Chapter 4
Section
4.03

# Information and Information Technology General Controls

## 1.0 Executive Summary

The Ontario government relies on information and information technology (I&IT) to deliver the wide variety of services and operations it administers for the public, including health, education, social services and justice. Our initial audit of I&IT looked at the government's I&IT policies and procedures and assessed whether there are effective general controls in place to maintain the integrity of I&IT systems.

The first government-wide I&IT strategy was released in 1998 to establish a common I&IT infrastructure and governance structure across all ministries (prior to 1998, the government had a decentralized approach to I&IT whereby each ministry had its own I&IT function). The strategy introduced a "clustering" approach whereby I&IT services would be delivered to "business clusters," which are groupings of government programs and services that have similar clients and need similar services, such as the grouping of the Community and Social Services and Children and Youth Services. Over the years, the government's I&IT strategy has evolved to address its changing needs and priorities. The current I&IT strategy (2016–2020) is focused on using technology to improve the delivery of government programs, updating old and outdated I&IT systems, and enabling the analysis of data for decision-making purposes.

The current I&IT organization is made up of the Office of the Corporate Chief Information Officer, three service branches responsible for certain common government-wide services and units supporting ministries organized into nine business clusters. The I&IT organization supports more than 1,200 I&IT systems across the government and has annual expenditures of about $1.3 billion.

We began our audit with a review of service-level agreements for all I&IT systems across the government's nine business 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 found that 75% of government I&IT systems do 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. Months into our audit, in April 2016, the Central Agencies cluster drew up a second agreement (for a total of two of the 168 systems it supports); it plans to use these as templates for rolling out more I&IT service level agreements.

To understand how I&IT general controls are managed, we selected three key systems in three separate business clusters to review:

- 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' licenses.

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. They control authorized access to the I&IT systems (*confidentiality*), changes to the I&IT systems (*integrity*), and backup and recovery of systems (*availability*).

Overall, we found that I&IT management is moving in the right direction when it comes to the backup, recovery and operation of I&IT general controls, particularly with the Tax System, which is a relatively newer system than the other two. However, we did find that all three systems needed improvement with implementing controls to prevent unauthorized access to confidential information.

We also noted challenges implementing changes to the Court and Licensing systems, due to concerns that making changes to these outdated systems could corrupt functionality or possibly cause them to crash. Innovation that could improve service delivery is not occurring as a result. When programmers did make changes, we found examples that go against best practice in computer management, such as programmers entering actual data into the Court System. This could result in programmers inadvertently—or fraudulently—entering inaccurate data or altering existing data.

The government initiated projects to replace outdated I&IT systems, however these projects have been significantly delayed. In 2009/10, the Treasury Board approved spending $600 million under the Major Application Portfolio Strategy (MAPS) for the replacement and remediation of 77 I&IT systems across the government. As of June 2016, 66 of these applications had either been retired (17) or upgraded (49). In 2012, the government moved responsibility for the replacement and upgrading of I&IT systems from a central team, which was managed by the Ministry of Government Services, to the individual I&IT clusters supporting the ministries. At the time, $121 million had been spent on MAPS. Of the remaining $479 million, $316 million was transferred by Treasury Board to the relevant Ministries that would ultimately have ownership of the modernized systems. The rest ($163 million) was retained by the Treasury Board. By doing this, Treasury Board hoped that the individual ministries would find additional funding from within their regular capital expenditure budgets to support the I&IT modernization projects.

Although two of the three systems we audited, the Court System and Licensing System, were flagged as overdue for replacement and modernization under MAPS in 2009/10, they still have not been replaced or modernized:

- $11 million was initially spent with a goal of replacing the Court System as part of a much larger I&IT project. The project was unsuccessful mainly due to weak project governance and oversight; insufficient project management procedures; and lack of functionality and integration of the vendor-developed modules. Accordingly no new system was developed, though the government was able to reallocate about $6.5 million worth of hardware and software to other operations. The remaining $4.5 million was written off. Since then, no plan has been put in place that estimates when the existing Court System will be replaced.

- The Licensing System was initially planned to be replaced as part of the Road User Safety Modernization Project (initiated in 2009) by 2016. The project was delayed because management revised their original approach of modernizing the complete system in five years to a phased roll out of the project in three segments. Poor performance from the external vendor, whose contract was terminated, also delayed the project. As of March 2016, $182 million had been spent on the first segment, now expected to be finished by the end of 2016, at an estimated cost of $203 million. The cluster has not yet done an assessment on the timelines and costs associated with the remaining two segments.

The age of the Court System and Licensing System in itself might not be a critical issue if the Ministries were regularly updating them and managing their staffing in an efficient way. However, we noted concerns with the lack of continuous training and knowledge transfer, maintenance being limited, and functionality issues in the government I&IT systems we audited. Because the Court and Licensing systems were originally slated for replacement, annual funding for maintenance to these systems was reduced significantly. Maintenance for these systems has been minimal since 2009, and restricted to levels that allow the ministries to meet only their legislative requirements, rather than enhance their service delivery as had been the intent under MAPS.



# 2.0 Background

## 2.1 The Ontario Government's Information and Information Technology (I&IT) Needs

The Ontario government needs 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 government processes billions of transactions each year and uses I&IT to support and enable the government in areas such as:

- planning, (for example, providing financial data and information as part of the annual budgeting exercise) which requires accessing and analyzing information stored in large databases;
- delivering services to the public (for example, paying social assistance, registering businesses, renewing vehicle licences), which requires information linkages with provincially-funded organizations that serve the public's health, education, social services, justice and safety needs;
- administering its activities, which requires operations to, for example, process health insurance claims; keep records of births and deaths; manage its human resources, finances and business processes; and interact with businesses, investors, trading partners and other governments; and
- evaluating and improving its activities, which requires establishing standards, and measuring and managing outcomes.

## 2.2 The Evolution of the Government's Vision and Strategy for I&IT

### 2.2.1 The 1998 I&IT Strategy

Before 1998, the Ontario government had many different I&IT systems and organizations serving each ministry. This began to change when an I&IT strategy document titled *Using Information Technology to Transform Government for the 21st Century* was released in 1998. This document stated:

> At present, the government has too many different information technology systems with little integration between ministries and weak links to the broader

public sector. Computers acquired for particular purposes are incompatible and cannot talk to each other electronically, while different networks make it hard to implement systems across ministries. Diffuse accountability undermines overall financial control of Information Technology (IT) spending. Single-year budgeting means that IT is treated as a cost not an investment, creating barriers to the replacement of older, fragile systems. Moreover, given the tight market for information and information technology skills, ministries on their own cannot assemble the human resources needed to meet all their information technology objectives.

The 1998 strategy:

- put a new government-wide I&IT organization in place, headed by the first Corporate Chief Information Officer;
- introduced "clustering": rather than having I&IT services delivered to individual ministries, I&IT services would be delivered to "business clusters," which are groupings of government programs and services that have similar clients and similar client needs, and need similar services; and
- set up a governance structure that included assigning a Chief Information Officer to each business cluster, who would report to both the deputy ministers in the cluster and the Corporate Chief Information Officer.

A key goal of the 1998 strategy was a common I&IT infrastructure, with underlying I&IT systems that could exchange information with each other. Such an infrastructure would enable a "one-window" approach to service delivery. This means services are delivered electronically instead of using paper forms, and should be delivered more quickly and simply as a result. ServiceOntario, the "one window" delivering services to individuals, was one of the business initiatives under way at the time that urgently required changes to the government's I&IT capacity. (ServiceOntario provides Ontarians with centralized access to a variety of services, such as renewing drivers' licences, registering a business name and applying for an OHIP card, all in one location.) The strategy was to lead the government to set up other "one-stop" service centres where clients need go to just one physical place for all kinds of different services. This was envisioned as a way to both improve service delivery and achieve cost efficiencies in I&IT.

### 2.2.2 The 2005 eOntario Strategy

In 2005, Cabinet approved eOntario as the government's updated I&IT strategy. The eOntario strategy focused on consolidating I&IT resources and centralizing I&IT infrastructure. This included:

- moving from eight help desks to one service desk;
- moving from eight email systems to one;
- centralizing the separate IT departments serving the 22 ministries in government at the time;
- replacing the Office of the Corporate Chief Service Delivery and iSERV (the government's I&IT infrastructure provider) organizations with a central organization called Infrastructure Technology Services.

