Chapter 1
Section
1.15

Information and Information Technology General Controls

Follow-Up on VFM Section 4.03, *2016 Annual Report*

RECOMMENDATION STATUS OVERVIEW						
	# of	Status of Actions Recommended				
	Actions Recommended	Fully Implemented	In Process of Being Implemented	Little or No Progress	Will Not Be Implemented	No Longer Applicable
Recommendation 1	7		7			
Recommendation 2	13	5	6	2		
Recommendation 3	6	3	3			
Recommendation 4	4	4				
Recommendation 5	1		1			
Recommendation 6	1		1			
Recommendation 7	1		1			
Total	**33**	**12**	**19**	**2**	**0**	**0**
%	**100**	**36**	**58**	**6**	**0**	**0**

Overall Conclusion

The Office of the Corporate Chief Information Officer and information and information technology (I&IT) clusters provided us, as of August 16, 2018, with information on the current status of the recommendations made in our *2016 Annual Report*. (Clusters are groupings of government programs and services that have similar clients and need similar I&IT services. They operate as part of the government-wide I&IT organization.) The I&IT organization has fully implemented 36% of our Office's recommendations relating to developing service-level agreements for all I&IT systems and addressing risks related to areas such as security and aging I&IT systems. Included in the recommendations that have been implemented are those that relate to preventing unauthorized access to I&IT systems and data. This involves setting up safeguards such as reviewing I&IT users who are accessing the systems and maintaining logs of system use.

The I&IT organization is in the process of implementing 58% of our recommendations. One such action is looking into modernizing systems that are deemed to be at the end of their life cycle. The I&IT organization and ministries oversee more than 1,200 I&IT systems, which helps account for the large number of our recommendations that are still in the process of being implemented.

The I&IT organization has made little progress on 6% of our recommendations. These recommendations pertain to one I&IT cluster, and involve the need to create succession plans for I&IT staff, and improve training and materials available to them. This cluster informed us that it intends to implement these recommendations.

The status of actions taken on each of our recommendations is described in this report.

Background

The Ontario Government uses information and information technology (I&IT) to help deliver the wide variety of services and operations it administers for the public and to manage its finances and affairs, such as making payments and collecting revenues. The I&IT Strategy (2016–20) helps set the direction of I&IT by focusing on using technology to improve the delivery of government programs, updating old and outdated I&IT systems, and enabling the analysis of data for decision-making purposes.

At the time of our 2016 audit, the I&IT organization's head office was located within the Province's Treasury Board Secretariat. The head office of the I&IT organization was relocated to the Ministry of Government and Consumer Services in late June 2018. It is made up of the Office of the Corporate Chief Information Officer, service branches responsible for certain common government-wide services, and nine I&IT units supporting ministries organized into business clusters. The I&IT organization supports more than 1,200 I&IT systems across the government and has annual expenditures of about $1.1 billion.

The Corporate Chief Information Officer heads the I&IT organization and works with the Ministry of Government and Consumer Services to make strategic and security decisions on technology and to set information management policy for all government I&IT operations. The Office of the Corporate Chief Information Officer is responsible for:

- aligning I&IT work to support the government's direction and vision;
- managing all servers, computers, software and mobile devices; and
- keeping networks, information and public records secure.

Our 2016 audit involved a review of service-level agreements for key I&IT systems in three I&IT clusters. Service-level agreements are important because they clarify the types and quality of service to be provided, how decisions over I&IT systems will be made and how performance will be assessed.

We also looked at whether the government had effective I&IT policies, procedures and controls in place covering security, change management, operations, availability, capacity, continuity and disaster recovery to ensure the integrity of government I&IT systems and data files. Specifically, we focused on I&IT general controls, which are controls that apply to the overall design, security and use of computer programs and data files throughout an organization. They consist of system software and manual procedures that help ensure that the organization's I&IT systems are operating reliably and as intended. To do this, we examined I&IT general controls for three key I&IT systems managed by the I&IT organization:

- the Ministry of the Attorney General's Integrated Court Offences Network (Court System), serviced by I&IT's Justice Technology Services cluster—provides case administration support to the Ontario Court of Justice;
- the Ministry of Finance's Tax Administration System (Tax System), serviced by I&IT's

Central Agencies cluster—administers the provincial tax system; and

- the Ministry of Transportation's Licensing Control System (Licensing System), serviced by I&IT's Labour and Transportation cluster—administers the registration of vehicles and drivers' licences.

