Office of the Auditor General of Ontario
Bureau de la vérificatrice générale de l'Ontario

Office of the Corporate Chief Information Officer

2022 Value-for-Money Audit

Why we did this audit

- The Ontario government relies on the Corporate Chief Information Officer (CCIO) for Information Technology (IT) services such as data security, delivery of government programs and services, IT infrastructure, such as data centres, and computer and communications hardware, software and applications for Ontario Public Service (OPS) staff.
- IT systems are essential for ensuring the privacy, security, and integrity of critical government information, IT operations, networks and systems.

Why it matters

- The Province's IT services enable the Ontario government to provide various programs and services to Ontarians such as health cards, driver's licences, family support programs and COVID-19 grants.
- Cybersecurity attacks to IT systems or data may result in significant security breaches and outages. Ontarians' personal and sensitive data is stored in the Province's IT systems, and should be protected from unauthorized or accidental disclosure.

What we found

Weak IT Oversight of IT Clusters' Operations

- Because the CCIO does not have oversight of IT operations across the OPS and its eight IT service 'clusters', it is unable to meet its mandate of ensuring that government's IT services are managed and delivered effectively.
- IT 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.
- IT risks are not being identified within the CCIO and the CCIO does not have an overarching strategy across the OPS to identify enterprise IT risks and implement mitigating and remediation strategies. Upon our review of these identified risks, the CCIO has not identified major IT risks that would impact the OPS, or any risks commonly identified by industry best practice.

RECOMMENDATION 1, 2

Highly Rated Guelph Data Centre Underutilized by OPS

- Ontario's primary data centre was only 30% utilized at the time of our audit, even though it has been awarded the highest rating available, indicating that its IT systems are able to withstand any type of failure.
- Usage has declined over the past five years, during which time a $31 million loss was incurred for operating costs for the unoccupied space for power, cooling, maintenance and physical security.
- Utilization is low due to the higher rate, more than double the rate other private Tier IV data centre operators charge, and the lack of a marketing strategy to promote the data centre outside the OPS to Crown agencies and the broader public sector.

RECOMMENDATION 3

..../2

Almost Half of Ontario's Critical IT Systems Have No Disaster Recovery Plan

- Almost half (44%) of all IT systems critical to the continuity of government services, such as health, education, and drivers' licensing, do not have a Disaster Recovery Plan.
- The CCIO does not have a redundant secondary network provider for some of its critical operations, such as 44 contact centres. As a result, the Province was unable to provide Ontarians services through contact centres such as Service Ontario, COVID-19 Vaccination, and social assistance payments websites during the nation-wide Rogers outage on July 8, 2022. The outage resulted in a direct productivity loss of half a million dollars.

RECOMMENDATION 4, 5

Cybersecurity Practices Need Improvement

- 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 Ministry of Public and Business Service Delivery, personal and sensitive information was not encrypted in any of them as required by the security standard.
- Only 11,000 of 40,000 OPS staff completed the mandatory cybersecurity awareness course in 2021. 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.

RECOMMENDATION 8, 9

Conclusions

- The CCIO does not have oversight of information technology (IT) operations and the delivery of IT services across the Ontario Public Service (OPS). This reporting structure is a barrier to the CCIO achieving its mandate.
- OPS's primary data centre, located in Guelph, which has the highest data centre rating, has been significantly underutilized, resulting in an additional $31 million in operating costs over the past five years for the unoccupied space. Although the data centre has capacity to service outside of the OPS, there has been little outreach and currently minimal use from the broader public sector and Crown agencies.
- The CCIO does not have disaster recovery plans for almost half of the critical IT systems in the OPS. Cybersecurity practices at the OPS need improvement. Ontarians' personal and sensitive information is not fully protected within IT systems that we reviewed in accordance with the security standard for example, through data encryption.

Read the report at www.auditor.on.ca