The vision was for Ontario Public Service employees to get help from a single service desk, communicate across a single email system and have their desktop computers set up and maintained under a single provincial standard.

By 2007, major changes to I&IT had been completed, including refining the clusters. Those advances notwithstanding, the task of infrastructure consolidation is a gradual process and to a certain extent is still ongoing.

### 2.2.3 The 2008 Strategic Plan: *Beyond eOntario 2008–13*

The focus of the 2008 strategic plan, titled *Beyond eOntario 2008–13*, was on containing I&IT costs by

coming up with more cost-effective I&IT solutions. The 2008 strategic plan also continued the push toward a more centralized co-ordination approach to overseeing upgrading of I&IT systems, which it called developing "enterprise" systems or "enterprise-wide" services. ("Enterprise-wide" means encompassing the entire organization rather than a single business department or function.) Other continuing goals were improved service delivery, information management and collaboration, as well as acquiring dependable and professional I&IT staff.

### 2.2.4 From 2013 to 2016

Between 2013 and 2016, there was no corporate I&IT strategy. The I&IT organization was still working on achieving the goals of the strategy for 2008–13. However, consultations on the next iteration of the I&IT organization's multi-year strategy started in 2011, well before the expiration of the Beyond eOntario Strategic Plan. These consultations revealed a major shift in concepts about how public services should be delivered, focusing on consumer technologies and evolving digital approaches (such as Internet-based delivery of services and the use of mobile apps) that needed to be reflected in the long-term objectives of the organization. Also, significant changes in senior leadership within I&IT distracted management from setting strategy.

### 2.2.5 The 2016 Strategy: *Digital Government*

The latest five-year strategy plan was released in April 2016 for the period 2016–20. Its key priorities are:

- digital public services—improve the delivery of government programs with better digital technologies and services;
- business innovation—update old and outdated IT systems (or at least make them compatible with newer technologies) to improve service and the speed of delivery, improve responsiveness, and move away from relying on products tied to a specific vendor; and
- information assets—help the government store, access, process, manage, analyze and use the huge amounts of data it collects to be more effective and bring real value to ministries, citizens and businesses.

## 2.3 Current I&IT Organization

The current I&IT organization has its head office within the Province's Treasury Board Secretariat. It is made up of the Office of the Corporate Chief Information Officer, three service branches responsible for certain common government-wide services and nine I&IT units supporting ministries organized into business clusters. **Figure 1** shows the relationships between these three I&IT organization components, and the role of the Treasury Board Secretariat, which funds enterprise-wide IT initiatives and oversees the co-ordination of the standardization of I&IT for all of government.

The I&IT organization as a whole had about 4,400 staff and 1,153 full-time consultants working as of March 31, 2016.

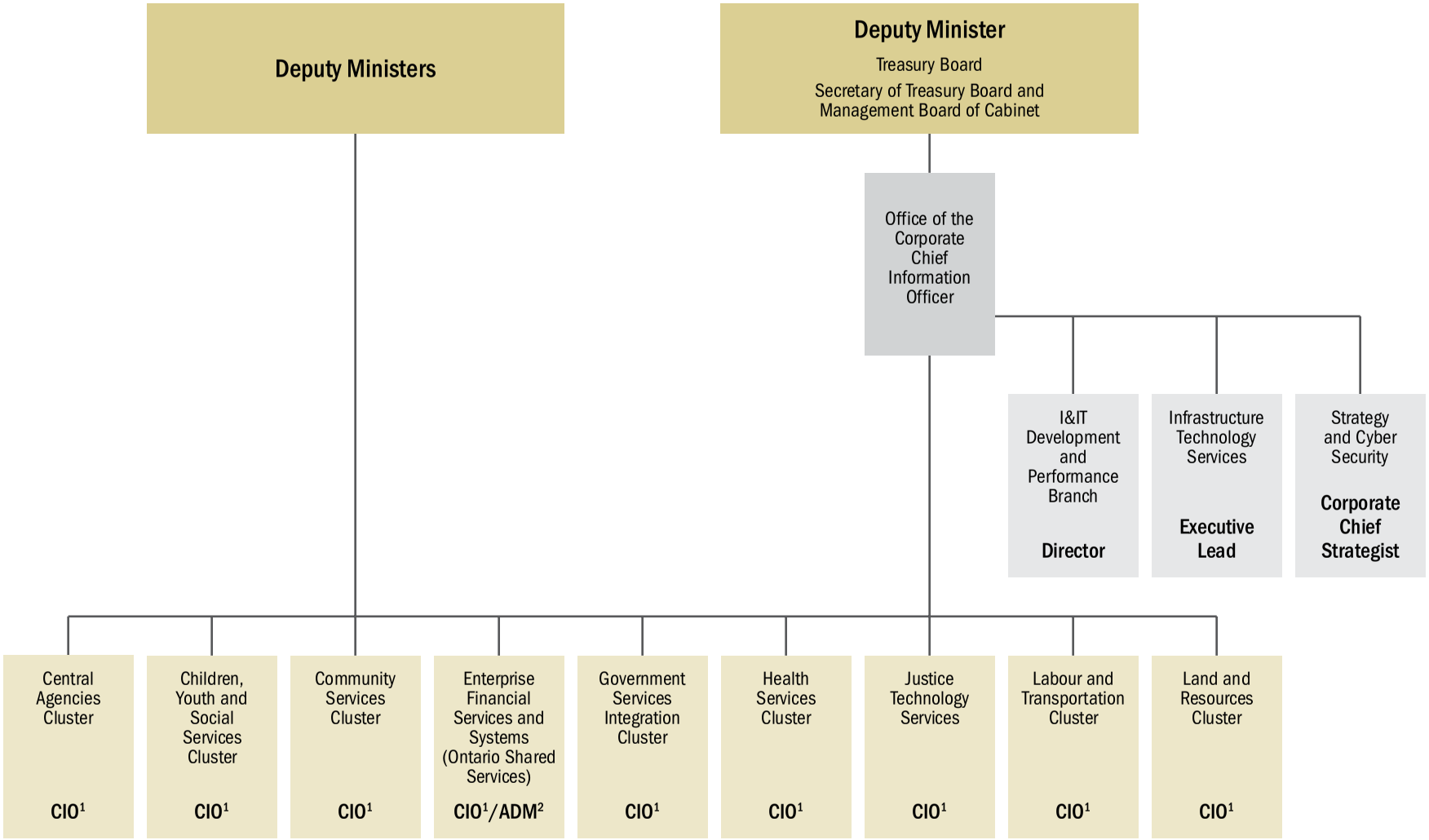
### 2.3.1 Office of the Corporate Chief Information Officer

The Corporate Chief Information Officer heads the I&IT organization and works with the Treasury Board Secretariat to make strategic and security decisions on technology and 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.

## Figure 1: I&IT Organization Structure

Source of data: Office of the Corporate Chief Information Officer




1. Chief Information Officer
2. Assistant Deputy Minister

### 2.3.2 Three Service Branches

The three service branches are responsible for government-wide services and report to the Corporate Chief Information Officer.

#### Infrastructure Technology Services

The Infrastructure Technology Services branch is responsible for:

- corporate services —includes I&IT procurement oversight and execution and the costing and pricing of I&IT services government-wide;
- customer relationship management—ensures the delivery of services to the I&IT clusters and their ministry business areas;
- data centre operations;
- desktop and field support services;
- enterprise planning and project delivery services for ministry clients;
- I&IT infrastructure project delivery;
- service management—ensures incident, change, and service level management are functioning efficiently;
- telecommunications—such as telephone, voicemail, audio and video conferencing services; and
- business continuity planning.

#### I&IT Strategy and Cyber Security

The I&IT Strategy and Cyber Security branch leads the development of I&IT strategy and policies. It is also concerned with performing corporate technical reviews of I&IT systems and provides advice to the I&IT Project Approval Committee on relevant I&IT projects.

#### I&IT Development and Performance

The I&IT Development and Performance branch is made up of three units:

- I&IT learning;
- I&IT strategic marketing and communications; and
- performance measurement and reporting.

