Office of the Auditor General of Ontario

Value-for-Money Audit:

Security and Operations of IT Systems

December 2023

Security and Operations of IT Systems

1.0 Summary

The government of Ontario has an expansive portfolio of more than 1,200 Information Technology (IT) systems that are responsible for the operation of provincial programs across the Ontario Public Service (OPS). These IT systems have become increasingly important for the people and businesses of Ontario, providing government services in areas such as education, child welfare, social assistance and financial reporting.

To more efficiently manage these systems, the government has organized the IT operations at its 29 ministries into eight groups called IT clusters. The clusters provide day-to-day operational support to their associated ministries, including implementation of IT systems, technical support, securing confidential data, granting access to staff based on their job function, reviewing critical IT events (audit logs), monitoring the health of IT systems, and managing IT vendors and their performance. Each of the eight IT clusters is headed by a Chief Information Officer (CIO), who is responsible for supporting the IT needs of the ministries in each cluster. The IT clusters also indirectly (administratively) report to the Office of the Corporate Chief Information Officer (CCIO), which is responsible for province-wide IT needs.

This audit focused on four of the eight IT clusters to assess the security and effectiveness of the IT systems and processes used to deliver government programs and services. We selected a sample of IT systems across the four clusters.

The audit reviewed and examined security controls such as password policy and password settings to assess adherence and compliance with the OPS-wide password policy and industry standards. In addition, the audit also assessed whether the IT clusters had a process in place to apply critical security patches to its IT systems and databases on a timely basis to mitigate the risk of cybersecurity vulnerabilities. We also reviewed system access to assess whether controls were designed and operating effectively for the segregation of duties, timely removal of terminated staff's access, and periodic review of superuser access to ensure access to the privileged accounts was appropriately segregated and restricted to authorized staff.

In addition, we reviewed the controls in place to maintain audit logs for highly confidential information, including whether these audit logs were appropriately monitored, whether the audit logs captured all critical events necessary to track activities performed by staff, and whether the retention procedures were in accordance with OPS regulations.

We also reviewed various operational Key Performance Indicators identifying the performance of IT systems to ensure they were being measured and reported consistently. Further, we reviewed the controls to monitor IT vendors' performance and reviewed documents to assess whether the IT clusters were

sharing vendor performance reports and leveraging existing contracts for IT vendors in an effort to prevent duplicated and redundant services.

Limited Publication

Overall, we found that the OPS continues to implement a number of controls to enhance its security. However, our audit identified areas that require improvement and controls to be further strengthened. Due to the sensitive nature of our findings in this audit and the related IT systems that have confidential information, details were not published in the *2023 Annual Report* to minimize the risks to the OPS. However, all of the relevant details of our findings and recommendations were provided to the CCIO and respective IT clusters for remediation. The CCIO and clusters were in agreement with the recommendations and we have received a commitment from them to act on a timely basis to implement our recommendations in full.

Because our findings were systemic in nature, we believe they are relevant to all IT clusters in the OPS. Therefore, we also recommend that the CCIO work with the clusters that were not reviewed as part of our audit to identify if our recommendations are applicable to them and implement the relevant recommendations.

OVERALL RESPONSE

We appreciate the work done by the Office of the Auditor General of Ontario in preparing this report. The OPS is committed to safeguarding the data entrusted to the government by the people and businesses of Ontario and is always working to enhance its cybersecurity practices.

The OPS continues to work toward improving its current security controls and practices to address the rapidly evolving global security threats and enabling secure digital service delivery commitments for the people of Ontario. The Office of the Corporate Chief Information Officer and IT clusters agree with the OAGO recommendations and commit to these recommendations and to work together with all IT clusters and enterprise divisions to implement the OAGO recommendations in full on a timely basis.

2.0 Background

2.1 Overview

The provincial government uses more than 1,200 Information Technology (IT) systems to operate its programs and deliver services to the people of Ontario. Management of these systems for the government's 29 ministries has been organized into eight groups known as IT clusters. These clusters are responsible for day-to-day IT operations at the ministries they support, implementing new IT systems, and providing oversight to manage IT operations for existing systems to deliver government programs and services. The clusters also are accountable for ensuring the security and integrity of the data processed and stored on its systems and databases.

Each of the eight IT clusters is headed by a Chief Information Officer (CIO), who reports to the deputy minister of one of the ministries in the cluster. The clusters also indirectly report to the Office of the Corporate Chief Information Officer (CCIO), which is responsible for province-wide IT needs. The CCIO, through its enterprise divisions, provides guidance to clusters by establishing policies and procedures for areas such as cybersecurity, password policies, monitoring the health of IT systems, and the measurement of IT vendor performance. The clusters are responsible for ensuring data security and operational processes are aligned and comply with requirements outlined within CCIO-established policies and standards. Our Office audited the CCIO and its three enterprise divisions as a part of our 2022 value-for-money audit Office of the Corporate Chief Information Officer.