We evaluated these systems against best practices identified for strong I&IT general controls, as these controls should provide the first level of defence against threats such as hacking, viruses, sabotage, theft and unauthorized access to information and data.

To conduct the audit, we interviewed staff from the I&IT clusters and ministries, reviewed key documents and reports, and observed procedures and controls in action at the three ministries that own the three systems (the ministries of the Attorney General, Finance and Transportation). We also tested both automated controls and manual procedures carried out by I&IT staff. We followed a risk-based approach—if the risk likelihood and impact were high, we performed more in-depth procedures. In addition, we inquired with other I&IT clusters to determine whether the issues we identified around service-level agreements being inadequate were prevalent in other clusters.

In our *2016 Annual Report* we found that 75% of government I&IT systems did not have service-level agreements in place. Without service-level agreements, ministries and their I&IT clusters leave themselves open to a variety of issues, such as not having sufficient infrastructure to meet the ministries' needs. The service-level agreements that were in place were very generic, poorly formulated and not reflective of current processes.

We found that all three systems needed to improve controls to prevent unauthorized access to confidential information. For example, we found:

- There was need for improvement in the management of I&IT human resources. For example, the Court System had an inadequate number of staff to maintain the system.
- There was insufficient security over the access of systems and sensitive information.
- There was a lack of documented procedures around verifying that batch updates and system changes were correctly implemented and were done in the most efficient way possible.

We found a lack of staff training, knowledge transfer and maintenance of systems. This led to issues with service delivery in the government I&IT systems we audited. Additionally, modernization efforts by the government to replace some outdated I&IT systems were significantly delayed. Specifically, the government attempted to modernize the Court System, but the project failed due to inadequate project management and project reporting, as well as inefficient governance and oversight practices.

We made several recommendations to the ministries and I&IT clusters in order to address the issues we found. We recommended that the ministries establish formal service-level agreements for all I&IT systems (including the three we reviewed) that align with the overall I&IT strategy. We also recommended that the I&IT clusters improve staff training, increase knowledge transfer, and create several operational controls and procedures that would affect system security and maintenance.

We recommended that the Office of the Corporate Chief Information Officer assess existing I&IT systems for compliance with the nine key risk areas that effective I&IT general controls should address. We also recommended that the I&IT clusters review their system replacement and modernization timelines and identify areas where these timelines could be shortened to ensure that I&IT systems continue to meet user needs. This includes the need to ensure that systems are sufficiently maintained and supported to mitigate the deterioration of their performance over time.

Lastly, we recommended that the I&IT organization along with the respective ministries assess the cost and need to update and maintain current systems and the risks arising from using aged systems versus the costs and benefits of

replacing these systems. This included a review and revision of the current five-year strategy plan released in 2016.

Our report contained seven recommendations, consisting of 33 actions, to address our audit findings.

We received commitments from the ministries and I&IT clusters involved in our audit that they would take actions to address our recommendations.

Status of Actions Taken on Recommendations

We conducted assurance work between April 1, 2018, and August 30, 2018. On October 31, 2018, we obtained written representation from the Ministry of Government and Consumer Services that it has provided us with a complete update of the status of the recommendations we made in the original audit two years prior.

Key to High-Performing I&IT Systems—Service-Level Agreements—Not in Place between I&IT Clusters and Ministries

Recommendation 1

To ensure ministries receive high-quality I&IT services that meet their needs, the I&IT clusters and ministries should establish formal service-level agreements that are aligned with the overall I&IT strategy and:

- *document the roles and responsibilities of both parties;*
  Status: In the process of being implemented by March 2019.

Details

In our 2016 audit, we found that formal service-level agreements (SLAs) were lacking between I&IT clusters and ministries for 75% of government I&IT systems. Those that were in place were generic, poorly formulated and not reflective of current processes. Until well into the course of our audit, there were no SLAs in place between the ministries and I&IT clusters for the three systems in the scope of our audit. In April 2016, however, the Central Agencies cluster drew up a second SLA (for a total of two of the 168 systems it supports), which was signed and approved by the Ministry of Finance.

In October 2016, the Treasury Board Secretariat established the Enterprise Service Management (eSM) Division to centralize the provisioning, management and development of I&IT services and to establish SLAs. eSM developed a risk-based approach consisting of two separate phases. The first phase involved completing SLAs for mission-critical I&IT systems, while the second phase plans to complete SLAs for the other two categories of less critical I&IT systems: business-critical and business-support systems.

