It does not have all relevant and critical information about each IT system recorded. See **Figure 9** for a list of key data attributes missing from CMDB.

In addition, we found that the current process to review the CMDB lacks thorough, frequent, and consistent criteria-based reviews to verify or ensure that information stored there was accurate and complete or current. Although the CCIO's asset management team undertakes informal reviews to identify outdated and missing data within the CMDB, the reviews are not performed with any frequency or defined criteria. As a result, the CCIO does not have an accurate recording of the assets' ages.

The Ontario Internal Audit Division issued an audit report in October 2021 regarding outdated IT systems in the OPS. The audit report concluded that 23.5% of all IT systems in the OPS have aged and as a result are out of vendor support. Because this recent audit was performed by Internal Audit, we excluded an assessment of the age status of IT systems in the OPS from our scope of work. The CCIO was in the process of acting upon Internal Audit's report and recommendation, which was to update the IT inventory for an estimated completion target of early 2023.

RECOMMENDATION 10

To improve the accuracy and completeness of the IT system inventory and to more easily identify aging IT systems, we recommend that the Office of the Corporate Chief Information Officer:

- develop a guideline for all employees that outlines a process to update the Configuration Management Database using a defined set of criteria;
- complete any empty, mandatory fields in the Configuration Management Database; and
- perform a systematic review of the database on an annual basis and whenever a system is onboarded or retired.

MINISTRY RESPONSE

The Ministry agrees with this recommendation and is committed to improving the accuracy and completeness of the IT system inventory and to more easily identify aging IT systems. In this regard, the Infrastructure Technology Services division will work with the Enterprise Technology Strategy division and Clusters to:

- enhance the existing process for its staff so that the Configuration Management Database is updated using a defined set of criteria;
- review and populate mandatory fields in the Configuration Management Database for IT systems; and
- develop a systematic, annual review process, or whenever a new system is onboarded, for Clusters/IT system owners to identify missing data, update, and report on completeness.

4.7.1 Not all Software Licenses Are Managed or Accounted For

A complete and accurate register of all software licenses and installed software is helpful for an organization to effectively procure, manage, and terminate licenses as needed. It is part of an effective asset management process to avoid costs of any unused surplus software licenses, manage the licenses needed to continue operations, and detect and avoid the use of pirated software.

We noted that the CCIO does not have a process to effectively and efficiently manage the software licenses for all IT vendor systems. At present, software licenses are being managed using a central tracking system called Snow. As of August 31, 2022, the CCIO has enrolled only three vendors (Oracle, IBM, and Microsoft) in order to track software licenses and utilization. However, it does not track utilization for the remaining 137 IT vendors for which it has procured a software license. As a result, the CCIO does not currently have an inventory of any other software licenses installed on employee workstations and their associated costs and usage.

We also noted that there is no process at the CCIO to appropriately reconcile the number of licenses purchased to the fees being paid to vendors for these licenses. The CCIO relies on the vendors to perform their own audits of the number of licenses purchased and is unaware, then, and does not do any work to determine if there are any potential underpayment or overpayment to vendors for software licenses.

RECOMMENDATION 11

To ensure a robust software license management process and avoid underpayment or overpayment to vendors, we recommend that the Office of the Corporate Chief Information Officer:

- onboard its key IT systems into its software asset management system so that it is able to track utilization to assess optimal and economical use of resources;
- adopt a process to verify and confirm the licenses on hand match the fees being paid to vendors; and
- perform regular audits of installed software to identify the need to purchase or retire software licenses.

MINISTRY RESPONSE

The Ministry agrees with this recommendation and is committed to:

- continuing to expand the utilization of a software asset management tool to onboard other key software vendors into its software asset management system; and
- ensuring processes are in place to verify and validate license entitlements and correct payments made to vendors, and to assist in audits of installed software when required.

4.8 Insufficient Due Diligence When Hiring IT Consultants

The CCIO hires all contract IT consultants via a single recruitment service provider, Flextrack, and has paid approximately $16 million to Flextrack from 2020/21–2021/22. In addition, the ministries and clusters have paid Flextrack approximately $146 million over this period to procure contractors for non-IT and IT roles. We selected a sample of 30 IT consultants from a total list of 244 consultants working for the CCIO during the period April 1, 2021–April 2023. For each employee, we reviewed the business justification to hire a contract employee, internal capability assessments, interview notes and scoring evaluation sheet, timesheet

approvals by supervisors and approved timesheets are sent to Flextrack. According to the OPS Procurement Directive, before requesting external consulting services, an organization must first consider its internal human resources and provide a rationale for hiring contingent staff. The internal capability assessment involves performing a cost/benefit analysis to evaluate the relative cost of hiring a consultant compared to hiring a full-time equivalent employee for the role.