### 2.3.3 Nine I&IT Clusters

In each of nine business clusters, I&IT staff and consultants support the ministries' I&IT systems. The clusters service more than 1,200 I&IT systems in 30 ministries and offices. **Figure 2** lists the ministry clients of each business cluster and examples of key I&IT systems that each business cluster supports.

Each cluster provides day-to-day I&IT support to its ministry clients and for the ministry-owned I&IT systems. The support covers I&IT security, managing hardware and software program changes, and ensuring the systems operate continuously and reliably. Each cluster is led by its own Chief Information Officer, who reports to the deputy ministers of the individual ministries that the cluster supports as well as to the Corporate Chief Information Officer.

## 2.4 I&IT Funding

The Treasury Board Secretariat funds most enterprise-wide I&IT initiatives. The ministries fund their own ministry-specific I&IT initiatives and services.

During 2015/16, the Treasury Board Secretariat and individual ministries combined spent $1.3 billion on I&IT expenditures. **Figure 3** shows the total expenditures for the 10-year period from 2006/07 to 2015/16. Expenditures (mainly capital) climbed sharply in 2011/12—by almost $122 million—due to the completion of projects to modernize several older systems, and in 2015/16 (mainly operational) by almost $119 million mainly due to several smaller projects being initiated.

**Figure 4** and **Figure 5** show the operational and capital expenditures of the I&IT organizational units from 2013/14 to 2015/16.

## 2.5 Controls over I&IT Systems

There are two types of controls over I&IT systems: application controls and general controls.

I&IT application controls (also known as program controls) are checks embedded within specific computerized software applications (for

## Figure 2: I&IT Business Clusters' Clients and Select Key I&IT Systems Supported

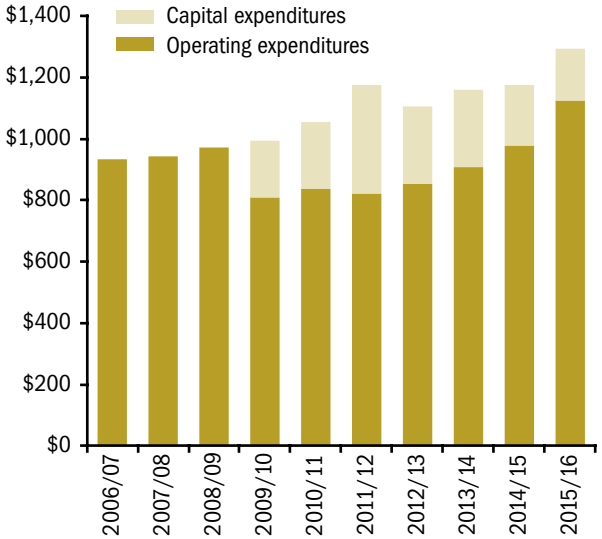
Source of data: Office of the Corporate Chief Information Officer

| I&IT Cluster | Ministry/Office Client | Select Key I&IT Systems Supported |
|---|---|---|
| Central Agencies | • Cabinet Office<br>• Finance<br>• Intergovernmental Affairs<br>• Treasury Board Secretariat | • Ontario Tax Administration System* (records all tax revenue collected) |
| Children, Youth and Social Services | • Children and Youth Services<br>• Community and Social Services | • Child Protection Information Network (documents child protection case information)<br>• Social Assistance Management System (used for administration of social assistance cases) |
| Community Services | • Advanced Education and Skills Development<br>• Citizenship and Immigration<br>• Education<br>• International Trade<br>• Municipal Affairs Housing<br>• Tourism, Culture and Sport<br>• Women's Directorate | • Case Management System (supports the administration of clients participating in Employment Ontario programs)<br>• Ontario Student Assistance Program system (processes student loan applications) |
| Enterprise Financial Services and Systems | • Ontario Shared Services (part of Government and Consumer Services) | • Integrated Financial Information System (records the Province's financial information) |
| Government Services Integration | • Economic Development and Growth<br>• Energy<br>• Francophone Affairs<br>• Government and Consumer Services<br>• Infrastructure<br>• Research, Innovation and Science<br>• Seniors' Secretariat | • Ontario Business Information System (records information pertaining to organizations registered to do business in Ontario)<br>• Workforce Information Network (processes payroll for all employees of the Ontario Public Service) |
| Health Services | • Health and Long-Term Care | • Medical Claims Processing System (processes medical claims submitted under the Ontario Health Insurance Plan)<br>• Health Network System (processes claims submitted under the Ontario Drug Benefit Program) |
| Justice Technology Services | • Attorney General<br>• Community Safety and Correctional Services | • Integrated Court Offences Network* (supports the administration of the Ontario Courts of Justice)<br>• Offender Tracking Information System (records data pertaining to offenders) |
| Labour and Transportation | • Labour<br>• Transportation | • Licensing Control System* (processes licensing and registration transactions relating to drivers and vehicles)<br>• Capital Improvement Delivery System (maintains construction plans and manages expenditures for all road improvements) |
| Land and Resources | • Agriculture, Food and Rural Affairs<br>• Environment and Climate Change<br>• Indigenous Relations and Reconciliation<br>• Natural Resources and Forestry<br>• Northern Development and Mines | • Drinking Water Information Management System (manages and reports data on drinking water facilities and water quality)<br>• Environmental Approvals and Sector Registry (registration for low-risk businesses having a possible impact on the environment) |

* These I&IT systems were reviewed for this report.

**Figure 3: I&IT Total Operating and Capital Expenditures, 2006/07–2015/16 ($ million)**

Source of data: Office of the Corporate Chief Information Officer




Note: Before 2009/10, the Office of the Provincial Controller had not instituted capitalization of IT assets and services and there was no government policy in place for them.

example, payroll, accounts receivable and order processing) that I&IT systems automatically perform to ensure that data entered and transactions processed are done completely and accurately, from input through output. For example, an edit check where a user cannot input an alphabet character in a numeric field.

I&IT general controls, the focus of our audit, 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. I&IT general controls typically cover security over who can access the system and perform maintenance and changes to the system, and procedures for backing up and restoring should the system fail. The following subsection describes I&IT general controls in detail.

### 2.5.1 Specific Outcomes of Good I&IT General Controls

When an organization has established comprehensive and effective I&IT general controls, it has reasonable assurance that its I&IT systems are secure and operating in a proper environment, in that:

- Only authorized staff can access I&IT systems and data; unauthorized access is prevented.
- Computer hardware is physically secure (for example, access to rooms where servers operate is restricted to I&IT staff; computer equipment is protected against fires and extremes of temperature and humidity).
- The process of developing new systems or changing existing systems is managed and controlled to ensure only planned outcomes are achieved and properly documented.
- Processing problems (for example data is not transferred completely and accurately between two systems) are identified and resolved completely, accurately and quickly so data integrity and system reliability is maintained.
- Backup, restart and recovery procedures are in place with the technical documentation available, so processing that ends abnormally does not result in system damage or data loss, and recovery time to full functionality is minimal.
- I&IT staff follow procedures for setting up computer processing jobs (such as batch jobs used to process multiple transactions at the same time), operating software and hardware.