In April 2017, the eSM Division created a standardized SLA template that incorporated the nine elements recommended in our 2016 audit: roles and responsibilities, service times, availability considerations, performance requirements, capacity needs, security requirements, system and service continuity, compliance and regulatory issues, and demand constraints. The SLA template is a model agreement that outlines standard roles and responsibilities of the ministry and I&IT cluster involved in the management and use of the I&IT system. The template states that the cluster has overall responsibility for the delivery of I&IT services. Its terms are binding on both parties: the cluster and ministry are both responsible for achieving the stated objectives of the SLA.

Additionally, the Treasury Board Secretariat created a Government of Ontario Information Technology Standard (GO-ITS), which was approved in January 2018, to provide information on managing the SLA process properly. GO-ITS are the official I&IT standards adopted for use across the entire Ontario Government.

eSM has completed SLAs for 387 of Ontario's 1,278 I&IT systems; 670 of these systems are not yet covered in an SLA, and the remaining 221 systems are outside of eSM's scope. Of the total number of I&IT systems, 122 are mission-critical: 82 of these are covered in an SLA, 25 are not yet covered, and 15 are outside eSM's scope. Business-critical systems account for 437 systems: 111 are covered in an SLA, 278 are not yet covered, and 48 are outside eSM's scope. Business-support systems account for the remaining 437 systems: 194 of these are covered in an SLA, 367 are not yet covered, and 158 are outside eSM's scope.

The 221 I&IT systems outside of eSM's scope are managed by ministries and so are not covered in eSM's process. Therefore, there is a risk that SLAs will not be developed for them.

- *set out specific, measurable, attainable, reportable and time-bound performance requirements;*
  Status: In the process of being implemented by March 2019.

Details

Our 2016 audit noted the importance of including performance requirements in SLAs—that is, explicit targets geared to each different operation. At the time of our follow-up, the Ministry of Government and Consumer Services was in the process of setting out performance requirements for all I&IT clusters. The majority of these performance requirements are standardized and are included in the SLA template, whose objectives are binding on the clusters and ministries. Enterprise Service Management has begun reporting on these targets for some of the finalized SLAs; the clusters and ministries are receiving these reports monthly.

- *state agreed service times;*
  Status: In the process of being implemented by March 2019.

Details

The SLA template incorporates standardized service times, which are prioritized according to the three risk-based classifications. For example, for mission-critical I&IT systems, the target for service restoration is 4.5 hours. The SLA template also states the business hours when service requests will be fulfilled. All the SLAs that we reviewed included agreed service times.

- *outline availability and compliance and regulatory considerations;*
  Status: In the process of being implemented by March 2019.

Details

In our 2016 audit, we noted that all three systems we selected had adequate controls in place to ensure that services are available when needed, performance expectations are met, and plans are made to predict and meet future user needs. The SLA template states guidelines for availability, and the completed SLAs we reviewed include hours of operation for application support, scheduled maintenance windows and targets for server availability.

Our 2016 audit also noted the importance of having SLAs address compliance and regulatory considerations to help ensure that relevant regulations are followed. The SLA template includes the GO-ITS standards on compliance and regulations that ministries and clusters are subject to. Compliance and regulatory considerations are built into several sections of the template. Along with regulatory considerations, compliance targets measuring how often the cluster met a specific goal under a performance target were included in the SLAs we reviewed.

- *identify security requirements and capacity needs;*
  Status: In the process of being implemented by March 2019.

Details

Our 2016 audit noted the importance of preserving the confidentiality of I&IT systems and data, to prevent unauthorized access and/or changes to sensitive information. The SLA template states that all Ontario public service employees must comply with security requirements outlined in the GO-ITS Corporate Policy on Information and Information Technology (I&IT) Security, the Information and the Acceptable Use of I&IT Resources Policy, and the General Security Requirements. The I&IT clusters and ministries are identifying security requirements for the I&IT systems they manage.

Capacity needs are included in the SLA template and examples of SLAs we reviewed. Before completing any new implementation, the cluster is responsible for completing an assessment of a ministry's capacity needs so that I&IT can assess whether the existing infrastructure is sufficient or needs to expand to accommodate the new service. We reviewed a sample of these capacity needs assessments and found that they adequately assessed the risks for the infrastructure the I&IT systems resided on.

- *set out the policies and procedures for system and service continuity;*
  Status: In the process of being implemented by March 2019.