2.2 Role of IT Clusters

Clusters are responsible for providing technology services to ministries that support specific government programs for Ontarians. Their specific responsibilities include:

- securing IT systems through enforcing strong passwords;
- managing access to IT systems by performing regular attestation reviews;
- ensuring privileged superuser access to IT systems is appropriate;
- maintaining critical audit logs, and reviewing them on a timely basis;
- measuring the health of IT systems through established metrics and service targets;
- managing vendors that provide IT services and monitoring their performance; and
- developing standard operating procedures to equip staff with knowledge and tools to promote consistent delivery of operations.

The clusters rely on CCIO for guidance on managing and conducting these operations through CCIO-established IT policies and standards.

2.3 Security and Integrity of IT Systems

Poorly designed IT systems or a lack of robust controls can result in unauthorized access and disclosure of confidential information, data breaches and unsatisfactory services delivered by vendors. In response, IT clusters put in place controls to detect and prevent risks of collusion and fraud and to assess whether IT systems are managed effectively. These controls include strong passwords, restricted and controlled access to IT systems, and periodic monitoring of audit logs. The following briefly describes the key IT controls.

2.3.1 Security of Data (Password Controls)

Passwords act as a first line of defence against cybersecurity threats and help IT teams keep confidential data secure and reliable. It is imperative for organizations to adhere to their established password policy, which at a minimum should define password requirements for IT systems. Below are some common attributes of a strong password policy:

- **Password complexity**: Password policies often require that passwords meet specific complexity criteria, which may include a combination of the following:
    - A minimum number of characters is required for a password (eight character length).
    - Use of a mix of uppercase (A-Z) and lowercase letters (a-z), numbers (0-9), and special characters (!@#$&).
- **Password expiration**: Passwords may have a defined expiration period, after which users are required to change their passwords. This helps prevent long-term exposure in case of a security breach.
- **Password reuse**: Password policies often include a rule that prevents users from reusing their previous passwords for a certain number of times.

Having weak passwords can pose a significant security risk. For instance, recycling passwords, where users repeatedly use the same or similar passwords across multiple accounts, makes it easier for attackers to gain unauthorized access. Implementing password history policies is a fundamental security measure to help protect user accounts and confidential information from unauthorized access and breaches.

2.3.2 Multi-Factor Authentication

Multi-factor authentication (MFA) is a multi-step account log-in process that adds a security mechanism such as a one-time code sent to a user’s registered email address or mobile phone. MFA makes it more difficult for unauthorized individuals to access IT systems because hackers would need to possess multiple pieces of information or devices—and is an effective way to enhance security and protect confidential information from cyber threats.

2.4 Privileged User Accounts or IT Superusers

Privileged User Accounts, also referred to as superuser accounts, are used by IT staff to administer and manage IT systems, and they typically have unrestricted access to all data and permissions on an IT system. These accounts are also used to make changes to IT systems. As such, access to superuser accounts should be controlled so that activities performed by superuser accounts can be tracked, monitored and traced back when required, such as in the event of fraud.

2.5 Attestation of Privileged IT Accounts

By virtue of their role, staff with privileged IT access are able to add, modify or delete records and transactions, and in some cases even alter audit logs. For these reasons, organizations need to control or limit which staff receive access to superuser roles, and perform periodic reviews of users' access to IT systems to ensure that access is limited to staff with specific job functions. As per industry best practices, such attestations should be performed at least annually or whenever there are staffing changes within the department.

2.6 Audit Logging

Audit logs are systems-generated trails that capture detailed chronological events and activities performed by a user on an IT system. Audit logs include activities such as user log-in timestamps, type of data accessed, transactions modified or deleted, and anomalies or exceptions identified. It is essential for organizations to enable audit logging for critical events within IT systems so that they are able to establish accountability, identify unauthorized data modification, and detect fraud-related activities.

2.7 Availability of Data—Performance of IT Systems

In order to reduce the risk of disruptions to business operations from IT-related outages, organizations need to continuously monitor the performance of IT systems. Monitoring IT controls using defined performance metrics provides insight to IT teams and management to assess whether IT systems are performing at optimal capacity. These metrics range from monitoring the IT system's capacity to backing up data successfully and applying security patches in a timely manner.

2.8 Monitoring of Service Delivery

Key Performance Indicators (KPIs) are used to measure the service being delivered. They are critical for assessing performance and the benefits provided by an IT asset such as software or hardware. Organizations also use and monitor KPIs to ensure the expected level of service is being delivered.

2.9 Patch Management

Applying up-to-date security patches (security fixes) for IT systems and databases is critical for an organization to ensure that IT vulnerabilities are not exploited to cause data breaches and outages and ensure that confidential data remains secure.

The OPS has established a security standard that lists requirements about how and when to apply security patches for cybersecurity-related vulnerabilities.