### 2.5.2 Key Risk Areas that Good I&IT General Controls Should Address

We identified, based on research and best practices, nine key risk areas that effective I&IT general controls should address:

- *Service-level agreements*—A contract between the I&IT cluster management and ministries it serves should be established that formally and clearly sets out each party's roles and responsibilities for governance, accountability and

### Figure 4: I&IT Operational Expenditures by Organizational Unit, 2013/14–2015/16 ($ million)

Source of data: Office of the Corporate Chief Information Officer

| I&IT Unit Area | 2013/14 | 2014/15 | 2015/16 | Total |
|---|---|---|---|---|
| Office of the Corporate Chief Information Officer | 175 | 172 | 147 | **494** |
| Children and Youth cluster | 114 | 132 | 153 | **399** |
| Health cluster | 84 | 129 | 140 | **353** |
| Central Agencies cluster | 129 | 123 | 98 | **350** |
| Community Services cluster | 105 | 119 | 115 | **339** |
| Justice cluster | 51 | 51 | 171 | **273** |
| Labour and Transportation cluster | 85 | 90 | 90 | **265** |
| Land and Resources cluster | 87 | 76 | 85 | **248** |
| Government Services cluster | 58 | 68 | 110 | **236** |
| Enterprise Financial cluster | 19 | 19 | 17 | **55** |
| **Total** | **907** | **979** | **1,126** | **3,012** |

### Figure 5: I&IT Capital Expenditures by Organizational Unit, 2013/14–2015/16 ($ million)

Source of data: Office of the Corporate Chief Information Officer

| I&IT Unit Area | 2013/14 | 2014/15 | 2015/16 | Total |
|---|---|---|---|---|
| Office of the Corporate Chief Information Officer | 30 | 57 | 52 | **139** |
| Labour and Transportation cluster | 32 | 47 | 48 | **127** |
| Children and Youth cluster | 79 | 35 | 12 | **126** |
| Health cluster | 43 | 21 | 20 | **84** |
| Community Services cluster | 21 | 19 | 4 | **44** |
| Government Services cluster | 25 | 7 | 7 | **39** |
| Justice cluster | 4 | 4 | 19 | **27** |
| Land and Resources cluster | 16 | 5 | 3 | **24** |
| Central Agencies cluster | 5 | 3 | 4 | **12** |
| **Total** | **255** | **198** | **169** | **622** |

Note: Capital expenditures are based on Ministry allocations as opposed to I&IT clusters. The Office of the Corporate Chief Information Officer does not have oversight over these expenditures as they are the responsibility of each ministry. Therefore the Office of the Corporate Chief Information Officer did not have the source data to calculate expenditures at a cluster level. We have combined the Ministry capital allocations under supporting clusters to provide an indication of the amount being spent on capital expenditure pertaining to IT. This expenditure would include both I&IT related and Ministry related IT capital expenditures.

expected performance and quality of service in accordance with the ministries' current and future needs.

- *I&IT human resource management*—Adequate staffing levels and skills should exist to ensure effective controls, maintenance and operations are achieved to meet expected service levels.
- *Logical security*—Controls should exist to ensure only authorized users have access to and can use data, programs and networks. Examples of controls are user IDs and passwords to authenticate users, and restricting access to systems.
- *I&IT operations*—Activities and operational procedures required to support the delivery of I&IT services, including the execution of pre-defined standard operating procedures and the required monitoring activities should be in place.

- *Change management*—Controls should exist to ensure changes to key systems are made quickly, reliably and have minimal negative impact on the system's stability or integrity.
- *Incident management*—Controls should exist to ensure user queries and incidents (such as service interruptions) are resolved as soon as possible.
- *Problem management*—Controls should exist to ensure not only that there are as few operational issues as possible, but that the number of issues steadily decreases, thereby increasing system availability, improving service levels, reducing costs and improving customer convenience and satisfaction.
- *Availability and capacity management*—Controls should exist to ensure that the use of I&IT services is monitored, performance expectations are met and plans are made to predict and meet future user needs. This will enable services to be available whenever needed, resources to be managed efficiently and systems to be high-performing.
- *Business continuity and disaster recovery*—Effective processes should exist to address unexpected events that disrupt operations (for example, power failures, IT system crashes) in order to restore or recover operations and information as quickly as possible.

## 3.0 What We Looked At

For our first audit of government I&IT systems, we looked at whether the government has effective I&IT policies, procedures and controls in place covering security, changes, operations, availability, capacity, continuity and disaster recovery to ensure the integrity of government I&IT systems and data files.

To do this, we examined I&IT general controls for three key I&IT systems managed by the I&IT organizations:

- the Ministry of Transportation's Licensing Control System (Licensing System), serviced by the Labour and Transportation Cluster;
- the Ministry of the Attorney General's Integrated Court Offences Network (Court System), serviced by the Justice Technology Services Cluster; and
- the Ministry of Finance's Ontario Tax Administration System (Tax System), serviced by the Central Agencies Cluster.

**Figure 6** outlines the key features of these three I&IT systems.

The selection of these three systems allowed us to audit systems across three different ministries and I&IT clusters and look at two older I&IT systems (Court System and Licensing System) and one relatively newer one (Tax System). We interviewed I&IT cluster and ministry staff, reviewed key documents and reports, and observed procedures and controls in action at the three ministries that own the three systems (that is, 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 was 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.

Prior to commencing our work we identified the criteria we would use, which were reviewed and agreed to by the Chief Information Officers of the I&IT clusters for the three ministries. We also reviewed relevant audit reports issued by the province's Internal Audit Division. These reports were helpful in determining the scope and extent of our audit work. Most of our work was conducted between December 2015 and June 2016.

**Figure 6: Key Features of I&IT Systems We Audited**

Source of data: Central Agencies cluster, Justice Technology Services cluster and Labour and Transportation cluster

| | Ministry of the Attorney General's Court System | Ministry of Transportation's Licensing System | Ministry of Finance's Tax System |
|---|---|---|---|
| Main function | Supports the administration of the Ontario Court of Justice | Processes licensing and registration transactions relating to drivers and vehicles | Administers tax revenue and benefits programs |
| Core applications/ subsystems/modules | • Case Management (adult and youth criminals and offenders)<br>• Scheduling of court cases<br>• Financial (fines, fees, costs, bail and restitution) | • Driver Licensing and Control System<br>• Vehicle Registration System<br>• Commercial Vehicle Operator Registration System<br>• Motor Vehicle Inspection Station System | Manages client tax rolls, assessments, payments, collections and audits for:<br>• retail sales tax<br>• gas and fuel tax<br>• tobacco tax<br>• land transfer tax<br>• beer and wine tax<br>• debt retirement charge |
| Year implemented | 1989 | 1967 | 2006 |
| Last major upgrade | 2013 | 2010 | 2014 |
| Number of users | 5,000 | 3,300 | 1,000 |
| Average transactions/ month | 10 million (2015) | 30 million (2015) | 400,000 (2015) |
| Total Annual Revenue processed | $270 million (2016) | $1.5 billion (2016) | $16 billion (2016) |
| Data volume | • 18.5 million court cases<br>• 120 courts | • 10 million drivers<br>• 33 million vehicles | • 2.2 million taxpayers |
| Number of I&IT staff/ contractors servicing system | • 1 staff, 1 contractor dedicated to system<br>• 3 other staff support this and other systems | • 10 staff, 14 contractors dedicated to system<br>• 114 other staff, 61 contractors support this and other systems | • 37 staff, 15 contractors dedicated to system |

# 4.0 Key Observations and Recommendations

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

Although the establishment and monitoring of service-level agreements between a client (such as a ministry) and its service provider (such as an associated I&IT cluster) is one of the criteria that good I&IT general controls should address (see **Section 2.5.2**), until June 2016, which is when our audit was substantially completed, few such agreements had been drawn up. 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. A service-level agreement ensures that I&IT clusters agree with the ministry's expectations and clearly sets out the roles and responsibilities of the I&IT cluster and ministries, performance expectations, and accountability measures to ensure they are consistently met by the individual I&IT clusters. Without service-level

agreements in place, ministries and their respective I&IT clusters leave themselves open to a variety of issues, such as not having sufficient infrastructure to meet the ministries' needs and unauthorized changes being made to information. **Figure 7** outlines key elements that should be included in service-level agreements and the potential risk or impact if they are not.

When we began our audit, there were no service-level agreements in place between the ministries and three I&IT clusters for the three systems in the scope of our audit. In cases where agreements were in place, such as with the Justice Technology Services cluster, they were very generic, poorly formulated and, being more than ten years old, not reflective of current processes. Moreover, I&IT staff were not using them and relevant staff at the Ministry of the Attorney General told us they were not aware the agreements even existed to hold the clusters to expected performances. When the I&IT clusters were being formed in the mid-2000s, there was the opportunity for service-level agreements to be drawn up as an integral part of the process as the ministries and clusters began working together. However, this did not occur. We also found no evidence of the Office of the Corporate Chief Information Officer establishing and monitoring the implementation and use of service-level agreements across the clusters.