Details

Our 2016 audit noted that all three systems we selected had effective processes in place to address unexpected disruptions to operations. Following our audit, system and service continuity considerations were incorporated in the SLA template, which directs the parties to provide descriptions of polices, standards and processes for preventing, predicting and managing potential and actual service disruptions. The completed SLAs we reviewed included a description of relevant legislation and policies that require the parties to establish emergency management programs and a continuity of operations program.

- *ensure that service levels are monitored by requiring I&IT clusters to report regularly to ministries on their achievement of expected performance.*
  Status: In the process of being implemented by March 2019.

Details

Following our 2016 audit, the eSM Division created a standard reporting framework that provides guidance for reporting on service performance. The eSM Division is monitoring service levels for several approved SLAs, and it produces a monthly report on the results. It informed us that it would be monitoring service levels for additional SLAs in the future. At the time of this follow-up, these performance reports have been created for seven SLAs, including the three SLAs that covered the Court System, the Tax System and the Licensing System. We reviewed some of these reports and found that they provided several different measures of whether service targets listed in the SLAs were met. The reports included type of service, target time to complete the service, number of service requests and percent of requests where service was completed within the stated target times.

I&IT General Controls Can Be Improved

Recommendation 2

The Justice Technology Services I&IT cluster should:

- *Establish formal service-level agreements covering the systems and implement formal monitoring and reporting over service levels.*
  Status: In the process of being implemented by March 2019.

Details

Our 2016 audit identified nine key risk areas that effective I&IT general controls should address: SLAs, human resource management, security, operations, change management, incident management, problem management, availability and capacity

management, and business continuity and disaster recovery. We assessed each of the three systems we selected on these nine elements, and made recommendations for each system individually, based on our findings.

Following our audit, in 2017 the Justice Technology Services I&IT cluster and the ministries involved created SLAs for all mission-critical I&IT applications. This includes the Court System, which is covered by an SLA completed by the Ministry of the Attorney General (Ministry) and the cluster. However, the Court System SLA does not have all nine key elements our Office recommended. eSM has stated that it will update this SLA to the new template as part of an annual review that began in September 2018. The cluster and ministries plan to complete SLAs and have them in place for all of the approximately 85 remaining I&IT applications by March 2019.

The cluster and ministries produce a monthly performance report that measures whether the cluster has delivered services within the target specified in the SLA. The Court System is included in this performance report.

- *Ensure they engage appropriate staff with the necessary skills and expertise.*
  Status: In the process of being implemented.

Details

At the time of our 2016 audit, the Court System was relying on just one external consultant and one staff member to maintain the system. In response to our recommendation, the Justice Technology Services cluster has added additional staff to ensure appropriate levels of support and maintenance. The cluster has stated that it has focused on providing on-the-job training and has not developed a set of complete training documents due to the fact that it plans on replacing the Court System. However, it has developed operational guides to assist staff with day-to-day tasks and system maintenance. Our Office believes that developing training documents would help improve the cluster's ability to transfer knowledge to staff.

- *Ensure succession plans are in place to allow for the transfer of knowledge.*
  Status: Little or no progress.

Details

The Justice Technology Services cluster has not developed a detailed succession plan for the Court System. The cluster's current plan identifies retirement eligibility for staff, but there is no process in place to transfer their knowledge to other staff. The cluster notified us that it will assess knowledge-transfer requirements and develop a strategy once it has replaced the Court System.

- *Establish job descriptions and service-level agreements for the services provided by all consultants and, on a regular basis, monitor consultants' performance and assess against the job descriptions and service-level agreements.*
  Status: Fully implemented.

Details

In November 2017, the Justice Technology Services cluster created a statement-of-work document that outlines job descriptions for prospective consultants. This document is an agreement between the consultant, the Ministry and the I&IT cluster that covers details of the consultant's contract and the work that will be performed. We reviewed the statement of work for a consultant performing duties for the Court System. It covered the scope of the work; deliverables the consultant was responsible for; and the skills, experience and qualifications required for the position. In addition, managers in this cluster are required to complete an IT source vendor performance scorecard.

- *Perform a review, in conjunction with the Ministry of the Attorney General (Ministry), of the current users' access to the system. The review should focus on the predefined access levels set up on the system and the employees' responsibilities. Where users have been granted access levels that pose potential conflicts related to segregation of duties (such as developers having*

access to make data changes), these access levels should be corrected immediately, and appropriate controls put in place to address any potential conflicts in the future.

Status: In the process of being implemented.

