

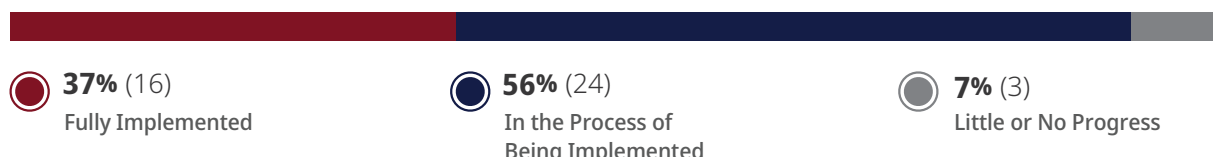
## Follow-Up on the 2022 Performance Audit:

Ministry of Public and Business Service Delivery  
and Procurement

# Office of the Corporate Chief Information Officer

## // Overall Conclusion

### 43 Recommended Actions



The Ministry of Public and Business Service Delivery and Procurement, as of August 20, 2024, has fully implemented 37% of actions we recommended in our 2022 audit of the **Office of the Corporate Chief Information Officer**. The Ministry has made progress in implementing an additional 56% of the recommended actions.

The Ministry has fully implemented recommendations such as acquiring a secondary, back-up network provider for its critical IT operations, ensuring a minimum of two candidates are interviewed by at least three evaluators for each IT consultant position and reassessing its compliance targets to ensure they are in accordance with industry standards.

The Ministry has made progress on recommendations such as enforcing IT clusters to follow the required security standard of applying robust cybersecurity controls, such as encryption, and extending mandatory cybersecurity training courses to all OPS staff, including contract employees.

However, the Ministry has made little progress on 7% of the recommendations, including assessing whether all IT systems require a disaster recovery plan on an ongoing basis, and reviewing and assessing IT clusters' compliance with the disaster recovery plans at least annually, and whenever there is a significant change to the OPS IT environment.

The status of actions taken on each of our recommendations is described in this report (see **Appendix** for more details).

## // Status of Actions Taken on Recommendations

We conducted assurance work between March 2024 and August 2024. We obtained written representation from the Ministry of Public and Business Service Delivery and Procurement that effective October 15, 2024, it has provided us with a complete update of the status of the recommendations we made in the original audit two years ago.

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

In our audit, we found that IT clusters report to their respective deputy ministers, not to the Office of the Corporate Chief Information Officer (CCIO). As a result, 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 IT cluster systems.

#### Recommendation 1: Action Items 1 and 2

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.

Status:  In the process of being implemented by January 2025.

#### Details

We found that in April 2023, CCIO redefined job responsibilities for Chief Information Officers (CIOs) of IT clusters through a competency model. These new competencies include a requirement for CIOs to identify opportunities for cross-ministry collaboration such as sharing of performance scorecards for IT vendors to assist in future procurements. In addition, throughout 2024, the Treasury Board Secretariat (TBS), in collaboration with IT partners, continued work to refresh the IT project gateway policy, including updating the review process for IT projects based on impact and risk. This updated review process requires input and communication from IT partners,

including CCIO, the IT clusters and the corporate architecture group, and redefines the roles and responsibilities for each. The refreshed policy is pending submission to and approval by the Treasury Board and Management Board of Cabinet by January 2025.

We reviewed feedback TBS had received from the clusters on the policy refresh and noted that criteria such as project significance or overall risk will be considered alongside the existing \$2 million threshold (financial risk). The policy also provides guidance for projects valued at less than \$2 million.

## 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

In our original audit, we found that CCIO does not have an overarching strategy across the OPS to identify enterprise IT risks and implement mitigation and remediation strategies.

### Recommendation 2: Action Items 1 and 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;

Status:  In the process of being implemented by March 2025.

### Details

We found that in February 2024, CCIO had developed a plan to establish a timeline and action plan to modernize mission-critical IT systems to address IT risks at the individual system level. We reviewed the modernization plan and noted that it considers application support, infrastructure support and likelihood of failure, and identifies an investment plan for any upgrades or modernizations required. While this plan, to be implemented by March 2025, will help address IT system-specific risks, it is not expected to directly mitigate or help identify IT risks that could be applicable at the cluster level or OPS-wide, a problem noted in our 2022 audit. However, these IT system-specific risks, once identified and consolidated will be used as an input to identify and mitigate OPS-wide IT risks.