Capabilities Assessments Were Not Performed Prior to Hiring Consultants, Resulting in Higher Costs

We reviewed hiring request forms and briefing notes submitted by the CCIO to the Treasury Board Secretariat for 30 IT consultants. The CCIO did not perform an internal capability assessment for 28 of the 30 roles. For the two roles where an assessment was performed, we calculated that hiring a full-time equivalent employee was cheaper on an annual basis than hiring a consultant. For example, the cost of hiring a consultant for the role of IT Quality Assurance Specialist was approximately $132,000 compared to the full-time employee's annual salary of approximately $86,000. The CCIO told us it hired a consultant because there were no full-time resources available internally.

We also noted that the CCIO did not perform an assessment to determine if hiring a full-time employee was more cost-effective than hiring a consultant. In another example, the CCIO ended up hiring two IT consultants for the role of IT Developer with a contract cost of approximately $403,000 for one year for both. The assessment noted that the cost to hire two full-time employees was approximately $248,000, excluding approximately 22% of the gross salary allocated to benefits.

We also noted that consultants' performance evaluations were not reviewed. The consultants' job performance had no bearing on whether or not they would be awarded another contract.

Consultants Were Paid Above Recommended Rate

The OPS People Placement Service Manual created by the Treasury Board Secretariat recommends that consultants be paid in accordance with the planning market rate card table developed for the manual. Pay rates are determined by a number of factors such as job title and responsibilities.

We compared the daily pay rate recommended on the planning market rate card table to the actual rates paid to all 244 IT consultants hired by the CCIO since April 1, 2021. We noted that 25 of these employees were approved for pay rates above the recommended level. No rationale or justification was provided by the CCIO for providing a higher pay rate. In addition, 25 consultants from a total of 244 were paid an average of $86 above the daily rate recommended. For example, one IT consultant was paid $1,199 per day although the recommended daily rate was $967 per day, a difference of $232, for a total additional cost of $51,736 for the contract duration of seven-and-a-half months. In total, for these 25 contractors, the CCIO paid approximately $470,000 more than the Treasury Board Secretariat recommended.

Interview Evaluation Process Needs Improvement

The interview assessment is a critical aspect of the process to select consultants, as it allows for the assessor to evaluate the candidate against the selection criteria. Candidates that are scored higher than 70% on their resume are granted an interview.

However, we noted that there is no requirement for a minimum number of candidates to be interviewed during the interview stage. This resulted in scenarios where there was only one candidate interviewed for the IT contract position, as occurred with four of the 30 consultants from our sample. We also noted that this contract position is a highly demanded role in organizations and typically receives a high number of applicants when a position is posted.

According to the People Placement Service Manual, competitors for contract positions should be interviewed by at least three full-time equivalent evaluators. For eight of the 30 employees in our sample, their interview was performed by two evaluators only.

Finally, we noted that 21 of 30 (70%) interviewers had no interview notes/comments captured in their scoring worksheet or within the VMS. There is no requirement to capture interview notes within the VMS

IT system. We also noted that 6 of 30 (20%) interviewers provided very limited interview notes.

RECOMMENDATION 12

To ensure that consultants are procured with the necessary due diligence and to maximize value for money, we recommend that the Office of the Corporate Chief Information Officer:

- ensure that when procuring additional services cost/benefit analyses are performed and the option of hiring a full-time employee is considered;
- pay consultants within the recommended rate ranges set out by the People Placement Service Manual, and that any deviation or exception from the Manual be formally documented and approved by the Office of the Corporate Chief Information Officer;
- ensure a minimum of two candidates, per position, are interviewed by at least three evaluators; and
- formally document and retain interview notes within the IT system.

MINISTRY RESPONSE

The Ministry would like to thank the Auditor General and her staff and agrees with the recommendation and is committed to improving its practices and to enhancing transparency and accountability.

In this regard, the Ministry is committed to:

- implementing a consistent approach to enable a review of capacity and resourcing options prior to procuring IT consultants. IT consultants will be hired in line with the recommendation, by the Treasury Board Secretariat planning market rates where it is possible;
- ensuring that the appropriate level of approval is obtained and documented to support exceptional cases; and
- reviewing the rules, controls, and best practices supporting the interviewing and selection process when hiring IT consultants. Specifically, it will be ensured that a minimum of two candidates, per position, are interviewed by at least three evaluators; and that the interview notes are formally documented and retained within the IT system.