Details

Our 2016 audit noted that the Court System had no formal process in place for creating and modifying users' access, and 41% of users had access to the system when their job status did not require access. Following our audit, the Justice Technology Services cluster informed us that it was developing a user review for the Court System based on predefined access levels and employee responsibilities. In preparation for this review, the cluster has developed a matrix to define user access levels and a process to conduct annual reviews of Court System user access privileges. We reviewed the matrix and noted that it defines user access privileges by job position and creates a segregation of duties.

The cluster conducted an initial access review in 2017. As a result, 4,505 inactive accounts and 24 user groups that were no longer required were removed. Accounts identified as inactive for 18 months or longer are now removed quarterly. The cluster is currently in the process of conducting reviews based on predefined access levels.

- *Ensure that on a regular basis, the Ministry reviews user access and revalidates it for appropriateness. On an annual basis, the Ministry should revisit the access granted to employees and their responsibilities to ensure there are no conflicts related to segregation of duties and reflect any changes in roles, procedures and processes as seen necessary.*

  Status: Fully implemented.

Details

The Justice Technology Services cluster has developed a process for an annual user access review to ensure that users have appropriate access levels. The process highlights the roles and responsibilities for the review, the steps to be taken, and the requirement to conduct the review on an annual basis.

- *Enable logging of all user access to information and transaction changes and monitor key activities on an ongoing basis. The extent of logging should be driven by the sensitivity and criticality of the data. The Ministry should define the data it considers sensitive and critical and that needs to be logged and proactively monitored.*

  Status: In the process of being implemented.

Details

In our 2016 audit, we noted that Court System user activity logs were not being reviewed for appropriateness. Following our audit, the Justice Technology Services cluster implemented logging of user activity against case data within the Court System. Each court receives a daily report that lists changes to cases for the previous day. As of December 2017, the IT operations manager and team lead receive nightly emails that include a report made on changes in the system. However, the Ministry and cluster have not defined data that is sensitive and critical for proactive logging and monitoring.

- *Implement a formal process for creating and modifying users' access, including a centralized list of authorized approvers who can request access on behalf of users.*

  Status: Fully implemented.

Details

The Justice Technology Services cluster has developed an account management process for the Court System and revised the user account request forms for Court System users. An authorized approvers list was created for individuals who can request access to the system on behalf of other users; approvers must sign the user account request form for access to be granted.

- *Implement automated controls to verify that batch job processing is successful and in line*

with end users' requirements. These controls must verify the completeness, accuracy and validity of the data output.

Status: Fully implemented.

Details

Following our 2016 audit, the Justice Technology Services cluster implemented batch input validation. This includes daily, weekly and monthly batch reports, which are reviewed and approved by the Court System manager daily. Copies of the nightly monitoring reports and batch summary reports are automatically emailed to the Court System manager and team lead for review.

- *Formally document, approve and communicate I&IT operational procedures.*

  Status: In the process of being implemented.

Details

Our 2016 audit noted that the Court System lacked documented I&IT procedures. The Justice Technology Services cluster is currently developing an operational procedures manual. We reviewed draft documents such as the Court System Daily Procedures Guide and Technical Operations Guide. The cluster indicated that these guides would be included in the operational procedures manual and that it would make the manual available to its staff after completion.

- *Ensure that the data being entered within the incident management tool is complete, accurate and valid. Once incident data quality is achieved, management should implement a formal problem-management process to identify trends, the root cause of recurring issues and remediation plans.*

  Status: In the process of being implemented.

Details

A Government of Ontario Information Technology Standard exists for problem management. The Court System support team received formal training on problem-management processes and operational training in October 2017. The cluster completed an assessment of tickets in the incident-management tool in the summer of 2017. However, this review of individual tickets did not produce any reports that identified trends, root causes of the problems or remediation plans for the problems identified. The manager of the cluster reviews individual tickets that are logged through the Ontario Public Service IT service desk and assigned to the Court System helpdesk. The Justice Cluster is currently looking into other applications to conduct trend and root-cause analysis.

- *Based on the service-level agreement:*
  - *identify logs that need to be maintained and monitored;*
  - *define thresholds for logs and implement log monitoring tools to facilitate the interpretation of log data;*
  - *configure system alerts for staff to follow up on potential issues; and*
  - *review monitoring protocols on a regular basis to ensure that they are still valid.*

  Status: Fully implemented.

Details

The Justice Technology Services cluster has implemented a change journal to log user activity against case data within the Court System, and it provides a daily report to every court in the system. A tracking tool records and tracks change requests for the Court System, tracking the types of changes made, their priority and date, and who made the change.