### Recommendation 2: Action Item 3

- periodically compare its risk register to industry standards to ensure the risks listed are relevant and up-to-date.

Status:  In the process of being implemented by December 2024.

### Details

We found that CCIO has conducted an analysis of the existing risk register, which logs all operational and IT risks identified by ministries. Through this analysis, CCIO noted that several IT risks in the risk register were incorrectly or insufficiently categorized under operational risk categories, as there was no standalone category for IT-related risks. It also found that IT risk has not been thoroughly defined for the OPS to appropriately identify, report and mitigate IT risks.

CCIO has used a globally accepted industry framework, the Information Systems Audit and Control Association's (ISACA's) Risk IT Framework, to map the existing IT risks on the risk register to four sub-categories of IT risk and provide a standardized methodology for identifying, reporting and mitigating these risks. However, CCIO still needs to engage the Office of the Chief Risk Officer (OCRO) to communicate this new approach to enterprise IT partners across the OPS and develop an action plan to mitigate already existing IT risks and identify new IT risks using the ISACA framework, which it is planning to complete by December 2024. Other than updating the categories of IT risks, CCIO did not compare its existing IT risk register to industry standards to compare and identify new IT risks.

## 3. Ontario's Highest Rated Data Centre is Significantly Underutilized

In our original audit, we found that Ontario's primary data centre was only 30% utilized, even though it has been awarded the highest rating available, indicating that its IT systems are able to withstand any type of failure. Usage had declined over the prior five years, during which time a \$31million loss was incurred for operating costs for the unoccupied space for power, cooling, maintenance and physical security.

### Recommendation 3: Action Item 1

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;

**Status:**  **In the process of being implemented by December 2024.**

### Details

We found that CCIO did not perform a cost/benefit analysis but instead engaged Infrastructure Ontario in August 2023 to perform an assessment of the Guelph Data Centre's (GDC's) utilization and to propose a future operating model. The assessment included feedback from the broader public service (BPS) and Crown agencies, other provincial governments, as well as private sector entities. The main reasons identified in the assessment for low utilization were the increased use of cloud solutions by BPS and Crown agencies, and a lack of interest or need for a Tier IV data centre and the associated premium cost of using one. At the time of our 2022 audit, we noted that the GDC was rated a Tier IV data centre, the highest possible rating for a data centre, indicating it can withstand any type of failure.

The assessment by Infrastructure Ontario proposed three options to address low utilization. One was to re-engineer the Tier IV GDC to a Tier III facility, which would reduce the need and cost of additional infrastructure to maintain the facility, thereby reducing the charge out rate for using the data centre. This would, in turn, reduce the cost to BPS and Crown agencies to onboard and use the facility. Another proposed option was to legally mandate BPS and Crown agencies to use the GDC. However, the assessment noted that many BPS and Crown agencies have either moved to cloud solutions or have expressed a desire to maintain their own data centres. The third proposed option was to sell part of the GDC and enter into a hybrid arrangement with other entities such as municipalities. CCIO and the Ministry of Public and Business Service Delivery and Procurement are expected to make their decision based on these options by December 2024.

### Recommendation 3: Action Item 2

- 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;

**Status:**  **Fully implemented.**

## Details

We found that, as part of the assessment conducted by Infrastructure Ontario, one of the options considered was to legally mandate BPS and Crown entities to move their data centre operations to the GDC. The assessment noted that, while technically feasible, a mandated move would be unlikely to be approved by Treasury Board due to the low demand and high cost for BPS and Crown entities, making it the least preferred of the proposal's three options. Infrastructure Ontario engaged 33 different public organizations, including provincial agencies such as the Toronto District School Board, multiple universities, and the Ontario Lottery and Gaming Corporation. The feedback noted from these organizations was that there is an increased demand for cloud storage solutions and little to no demand for a Tier IV data centre. It was also noted that many BPS and Crown entities have either moved to cloud solutions or have expressed a desire to maintain their own data centres.

### Recommendation 3: Action Item 3

- implement an outreach strategy to broader public sector and provincial agencies to increase the data centre adoption;

**Status:**  In the process of being implemented by December 2024.

## Details

We found that the implementation of any potential outreach strategy with respect to the GDC's use depends on which option from Infrastructure Ontario's assessment is chosen by CCIO and the Ministry of Public and Business Service Delivery and Procurement. Infrastructure Technology Services (ITS), a division of CCIO, had developed a colocation strategy in December 2023 to be implemented if the decision to market to BPS entities is chosen. The decision is expected by December 2024.