**Figure 7: Elements that Should Be Included in Service-Level Agreements, and Potential Risk or Impact If They Are Not**
Prepared by the Office of the Auditor General of Ontario

| Service-Level Element | What Should Be Included | Potential Risk or Impact When Not Addressed |
|---|---|---|
| Roles and Responsibilities | Which party (specific ministry department or I&IT cluster team) is responsible for what aspect of the service delivery, reporting and monitoring. | Lack of ownership of issues and accountability, and breakdown in communication. |
| Service times | How quickly service is to be provided. | Users dissatisfied with how quickly service is provided. |
| Availability considerations | Includes how much downtime is acceptable and what rate of service failure is allowed. | System is down or fails far more often than expected. |
| Performance requirements | Explicitly stated targets geared to each different operation (e.g., each user interaction with the system should have an ideal satisfactory response time). | System fails to function as required. |
| Capacity needs | Assessment of a ministry's capacity needs so that I&IT can assess whether the existing infrastructure is sufficient or needs to expand. | Existing system infrastructure is insufficient to meet the ministry's needs. |
| Security requirements | Requirements relating to the confidentiality of the system and its data. They need to be explicitly stated (including what must not be allowed to happen) for security testing to take place. They cover things like authenticating the user's identity and right to access the system, and backup procedures. | Unauthorized changes are made to information, unauthorized individuals access sensitive information, and ministry may not have any way of knowing about it. |
| System and service continuity | This includes, among other things, the policies, standards and processes for preventing, predicting and managing actual and potential disruptions of the system and services. | Ministry operations shut down for an unacceptably long period when systems stop working because of a disruption/disaster. |
| Compliance and regulatory issues | The steps to be taken to comply with laws and regulations, as well as internal and external guidelines and standards relevant to I&IT. | No controls designed to comply with—such as protection of personal information—leaving the ministry liable to be in violation of the relevant laws or regulations. |
| Demand constraints | The rate at which processes need to run to meet the demand placed on them needs to be specified. | Processes do not run at the right rate (fast enough and at the most efficient rate). |

**Figure 8: Current Status of Service-Level Agreements**
Source of data: I&IT clusters

| I&IT Business Clusters | Service-Level Agreements in Place? | Reporting Being Performed Over Service-Level Agreements? |
|---|---|---|
| Central Agencies | 1% (2 out of 168 systems) | None |
| Children, Youth and Social Services | 2% (3 out of 159 systems) | Limited |
| Community Services | 39% (46 out of 118 systems) | Limited |
| Government Services Integration | 55% (120 out of 210 systems) | Limited |
| Health Services | 100% (84 out of 84 systems) | Limited |
| Justice Technology Services | 0 out of 94 systems | None |
| Labour and Transportation | 0 out of 166 systems | None |
| Land and Resources | 22% (54 out of 246 systems) | None |
| **Overall** | **25% (309 out of 1,245 systems)** | |

Months into our audit, in April 2016, the Central Agencies cluster drew up a second service-level agreement (for a total of two of the 168 systems it supports), which was signed and approved by the Ministry of Finance. The cluster identified that they plan to use these service-level agreements as a template to roll out to the other 166 systems.

All of the nine I&IT clusters should have service-level agreements in place with the 30 ministries and offices they currently serve. These service-level agreements should cover the approximately 1,200 I&IT government systems. Depending on the size and nature of the I&IT systems being supported, one service-level agreement could cover multiple systems.

**Figure 8** outlines the status of service-level agreements across the clusters as of the completion of our audit.

### 4.1.1 Service-Level Agreements Essential to Meeting Current I&IT Strategic Objectives

Service-level agreements can be used as an effective tool for the implementation of the strategic objectives stated in I&IT's 2016-20 strategy. Service-level agreements help to translate objectives at the strategic level into more concrete key performance indicators. In other words, they help to clarify what performance levels at a minimum must be achieved in order for the overall strategic objectives to be met.

As mentioned in **Section 2.2.5**, key components of the I&IT strategy for 2016–20 are "digital services", "business innovation" and "information assets." Well-formulated service-level agreements are needed to spell out specifically what I&IT must do to achieve all of the above—that is, what it must do to make I&T services and responsiveness better and faster. Without having service-level agreements in place and reporting over these, the government will never be able to get a sense of how effective the I&IT strategy is. This is also highlighted by the fact that, between 2013 and 2016, there was no corporate I&IT strategy as I&IT was still working on achieving the 2008-13 strategy. Had there been appropriate service-level agreements in place earlier (aligned with the I&IT strategy) and sufficient reporting and monitoring over these, the government would have been able earlier to devote the additional efforts needed to ensure that actual performance stays on track to meet the strategic objectives.

#### 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;
- set out specific, measurable, attainable, reportable and time-bound performance requirements;
- state agreed service times;
- outline availability and compliance and regulatory considerations;
- identify security requirements and capacity needs;
- set out the policies and procedures for system and service continuity; and
- ensure that service levels are monitored by requiring I&IT clusters to report regularly to ministries on their achievement of expected performance.

### I&IT ORGANIZATION RESPONSE

The I&IT organization and ministries agree with the Auditor General and recognize and accept the critical importance of service management to the overall I&IT strategy and to ensuring high-quality services that meet the needs of government organizations. We acknowledge the need to ensure service-level agreements are in place for all I&IT systems and, to this end, the I&IT organization has recently established a new enterprise service management (eSM) division. Led by a Chief Information Officer and reporting directly to the Corporate Chief Information Officer, the mandate of eSM will include:

1. Establishing a defined Government of Ontario IT Standard (GO-ITS) for service level management that ensures service-level agreements are in place between all clusters and ministries and that they include the nine key elements identified in the audit report.
2. Expanding the scope of existing service-level agreements to more closely align with the current 2016 I&IT Strategy and also include performance metrics for mission and business critical ministry applications.
3. Ensure regular reporting to ministries on the performance of mission and business critical applications compared to the expected performance.

## 4.2 I&IT General Controls Can Be Improved

We assessed each of the three systems selected on the nine risk areas of I&IT general controls (**Figure 9** presents a summary of our findings). Based on our audit, we noted weaknesses (to various degrees) in seven areas for the three systems we looked at:

- *Service-level agreements*—At the time of our audit, neither the Court System nor the Licensing System had formal service-level agreements in place. In addition, we noted that there is no formal monitoring and reporting of service performance, an expectation that should be included in such agreements.
- *I&IT human resource management*—Of the three systems audited, we noted that the Court System had inadequate support staff, relying on just one external consultant and one staff member to maintain the system. The age of this system is a factor to these staffing challenges, as described in **Section 4.3.1**.
- *Logical security*—There were issues with all three I&IT systems (in varying degrees) noted where users were granted inappropriate access to sensitive and confidential data. With the Court System in particular, there was 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 any access at all. Activity logs are not reviewed for appropriateness for the Court and Licensing Systems. Management for all three systems have not reviewed user roles and access permissions on a regular basis to validate if individuals still require access based on their current job function.

**Figure 9: Summary of I&IT General Controls In Place at Three Systems Audited**
Prepared by the Office of the Auditor General of Ontario

| I&IT General Controls Area | Court System | Licensing System | Tax System |
|---|---|---|---|
| Service-level agreements in place | No | No | Yes |
| Adequate human resources and staffing | No | Yes | Yes |
| Sufficient logical security controls to prevent unauthorized use | No | No | No |
| Adequate operational procedures to support service delivery | No | Yes | Yes |
| Effective change management procedures in place | No* | No* | Yes |
| Efficient incident management controls | No | Yes | Yes |
| Formal problem management procedures in place | No | No | No |
| Monitoring and planning for system availability and capacity management | Yes | Yes | Yes |
| Effective business continuity and disaster recovery processes | Yes | Yes | Yes |
| **Areas that need improvement** | **7/9** | **4/9** | **2/9** |

* Formal change management procedures are in place, but system changes are taking more time and effort to implement due to system age and complexity.

- *I&IT operations*—The Court System lacked documented I&IT operational procedures and had no process in place to verify that batch jobs (functions that process multiple transactions at the same time, usually overnight) were completed successfully.
- *Change management*—We noted that while all three systems had formal change management procedures in place, system changes (to the Court and Licensing Systems in particular) take more time and effort to implement due to the age of the systems.
- *Incident management*—The Licensing and Tax systems both had good quality data related to incident records and operational logs. However, we noted that the incident records and program change records for the Licensing System were poorly linked, which would have corrected the cause of the incident. The Court System had a poor quality of incident records and did not maintain operational logs, which provide vital information relating to I&IT operations.
- *Problem management*—None of the three systems we audited conducted root-cause or trend analysis on incidents. This analysis would enable the I&IT clusters to identify and address interrelated and recurring incidents having a wider impact on I&IT performance.