The cluster also produces a monthly report that measures database capacity on the mainframe. Issues found in this report are flagged and brought to the attention of the cluster's manager. The Court System support team maintains a log of all program errors and requests for data correction. The cluster also produces a daily batch processing performance log that provides a summary of batch reports.

- *Utilize I&IT cluster staff efficiently by:*
  - *implementing a self-serve functionality on the system so end users can resolve basic incidents, such as forgetting their passwords, without direct interaction with helpdesk staff;*
  - *training helpdesk staff to resolve more complex user incidents; and*
  - *assigning dedicated technical support staff to identify ongoing incident issues and develop permanent fixes.*

  Status: Little progress.

Details

The Justice Technology Services cluster has not made significant progress on this recommendation according to the documentation we have received. The cluster has stated that it will complete work on this recommendation by March 2019 and that it is currently reviewing existing help-based materials to identify opportunities for expanding self-help options.

Recommendation 3

The Labour and Transportation I&IT cluster should make the following improvements to the Licensing System:

- *Establish a formal service level agreement covering the system and implement formal monitoring and reporting over service levels.*

  Status: In the process of being implemented by December 2018.

Details

The Ministry of Transportation (Ministry) Licensing System, serviced by the Labour and Transportation I&IT cluster, was one of the three systems we selected for the scope of our 2016 audit. We assessed the Licensing System on the nine key risk areas that we found effective I&IT general controls should address, and made recommendations based on our findings.

Following our audit, in the spring of 2017 the Labour and Transportation I&IT cluster and the Ministry established an SLA that covers the Licensing System, as well as other I&IT systems shared by the Ministry and cluster. The cluster set up daily and monthly reporting and monitoring of compliance with SLA expectations in June 2017, along with monthly review meetings to review service provider compliance, identify opportunities for improvement, and propose, implement and monitor process improvements through to completion. The cluster notified us that it is planning to produce performance reports for Ministry use.

- *Perform a review, in conjunction with the Ministry of Transportation (Ministry), of the current users' access on the system. The review should focus on the predefined access levels set up on the systems and the employees' responsibilities. Where users have been granted access levels that pose potential conflicts related to segregation of duties, these access levels should be corrected immediately and appropriate controls put in place to address any potential conflicts in the future.*

  Status: Fully implemented.

Details

The Ministry and cluster completed a user access review of the Licensing System in 2017. The review looked at all users in the system according to the access levels that define the type of privileges each user should have. Users who had improper access either had their access level modified or were removed completely, if they no longer required access. The review resulted in approximately 1,900 users being removed from the system. The cluster created additional security controls over access level such as the requirement to have a security clearance and signing a disclosure statement.

- *Ensure that on a regular basis, ministries review user access and revalidate it for appropriateness. On an annual basis, ministries should*

revisit the access granted to employees and their responsibilities to ensure there are no conflicts related to segregation of duties and reflect any changes in roles, procedures and processes as seen necessary

Status: In the process of being implemented by March 2019.

Details

The Labour and Transportation cluster and Ministry have not finalized a process to conduct annual or periodic access reviews. Our Office believes that annual and periodic reviews would help ensure that user access is in line with the user's job description and that no one with access to the system should no longer have access. The Ministry has conducted annual reviews on dormant users who have not accessed the Licensing System for over one year. However, we did not find sufficient evidence that the cluster reviewed whether employees' access corresponds to their current responsibilities, and that there are no conflicts related to segregation of duties. The Ministry and cluster have created a project proposal that outlines the importance of conducting automated annual reviews and the required steps to expand the process. They notified us that they are still awaiting funding and approval before moving ahead with this project.

- *Enable logging of all user access to information and transaction changes and monitor key activities on an ongoing basis. The extent of logging should be driven by the sensitivity and criticality of the data. The Ministry should define the data it considers sensitive and critical and that needs to be logged and proactively monitored.*

  Status: In the process of being implemented by December 2018.

Details

In September 2016, the Labour and Transportation cluster consolidated all logging data to allow for user access reporting. These logs are available for ad hoc requests and informational reports only. The cluster and Ministry have reviewed and defined the sensitivity of user access data and have stated they would now focus on implementing proactive user access logs to allow for real-time monitoring of users who access sensitive or private information.

A privacy impact assessment and threat risk analysis have been completed on user access to the Licensing System and the system used to log user accounts. The privacy impact assessment defines sensitive and personal information for the Licensing System.