### Recommendation 3: Action Item 4

- 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;

**Status:**  In the process of being implemented by March 2025.

## Details

We found that the assessment performed in consultation with Infrastructure Ontario was detailed and included jurisdictional scans across multiple provinces and private and public entities, and

considered the costs of operation and costs charged for using the data centre. CCIO expects that after a full review of the proposed options, an option will be chosen by December 2024, followed by the preparation of a business case that it will submit for Treasury Board approval by March 2025.

### **Recommendation 3: Action Item 5**

- 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.

**Status:**  **Fully implemented.**

### **Details**

We found that in May 2023, the ITS division of CCIO defined a monthly attestation process that requires all vendors and non-OPS entities that use GDC for their data centre operations to provide an attestation to the ITS that they have been informed of any changes in employment status. This process is noted in the physical security access control policy and procedures guide. Additionally, a requirement has been added to the policy to notify data centre management of any termination of non-OPS employees within 24 hours. We noted that an attestation was completed in August 2024 and stored in a repository noting that any requests for access removal have been made.

## **4. Half of All Critical IT Systems Used by the OPS Do Not Have a Disaster Recovery Strategy**

In our original audit, we found that almost half (44%) of all IT systems critical to the continuity of government services did not have a disaster recovery (DR) strategy.

### **Recommendation 4: Action Item 1**

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;

**Status:**  **In the process of being implemented by March 2025.**

## Details

We found that in March 2024, CCIO drafted a detailed OPS-wide DR strategy. The draft strategy proposes several working groups and committees that would hold weekly, biweekly or monthly meetings to specifically develop the capability to recover existing IT systems, as well as establish the capability for DR for systems hosted in the cloud in a disaster situation. In addition, the DR strategy identifies the roles and responsibilities for clusters, ministries and ITS for the design, implementation, testing and recovery of systems. The strategy has mapped each recommendation from our Office for DR to an action plan. CCIO is in the process of getting the strategy and proposed governance model approved and implemented by March 2025.

### Recommendation 4: Action Items 2 and 3

- 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;

Status:  Little or no progress.

## Details

We found that CCIO's assessment of IT systems to determine where a DR plan is required is a later stage of the OPS-wide DR strategy that can only be initiated once the strategy is approved and implemented. CCIO is in the process of creating a full inventory of critical IT systems to conduct this assessment.

Likewise, a process to review and assess annual compliance with DR plans can only be achieved once the DR plan has been approved and implemented.

### Recommendation 4: Action Item 4

- periodically test its ability to ensure IT systems can recover on a timely basis in a disaster scenario.

Status:  Little or no progress.

## Details

We found that periodic testing of IT systems to ensure timely recovery is also expected to be conducted as part of the not-yet-approved DR plans. We also noted that although the Children, Youth and Social Services Cluster and the Justice Cluster conducted their own DR tests in 2023 for



a sample of critical IT systems, this was done independently and was not incorporated into the overall DR strategy.

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

In our original audit, we found that CCIO did not have a redundant secondary network provider for some of its critical operations, such as 44 contact centres.

### Recommendation 5: Action Item 1

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;

Status:  Fully implemented.

### Details

We found that CCIO conducted a cost/benefit analysis across three different areas of operations to determine the need for a secondary, back-up network. CCIO subsequently signed contracts with Bell for the OPS data network in January 2023 (wired and wireless Internet access for OPS computers), as well as the voice services contact centres and mobility network (cell phone connectivity for OPS-issued mobile phones) in August 2023. The agreements have been implemented and Bell is operational as a back-up service provider for the OPS.

### Recommendation 5: Action Item 2

- 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.

Status:  In the process of being implemented by March 2025.

### Details

We found that CCIO has included new mandatory requirements in existing contracts for network resiliency, instead of adding a penalty clause to ensure business continuity of government operations.

Specifically, a requirement for additional redundancy has been added, such that if a certain portion of the network fails, all traffic can still be serviced on another portion of the network. This requirement will be implemented by March 2025.