Our audit found that all three systems adequately addressed the remaining two risk areas:

- *Availability and capacity management*—all three systems had adequate controls in place to ensure that the use of I&IT services is monitored, performance expectations are met and plans are made to predict and meet future user needs.
- *Business continuity and disaster recovery*—all three systems had effective processes in place to address unexpected events that disrupt operations, such as power failures and system crashes.

Our detailed assessment of the nine I&IT general control risk areas for each of the three systems we looked at is provided in the **Appendix**.

## 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.

- Ensure they engage appropriate staff with the necessary skills and expertise.
- Ensure succession plans are in place to allow for the transfer of knowledge.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- Formally document, approve and communicate I&IT operational procedures.
- 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.
- 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.
- 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.

## I&IT CLUSTER RESPONSE

The Justice Technology Services I&IT cluster agrees with the Auditor General and plans to address these recommendations by implementing the following:

- The cluster is currently drafting service-level agreements for the Court System. Logging, alerting, monitoring and reporting protocols, and the tools necessary to perform these tasks will be developed to support the terms of the service-level agreements.
- The cluster is developing a strategy for providing ongoing support (incorporating succession planning and knowledge transfer) for the Court System. As an initial step, the cluster has acquired the services of an additional development resource. In conjunction, the manner in which existing roles are utilized will be reviewed to assess efficient use and necessary skills and expertise.
- Consultant's performance will be monitored and assessed on an ongoing basis against the requirements of the role and the Statement of Work associated with their contract, which defines the terms of their engagement.
- The cluster will facilitate a user access review, in partnership with the Ministry of the Attorney General (Ministry), including establishing appropriate thresholds for user account inactivity and ongoing access level review. The cluster will work with the Ministry to strengthen the process for creating and modifying user access and identify areas for improvement (including reviewing potential conflicts related to segregation of duties).
- The cluster will investigate means for introducing automated controls for the tracking, monitoring, alerting and reporting/recording of batch process results. Operational procedures documentation requiring an update will be reviewed, updated as necessary and communicated.
- The cluster will document and communicate approved I&IT operational procedures.
- The cluster will continue to develop and enhance the operational reporting analysis established in January 2016, which includes Helpdesk operations, to identify improvements to the recording of incidents, including modification of defined support templates.
- The cluster will utilize I&IT staff efficiently by implementing functionality to deal with basic and complex issues, as well as permanent fixes.

## 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.
- 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.
- 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.
- 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.

- Ensure that there is clear linkage between the incident records in the incident management tool and the program change records addressing those incidents.
- Implement a formal problem management process to identify trends, the root cause of recurring issues and remediation plans.

## I&IT CLUSTER RESPONSE

The Labour and Transportation I&IT cluster agrees with the Auditor General and in conjunction with the Ministry of Transportation (Ministry) will work to implement all of the auditor's recommendations.

To address the individual recommendations:

- The cluster will follow the defined Government of Ontario IT Standard for service level management. The cluster's work will include application reporting timelines consistent with the advice provided by the Auditor General such as:
  - defined service-level agreements with implementation targets; and
  - implementing quarterly and annual service-level agreements service metrics and report results.
- The cluster, in collaboration with the Ministry, will continue to make this a priority including implementation of associated procedures for continued monitoring and review of user access.
- Work is underway to complete a procedure guideline for regular periodic review of user access. The cluster, in collaboration with the Ministry, will continue to make this work a priority.
- The cluster recognizes that effective monitoring and logging of user access to sensitive and critical data is a priority. Logging of user access to information and transactions is now in place and the Licensing System activity logs are available. The Road User Safety Modernization project is defining the data it considers sensitive and is implementing role-based security as systems go live to limit access to sensitive data based on job requirements.
- The cluster will ensure more robust procedures are in place to ensure clear linkage between incident records and program change records used to address these incidents. This will form part of our service-level agreements discussion.
- The cluster will ensure more robust procedures are in place to ensure root cause of recurring issues and remediation plans are captured within the incident management tool to support trend analysis and required remediation plans. This will form part of our service-level agreements discussion.

## 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.
- 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.
- 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.

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

## I&IT CLUSTER RESPONSE

The Central Agencies I&IT Cluster agrees with the Auditor General and will address these recommendations by implementing the following:

- The cluster has formalized a management oversight process to monitor and report on service levels outlined in service-level agreements for our two largest systems, OntTax, and imageON. Working with our business partners, the cluster is drafting service-level agreements for our next three largest systems/services and additional service-level agreements, or their equivalents, will be implemented to address numerous smaller systems, as recommended in the report.
- The cluster will facilitate a user access review, in partnership with Ministry of Finance, to assess segregation of duty controls. Any identified conflicts will be corrected immediately.
- The cluster has strengthened user access controls by implementing regular monthly reporting processes to ensure users are appropriately authorized. Regular access reviews will be implemented to ensure appropriateness.
- The cluster is implementing a problem management process for all supported major applications. This will include trend analysis, root cause identification and problem remediation/resolution.

## 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.

## I&IT ORGANIZATION RESPONSE

The Office of the Corporate Chief Information Officer agrees with the Auditor General and recognizes the need to assess all I&IT systems against the nine key risk areas that effective I&IT general controls should address.

To enable this analysis, the I&IT organization has defined and established an Application Portfolio Management (APM) approach to address risks associated with aging systems and to inform application rationalization opportunities. An inventory of all I&IT applications has been established and key data elements associated with each application have been collected and analyzed. This data can be used as a starting point (and then built upon to ensure inclusion of all nine risk categories) to assess each application's I&IT general controls risk.

Through the new Enterprise Service Management division and the development of APM processes and guidelines—the I&IT organization will establish standards for service-level agreement creation and management of I&IT systems, starting with those classified as mission and business critical.

The I&IT organization will improve service by:

- enabling greater consistency in how service management processes are delivered, driving increased quality and effectiveness;

- establishing a service-level agreement framework aligned to the nine key risk areas; and
- improving the service management process across the I&IT organization.

Also, the I&IT organization will continue to work with the Centre for Leadership and Learning and HR-Strategy Business Units to continue to focus on skills development and succession planning for key mission critical IT systems.

## 4.3 Maintenance of Aging Systems is Inefficient and Staff Lack Training

Ontario has some very old I&IT systems that are becoming increasingly obsolete due to their age (**Figure 10** provides examples of key systems that are more than 25 years old and that use obsolete software). Of the three systems we audited, two are more than 25 years old: the Licensing System is 48 years old and the Court System is 27 years old.

The age of the systems in itself might not be a critical issue if the government was regularly updating them and managing their staffing in an efficient way. However, we noted concerns specific to the lack of continuous training and knowledge transfer, maintenance being limited, and functionalities issues in the government I&IT systems we audited.

### 4.3.1 Systems Vulnerable Due to a Lack of Continuous Training and Knowledge Transfer

#### Court System

The Court System, which is used by 120 courts and 5,000 users across Ontario, was written in a version of a programming language that is no longer supported by the vendor who produced it. All programming changes in the Court System are currently made by two individuals (both of whom are eligible for retirement)—one staff member and one consultant who is not as proficient in the Court System programming as the staff member. The Justice Technology cluster has no succession plan in place for either individual, so if they were to leave or retire soon, it will be difficult to find qualified replacements and get them up to speed quickly. Even if the Ministry of Justice was able to find people who know the programming language of the system, there would be a significant problem because the documentation they would need to perform their duties is incomplete, outdated or, in some cases, non-existent.

As with all I&IT systems, two types of documentation should be available for the Court System:

- documentation tracking all programming changes or modifications to code that have been made to the system over time; and
- operational documentation, such as procedural manuals, instructing I&IT operations staff how to support the system.