- *Ensure that there is clear linkage between the incident records in the incident management tool and the program change records addressing those incidents.*

  Status: Fully implemented.

Details

The Labour and Transportation I&IT cluster uses the Enterprise Service Management Tool to link incident records and program change records. The cluster provided its staff with training in ensuring that proper relationships and linkages are created between change, release, incident and problem records. This training is complemented by a Government of Ontario IT Standard for Enterprise Change Management, which provides additional advice on creating linkages between incident records and program change records.

- *Implement a formal problem management process to identify trends, the root cause of recurring issues and remediation plans.*

  Status: Fully implemented.

Details

The Labour and Transportation I&IT cluster has implemented a problem-management process based on the standardized process created by the Office of the Corporate Chief Information Officer, which provided the cluster with operational training in the process. This process complements the Government of Ontario IT standard on Problem Management. These guides and standards provide information on how to conduct problem management, the roles and

responsibilities of those involved, and procedures for detecting and resolving problems. The cluster conducts root-cause analysis and remediation work through the Enterprise Service Management Tool.

Recommendation 4

The Central Agencies I&IT cluster should make the following improvements to the Tax System:

- *Implement formal monitoring and reporting over service levels against the Ministry of Finance (Ministry) approved service level agreements.*
  Status: Fully implemented.

Details

The Ministry of Finance (Ministry) Tax System, serviced by the Central Agencies I&IT cluster, was one of the three systems we selected to examine in our 2016 audit. We assessed the Tax System on the nine key risk areas that effective I&IT general controls should address, and made recommendations based on our findings.

Following our audit, the Central Agencies I&IT cluster developed and implemented an SLA for the Tax System, and additional SLAs for some of its smaller applications. It also consulted with the Ministry to formalize a management oversight process to monitor and report on service levels outlined in SLAs for the Tax System. We reviewed these reports and found that they had the necessary service standards and targets to ensure that the Tax System is meeting the requirements set out in the SLA.

- *Perform a review, in conjunction with the Ministry, of the current users' access on the system. The review should focus on the predefined access levels set up on the system and the employees' responsibilities. Where users have been granted access levels that pose potential conflicts related to segregation of duties, these access levels should be corrected immediately and appropriate controls put in place to address any potential conflicts in the future.*
  Status: Fully implemented.

Details

The Central Agencies I&IT cluster worked with the Ministry to establish a new process to review whether users have appropriate access to the system, given their job responsibilities. It completed this process in July 2017 and has implemented additional processes to flag potential issues with user access. The cluster has also created a process to review access levels to ensure a proper segregation of duties is maintained and procedures are in place to correct access if conflicts are identified. A list of users is sent monthly to business managers in the Ministry to ensure that the individuals listed have proper segregation of duties according to their access level.

- *Ensure that on a regular basis, ministries review user access and revalidate it for appropriateness. On an annual basis, ministries should revisit the access granted to employees and their responsibilities to ensure there are no conflicts related to segregation of duties and reflect any changes in roles, procedures and processes as seen necessary.*
  Status: Fully implemented.

Details

The Central Agencies I&IT cluster performs a monthly review to confirm the appropriateness of user access levels. The cluster reviews all users against the predefined access levels and the employees' responsibilities to ensure a segregation of duties. Additionally, the cluster tracks user access to the system to determine if any accounts have been inactive for a long time, and therefore should have their access removed.

- *Implement a formal problem-management process to identify trends, the root cause of recurring issues and remediation plans.*
  Status: Fully implemented.

Details

In February 2018, the Central Agencies I&IT cluster implemented a formal defect-management process

to address this recommendation. The cluster's staff received formal training in problem and defect management delivered by Enterprise Service Management. We reviewed defect-management status reports presented to the cluster's senior management and found that the reports produced trends and data reports for defects in the Tax System. The defect-management process produces a data report for problems that arise in the cluster's I&IT systems. We reviewed these reports and found that they contained descriptions and interpretations of the root cause of problems. Additionally, the cluster has prioritized problems and has provided documented resolutions to address them.

Recommendation 5

The Office of the Corporate Chief Information Officer should assess existing I&IT systems for compliance with the nine key risk areas that effective I&IT general controls should address. Action should be taken to strengthen areas that need to be improved, for example, establishing formal service-level agreements that are aligned with the overall I&IT strategy.

Status: In the process of being implemented by March 2022.