## 6. OPS Cybersecurity Practices Need Improvement

In our original audit, we found that personal and sensitive data was not consistently secured through encryption in accordance with CCIO's security standard. We also found that approximately only 11,000 of 40,000 OPS staff completed the mandatory cybersecurity awareness course in 2021. The cybersecurity awareness training was not required for about 7,000 contract employees, nor was it provided annually to all OPS employees even though it is regarded as a best practice.

### Recommendation 6: Action Items 1 and 2

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.

**Status:**  In the process of being implemented by November 2025.

### Details

We found that in August 2023, CCIO engaged with the Office of the Chief Risk Officer (OCRO), Privacy, Archives, Digital and Data, a division of the MPBSDP, and the Ontario Provincial Security Advisor to create a critical value assets (CVAs) identification framework to identify mission and business-critical IT assets, such as IT systems that have a critical impact on the OPS or Ontarians if data is compromised.

We reviewed a draft of the CVAs identification framework, which includes a timeline to identify CVAs across the OPS and evaluate them for cybersecurity threats. The objective of the framework, once assets have been identified, is to enable protection mechanisms, such as encryption and monitoring compliance with encryption requirements. This framework was still in draft form at the time of our follow-up, and CVAs had not yet been identified in order to apply robust cybersecurity controls. Once the framework has been developed, the CVAs will be identified so that security controls such as encryption can be applied. The implementation of these security controls is targeted for November 2025.

### **Recommendation 7: Action Items 1 and 2**

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;

**Status:**  **In the process of being implemented by March 2025.**

### **Details**

We found that access to LearnON, the platform the OPS uses to provide cybersecurity training, has not been extended to contract employees, as they need an OPS WIN ID (employee ID number) to access the OPS IT network. CCIO conducted an assessment in March 2023 and noted that it is not possible to grant non-OPS staff access to LearnON and instead identified the need for a new training tool in order to do this. TBS is in the process of procuring a new training tool with the ability to grant access to contract employees and will implement it by March 2025.

We also found that in order to address and escalate incomplete trainings, CCIO has established regular reporting on course completion, with results presented to the Information Technology Executive Leadership Council committee on a quarterly basis. We reviewed the cyber intelligence report from February 2024 and noted that 44% of all OPS staff had already completed the mandatory information classification course.

### **Recommendation 7: Action Item 3**

- provide cybersecurity training to all OPS staff at least on an annual basis;

**Status:**  **In the process of being implemented by March 2025.**

### **Details**

We found that two mandatory cybersecurity courses, information classification and cybersecurity basics, have been developed and made available to all OPS staff through LearnON. The courses have been communicated to all OPS staff by the Deputy Minister of Public and Business Service Delivery and Procurement via email, as well as through an annual cybersecurity campaign in October of each year to provide additional resources on phishing best practices. However, as of

August 2024, these courses are not required to be completed annually, but rather just when staff are onboarded and when any significant change to the course is made. CCIO is in the process of exploring a mechanism to require these courses to be completed on an annual basis and will implement it by March 2025.

#### **Recommendation 7: Action Item 4**

- implement IT controls to restrict use of personal devices to prevent OPS employees who are working remotely from storing data on non-OPS devices;

**Status:**  **In the process of being implemented by December 2024.**

#### **Details**

We found that CCIO has implemented controls through Microsoft 365 to all OPS devices in order to restrict staff from downloading files to personal devices such as USBs or external drives. This is done through Microsoft Intune, an IT system that can disable USB ports on devices so that a removable storage device does not show up to users. This is also used to restrict unmanaged or unrecognized devices from downloading and printing documents. Staff are able to request an exemption to this process. CCIO is currently reviewing the list of exemptions to assess their appropriateness. In addition, in order to enable the functionality through Microsoft 365, some staff are required to update their computers to Microsoft Windows 11. Computers are being updated to Windows 11 into December 2024.

#### **Recommendation 7: Action Item 5**

- enforce a screensaver policy for all users.

**Status:**  **Fully implemented.**

#### **Details**

We found that since April 1, 2024, all new devices, such as end user computing devices/laptops, in the OPS are deployed with Windows 11 and all existing/in-use OPS devices will be upgraded from Windows 10 to 11 according to their refresh cycle. We reviewed the global Windows setting and noted that all Windows 10 and 11 devices have been set to have a 15-minute inactivity time limit before screens are locked and a password is required. This should increase compliance with the OPS's mandatory automatic screensaver policy. Any exemptions to this policy and the associated Windows screensaver setting will require staff to complete a deferral of risk treatment form that requires approvals from both their program areas and IT.