4.9 IT Incident Resolution Targets Are Outdated

The CCIO has established an IT incident classification process that distinguishes the priority of an incident, ranging from those with the most significant impact ("critical") to those with the least impact ("low"). The CCIO considers critical incidents to be those that could result in customer data loss, security breaches or customers being unable to access client-facing webpages.

Our Office reviewed IT incident data from April 2017 to March 2022 and noted a total of 2,057,917 incidents occurred for all IT systems at the OPS. These incidents were logged within Remedy, the IT system used by different IT clusters in the OPS to view and resolve IT incidents. When an IT incident is resolved within the time frame defined by the applicable service level agreement, it is marked as "met" within the Remedy IT system. Incidents that are resolved outside of the time frame of the service level agreement are marked as "missed." See **Figure 10** for a breakdown of the 2,057,917 incidents by priority level, along with the percentage of IT incidents that met the agreed-upon resolution time. We noted there were 803 priority critical IT incidents.

4.9.1 The CCIO's Compliance Targets to Resolve IT Incidents Are Outdated

The CCIO has a compliance target of 90% for all service delivery tickets relating to IT incidents based on target time frames for business critical, mission critical, and business support systems. **Figure 11** indicates the target resolution times required for IT incidents by IT system classification.

The CCIO's compliance target of 90% was established in 2016 and has not been revaluated since then. Further,

Figure 10: Number of IT Incidents by Priority Level and Percentage Resolved, April 2017 to March 2022

Prepared by the Office of the Auditor General of Ontario

Priority Level	Number of Incidents	% Resolved (CCIO)[1]	% Resolved (OAGO)[2]	% Resolved (OAGO)[3]
Critical	803	73.2	66.5	47.8
High	4,215	86.8	85.8	75.8
Medium	905,316	93.4	93.4	83.1
Low	1,147,583	96.6	96.6	92.5
Total	**2,057,917**	**95.2**	**85.6**	**74.8**

1. Percentage resolved as calculated by CCIO's IT incident ticketing system (Remedy)
2. Percentage resolved as calculated by OAGO by comparing the IT incident ticket logged time against the resolved time
3. Percentage resolved as calculated by OAGO by comparing the IT incident ticket logged time against the resolved time, excluding any pending time

Figure 11: Target Resolution Times for Types of IT Incidents

Prepared by the Office of the Auditor General of Ontario

IT System Classification	Priority Critical Incident	Priority High Incident	Priority Medium Incident
Mission Critical[1]	4.5 hours	1 day	5 days
Business Critical[2]	4.5 hours	1 day	10 days
Business Support[3]	No time limit	1 day	15 days

1. **Mission Critical**: Used for solutions only where failure may i) cause harm to the health of Ontarians, and/or ii) endanger Ontarians' lives or create safety hazards, and/or iii) reduce government's revenue generating capacity, and/or iv) prevent critical payments.
2. **Business Critical**: Used for solution only where the solution i) supports the government's priorities, and/or ii) demonstrates a direct link to mission critical systems, application, infrastructure, and/or iii) demonstrates that failure will threaten mission critical projects, and/or iv) supports government's stewardship role.
3. **Business Support**: Used only where solutions are critical to the operation of a business unit or department, but are not directly essential to the delivery of a public program or service. Its scope is limited to a smaller business unit than Business Critical.

the CCIO's service targets are set lower than industry best practice. For example, an IT incident with a critical status should be resolved within 1–2 hours, whereas the CCIO's target is set at 4.5 hours.

4.9.2 IT Incident Resolution Targets Missed

Using data analysis, we re-evaluated the 2,057,917 IT incidents to assess if they were resolved as per the 90% compliance target defined by the CCIO and in the time frame specified by the service level agreements. **Figure 10** provides a breakdown of incidents by priority level and percentage of resolution reported by the CCIO and the Office of the Auditor General of Ontario (OAGO). We noted that the CCIO reported an overall compliance of 95% for all IT incidents in the past five years. However, based on our review and analysis, the overall compliance was, in fact, 85% for all IT incidents. This 10% discrepancy is due to the fact that CCIO calculates the compliance rate using the elapsed time, which is the time spent by the technician to resolve the incident ticket, whereas for our calculation, we compared the time when the incident ticket was created against the time when it was closed. Further, we noted that the compliance rate for IT incidents with the most significant impact ("critical") was 66%.