Details

In September 2017, the Office of the Corporate Chief Information Officer (Office) developed and updated the IT general control assessment toolkit to incorporate the nine risk areas we identified in our audit. The toolkit is used to assess the types of controls in place, how the controls operate, and whether there are gaps in the controls. The Office has provided training to clusters in completing the toolkit, and notified them of the changes made to the toolkit after our audit. Where the toolkit identifies gaps in controls, it recommends how to address these gaps.

The Office has categorized over 1,200 I&IT systems by risk level. It prioritized mission-critical systems for IT general control assessments, followed by business critical and then business support. At the time of this follow-up, the Office had completed IT general control assessments for 98 I&IT systems (mostly mission critical) and had plans to complete an additional 479 assessments by March 2020. It informed us that it intends to complete the remainder of the assessments by March 2022.

Maintenance of Aging Systems Is Inefficient and Staff Lack Training

Recommendation 6

In order to mitigate the risk arising from using older and outdated I&IT systems, the I&IT cluster should revisit system replacement and modernization timelines and identify areas where these timelines could be escalated to ensure that I&IT systems continue to meet user needs.

Where the replacement of outdated I&IT systems cannot be escalated, appropriate strategies should be put in place to ensure that systems are sufficiently maintained and supported to mitigate the deterioration of system performance.

Status: In the process of being implemented by September 2022.

Details

Our 2016 audit found that Ontario was using many older and outdated I&IT systems that were not being updated regularly. For example, at the time of our audit, the Licensing System was 48 years old and the Court System was 27 years old. We also noted problems with continuous training and knowledge transfer among staff who operate these older systems. This increases the risk of functions being delayed or becoming unavailable, which in turn could impact service delivery.

The Ministry of Government and Consumer Services is working with I&IT clusters to develop an Ontario Public Service Enterprise Application Portfolio Management (APM) Framework to address the risks associated with older systems. As part of this framework, the clusters have defined the type of data they want to monitor to ensure their systems meet user needs. This data includes information on the criticality of the system, the age

of the system and whether there is a plan to update or replace the system in the next two years. This data has been collected for all I&IT systems and is used by I&IT clusters and the Ministry of Government and Consumer Services to conduct high-level risk assessments. We reviewed documentation that assessed the risks identified through the APM system and identified action plans to address the risks.

The I&IT organization is currently implementing a strategy to identify and review end-of-life I&IT systems and servers. The Office of the Corporate Chief Information Officer and I&IT clusters have created risk profiles of Ontario Public Service servers. These risk profiles highlighted servers running end-of-life software and operating systems, and flagged related business risks. They also provided updates to ministries on how risks are evolving, to support planning and priority setting. Additionally, the Ministry of Government and Consumer Services plans to conduct annual proactive cyber-risk assessments on prioritized systems that have been identified as presenting a risk.

Modernization Efforts Significantly Delayed

Recommendation 7

We recommend that the I&IT organization along with their respective ministries assess the cost and need to update and maintain current systems and the risks arising from using aged systems versus the costs and benefits of replacing these systems. Based on the assessments, review and revise the current five-year strategy plan released in 2016.

Status: In the process of being implemented by March 2021.

Details

In our 2016 audit, we noted that in 2006, Ontario's Major Application Portfolio Strategy (MAPS) had identified 77 of 153 major applications that needed to be replaced or upgraded. At the time of our audit, 11 systems were still overdue for replacement or upgrading, including the Court System and Licensing System. We noted as well issues with project management and costs related to the modernization of some I&IT systems.

At the time of this follow-up, the I&IT clusters have completed over 450 (40%) of 1,153 cost-benefit assessments. There is a large difference in the number of assessments completed by each cluster. Some have completed assessments on all or most of their I&IT systems, while others have completed assessments on only 3–5% of their systems.

As stated earlier, risk assessments on aging systems are done under the Application Portfolio Management Framework. We reviewed a sample of the documentation from several clusters and found that risk assessments had been completed to analyze the need to upgrade systems, and that these assessments stated the risks of using aging systems. The clusters analyzed the costs and benefits of modernization of systems through business cases, assessment reports, and program review renewal and transformation exercises.

An IT Governance Branch was created within the Office of the Treasury Board to establish and maintain effective IT governance frameworks. It is working with I&IT clusters to co-ordinate investment in new systems.

The Office of the Corporate Chief Information Officer and the Information Technology Executive Leadership Council have begun preparing for an update of the 2016 five-year strategy. The next I&IT strategy will begin to be revised in 2019 and will be released in 2020.