### **Recommendation 8: Action Item 1**

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.

**Status:**  **In the process of being implemented by November 2025.**

### **Details**

We found that CCIO has worked with TBS to include cybersecurity provisions in updated amendments proposed for the Memorandum of Understanding template between ministries and BPS entities, and for use in any new memoranda of understanding. Specifically, CCIO has proposed a mandatory requirement for a dedicated role at ministries or BPS entities that is responsible for education and awareness of employees on cybersecurity best practices. In addition, the proposed amendments include the establishment and execution of a holistic cybersecurity program and reporting of critical cyber incidents to the entity's board of directors and to the cybersecurity division of CCIO. There are also proposed inclusions for the documentation of IT risks, frequent cybersecurity assessments and quarterly reporting of any IT threats to CCIO. The updated Memorandum of Understanding template is expected to be implemented by November 2025.

### **Recommendation 9: Action Items 1, 2 and 3**

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.

**Status:**  **In the process of being implemented by October 2025.**

## Details

We found that CCIO has established an interim IT Vendor Management Office. This office's responsibility is to provide oversight and monitoring of third-party IT vendors and any associated risks. IT clusters will be responsible for receiving and reviewing third-party system and organization control (SOC) assurance reports to identify any exceptions, address them directly with vendors and share results with the IT Vendor Management Office. In addition, the IT clusters are now responsible for the identification of vendors storing data outside of Canada, to assess the data residency risks and, where necessary, take corrective action. Further, the IT clusters and ministries can now contact the Cyber Security Division directly through a new OPS-wide service, the Cyber Procurement Advice, which was deployed in September 2023 to receive guidance on how to assess and address data residency risks. The mandate of the IT Vendor Management Office has been included as part of the Cyber Security Risk Management policy, approved in April 2023. Until a dedicated IT Vendor Management Office is established (expected October 2025), CCIO has put in place a pilot process for IT clusters to review the SOC assurance reports for the top five vendors by CCIO spending. The interim Vendor Management Office will review the IT clusters' reported findings and proposed mitigation plans to assess whether additional training on SOC reports is required for clusters.

## 7. Ontario Government's IT System Inventory is Incomplete and Inaccurate

In our original audit, we found that the IT system inventory did not have all relevant and critical information about each IT system recorded. We also found that the process to review the inventory lacked thorough, frequent and consistent criteria-based reviews to verify or ensure that information stored there was accurate and complete or current.

### **Recommendation 10: Action Items 1, 2 and 3**

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.

**Status:**  **Fully implemented.**

## Details

We found that in June 2023, CCIO established training sessions on the configuration management database (CMDB), detailing how assets are managed within the CMDB and the necessary data required. The training was provided for configuration item owners, the individuals responsible for keeping information accurate in the CMDB for a particular IT system. The training specifies the data entry fields available in CMDB and what data should be provided in them, and common scenarios or errors that can be encountered in the CMDB and what additional information is needed.

We found that CCIO has established biweekly meetings to review overall data quality within CMDB through a data quality report that can be generated from a PowerBI dashboard and notes incorrect, outdated or empty fields. We reviewed data quality reports in both March and July 2024 and noted that the number of empty fields has significantly reduced, and overall data quality has improved from the time of our 2022 audit. Fields are not expected to be 100% filled as there is always a reasonable margin of error. The biweekly meetings to review data quality are comprehensive and would include any IT system that had been onboarded or retired on a continuous basis.

### **Recommendation 11: Action Items 1, 2 and 3**

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.

**Status:**  **In the process of being implemented by June 2025.**

## Details

We noted that in January 2024, CCIO signed a contract with a vendor to manage the software license management process for the OPS. The vendor has specified a timeline of June 2025 to onboard existing software into Snow, the OPS's software license management tool, as well as to develop a process to perform reconciliations of software licenses to fees paid and audits of installed software.

## 8. Insufficient Due Diligence When Hiring IT Consultants

In our original audit, we found that CCIO was not performing internal capability assessments to determine whether an IT consultant was required before hiring one. We also found IT consultants were being paid above the recommended rate listed in the OPS People Placement Service Manual, without any rationale. We also noted that there were no requirements for the minimum number of candidates to be interviewed for a position or number of interview evaluators.