**Figure 10: Examples of Old I&IT Systems In Use**

Source of data: I&IT clusters

| System | Ministry | Age (Years) | Purpose |
|---|---|---|---|
| Licensing System | Transportation | 48 | Processes transactions relating to licensing drivers and registering vehicles. |
| Payment Processing | Government and Consumer Services | 31 | Records and reports cheque payments. |
| Employment Standards | Labour | 27 | Maintains information on *Employment Standards Act* decisions. |
| Personal Property Security Registration | Government and Consumer Services | 27 | Maintains public database for creditors to register and conduct searches. |
| Court System | Attorney General | 27 | Supports the administration of the Ontario Court of Justice |

We noted that there is no documentation of programming changes to the system prior to 2009, and also no operational documentation that is referenced, which will make the transfer of knowledge difficult.

We also found that there is no formal job description or any defined performance metrics and expected service levels in place to evaluate the consultant responsible for the system's performance.

#### Licensing System

The Licensing System is in a stronger position than the Court System with respect to the ongoing availability of trained staff because there continues to be vendor support for the key programming languages it uses and because it has a larger team. Twenty-four experts (10 staff and 14 consultants) support the Licensing System; their anticipated retirements are spread out over a number of years, allowing for more effective succession than is the case with the Court System. Further, management has thought about ways to facilitate knowledge transfer from retiring personnel to remaining employees.

However, we did note instances where problems occurred because support staff did not have the right skills to perform their job responsibilities. For example, in January 2016 the system went down temporarily (for about an hour) and was unavailable for front-line staff because multiple programmers had been working on making changes to the code at the same time, without knowing each other was doing so. This caused incorrect and incomplete code to be applied to the system, ultimately resulting in functions within the system being unavailable until programmers could fix it. There is functionality available in the existing tools supporting the Licensing System that could prevent this from happening but, at the time of our audit, staff did not know how to configure this tool in order for it to be used.

#### Tax System

In contrast to the Court System and Licensing System, we did not find issues of knowledge transfer and training with the Tax System and the I&IT Central Agencies cluster. This cluster is sufficiently staffed to manage anticipated turnover and retirements without jeopardizing knowledge transfer and the continued operation of the Tax System. We also noted that management has been facilitating additional training for staff so that they can assume duties previously performed by consultants, thereby reducing reliance on external parties.

### 4.3.2 Maintenance of Aging Systems is Insufficient

The government has taken steps to modernize some of its aging systems, however the modernization of the Court System and Licensing System has been significantly delayed. Because they were slated for replacement by 2011, funding for their maintenance was reduced significantly—to a level described to us by their I&IT cluster staff as "just enough to keep the lights on." Replacement of the systems was subsequently delayed (with no clear completion timeline for the Court System and a 2025 target for the Licensing System), but funding for their maintenance was not returned to previous levels.

Maintenance for these systems has been minimal, and restricted to levels that allow the ministries to meet only their legislative requirements, rather than enhance their service delivery. There have been limited functionality improvements to these systems.

### 4.3.3 Aging Systems Hinder Effective Service Delivery

The Court System and Licensing System, as aging systems, are experiencing functionality issues, such as:

- they are unable or have difficulties communicating with other systems;

- it is challenging to modify them to address the changing requirements of their users; and
- they do not readily generate reports that management needs for analyzing trends.

There is a concern that making changes to modules in these systems could corrupt functionality or cause the systems to crash. Because of the lack of reliable documentation of past system programming changes, programmers avoid making direct changes in the system that might actually be viable and help ministry employees and/or the public use the systems more effectively. Innovation is therefore not occurring because users, knowing the severe limitations of the systems, no longer request anything but the most essential changes.

We noted several examples where limitations with the Court System meant that user needs were not being met, including:

- categories (such as new criminal code offences) cannot be added easily in the system when new legislation is passed;
- the system cannot record cases that have multiple hearings over an extended period of time; and
- special instructions cannot be recorded in the system (for example, identifying the need for interpreters, listening devices for the hearing impaired, or other special equipment).

Staff currently track special instructions using workaround solutions, such as recording it in the "general notes" section or maintaining separate Excel documents that are not linked with the system. We also noted that in making fixes in the Court System, the programmers have themselves been entering actual data related to the court cases. This goes against best practice in computer management that system programming be kept separate from data entry. As a result, there is the risk that the programmers could inadvertently, or fraudulently, enter inaccurate data or alter existing data.

## 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.

## I&IT ORGANIZATION RESPONSE

The I&IT organization agrees with the Auditor General and acknowledges the importance of having a comprehensive inventory, lifecycle management and planning approach to ensure sufficient system maintenance and/or replacement.

To enable this, the I&IT organization has defined and established an Application Portfolio Management (APM) approach to address risks associated with aging systems and to inform application rationalization opportunities. I&IT will work with their respective ministry business partners to develop and submit plans through the annual Program Review, Renewal and Transformation (PRRT) exercise.

The I&IT organization will work with program areas to investigate long-term IT capital investment approaches for business and enterprise applications and will provide recommendations to Treasury Board/Management Board of Cabinet for any replacement of outdated I&IT systems.

## 4.4 Modernization Efforts Significantly Delayed

Although the government has initiated projects to replace some of its outdated I&IT systems, there is considerably more work to be done. In 2006, the Major Application Portfolio Strategy (MAPS) identified 77 of 153 major applications that needed to be replaced or upgraded. In the fiscal year ending March 31, 2010, the Treasury Board/Management Board of Cabinet authorized spending of $600 million to replace or upgrade these 77 applications. As of June 2016, 66 of these applications had either been retired or upgraded, including some significant projects, such as the Ontario Health Insurance Plan and Aircraft Tracking systems. However, we question whether $600 million would have been adequate to successfully address the needs of all 77 applications. By way of context, one project alone, the Social Assistance Management System (SAMS), although budgeted for $164.9 million, resulted in a total cost of $290 million. (See our *2015 Annual Report* for our value-for-money audit of SAMS.)

In 2012, the government moved responsibility for the replacement and upgrading of I&IT systems from a central team, which was managed by the Ministry of Government Services, to the individual I&IT clusters supporting the ministries. At the time the government had spent $121 million on MAPS. Of the remaining $479 million, $316 million was transferred to the relevant ministries that would ultimately have ownership of the modernized systems. The rest ($163 million) was retained by the Treasury Board. This was done due to a freeze on all capital expenditures by the government as part of the fiscal restraint measures at that time. It became evident that a significant investment in capital beyond the 2011 capital expenditure levels would be required to complete the MAPS projects. Therefore, the Treasury Board Secretariat decided to make the ministries rather than the Ministry of Government Services responsible for the outstanding and in-progress initiatives. By doing this, the Treasury Board hoped that the individual ministries would find funding from within their regular capital expenditure budgets to support the I&IT modernization projects. The process of upgrading and retiring outdated applications did continue within the clusters with significant upgrades made to the Integrated Financial Information System and the Ontario Student Assistance Program. However, we noted that 11 systems that MAPS had flagged as being overdue for replacement or upgrading still have not been modernized. These include the Court System and the Licensing System.

### Court System and Licensing System

An unsuccessful attempt was made in September 2010 to initiate the modernization of the Court System as part of another I&IT project at the Ministry of the Attorney General, the Court Information Management System (CIMS). Although about $11 million was spent on CIMS, the project failed, resulting in no new system for that ministry. While the government was able to reallocate about $6.5 million worth of hardware and software to other operations, the project still lost about $4.5 million overall. The CIMS project was originally scheduled for completion in March 2012. Only nearing its expected completion was it revealed that the project was still in planning phase.

The two oversight bodies for the CIMS project were the Executive Steering Committee and the Office of the Corporate Chief Information Officer. Subsequent to March 2012, the Executive Steering Committee decided to put the project on hold until further review. The province's Internal Audit Division and a third party vendor conducted separate reviews. Based on these reviews, the project failure was attributed to the following issues:

- Governance and oversight processes failed to:
  1. identify risks and issues and steer the project in the right direction;
  2. adequately resolve issues identified;
  3. adequately monitor and supervise the performance of a key member of the project team (Functional Manager – who

was absent from meetings of the Executive Steering Committee 40% of the time); and
4. ensure that reporting requirements were met.

- Project management:
  1. lack of project planning, monitoring, supervision and co-ordination; and
  2. no evidence that deliverables as defined by the agreed upon Statement of Work had been completed or verified prior to authorization for payment to the vendor.
- Project reporting:
  1. project reports were incomplete, unreliable and inconsistently presented;
  2. project status was reported as 'on track' for seven of ten reports, which contradicted other indications that the project was experiencing delays and setbacks; and
  3. not all reports were presented to the Executive Steering Committee.