In addition, we also noted that the CCIO's reported compliance of 95% includes "pending" time, that is, the time when IT incident tickets are put on hold, as they are awaiting confirmation from the employee or affected users to validate whether the IT incident has been resolved. We noted that out of 2,057,917 IT incidents 418,145 (20%) were marked as pending status before these tickets were resolved. We also noted that there is no process in place to verify that all 20% of tickets require a justified pending time, since the system

does not capture this level of detail in the audit logs. We performed another analysis which excluded the pending time, and noted that the overall compliance of IT incidents dropped to 75%. Refer to **Figure 10**.

RECOMMENDATION 13

To efficiently restore IT services with minimal interruption to Ontarians, and to accurately calculate and report on compliance with service delivery targets, we recommend that the Office of the Corporate Chief Information Officer:

- re-assess its compliance targets to ensure they are in accordance with industry standards;
- review the calculation of incident resolution time to ensure it aligns with industry best practices; and
- put in place remedies to improve the time taken to restore IT services.

MINISTRY RESPONSE

The Ministry agrees with this recommendation and is committed to:

- identifying enhancements to service delivery targets for critical systems and high priority incidents, based on the industry scan findings;
- reviewing and updating Incident Resolution Time to ensure metrics and reporting align with industry best practice; and
- implementing any changes to existing service delivery targets for the fiscal year 2025/26.

Appendix 1: Glossary of Acronyms

Prepared by the Office of the Auditor General of Ontario

Term/Acronym	Definition
CAC	Central Agencies Cluster
CCIO	Office of the Corporate Chief Information Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMDB	Configuration Management Database – IT system used to track IT asset-related information such as name, user, and deployment date.
CTO	Chief Technology Officer
CVOR	Commercial Vehicle Operator Registration – automated IT system used to store information about large vehicle carriers
DR	Disaster Recovery
ERM	Enterprise Risk Management
ETD	Enterprise Technology Delivery
ETS	Enterprise Technology Strategy
FTE	full-time equivalent
GSIC	Government Services and Integration Cluster
HSC	Health Services Cluster
IRP	International Registration Plan
IT	information technology
ITQF	Information Technology Qualified Firms
ITS	Infrastructure Technology Services
MTO	Ministry of Transportation
OCL	Office of the Children's Lawyer
OPAC	Ontario Police Arbitration Commission
OPS	Ontario Public Service
PIA	Privacy Impact Assessment
PRIO	Permitting and Registration for International Registration Plan and Oversize/Overweight
TRA	Threat Risk Assessment
VMS	Vendor Management System – processes and maintains vendor-related documents

Appendix 2: Individuals Overseeing the Eight IT Clusters, as of September 2022

Prepared by the Office of the Auditor General of Ontario

Cluster	Chief Information Officer or Assistant Deputy Minister	Deputy Minister	Minister
Community Services	Soussan Tabari	Nancy Naylor	Stephen Lecce
Children, Youth and Social Services	Alex Coleman	Denise Allyson Cole	Merrilee Fullertone
Health Services	Angela Copeland	Catherine Zahn	Christine Elliott
Justice Technology Services	Catherine Emile	David Corbett	Douglas Downey
Land and Resources	Rocco Passero	Monique Rolf von den Baumen Clark	Gregory Rickford
Labour and Transportation	Roman Corpuz	Douglas Jones	Caroline Mulroney
Central Agencies	Liz Mackenzie	Deborah Richardson	Prabmeet Sarkaria
Government Services and Integration	Manish Agarwal	Renu Kulendran	Kaleed Rasheed

Appendix 3: High-level Responsibilities of the Office of the Corporate Chief Information Officer as Compared to the Clusters

Prepared by the Office of the Auditor General of Ontario

Services	CCIO	Clusters
Cybersecurity	Performs security-related scans and incident responses for: 1. Threat Risk Assessments 2. Cybersecurity Scans 3. Vulnerability scans 4. Incident Response	Identify applicable IT systems and request cyber scans and assessments
Asset Management	ITS manages, tracks, and distributes physical assets such as laptops and servers	Request new hardware and work with ITS to get required assets
IT Service Delivery	Sets goals and compliance targets for service delivery for entire OPS	Incident management teams work within the cluster and report performance metrics to CCIO
Vendor Management	Manages enterprise-level vendor contracts like Compucom, TELUS	Procure vendors with the help of their own contract managers

Appendix 4: Highest Recommended Daily Pay Rates for IT Contractors, as Established by Treasury Board Secretariat

Prepared by the Office of the Auditor General of Ontario

Role	Recommended Daily (per diem) Rate ($)
Program Manager	1,015.00
Project Manager/Leader	983.00
Application Architect	967.00
Technology Architect	967.00
Privacy Impact Assessment (PIA) Specialist	966.00
Automation Solution Consultant	954.00
Business Architect	954.00
Solutions Designer	940.00
DevOPS/Cloud Engineer	936.00
Business Intelligence Specialist	925.00