### Recommendation 12: Action Items 1, 2, 3 and 4

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.

Status:  Fully implemented.

## Details

We found that CCIO has worked with Supply Chain Ontario (SCO) to implement a cost/benefit analysis template based on the requirement originally listed in the OPS Procurement Directive since 2018. Further, CCIO updated the Vendor Management System (VMS) in August 2023 to include a mandatory attestation noting that the ministry or cluster has completed the cost/benefit analysis as part of the approval process for a particular procurement. Managers filling out a procurement



form within the VMS are restricted from completing the form until the attestation is completed. A formal bulletin of these changes was sent to Central Agencies Cluster (CAC) staff in October 2023. CAC also conducts quarterly spot checks for compliance to the Procurement Directive and People Placement Service Manual and, as of August 2023, has included a new item to check if cost/benefit analyses were conducted. As of July 2024, CAC has not identified any non-compliance with the cost/benefit analysis requirement.

We also noted that CCIO has updated the VMS tool's configuration to prevent a pay rate outside of the recommended range from the People Placement Service Manual to be entered into the tool without selecting a new field that notes that an exception has been approved by the CCIO. The VMS also requires an additional reason to be selected from a dropdown menu as to why the exception was made, such as niche skill sets.

We noted that CCIO sent out a best practices bulletin in July 2023 to all hiring managers noting the requirement for at least two candidates and at least three evaluators for every IT consultant position. An attestation has also been added into the VMS to document that these requirements have been followed, and that interview notes have been uploaded to the VMS. The uploaded interview notes and attestations have also been added to the quarterly spot check performed by the CAC cluster.

### **Recommendation 13: Action Items 1, 2 and 3**

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.

**Status:**  **Fully implemented.**

### **Details**

We found that CCIO collaborated on an extensive industry scan of service level agreements with Gartner, an industry-leading IT research firm, and concluded, based on the results of the scan, that its compliance targets are aligned with industry best practices and existing OPS requirements. CCIO informed us that it follows the best practices noted in the documentation provided with its IT service management software. In addition, CCIO has also conducted a

comparison of its calculation method with those used with other similar service management tools, and found its timelines for resolving IT incidents adequate or on par with industry standards. We also noted that CCIO performs analyses of historical and current performance data to identify any gaps for improvement, specifically regarding improvements in incident resolution time by IT service providers.

#### **Recommendation 14: Action Items 1 and 2**

**Status:**  **Fully implemented.**

##### **Details**

Due to the sensitive nature of cybersecurity, and so as to minimize the risk of exposure for the OPS, relevant details of this finding and recommendation were not published in our 2022 audit and were instead provided directly to CCIO for remediation. We received commitment from CCIO that it would address these findings in a timely manner, and we will track the status of this recommendation directly with CCIO. The detailed status of this recommendation will not be published in the follow-up report.

#### **Recommendation 14: Action Item 3**






**Status:**  **In the process of being implemented by March 2025.**

##### **Details**

Due to the sensitive nature of cybersecurity, and so as to minimize the risk of exposure for the OPS, relevant details of this finding and recommendation were not published in our 2022 audit and were instead provided directly to CCIO for remediation. We received commitment from CCIO that it would address these findings in a timely manner, and we will track the status of this recommendation directly with CCIO. The detailed status of this recommendation will not be published in the follow-up report.

## // Appendix

### Recommendation Status Overview

	# of Action Items	Fully Implemented 	In the Process of Being Implemented 	Little or No Progress 	Will Not Be Implemented 	No Longer Applicable 
Recommendation 1	2		2			
Recommendation 2	3		3			
Recommendation 3	5	2	3			
Recommendation 4	4		1	3		
Recommendation 5	2	1	1			
Recommendation 6	2		2			
Recommendation 7	5	1	4			
Recommendation 8	1		1			
Recommendation 9	3		3			
Recommendation 10	3	3				
Recommendation 11	3		3			
Recommendation 12	4	4				
Recommendation 13	3	3				
Recommendation 14	3	2	1			
<b>Total</b>	<b>43</b>	<b>16</b>	<b>24</b>	<b>3</b>	<b>0</b>	<b>0</b>
%	100	37	56	7	0	0