Since the failure of the CIMS project, no plan has been put in place that estimates when the Court System will be modernized. Revised timelines indicate that planning will begin in 2018/19, but no estimated completion date has been provided.

A business case for modernizing the Licensing System was submitted in 2008. It was approved in 2009 (as part of MAPS) with a budget of $230 million and estimated completion by 2016. In 2011, management revised their approach to roll out the project in three segments as opposed to modernizing the complete system in five years. The revised approval from Treasury Board for the first segment was $136 million, but the approved amount had to be revised again in 2014 to $190 million, and then again in 2015 to $195 million. This was due to poor performance from the external vendor, whose contract was terminated.

As of March 2016, $182 million had been spent on the first segment, now expected to be finished by the end of 2016, at an estimated cost of $203 million. The cluster has not yet done an assessment on the timelines and costs associated with the remaining two segments.

Delays in implementing the modernization of the Court System and Licensing System mean that by the time the I&IT clusters complete the planning for what they intend to do, the plan is already outdated.

### Tax System

Vendor support for the current version of the Tax System's software will continue until 2018. Management is currently developing a business case to determine options for business requirements.

## 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.

## I&IT ORGANIZATION RESPONSE

The I&IT organization acknowledges the need to mitigate and address risk across the application environment and will work with Office of the Treasury Board and the Ministry of Infrastructure to determine options on how we should address the modernization and remediation of the application portfolio.

The I&IT organization will work with its respective ministry business partners to assess the cost and need to update and maintain current systems and the risks arising from using aged systems and develop and submit cost and benefit analyses for the replacement of any systems through the annual Program Review, Renewal and Transformation (PRRT) exercise.

# Appendix: Detailed Observations of I&IT General Control Risk Areas for the Three Systems Reviewed

Prepared by the Office of the Auditor General of Ontario

| | |
|---|---|
| **1. Service-level Agreements** | |
| A contract between the I&IT cluster management and ministries it serves should be established that formally and clearly sets out each party's roles and responsibilities for governance, accountability and expected performance and quality of service in accordance with the ministries' current and future needs. | |
| Court System | • No formal service level agreements in place covering the system<br>• No service level agreements in place at the cluster level<br>• No formal monitoring and reporting being performed over service levels |
| Licensing System | • No formal service level agreements in place covering the system<br>• No service level agreements in place at the cluster level<br>• No formal monitoring and reporting being performed over service levels |
| Tax System | • A formal service level agreement is in place covering the system<br>• Service level agreements in place at the cluster level relating to only two systems; none for the other systems<br>• No formal monitoring and reporting being performed over service levels |
| **2. I&IT Human Resource Management** | |
| Adequate staffing levels and skills should exist to ensure effective controls, maintenance and operations are achieved to meet expected service levels. | |
| Court System | • Inadequate support staff; over reliance on one external consultant and one in-house staff (eligible for retirement) for support<br>• No formalized job descriptions in place for support staff responsibilities<br>• No succession plan in place for replacement of experienced staff |
| Licensing System | • Adequate support staff—24 experts<br>• Formalized job descriptions in place for support staff responsibilities<br>• Appropriate succession planning in place for replacement of experienced staff |
| Tax System | • Adequate support staff—52 experts<br>• Formalized job descriptions in place for support staff responsibilities<br>• Appropriate succession planning in place for replacement of experienced and external staff |
| **3. Logical Security** | |
| Controls should exist to ensure only authorized users have access to and can use data, programs and networks. Examples of controls are user IDs and passwords to authenticate users and restricting access to systems. | |
| Court System | • 41% of the users had access to the system when their job roles did not require any access at all<br>• Management has not reviewed user roles and access permissions on a regular basis to validate if these individuals still require access<br>• Segregation of duties[1] are not regularly assessed and maintained<br>• User activity logs are not reviewed on a regular basis<br>• No formal process in place for creating and modifying users' access<br>• No centralized list of authorized approvers who can request access on behalf of users |
| Licensing System | • 5% of the users had access to the system when their job roles did not require any access at all<br>• Management has not reviewed user roles and access permissions on a regular basis to validate if these individuals still require access<br>• Segregation of duties are not regularly assessed and maintained<br>• User activity logs are not reviewed on a regular basis<br>• A formal process is in place for creating and modifying users' access<br>• A centralized list of authorized approvers who can request access on behalf of users does exist |

| | |
|---|---|
| **3. Logical Security (continued)** | |
| Tax System | • 5% of the users had access to the system when their job roles did not require any access at all<br>• Management has not reviewed user roles and access permissions on a regular basis to validate if these individuals still require access<br>• Segregation of duties are not regularly assessed and maintained<br>• User activity logs are reviewed on a regular basis<br>• A formal process is in place for creating and modifying users' access<br>• A centralized list of authorized approvers who can request access on behalf of users does exist |
| **4. I&IT Operations** | |
| Activities and operational procedures required to support the delivery of I&IT services, including the execution of pre-defined standard operating procedures and the required monitoring activities, should be in place. | |
| Court System | • No post-batch[2] verification process in place<br>• No formally documented I&IT operational procedures exist |
| Licensing System | • Post-batch verification processes are in place<br>• Documented I&IT operational procedures exist |
| Tax System | • Post-batch verification processes are in place<br>• Documented I&IT operational procedures exist |
| **5. Change Management** | |
| Controls should exist to ensure changes to key systems are made quickly, reliably and have minimal negative impact on the system's stability or integrity. | |
| Court System | • Formal change management procedures are in place, but system changes are taking more time and effort to implement due to system age and complexity<br>• Programmers have access to make data changes.[3] |
| Licensing System | • Formal change management procedures are in place, but system changes are taking more time (approximately 66% longer) and effort to implement due to system age and complexity |
| Tax System | • Formal change management procedures are in place |
| **6. Incident Management** | |
| Controls should exist to ensure user queries and incidents (such as service interruptions) are resolved as soon as possible. | |
| Court System | • Poor quality of data pertaining to incidents<br>• No operational logs, which provide vital information relating to I&IT operations, are maintained for the system<br>• Support staff spend an unnecessary amount of time (60% of support calls) resolving very basic service requests |
| Licensing System | • Good data quality of incident records, but there is poor linkage between the incident records and the program change records addressing those incidents<br>• Operational logs are maintained for the system<br>• Support staff spend reasonable amount of time resolving basic service requests |
| Tax System | • Good data quality of incident records<br>• Operational logs are maintained for the system<br>• Support staff spend reasonable amount of time resolving basic service requests |
| **7. Problem Management** | |
| Controls should exist to ensure not only that there are as few operational issues as possible, but that the number of issues steadily decreases, thereby increasing system availability, improving service levels, reducing costs and improving customer convenience and satisfaction. | |
| Court System | • No formal problem management procedures (such as root cause analysis and trend analysis of incidents) are in place |
| Licensing System | • No formal problem management procedures are in place |
| Tax System | • No formal problem management procedures are in place |

| 8. Availability and Capacity Management | |
|---|---|
| Controls should exist to ensure that the use of I&IT services is monitored, performance expectations are met and plans are made to predict and meet future user needs. This will enable services to be available whenever needed, resources to be managed efficiently and systems to be high-performing. | |
| Court System | • Adequate controls in place |
| Licensing System | • Adequate controls in place |
| Tax System | • Adequate controls in place |
| **9. Business Continuity and Disaster Recovery** | |
| Effective processes should exist to address unexpected events that disrupt operations (for example, power failures and IT system crashes) in order to restore or recover operations and information as quickly as possible. | |
| Court System | • Effective processes exist |
| Licensing System | • Effective processes exist |
| Tax System | • Effective processes exist |

1. Segregation of duties involves breaking down tasks that might reasonably be completed by a single individual into multiple tasks so that one person is not solely in control, to decrease the likelihood of error or fraud. The traditional example is that the person who produces a cheque should not also be authorized to sign it.
2. A batch job is a system functionality used to process multiple transactions at the same time. Batch jobs are often run overnight when there is less activity on the system.
3. It is best practice in computer management that system programming be kept separate from data entry. Otherwise, there is the risk that the programmers could inadvertently—or fraudulently—enter inaccurate data or alter existing data.