Appendix 5: Audit Objective and Criteria

Prepared by the Office of the Auditor General of Ontario

Audit Objective

The objective of this audit is to assess whether the Office of the Corporate Chief Information Officer has effective IT systems and governance in place to ensure:

1.	A governance framework is implemented that encompasses an overall IT strategy that demonstrates effective oversight of IT functions to deliver IT services to the Ontario Public Service and Ontarians efficiently and effectively.
2.	IT operations and systems are effectively monitored in accordance with established performance metrics and corrective actions are taken upon review.
3.	Ontarians' data and IT assets including hardware and software are secure, reliable and protected against cyberattacks.
4.	IT resources including IT vendors are procured in accordance with legislative, regulatory and contractual requirements with due regard for economy.

Audit Criteria

1.	Effective governance framework with adequate oversight of IT operations, strategy and accountability with clear roles and responsibilities are in place to achieve IT strategic objectives and goals.
2.	Appropriate IT performance measures and targets have been defined, approved and a monitoring process is in place to evaluate IT performance and services provided to the the Ontario Public Service and report regularly.
3.	Cybersecurity IT systems and controls are in place to detect, prevent and mitigate anomalies and threats to OPS operations in a timely manner including the safeguarding of legislatively protected, personal identifiable and OPS sensitive data.
4.	Processes are in place to ensure procurement is managed economically in accordance with applicable regulations and vendor performance is monitored for satisfactory delivery of goods and services.

Appendix 6: List of OPS and Crown Agencies and Related Public Services Affected Due to Rogers Outage, July 8, 2022

Prepared by the Office of the Auditor General of Ontario

Service/Organization	Description	Impact
Agrisuite GoCloud	IT system used by farmers and agricultural consultants	Website was not available
Attorney General	To contact the Ministry of the Attorney General	Phone line was not available
Child Empanelment Portal	Interact with OCL to access case information and submit information relating to Child (Core) IT system	Website was not available
Drivers Medical Review (DMR)	The DMR program reviews drivers with medical conditions and driver fitness assessments based on legislated MTO policies.	Website was not available
Hospitals	Many hospitals were affected by the outage. Hospitals had difficulty reaching staff who were at home, causing longer wait times at hospitals. Additionally, hospitals have difficulty contacting family members, and health systems partners (such as long-term-care facilities).	Website and phone communications were not available
Metrolinx and GO Transit	Public transportation services in the Greater Toronto Area	Some locations and fares could not be purchased using debit or credit. E-tickets were unavailable for purchase.
Ministry of Transportation 511 website	Access to road information	Website was not available
MTO iCorridor	iCorridor is a map-based data visualization and information sharing tool to increase understanding of historical, real-time, and forecast information in transportation and land use planning.	Website was not available
MTO Online Carrier Records	Public portal to access their CVOR Record online	Website was not available
MTO Technical Consultation Portal	Provides an IT system used by MTO and its vendor	Website was not available
MyBenefits	Social Assistance recipients unable to access their accounts	Website was not available
Office of the Premier	To contact the premier	Phone line was not available
Ontario Lottery and Gaming Corporation	Gaming services for Ontario public	Lottery ticket purchase was not available
Ontario Pension Board Client Care Centre	Contact centre used for general inquiries	Longer than normal wait times for call centre
Ontario Police Arbitration Commission (OPAC)	The OPAC website allows for a search into collective agreements, interest and rights disputes and related content around the conciliation and mediation arbitration process under the *Police Services Act.*	Website was not available

Service/Organization	Description	Impact
Permitting and Registration for IRP/OO (PRIO)	Permitting and registration for Ontario-based commercial carriers for inter-jurisdictional travel in Canada/US/Mexico	Website was not available
Public Health Unit Locator	Geographical search for the health unit that governs the user's area	Website was not available
The Toronto District School Board	Students and staff in remote learning summer sessions	Online learning not available; participants had to switch to asynchronous learning
Tribunals Ontario (Landlord Tenant Board)	Contact line to speak to a customer service officer	Phone line was not available
Volunteer Corps Ontario	Inquiry with contact centre for Volunteer Corps Ontario	Phone line was not available

Office of the Auditor General of Ontario

20 Dundas Street West, Suite 1530
Toronto, Ontario
M5G 2C2

www.auditor.on.ca

ISBN 978-1-4868-6517-8 (PDF)