The cybersecurity division of the CCIO is responsible for the identification of vulnerabilities on IT systems and databases. This is done through a security software that scans all IT systems and databases on a real-time (continuous) basis to identify cybersecurity-related vulnerabilities against publicly known vulnerabilities identified by vendors and security experts.

Once a vulnerability is identified, the cybersecurity division informs the IT cluster of the issue so that they can apply necessary security patches, which can also be provided by the vendor. Vulnerabilities are assigned a severity score from zero to four based on their risk of occurrence and potential impact. The severity score indicates how quickly patches should be installed, with severity zero being the most urgent (within two calendar days) and severity four being the least (within 90 calendar days). IT clusters are responsible for applying these patches within these timelines, as outlined in the Government of Ontario Information Technology Standards (GO-ITS).

2.10 Vendor Management by Clusters

While the CCIO is responsible for procuring goods and services used across the entire OPS, IT vendors that provide services and support for IT systems used by ministries are engaged directly by their respective IT clusters. The management of vendors for the delivery of goods and services is done at the individual engagement or contract level by the particular ministry or IT cluster that owns the contract.

3.0 Audit Objective and Scope

Our audit objective was to assess whether the selected Information Technology (IT) systems at four of the eight IT clusters in the Ontario Public Service (OPS) have effective systems and processes in place so that:

- Ontarians' data and IT systems that deliver critical government programs and services are secure and reliable, including the restricted use of privileged access and the monitoring of it to prevent unauthorized access to information systems;
- IT systems are effectively monitored, utilized at optimal capacity, and are assessed against established performance metrics; and
- systems and processes prevent the IT clusters from procuring duplicate IT vendors that provide similar services, and that vendors are effectively monitored so that services are rendered with due regard for economy, and that corrective action is taken on a timely basis when necessary.

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

We conducted our audit between January 2023 and September 2023. We obtained written representation from management that, effective November 17, 2023, 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 Chief Information Officers (CIOs), IT staff and relevant stakeholders at the four IT clusters at various positions to review their roles and responsibilities related to the management of IT systems they were responsible for and processes established to deliver government programs. We reviewed established procedures that define the objectives and mandate of the clusters.

We selected a sample of key IT systems across the four clusters. We reviewed security controls such as password policy and password settings to assess adherence and compliance with OPS-wide password policy in the form of the Government of Ontario Information Technology Standards (GO-ITS) and industry security standards.

We reviewed the system access listing to assess if superuser access was appropriately segregated and restricted to authorized staff. We also assessed if the clusters had controls in place to review superuser access periodically and whether access for inactive accounts was removed in accordance with GO-ITS security standards.

We reviewed the controls in place to maintain audit logs for highly confidential information, including the monitoring of these audit logs and retention in accordance with OPS regulations. We also reviewed various operational Key Performance Indicator reports identifying the performance of IT systems to ensure they were being correctly utilized and were performing at optimal capacity. Further, we reviewed the controls to monitor IT vendors' performance and reviewed documents to assess if the clusters were sharing performance reports with each other. We also assessed if the clusters were collaborating and leveraging existing contracts for IT vendors in an effort to prevent duplicated and redundant services.

We conducted our work and reported on the results of our examination in accordance with the applicable Canadian Standards on Assurance Engagements—Direct Engagements issued by the Auditing and Assurance Standards Board of the Chartered Professional Accountants of Canada. This included obtaining a reasonable level of assurance.

The Office of the Auditor General of Ontario applies the Canadian Standards on Quality Management and, as a result, maintains a comprehensive quality control system that includes documented policies and procedures with respect to compliance with rules of professional conduct, professional standards and applicable legal and regulatory requirements.

We have complied with the independence and other ethical requirements of the Code of Professional Conduct of the Chartered Professional Accountants of Ontario, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

Out of Scope

This audit did not specifically focus on OPS-wide centralized IT functions such as cybersecurity, the Enterprise Risk Management process, procurement of IT contractors, IT assets such as laptops and vendors valued over $2 million, and service level agreements and key performance metrics for IT incidents. Those topics were reviewed as part of our 2022 value-for-money audit Office of the Corporate Chief Information Officer.

Appendix: Audit Criteria

Prepared by the Office of the Auditor General of Ontario

1. Privileged access to key Information Technology (IT) systems critical for delivery of government programs and services is restricted to staff on a need-to-know basis to prevent unauthorized access to personal and sensitive data.
2. Performance indicators of key IT systems such as system availability, capacity utilization, patching status, aging, and system downtime are established, measured against targets, and monitored for effective system performance oversight.
3. Existing IT vendor contracts are leveraged before procuring new vendors to avoid procuring duplicate services, and vendor performance is monitored.
4. Controls are in place to prevent the procurement of duplicate IT vendors that provide the same services and software.
5. Clusters review vendor performance on an ongoing basis as per established criteria.

Office of the Auditor General of Ontario

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

www.auditor.on.ca

ISBN 978-1-4868-7494-1 (PDF)

Cover photograph credit:
© iStockphoto.com/Melpomenem